山东通信技术

（1979 年创刊 总第 138 期）

Shandong Tongxin Jishu

第 33 卷 第 1 期

2013 年 3 月

（季刊）

（公开发行）

目 次

主管单位：山东省通信管理局

主办单位：山东通信学会

编 委：孔建坤 王剑峰 吕雪峰
刘梦溪 张学辉 赵 珑
高兆法 郭 彬 董士宝
傅玉林 谢绍富
(按姓氏笔画为序)

主 编：张 渲

编 辑：刘 伟

地 址：济南市经十一路 40 号

邮 编：250002

电 话：0531-82092813

Q Q：1207011839

Email：txjs@sdca.gov.cn
1207011839@qq.com

国内统一刊号：CN37-1161/TN

广告经营许可证号：3700004000133

国内定价：5.00 元

面向维护人员的网络安全管控平台建设与应用

吕雪峰 刘松森 王自亮

（中国移动山东公司,济南 250001）

摘 要:本文着眼于维护人员维护操作的合规性管理,依据事前授权、事中监控、事后审计的安全管控思路,探讨了如何建设统一的安全管控平台。平台有机整合了集中接入控制、账号口令集中管理和日志管理与审计等手段,对维护人员操作业务系统和支撑系统的全过程实施管控,为资源访问、日常维护操作提供了安全、可靠的途径,确保合法的人做合法的事、非法的事能够及时发现。

关键词:安全管控 账号口令 访问控制 日志审计

1 引言

随着通信业务的发展,各种信息系统的数量不断增加,对运维安全提出了新的要求。口令变更不及时、过期账号未清理、敏感操作无法追溯等安全隐患的普遍存在,极大增加了网络的安全风险,存在的问题主要表现在:

(1)账号管理难度大

各应用系统相对独立且数量众多, 账号变更频繁、管理任务繁重,单纯依靠人工方式难以实现及时规范的账号管理,各系统上经常出现过期账号、孤立账号,易导致重要信息泄漏事件。

(2)口令管理不规范

维护人员所维护的设备众多,需记忆大量账号口令,不少人以明文方式存储账号口令信息,加大了系统信息泄漏的风险;依靠人工方式难以实现对口令的有效管理,易出现弱口令或长期不修改的口令。

(3)独立的系统权限授权管理,无法保证系统安全性

各系统分别管理系统资源和应用资源,并为本系统的用户分配权限,由于缺乏集中统一的资源授权管理,无法集中按照最小权限原则分配权限,导致系统安全性无法得到充分保证。

(4)安全审计不健全

各系统登录接入点分散,难以对各种操作行为进行审计,出现安全事件无法审计到人,很难落实事件责任。

为加强通信网、业务系统和各支撑系统的安全防护,防范因内部人员或第三方人员引发的内部安全事件,必须加强日常维护安全管控,确保合法的人做合法的事、非法的事能够及时发现。为此,需要全方位规范用户账号安全管理、规范用户授权和访问行为,对用户的维护操作和数据访问进行集中的认证、审计监督,为用户访问资源、进行维护操作提供安全、可靠的途径, 同时也为加强企业内部网络与信息安全控制、满足相关监管要求提供技术保证。具体功能需求包括:

(1)账号管理:实现对所有的自然人以及核心设备账号的统一集中管理。

(2)身份管理:有效解决传统模式下的共享账号问题,通过自然人账号与系统账号的关联实现网络操作的实名制。

(3)访问控制:实现基于主账号的集中强身份认证和访问入口,通过自定义访问控制规则为每个用户分配适当的网络资源, 只允许合法的人做合法的访问。

(4)操作审计:对所有访问维护操作(包括输入命令与输出结果)进行记录并回放,阻止非法访问、违规操作。

本文着眼于维护人员维护操作的合规性管理,探

讨了如何通过建设安全管控平台，加强安全要求落实,实现安全管理目标。

2 安全管控平台

2.1 总体架构

安全管控平台总体架构如图 1 所示。

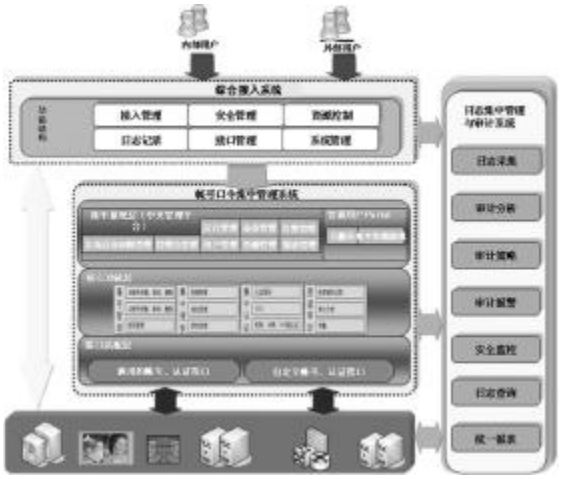


图 1 安全管控平台总体功能架构设计

安全管控平台由综合接入子系统、账号口令集中管理子系统和日志集中管理与审计子系统等三个子模块组成,实现各类系统资源和应用资源的集中账号(Account)管理、集中认证(Authentication)管理、集中授权(Authorization)管理和集中安全审计(Audit),全面落实风险管理、安全运维要求。。

(1)综合维护接入子系统为所有通过的应用提供集中展现和集中转发的功能,访问能通过单一来源实现。

(2)账号口令集中管理子系统主要提供用户账号口令的集中管理功能。

(3)日志集中管理与审计子系统主要提供日志的采集和分析功能,实现日志的关联分析、审计预警、报表呈现等。

在账号口令方面,综合维护接入平台和日志集中管理与审计系统要接受账号口令集中管理系统的管理。综合维护接入平台利用账号口令集中管理系统提供的单点登录 Portal 功能，避免接入用户多次认证。日志集中管理与审计系统结合账号口令,集中管理系统形成的账号登录日志和综合维护接入平台的维护操作日志,实现操作日志和用户真实身份的关联。综合维护接入平台、账号口令集中管理系统、日志集中管理与审计系统在功能上彼此间具备独立性,一个系统的主体功能实现不依赖于另一个系统存在;同时又互相配合,从而更好地支撑内部控制目标的实现。

2.2 综合维护接入子系统

综合维护接入子系统作为维护接入的集中控制点,整合多种接入方式,提供集中接入控制,在完成对接入用户的身份认证后，根据事先确定的授权信息,控制接入用户能够访问的设备以及能使用的应用和服务,并对接入用户的操作进行记录,其总体框架如图 2 所示。

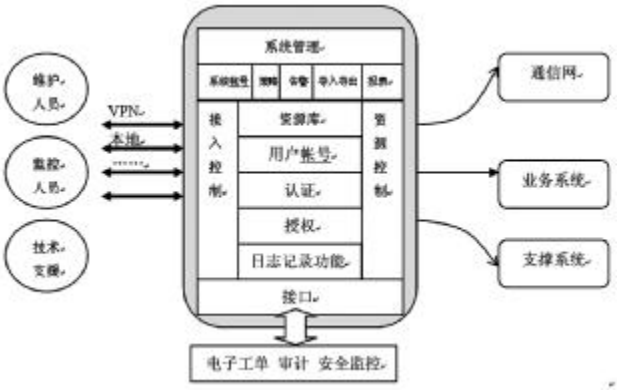


图 2 综合维护接入子系统总体框架

为满足实际需要,支持 VPN 等常用接入方式,采用堡垒主机技术,避免维护人员使用不安全的终端直接访问系统;能够纪录维护人员的操作,为安全审计和事件调查提供原始资料。

VPN 是安全接入和子网保护设备，由于其具有网关特性，可以将用户对 Web 应用的访问做到精确的 URL 级的访问控制，并能对 C/S 的应用进行基于 IP:PORT 的访问控制。

在确认了使用者的身份,规定了系统范围内的权限，具备了对该用户身份的操作检查审计机制后,通过使用堡垒主机对使用者的合法系统操作进行协议

层面的控制。字符堡垒主机可以对字符应用的访问做到命令的访问控制、会话内容的审计。图形堡垒主机能够实现 Windows Terminal、xWindows 等图形终端的集中接入和访问控制,做到应用边界的访问控制并进行全程录像和回放。

综合维护接入子系统实现了将运维工作通过统一入口进行管理，并根据用户真实身份统一权限与访问控制。另外,能够与账号口令集中管理系统、日志集中管理与审计系统相结合,从而简化认证过程,实现更为深入的授权及审计。平台通过集成维护 PORTAL,进一步方便了维护操作。

2.3 账号口令集中管理子系统

账号口令集中管理子系统采集、管理各类维护人员拥有的主账号、从账号信息,实现主账号与其拥有的全部从账号进行关联，并对账号密码进行集中管理,包括按照密码策略自动更改密码,实现不同系统间的账号密码数据变更。对各类应用资源进行集中管理,设立不同的用户角色,并将用户使用资源的具体情况进行合理分配,实现不同用户对系统不同部分资源的授权访问。通过统一的认证及 PORTAL 功能,实现用户身份的一次鉴别和单点登录访问控制功能。该系统框架结构如图 3 所示。

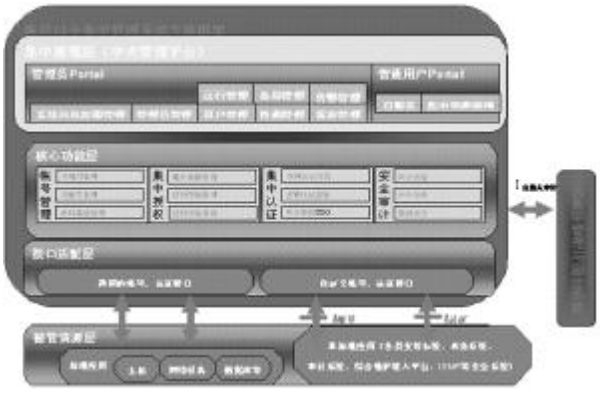


图 3 账号口令集中管理子系统总体框架

账号口令集中管理子系统分为接口适配层、核心功能层、集中展现层。

接口适配层提供系统和被管系统间的接口,分为通用接口、自定义接口。接口规定了系统和被管资源之间为完成账号管理、授权、认证等功能所采用的通信方式、协议、消息语义等信息。通用接口采用标准的协议（如 Telnet/SSH,RADIUS,SYSLOG/SNMP 等）、标准的命令(如标准数据库读取、操作系统自带命令等)。自定义接口则针对特定系统二次开发的接口,或通过定制 Agent 的方式实现与被管资源的通信。

核心功能层,是整个系统的基础和核心。其中,数据组成包括用户身份数据、资源数据、授权策略数据和日志数据等。系统通过功能框架实现上述数据的维护和管理;管理功能包括统一身份管理、资源及认证管理、账号授权管理、访问控制管理、安全审计管理。

集中展现层包括管理员 Portal 和普通用户 Portal 两个功能模块。管理员 Portal 为管理员提供管理员管理、普通用户管理、资源管理、系统自身权限管理、运行管理、备份管理、告警管理和报表管理等功能。普通用户 Portal 为普通用户提供自服务、集中资源展现及基于 B/S 模式的单点登录等功能。

2.4 日志集中管理与审计子系统

日志集中管理与审计子系统对各类系统和设备产生的人员操作维护日志进行统一采集、存储、管理。根据预先制定的审计策略对日志进行分析,发现高危操作,产生审计事件告警,其功能框架逻辑结构如图 4 所示。

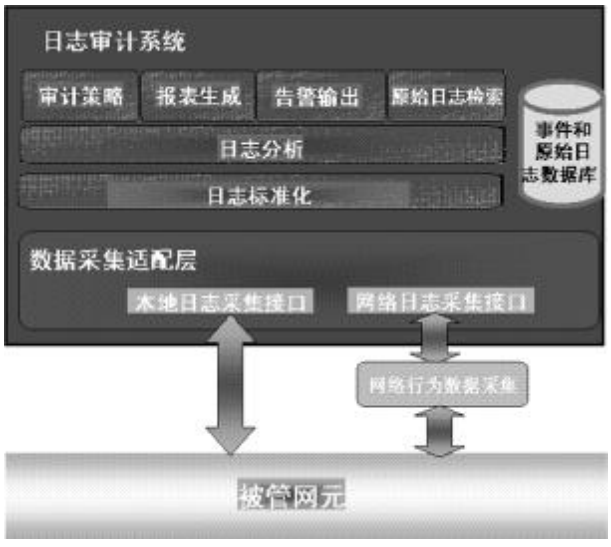


图 4 日志集中集中管理与审计子系统框架

日志集中管理与审计子系统整体功能分为四层:数据采集适配层、日志标准化层、日志分析层、展现层。

数据采集适配层实现各类日志数据的采集。日志集中管理与审计系统通过 Syslog、ODBC、SNMP Trap、Socket、File 等多种接口,采集各设备、系统和应用的本地型日志;通过镜像等方式采集网络型日志。通过两种采集方式的合理配置,实现对被管网元中所有用户操作行为的信息采集。

日志标准化层将采集层采集到的不同类型、不同格式的日志数据,通过标准化处理,形成归一化的日志格式,以便后续分析和审计。

日志分析层通过对日志的横向、纵向的关联分析,发现异常操作,找出可能存在的安全问题;对用户的操作、数据库访问进行回放,分析用户权限是否合理,发生问题时可用作责任认定;将分析发现的问题生成告警信息送上层处理,及时通知用户,也可转发到第三方系统处理,如直接向电子运维系统派单。

展现层以多种报告报表的方式,让用户能从多角度洞察系统的运行情况,实现对审计系统的配置管理,实现安全审计和报表展示,主要包括审计策略、报表、告警输出、原始日志检索等四个关键的功能模块。

日志集中管理与审计系统通过三个方面的日志来源完成审计功能,包括:堡垒主机审计会话数据、网络嗅探会话数据、系统日志数据,日志数据来源如图 5 所示。

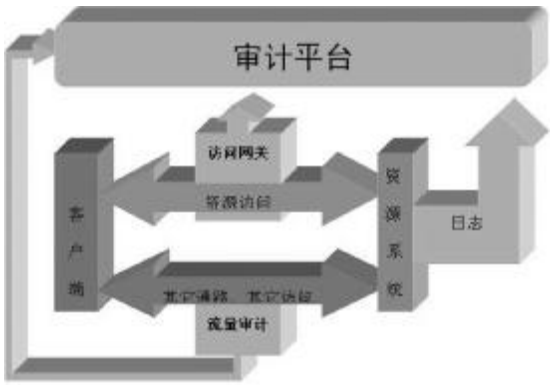


图 5 日志数据来源示意图

日志集中管理与审计系统还可与其他系统实现接口互联,通过接口能将日志或告警信息转发到其他系统做进一步的分析处理。

3 应用效果

平台建设前、后的维护模式对比如图 6、图 7 所示。

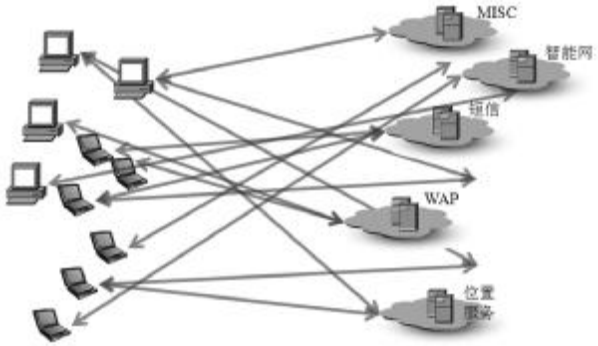


图 6 管控平台建设前的维护访问方式

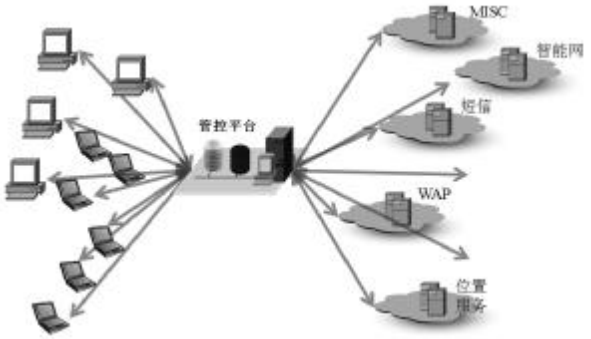


图 7 管控平台建设后的维护访问方式

目前,该平台已覆盖全网主要业务系统、网络(如话音网、智能网、GPRS、CMNet、IP 承载网、WAP、MISC、短信、彩信、DNS 等)以及重要网管应用(如话务网管、电子运维、信令监测)和自有业务,开通人员账号一千余个,接入资源上万台,管理设备账号数万个。

安全管控平台实现了各类网元和网管应用接入管控系统的接口标准化,解决了在通信系统实现集中安控管理的关键问题。维护人员可通过管控节点操作具有管理权限的被管资源,实现了“一点接入、统一授权、全网访问”。结合身份信息、堡垒主机技术,安全管控平台将用户身份信息与操作日志关联,实现海量日志的实名对应及快速检索,解决了网元日志记录不完整、存储时间有限、无法对应到人以及被恶意删除等安全隐患。

(下转第 7 页)

基于互联网技术的内部商城方案浅析

魏源[1] 张军[2] 张力舒[3]

(1 中国联合网络通信有限公司,北京 100033
2 联通系统集成山东分公司,济南 250100
3 济南大学信息科学与工程学院,济南 250022)

摘 要:本文主要探讨了如何在电信企业内部利用信息化手段、互联网技术实现采购工作的公开透明、人性化服务,达到加强采购管控、减少成本支出、降低采购风险的目的。

关键词:采购 互联网技术 电子商务 内部商城

1 引言

深入挖潜、降本增效,通过管理手段提高效率、效益,是电信运营商应对市场竞争、提升企业价值创造力的重要途径。

采购管理作为企业内部管理的重要组成部分,管理目标需要与企业的总目标一致,需要持续关注采购的公开透明、采购服务的支撑水平、采购预算和成本控制、采购质量和评价、采购过程管理控制和风险控制等问题。

随着电信运营商管理工作的不断深入,传统物资采购管理模式存在的问题逐渐凸显:

(1)成本费用类物资管控较弱

成本费用类物资采购行为没有实现统一管控,部分用品由各基层单位自行采购,造成质量管控尺度不一,流程审批控制层级不同,无法进行有效的管控和风险控制。成本费用类物资分散采购不仅难以形成规模效益,而且,为完成采购、报账等工作,基层单位的人力资源浪费严重。基层预算单位现金支付权限较大,容易造成管理缺失;部分预算开销缺少事前控制,不能达到全成本控制的要求。

(2)物资采购公开透明度不足,对一线人员的支撑较弱

物资采购工作原来是依托专业的采购管理系统实现,采购过程和结果没有好的途径实现透明、公开;采购过程相对专业,不能很好地支撑一线人员使用。

(3)物资采购事后评价体系较弱

物资的最终使用者,没有很好的途径对物资和供应商进行评价。

针对存在问题,本文结合互联网技术,借助电商模式的信息化手段,提出了内部商城方案,实现了采购透明化,保证采购产品质量,规避采购风险,提高内部服务水平,取得了较好的应用效果。

2 内部商城方案

2.1 设计思路

以淘宝、京东为代表的电商网站有鲜明特点:商品信息的展现直观透明;商品采购操作简单,一般人员都可以便捷完成;商品、店铺评价方便,评价结果公开透明。

借鉴电商网站的特点,借助互联网技术,结合内部采购流程审批和预算控制,以电商网站方式建立电信企业内部商城,实施内部采购管理;加大物资管控力度和精度,打造“阳光采购”,实现对物资的精细化管理和采购用户体验。

(1)建设类似淘宝方式的内部商城,用于内部物资采购;

(2) 将招标后的各类供应商商品放入内部商城,

供各单位选购;

(3)将各部门的预算按照预算类别转换成相应类别的虚拟货币(如办公费、招待费、维系费)放入商城,各部门可以使用虚拟货币到商城进行采购;

(4) 商城商品可以指定能够购买的虚拟货币类别,如“笔”类商品指定仅能用“办公费”虚拟货币进行购买;

(5)商品订单下达后,需要经过内部流程审批才能生效;

(6)月底公司统一与供应商结算。

内部商城具备类似淘宝商品展现、购物车、商品管理、订单管理、评价等网上商城的基本功能,并实现预算 / 虚拟货币管理、审批管理等内部控制,业务功能如图 1 所示。

图 1 内部商城业务功能图

2.2 技术实现

内部商城对于商品物资图片展现较多,需要专门考虑图片的存储和应用。对此,系统引入专用的图片服务,以实现对商品图片的快速访问(图 2)。

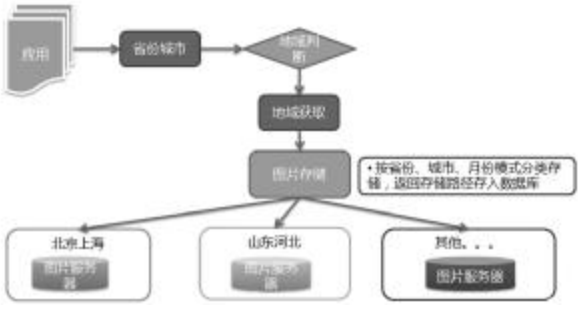


图 2 图片服务示意图

商城中的商品种类繁多,为达到良好的用户体验,商城需要能够快速定位客户所需商品。借助搜索引擎技术,提高了商品搜索速度与客户体验度(图 3)。

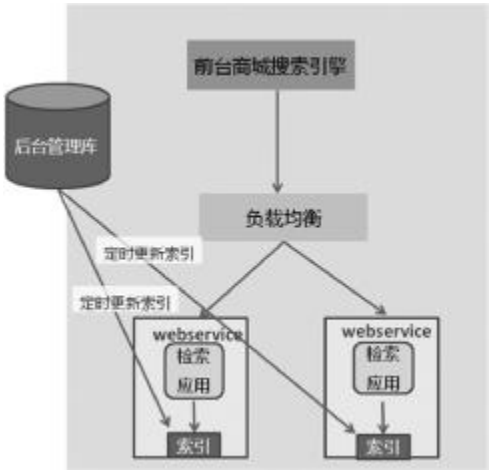


图 3 搜索引擎示意图

考虑到系统强大的可扩展性,利用读写分离和集群技术实现系统的弹性扩展、云化。

(1)商品库通过读写分离方式,实现云化扩展。后台管理库并发量如到达极限,可用读写分离方式进行云化扩展。为降低系统的访问压力,使用 mysql 的数据复制功能,实现读写分离,以提高系统的负载能力,降低主数据库的访问压力(图 4)。

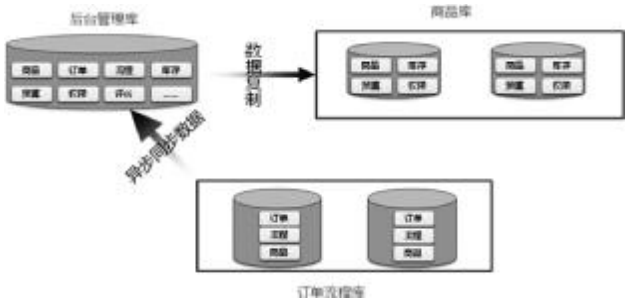


图 4 数据云化扩展示意图

(2)Web 服务器集群:借助负载均衡和集群技术,实现 Web 服务器、报表服务器的弹性扩展和失效转移。

利用数据分析技术,结合图表等方式,对整个物资采购情况进行综合分析,以便掌握物资采购情况、采购区域分布情况、商品分布情况、供应商占比情况等。

系统整体应用架构如图5所示。

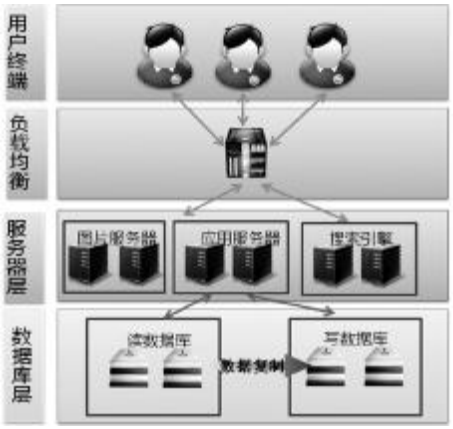


图5 系统整体应用架构图

3 应用效果

内部商城应用后,为企业物资采购与管理工作带来了重大提升。

(1)一线支撑服务更高效

通过引进电商模式,打通了前台需求、后台管理以及供应商响应的业务活动和管理链条,各基层单位可以方便地到内部商城采购所需物资。采购需求人员无需与供应商讨价还价,月底也不再需要安排专人到财务排队报账,省时、省心、省力。

(2)采购管理更透明

各类物资在内部商城以类似淘宝商品的方式展现,信息直观明了。同时,通过商品评价比价、供应商后评价等功能,使物资情况更加透明,并实现全员参与、全员监督,有效促进了采购工作的效果评估和公开透明。

(3)管控更有效

内部商城提交的订单需求,需要经过内部审批流程后才能生效,管控严格。财务方面管控更加精准。通过对各级各部门物资申领量的纵向、横向双维度比较,提升企业预算编制的精确度;通过对订购商品所需费用与预算剩余额度的实时对标,实现对预算的事前控制。

(4)降本增效

通过比价、商品公开透明等手段,使采购价格更加合理,使各单位采购数量更加合理。同时,将众多部门综合人员从采购、报账工作中解放出来,极大节省了人力资源,实现了向管理要增长、要质量、要效益。

(上接第4页)

通过安全管控平台的建设应用,实现了账号、认证、鉴权、审计的集中化、自动化管理,解决了账号管理、日志管理、接入管控方面的难题,提高了安全维护效率和水平,提升了网络安全防护能力。

4 结束语

安全管控平台通过设置集中维护接入门户,统一控制内、外部维护人员接入相关系统,并完整记录维护人员操作的全过程;自动采集、集中管理各被管系统中操作系统、数据库、网络设备的账号和口令,加强各种账号口令的管理;集中采集、存储、管理各被管资源中与维护操作相关的原始日志,将采集到的日志与维护人员的真实身份相关联,支持对原始维护操作日志的快速检索,并根据预定义规则发现高危操作且及时告警。集中体现了事前授权、事中监控、事后审计的安全管控思路,有机整合了集中接入控制、账号口令集中管理和日志管理与审计等手段,对内部维护人员、厂家人员操作业务系统和网管系统的全过程实施管控,有效提高了维护工作的安全性和效率。

随着管控平台逐渐成为日常接入维护的唯一通道,其重要性日益凸显。各类新型被管资源的接入、管控平台的自身安全以及维护通道的通畅,都将是平台长期发展需要关注的重要研究课题,仍需不断完善。

参考文献

1 胡立春,武友新,张烨,姜晓东.LDAP环境下的统一用户管理系统的研究与实现.计算机工程与设计,2007(4)

2 杨子江,宁国宁,周静等.用户管理系统中授权的设计和实现.东南大学学报,2002(32)

3 David A. Steven Akridge, How Can Security Be Measured, Information Systems Audit and Control Association, 2005

4 Ali M. Al-Khouri, Optimizing Identity and Access Management (IAM) Frameworks, International Journal of Engineering Research and Applications (IJERA),Vol. 1, Issue 3, pp. 461-477Caroline R. Hamilton.Risk Management and Security. Information Systems Security,1999,8(2):69-78

5 RFC 1777Lightweight Directory Access Protocol. W. Yeong, T. Howes, S. Kille.

6 GB/T 9387.2-1995《信息处理系统开放系统互连基本参考模型》第2部分:安全体系结构

云计算平台安全问题探讨

唐绍勇 董士宝

（中国电信山东分公司，济南 250101）

摘 要：本文介绍了具体场景的云平台架构层次，分析了云平台环境下产生的新安全风险。从建设维护的角度，提出利用技术手段、管理手段进行防护；从技术角度，重点分析了同一安全域内、运行在同一物理服务器上的虚拟机之间的安全防范；在管理方面，强调了从建设到运维的安全管理流程制定。

关键词：云计算 虚拟化 威胁 安全域

1 引言

云计算将计算任务按需分布在计算机集群中，合理利用了计算能力、存储空间、网络资源，使硬件效率得到大幅提升。然而，云计算技术的发展给信息安全提出了新的挑战，传统信息安全时代下的安全标准和规范已不能应对新形势，需要对云计算平台的安全问题进行多方面分析，从技术、管理两个角度加强防护。

2 云计算概述

云计算按照服务类型大致分为三类：将基础设施作为服务 IaaS(Infrastructure as a Service) 、将平台作为服务 PaaS(Platform as a Service)和将软件作为服务 SaaS(Software as a service)。IaaS 将硬件设备等基础资源封装成服务供用户使用，PaaS 提供应用程序的运行支撑环境，SaaS 将某些特定应用软件功能封装成服务。

云平台的架构分多个层次，各层次之间都是松耦合关系(图 1)。

图 1 云平台架构案例

如图 1 所示，硬件、虚拟机监视器(Virtual Machine Monitor)、虚拟机(Virtual Machine)三个层次对外提供 IaaS 服务。一个 IaaS 服务对应一些计算、存储、网络环境，对用户而言是透明的，一般是若干台虚拟机，由用户完全控制。

应用支撑层、能力层组成 PaaS 层。应用支撑层针对上层应用提供运行环境，能力层主要提供基本业务能力，比如传统电信服务中的短信、彩信、WAPpush 等，以及互联网服务中的地图、搜索引擎等，提供 IMS 中的彩铃 / 彩像、IVR 等能力。

SaaS 层主要是对用户提供具体的服务，比如 SNS 社区、在线办公、地图服务等。

对于云架构的不同服务层次有不同的安全关注点，相对于传统的业务架构，虚拟化层安全是云环境下特有的安全关注点。

3 云计算平台面临的安全问题

传统平台上，利用物理防火墙和交换机的隔离策略，可以在很大程度上对属于不同业务域物理服务器的安全起到保障作用。但虚拟机环境下的安全域划分就需要重新定义和隔离，一个物理计算机上可能会出现属于不同安全域的虚拟机，虚拟机的恶意代码防护可能会导致 AV 风暴，停用虚拟机再次上线可能会导致因病毒特征文件过期而产生安全薄弱环节等。

以下对因引入虚拟化技术而产生的两种新安全威胁进行分析。

3.1 逃逸威胁

逃逸即虚拟机逃逸,是指在已控制一个 VM 的前提下,利用各种安全漏洞,进一步拓展、渗透到 Hypervisor(虚拟层)甚至其它 VM 中。

(1)逃逸攻击前提

服务器虚拟化环境里,Hypervisor 直接安装在物理机上。另一方面,Hypervisor 并没有接口暴露在网络中,攻击者唯一能访问的就是上层的 VM。因此,实施逃逸攻击的前提是必须先利用 VM 的安全漏洞控制某个 VM, 再以它为跳板逐步尝试并达到逃逸目的。

(2)典型的逃逸模式

假设攻击者通过各种手段 (通常是漏洞攻击)已控制某个 VM,在此基础上,可衍生出以下三类逃逸模式。

1)模式一:从已控 VM 到 Hypervisor

由于对已控 VM 具有完全的操作权,如果 Hypervisor 各组件中存在漏洞、且漏洞可以从 VM 中触发的话, 则攻击者完全可能开发相应的漏洞利用程序,并实现在 Hypervisor 中以高权限执行任意代码或导致 Hypervisor 拒绝服务,如图 2 所示。

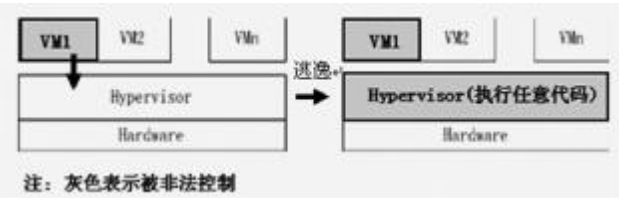


图 2 逃逸模式 1

2)模式二:从已控 VM 到 Hypervisor,再到其它 VM

以第一种逃逸模式为基础,在获取 Hypervisor 权限后,攻击者可以截获、篡改和转发其它 VM 对底层资源的请求或各 VM 之间的通信,并结合对应的安全漏洞实施攻击,最终逃逸到其它 VM 中,如图 3 所示。

图 3 逃逸模式 2

3)模式三:从已控 VM 直接到其它 VM

该模式利用了 VM 的动态迁移特性所引发的漏洞复制问题。动态迁移过程使得原始 VM 镜像中的安全漏洞也在不断地复制和传播。攻击者在充分收集已控 VM 特点及脆弱性的基础上,从网络中利用适合的渗透手段对其它 VM 进行攻击,从而实现逃逸。该逃逸模式与前两种的主要区别是不需要对 Hypervisor 进行漏洞攻击,如图 4 所示。

图 4 逃逸模式 3

3.2 隐蔽信道

隐蔽信道(Covert Channel)是指允许进程以危害系统安全策略的方式传输信息的通信信道,是导致信息泄露的重要威胁(图 5)。

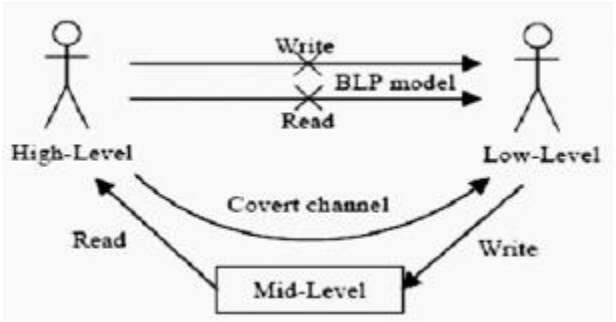


图 5 隐蔽信道示意图

如图 5 所示,即使在强制访问控制策略下,攻击者仍然可以构建隐蔽信道,实现从高安全级主体向低安全级别主体的信息传输。

虚拟化环境下,针对虚拟化服务器的网络攻击源头主要有三种可能:一是来自系统以外;二是来自系统其它物理机器上的 VM;三是来自相同物理机上的其它 VM。

针对第一、二种情况形成的隐蔽信道,传统的安全防护技术足以应对。而第三种情况形成的隐蔽信道,则是虚拟化引入产生的新威胁,需要在防护技术

上进行变革。

事实上,虚拟化环境下缺乏对 VM 间通信流量的可见性本身就是一大安全问题。同一硬件上 VM 之间的通信流量根本不经过安全网关、硬件防火墙等安全设备。无论是 VM 之间的攻击数据还是攻击之后传输数据的隐蔽信道,传统的基于网络的检测技术都完全失效,如图 6 所示。

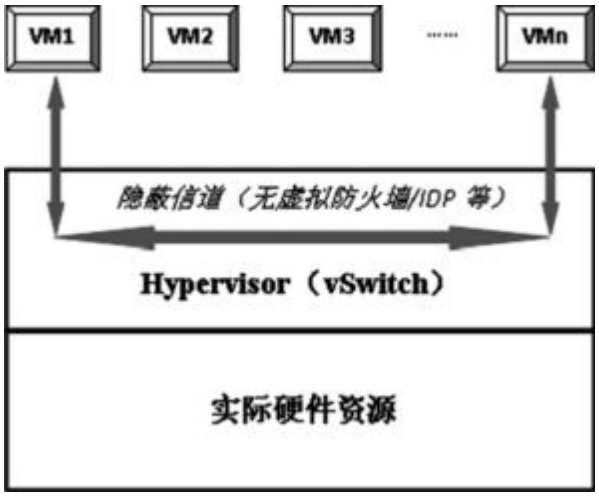


图 6 基于虚拟化环境的隐蔽信道示意图

4 云计算平台可采取的安全措施

云计算平台的安全防护,一方面可以借鉴传统平台的安全防护措施和手段,另一方面要针对云计算平台出现后带来的特有安全要求,从架构的设计到虚拟化软件的选择,从加密、认证的实现方式到兼容性的测试,全面考虑安全控制措施的实现方式。总的来说,不外乎技术手段和管理手段两方面。

4.1 技术方面

4.1.1 安全域防护

云平台下的安全域划分以具体业务系统应用为导向,是由共同协调完成一组任务的主体所组成的集合,就是部署在云平台下的同一个业务系统平台的虚拟机。内部的虚拟机具有较宽松的访问控制策略,但对于该安全域外部的虚拟机主体, 则具有较严格的、相同的安全防御需求和边界控制策略。

各安全域之间一般应根据安全需求,考虑综合采用虚拟 / 实体交换机、虚拟防火墙等措施,将不同用途的网络流量进行分隔,以保证通信流量不会相互干扰,从而提高网络资源的安全性和稳定性,用户访问流量可以分为跨安全域和安全域内部两种。

(1)跨安全域的流量

跨安全域访问分两种情况:一是用户从云平台外部,通过硬件防火墙、交换机访问;另一种是从一个 VM访问另一个 VM。在云平台内部,跨安全域的访问都属于三层转发,如图 7 所示。

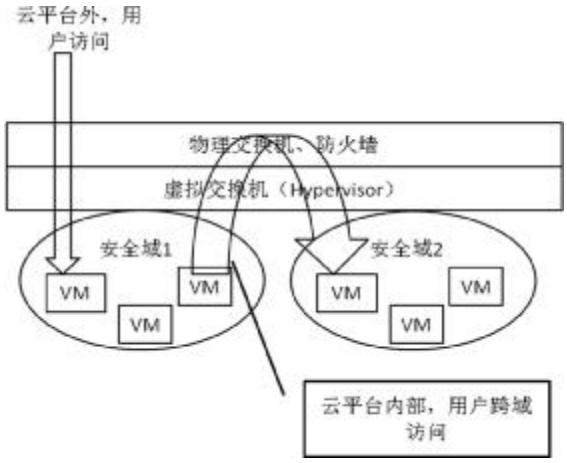


图 7 跨安全域访问

这种情况下, 需要在物理交换机上配置跨 Vlan 的物理隔离,实现虚拟化环境下的云安全部署,实现对常规的虚拟化实例进行转发隔离和安全策略配置。

(2)安全域内跨物理服务器的流量

安全域内部访问是通过一个物理服务器上的 VM 访问同安全域的另一个物理服务器上的 VM。这种方式由于需要跨服务器,因此数据流需要通过外部的物理交换机,走二层转发,如图 8 所示。

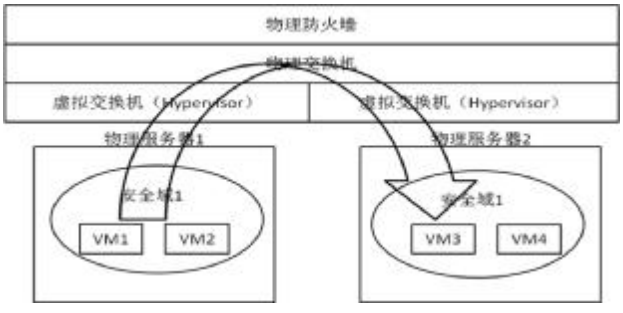


图 8 安全域内跨物理服务器访问

VM的访问流量要经过上层的物理交换设备,可以在物理交换设备上对特定 VM 的流量进行跟踪分析。如果需要对域内某 VM 的访问实现特殊要求的话,可以采用物理交换机的访问控制策略进行限制。

4.1.2 虚拟化层安全

在虚拟化环境下,同安全域内运行于同一个服务器上的 VM 之间,流量将直接在服务器内部实现交换,导致外层网络无法对这些流量进行监控或者实施各种高级安全策略。如图 9 所示。

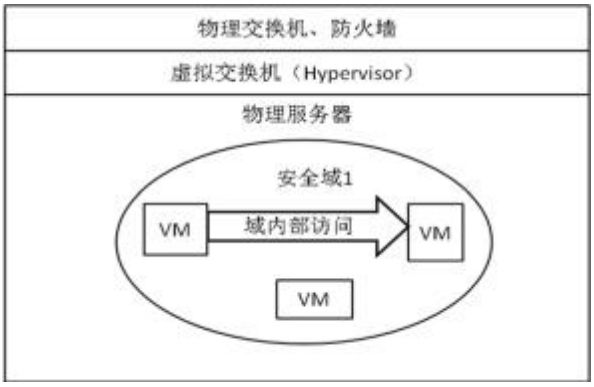


图 9 安全域内跨物理服务器访问

此类情况下的 VM 之间的流量,是通过服务器虚拟化软件提供的虚拟交换机（vSwitch）进行数据转发。通过在服务器上部署虚拟机安全软件,对此虚拟设备进行安全防护,并对 Hypervisor 层中的虚拟交换机进行整合,是解决此类问题的有效手段。比如,VMware 提供了新型安全技术 VMsafe,并开放了 API 接口,将所有 VM 之间的流量交换在进入 vSwitch 之前先引到虚拟机安全软件进行检查,以保障其访问安全。

实施时,可以安装一台虚拟机设备,通过 VMsafe 接口与虚拟交换机进行结合,为整个虚拟化环境提供安全服务,同时降低防护产品对伺服器资源的使用,维持或者提供虚拟机器的服务效能。

4.1.3 虚拟机容灾机制

虚拟化环境应制订应急预案,以确保在灾难发生时能迅速应对。云平台下有众多的容灾机制,包括 HA、热迁移、负载均衡等。从 VM 的角度看,如下容灾方式可供选择:

(1)建立快照。快照是对虚拟机文件在某个时间点的“拷贝”。这个“拷贝”并不是对虚拟机文件的复制,而是保持磁盘文件和系统内存在该时间点的状态。系统崩溃或系统异常,可以通过使用恢复到快照来保持磁盘文件系统和系统存储。但快照层次太多,影响虚拟机的运行效率,而且浪费存储资源。

(2)虚拟机备份。虚拟机备份可以将虚拟机的整个文件复制,从而实现彻底保留。一般服务器虚拟化厂商均提供虚拟机热备份工具,比如 convert 工具。也可以在每个 VM 中安装备份程序,就像以前在每台物理服务器中安装备份程序一样,数据通过 LAN 流入备份 / 恢复设施。

4.2 管理方面

除了技术因素外,云平台的安全防控还要制定从云平台建设到运行维护各个时期的管理制度,比如制定云平台运维的各个流程、落实相关的安全责任和控制等。

4.2.1 系统配置、更新

云计算系统中,支撑软件也同样会有补丁升级和配置错误的情况,要及时安装系统的各种更新,并调整可能的配置错误。

(1)系统补丁,包括 HyperVisor、管理软件、Guest-OS、病毒库等,补丁要及时升级并确认。

(2)VM 之间通讯的配置要合理,由于不同安全域的虚拟机限制比较严格,因此这里重点关注同一安全域内的通讯。

(3)对云平台管理接口的访问权限配置要严格,严控维护人员的访问等级。

(4)对 VM 可访问物理接口,主要是磁盘驱动器、网络适配器等的配置要满足业务系统的需求,并不扩大配置。

(5)配置虚拟化设施与可信任的授权时钟服务器同步。

4.2.2 虚拟机的安全管理

虚拟机的安全管理,主要是虚拟机的加固、虚拟机的隔离和访问控制。

(1)建立安全加固流程,以保证每个通过云平台交付出来的虚拟机镜像已通过安全策略的严格检测,去除了不安全的服务、协议、端口等可能导致入侵的因素,并通过内部防火墙设置流量入栈和出栈规则。

(下转第 25 页)

有关来 / 出访 LU 登记成功率下降故障原因的分析

陈森

（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：本文介绍了位置更新(LU)的业务特征及其信令流程、LU 登记成功率算法，进一步分析了可能影响来 / 出访 LU 登记成功率的故障原因，并对其导致的 LU 登记成功率下降提出了解决问题的分析思路和处理方法。

关键词：位置更新(LU) 来 / 出访 LU 登记成功率　分析思路　处理方法

1　引言

来 / 出访 LU 登记成功率是电信运营商 2G 网络 KPI 中一项重要指标，用于把握国际漫游来 / 出访用户对网络质量的真实体验情况，从而对网络进行优化、改进。

电信运营商对于来 / 出访 LU 登记成功率的波动较为敏感，当指标出现下降时，为及时高效地判明故障，必须对故障原因进行深入分析，形成有效的分析思路，以便尽快拿出解决办法，将故障排除。

2　来 / 出访 LU 登记成功率概述

2.1　位置更新(LU)业务

为使网络能够实现对移动用户当前位置的跟踪，MS（Mobile Station）必须在其改变位置区(location area)时通知系统的过程称为位置更新。位置区是由一个或几个 BTS 来处理的定义区域，在这个区域内，MS可以自由移动而不需要通知系统；位置区由一个或几个 BSC 控制，但只属于一个 MSC。

2.2　来 / 出访 LU 信令流程

LU 信令流程全过程主要经历了用户所在 MSC/VLR、HSTP、ISTP，国外运营商 ISTP，国外运营商 HLR 和原 MSC/VLR。可以看出，来 / 出访 LU 过程主要在国内信令网和国际信令网中实现。常用的监控 LU 信令流程正常与否的国际信令监测系统，就是通过 ISTP 获取国际来 / 出访 LU 的信令的。

来访 LU 信令流程和出访 LU 信令流程分别如图 1、图 2 所示。

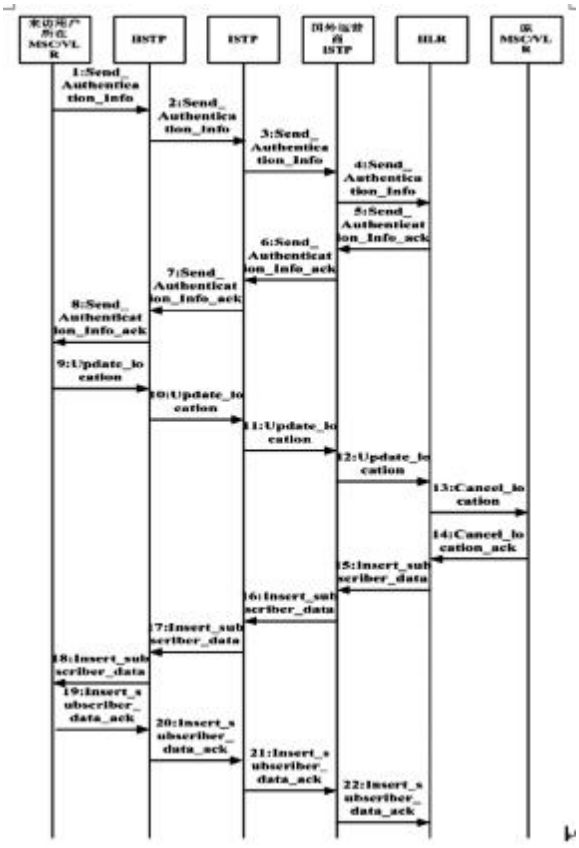


图 1 来访 LU 信令流程

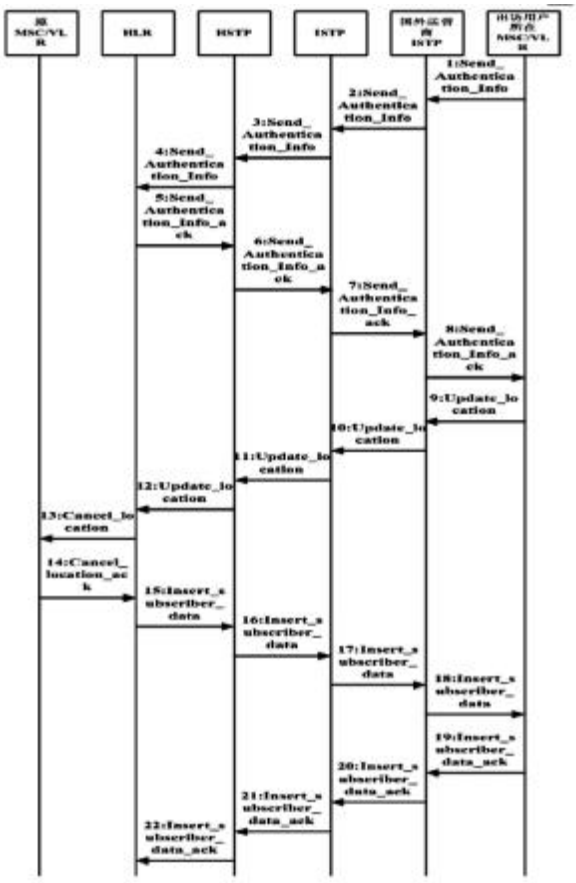


图 2 出访 LU 信令流程

2.3 来 / 出访 LU 登记成功率算法

2.3.1 来访 LU 登记成功率算法

来访 LU 登记成功率是由网络接通次数除以更新次数计算得来。其中,网络接通次数由以下几部分构成:用户成功次数,MAP 协议层:漫游失败:PLMN 不允许漫游,MAP 业务层:由于不支持的特性限制漫游,TCAP 协议层:U 诊断:无应用上下文名称。

也就是说,MAP 协议层:漫游失败:PLMN 不允许漫游,MAP 业务层:由于不支持的特性限制漫游,TCAP 协议层:U 诊断:无应用上下文名称,以上三种 LU 失败都不计入网络原因的失败。其中,MAP 业务层:由于不支持的特性限制漫游被列为非网络原因,是因为非洲一些国家运营商及香港一些运营商的用户漫游过来后不停地返回,造成来访位置登记成功率很低。与对端沟通,对方回复,这些为预付费用户,他们认为 HLR 返回这个原因是正常的。

鉴于此,需从以下 6 个因素中分析 LU 登记成功率低的原因:

(1)MAP 协议层:未知用户;

(2)MAP 协议层:系统故障;

(3)TCAP 协议层:P-Abort: 未识别的事务处理 ID;

(4)TCAP 协议层:U-Abort;

(5)TCAP 协议层:拒绝:重复调用 ID;

(6)信令采集不全。

2.3.2 出访 LU 登记成功率算法

出访 LU 登记成功率也是由网络接通次数除以更新次数计算得来。其中,网络接通次数由用户成功次数,MAP 协议层:漫游失败:PLMN 不允许漫游,MAP 业务层:由于不支持的特性限制漫游,TCAP 协议层:U 诊断:无应用上下文名称等部分构成。

MAP 协议层:漫游失败:PLMN 不允许漫游,MAP 业务层:由于不支持的特性限制漫游,TCAP 协议层:U 诊断:无应用上下文名称,以上三种 LU 失败都不计入网络原因的失败。其中,MAP 业务层:由于不支持的特性限制漫游,在实际计算中统计值近乎为零,可基本忽略不计。所以,国际信令监测系统中的来 / 出访 LU 登记成功率算法也是一致的。

出访 LU 登记成功率需从以下 14 种原因中分析 LU 登记成功率低的原因:

(1)MAP 协议层:非期望的数据值;

(2)MAP 协议层:设备不支持;

(3)MAP 协议层:未知用户;

(4)MAP 协议层:系统故障;

(5)MAP 协议层:数据丢失;

(6)MAP 业务层:由于不支持的特性限制漫游;

(7)SCCP 层:UDTS;

(8)SCCP 层:无法翻译地址;

(9)TCAP 协议层:P-Abort: 未识别的事务处理 ID;

(10)TCAP 协议层:P-Abort:未识别消息类型;

(11)TCAP 协议层:U-Abort;

(12)TCAP 协议层:对话中止 - 对话业务提供者;

(13)TCAP 协议层:拒绝:未被识别的调用 ID;

(14)信令采集不全。

3 影响来 / 出访 LU 登记成功率的故障

及分析思路

3.1 影响来 / 出访 LU 登记成功率的故障

从 LU 信令流程和电信运营商国际信令组网结构出发，总结可能影响来 / 出访 LU 登记成功率的故障因素如下：

(1)信令监测系统故障；

(2)ISTP 故障；

(3)HSTP 故障；

(4)转接商、运营商故障；

(5)漫游地故障；

(6)用户问题。

3.2 影响来 / 出访 LU 登记成功率的故障分析思路

(1)信令监测系统故障,有可能造成：

1)无法获取位置更新信令；

2)位置更新数据大量丢失；

3)采集到的位置更新信令不全。

此类故障不会影响业务,需联系网管厂家解决。

(2)ISTP 故障

1)双 ISTP 同时阻断：会造成来出访 LU 信令几乎完全失败或无法采集,影响几乎全部国际业务。需立即通知相关责任人并启动相关应急预案。

2)单 ISTP 阻断：有可能造成来 / 出访 LU 成功率降低。由于对所有国际局向 ISTP 均互为备份路由,所以单 ISTP 阻断不会使国际业务全阻，但有可能使正常的 ISTP 系统或链路负荷猛增而造成信令丢包,同时有很大的国际业务阻断隐患。需通知相关责任人并启动相关应急预案。

3)ISTP 至某方向链路组阻断：有可能造成到某些方向的来 / 出访 LU 成功率降低,甚至降为零。应首先登录交换机，使用 7599 或 241 命令确认告警确实存在。由于 ISTP 备份路由及转接商 ISTP 备份路由的存在,绝大部分情况下不会影响业务。但若因此出现到某方向目的信令点不可达告警,则需通知相关责任人并启动相关应急预案。同样,由于系统或链路负荷增加,可能引起 LU 登记成功率降低。

4)ISTP 至某方向链路阻断：有可能造成到某方向来 / 出访位置成功率降低,大部分情况下不影响业务。应首先登录交换机,使用 7539 或 241 命令确认告警确实存在。若存在，则派单 ISTP 出口所在故障省份。同样,由于系统或链路负荷增加,可能引起 LU 登记成功率降低。

5)ISTP 局数据配置错误：有可能造成到某些方向的来访或出访成功率下降,例如产生大量 SCCP 地址无法翻译错误。初步定位故障原因后,需通知相关局数据制作人处理。

(3)HSTP 故障

可参照 ISTP 故障处理。HSTP 采用双平面结构且平时负荷 / 容量较小,由于非局数据原因引发影响业务故障的可能性很小。

(4)转接商、运营商故障

1)转接商故障：可能造成一个或多个方向的来 / 出访 LU 成功率下降。例如由于设备或传输问题,造成到某运营商方向目的信令点不可达。初步定位故障原因后,需联系转接商处理。

2)运营商故障(国外运营商 ISTP、HSTP 故障)：可能造成该方向的来访或出访 LU 成功率下降。例如,由于自身原因造成其目的信令点不可达。初步定位故障原因后,需通知国外运营商处理。

(5)漫游地故障

漫游地故障（国内外 HLR、MSC/VLR 故障或局数据错误)可能造成该出访国家或地区某运营商的出访 LU 成功率下降，或国内某地区的来访 LU 成功率下降。同样,局数据故障可能产生大量 SCCP 地址无法翻译错误。初步定位故障原因后,需通知国外运营商或国内相关责任人处理。

(6)用户问题

用户问题可能造成某些业务量小的方向的来 / 出访 LU 成功率下降。初步定位故障原因后,需通知相关责任人处理。

4 来 / 出访 LU 登记成功率下降处理方法

4.1 获取数据

(1)查寻数据并勾选“显示其他项”；

(2)从前述来访 6 种、出访 14 种原因中找到失败

次数最多的一种或较多的几种;

(3) 双击该种失败原因所对应的数字, 可以从 MAP-TDR 关联查询中观察到逐次记录的详细的信令失败原因;

(4)单击合适的列名,可以正序或倒序排列(如有必要,将表单存为 EXCEL 以方便分析);

(5)需要进行更详细分析的时候,双击某条记录可以观察具体信令流程。

4.2 具体分析方法

一般情况下, 认为来 / 出访 LU 登记成功率都应该大于 95%。若低于此值,可利用以下两种方法进行故障定位:

4.2.1 排除法

(1) 排除因监测系统故障造成的 “LU 成功率下降”

1)在来 / 出访 LU 登记成功率报表出现明显异常情况时询问网管厂家。

2)查看报表,观察是否产生大量“其他”类故障。双击查看信令详情, 若出现大量 “MTP- 采集信令不全”错误,来访则单击“主叫 GT 地址”,出访则单击“被叫 GT 地址”,以进行分类。若发现 GT 地址分布较分散、都是单向消息,却存在信令交互过程,则判定为信令应答消息被监测系统丢失,判断“监测系统存在故障”。因为如果没有应答,对方不会继续发送消息。

(2)排除因信令网骨干节点故障造成的来 / 出访 LU 登记成功率下降

1)查看国际局告警,询问国际局所在地确认。

2) 利用成功的 LU 流程, 排除信令网骨干节点(HSTP、ISTP)系统级故障。(此时仍需判断失败的消息原因:如果失败过程均为消息送到 HSTP、ISTP 后终止, 则应怀疑 HSTP、ISTP 故障非系统级故障。)

3) 可以观察是否仅存在通过双 ISTP 其中之一的信令,以判断单 ISTP 故障。

4) 结合国际局告警和电话联系国际局所在地,判断是否为海底光缆中断或设备软硬件故障所导致的链路组、链路阻断故障或目的信令点不可达故障。

4.2.2 缩小范围法

排除以上两种原因后,按先国内、后国外的顺序缩小故障范围。

(1)来访选择 OPC 运营商、出访选择 DPC 运营商,首先观察国内侧是否存在某省出现大量错误。若确有一省出现大量失败:

1) 来访: 主叫 GT 地址为该用户所在 VLR 的 MSCID 地址,确认是否为某一 VLR 出现大量失败。

2)出访:被叫 GT 地址为移动手机号。若能确定为省里原因,可将跟踪信令发给该省查询。

(2)若国内侧没有问题。可以统计来访 DPC 运营商、出访 OPC 运营商,观察是否为某一转接商造成大量失败。若存在,可以考虑转接商、运营商故障。有可能的话, 进一步分析是否到某个被叫 VLR 有大量错误,进而定位为漫游地故障。

(3)发现失败的来访 LU 信令流程后,第一时间观察用户出访到对端国家 / 地区运营商的出访 LU 信令过程是否成功。失败的出访 LU 同理。观察反向过程对定位故障点非常有用。

5 LU 登记成功率下降故障原因分析案例

最近,某省级电信运营商网内的来访 LU 登记成功率一直波动较大, 较长时间处于 95%的门限值以下。以 3 月 1 日 07:00-08:00 为例,信令监测系统取到的数据参见表 1。

表 1 来访 LU 登记成功率异常情况

时间	更新次数	成功次数	网络接通次数	网络接通率	MAP协议层:系统故障	MAP协议层:数据丢失	MAP协议层:漫游失败:PLMN不允许漫游
2013-3-1 07:00:00	110324	68269	101833	92.30%	4312	3276	31665
MAP协议层:未知用户	MAP协议层:非期望的数据值	MAP业务层:由于不支持的特性限制漫游	TCAP协议层:P-Abort:未识别的事务处理 ID	TCAP协议层:U-Abort	TCAP协议层:U诊断:无应用上下文名称	TCAP协议层:拒绝:重复调用 ID	信令采集不全
95	49	469	54	81	1430	1	561

根据算法计算，来访LU登记成功率=(68269+31665+469+1430)/110324=92.3%。来访LU登记成功率从前一个时段的95.6%下降至92.3%,降幅非常明显,而且是一个小时内的突降。

对于该故障,第一步,先要判断故障点,以确定是信令转接点、转接商、任意一方运营商或者是网管(国际信令监测系统)出了问题。因为国际局网管没有活跃的目的信令点不可达或链路断开告警,证明国际信令转接点和信令链路状态正常;同时该表中“系统故障”、“数据丢失”占比较高,并未出现较多“信令采集不全”,故也排除网管故障的可能性。可初步判定是中转商或任意一方运营商的问题。

第二步,从呼损率最高的原因“MAP协议层:系统故障”、“MAP协议层: 数据丢失”开始分析,点击链接、跟踪全部故障信令。在确认来访用户登记端局的MSC ID并非为单一端局出现大量失败后,可进一步排除本方网络故障的可能性。

第三步,分析是中转商或对方运营商故障。统计DPC运营商，发现是香港reach转接的澳大利亚TELSTRA、香港1616转接的印度尼西亚运营商PT INDOSAT Tbk LU登记成功率大幅下降。其中,澳大利亚TELSTRA从95%下降至30%,印尼PT从98%下降至8%。分析发现:故障点都集中在一个转接商转接的单个方向的运营商出现大量LU失败信令,而非一个转接商多个方向运营商LU大量失败,也就排除了转接商的嫌疑。此时大致锁定是对方运营商的问题了。

第四步,根据信令释放原因判断,猜测对方运营商对其漫游来访用户采取了优选漫游,于是向对方发起申告，询问对方运营商是否采取了优选漫游措施。由于优选漫游是对方运营商控制,与本方没有任何协议约束,在对方没有理会的情况下,通过转接商的联络途径,证实本方的判断是对的,遂将上述进行了优选漫游设置的运营商排除在查询来访LU登记成功率之外。最终,排除优选漫游运营商后的来访LU登记成功率又保持在稳定的波动门限范围之内。

以3月3日07:00-08:00为例,信令监测系统取到的数据为95.39%(表2)。

表2 来访LU登记成功率正常情况

时间	更新次数	成功次数	网络接通次数	网络接通率	MAP协议层:系统故障	MAP协议层:数据丢失	MAP协议层:漫游失败:PLMN不允许漫游
2013-3-3 07:00:00	104955	81475	100115	95.39%	1720	1353	16675
MAP协议层:未知用户	MAP协议层:非期望的数据值	MAP业务层:由于不支持的特性限制漫游	TCAP协议层:P-Abort:未识别的事务处理ID	TCAP协议层:U-Abort	TCAP协议层:U诊断:无应用上下文名称	TCAP协议层:拒绝:重复调用ID	信令采集不全
167	77	792	109	373	1173	121	920

6 结束语

电信运营商必须始终将用户体验放在首位,通过不断优化、改进网络,吸引来访用户都愿意登记在本网内、出访用户都愿意留在本网内。凭借我国移动用户基数大、网络质量好等有利条件,再加上用户亲身的良好体验,不仅有助于增强现网用户的黏性,也有利于提高我国电信运营商与国外运营商的国漫业务议价能力。本文提出的来/出访LU登记成功率下降故障原因的分析思路和处理方法,可以有效地在源头厘清故障原因,并及时消除,从而确保来/出访LU登记成功率的指标值处于稳定波动范围内。

PTN网络保护技术对比分析

迟柏洋

（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：本文通过对 PTN 网络各种保护技术的分类研究，分析了各种保护技术的原理，总结了其优缺点、适用场景。结合运营商在 PTN 网络配置方面的实际需求，提出了有针对性的技术选择与配置建议。

关键词：链路保护　设备保护　LAG　APS

1　引言

随着 3G、LTE 等无线侧分组业务的日益增多，分组传送网（PTN，Packet Transport Network）网络现已面向全业务承载；随着网络规模、网络业务的迅速发展，以 PTN 技术为基础的城域传送网在可靠性、可用性等方面提出了更高要求。PTN 网络有多种保护技术，由于 PTN 网络标准正处于发展、完善阶段，各种保护技术多样且复杂，不同技术的应用场景、应用范围也各有不同，因此，深入研究各种 PTN 网络保护技术的原理、优缺点、适用场景，针对性地进行选择、部署，对于提高运营商 PTN 网络的可靠性、可用性是十分必要的。

2　PTN 保护技术分类

PTN 保护技术可分为三大类，网络边缘保护（UNI 侧保护）、网络内部保护（NNI 侧保护）和设备级保护。

（1）网络边缘保护技术包括 LMSP 线性复用段保护、LAG 保护、ML-PPP 多链路保护、IMA 保护。

（2）网络内部保护技术包括 MPLS APS 保护、MS-PW 保护、PW 双归保护、VRRP 保护。

（3）设备级保护包括关键板卡的冗余备份、TPS 保护等。

3　网络边缘保护（UNI 侧保护）

网络边缘保护是 PTN 网络边缘设备与用户设备之间的保护技术，因此又叫用户网络接口（UNI，User Node Interface）。由于直接对接用户设备，这一段的保护技术主要是针对边缘设备端口、链路的保护，其具体保护技术根据业务类型的不同也有不同。

常见的保护技术包括：LMSP 线性复用段保护、LAG 聚合链路保护、ML-PPP 多链路保护等。

3.1　LMSP 线性复用段保护技术

（1）LMSP（Linear Multiplex Section Protection ）线性复用段保护是一种 SDH 端口间的保护倒换技术，通过 SDH 帧中复用段的开销 K1/K2 字节来完成倒换协议的交互，通过 SDH 层面的告警来触发倒换。

（2）保护对象及应用场景

SDH 链路及端口，多用于 NodB 与 BSC 的接口链路。

（3）工作方式及保护原理

LMSP 分为 1+1 单向倒换、1+1 双向倒换和 1:1 双向倒换三种模式。

1+1模式是指发送侧在主备通道上双发业务，在接收侧选收业务，如图 1 所示。

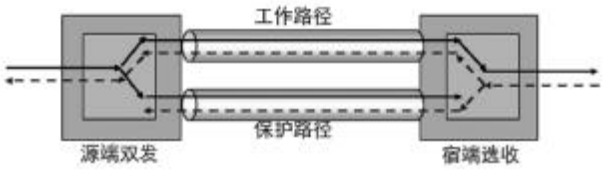


图 1 LMSP 工作原理示意图

1:1 模式是指发送侧在主备通道中选择一个通道发送业务,在接收侧选择接收业务。

1+1 单向倒换是指发送侧在主备通道上双发业务,在接收侧选收业务,当某个方向的通道发生故障时,只会造成这个方向的业务发生倒换。由于是双发业务,因此只在接收侧发生倒换即可。由于只有一侧倒换,因此倒换时间快,对业务影响也最小。

1+1 双向倒换是指发送侧在主备通道上双发业务,在接收侧选收业务,当某个方向的通道发生故障时,则两个方向的业务都要发生倒换。故障时需要发送端与接收端同时触发倒换,倒换时间稍长。

1:1 双向倒换是指发送侧仅在主备通道中选择一个通道发送业务,当某个方向的通道发生故障时,则两个方向的业务都要发生倒换。故障时需要发送端与接收端同时触发倒换,但业务仅在一个通道中发送,因此较为节省带宽资源。

值得注意的是,双向倒换能够保证业务双向路径一致,因此更适合对于时间同步要求较高的业务。

(4)技术优势

技术标准成熟,各厂家均支持;配置简单高效,可以满足 50ms 倒换要求。

(5)配置建议

对语音业务的保护,建议选择 1+1 双发选收单向倒换,以提高故障收敛速度。

3.2 LAG 保护技术

(1)LAG(Link Aggregation,链路聚合)是将一组以太网端口捆绑在一起作为一个逻辑接口以增加带宽并提供链路保护的一种方法。当某一链路发生故障时,其他链路能迅速接替故障链路。通过捆绑多条物理链路,也起到了增加带宽容量的作用。LAG 无需更改高层协议或应用程序,工作在数据链路层与高层协议及应用程序无关。

LAG 的聚合方式分为手工聚合、静态聚合两种。每一种的业务分担方式有负载分担、非负载分担两种。如图 2 所示。

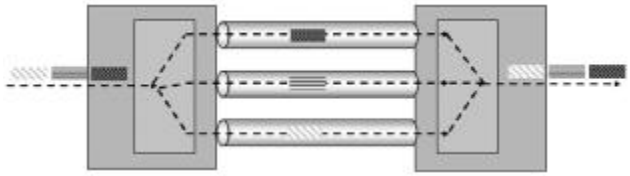


图 2 LAG 负载分担模式

负载分担方式下,业务均匀分布在 LAG 组内的所有成员上传送,每个 LAG 组一般最多配置 16 个成员,系统自动根据负荷分担算法将报文分发到聚合组的各链路上。

值得注意的是,该模式无法对 Qos 提供很好的保证,因此在 PTN 产品中,该模式只能应用在用户侧,而不能应用在网络侧。

非负载分担方式如图 3 所示,业务只在工作端口上传送,保护端口上不传送业务,每个 LAG 组只能配置两个成员。

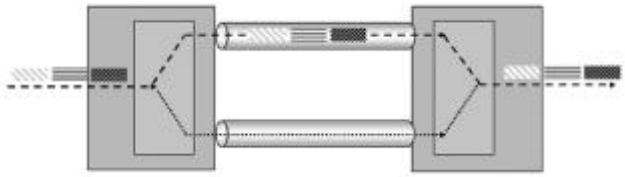


图 3 LAG 非负载分担模式

静态聚合模式由用户创建聚合组,增删成员端口,并运行链路聚合控制协议 LACP(Link Aggregation Control Protocol)。通过 LACP 协议在设备之间交互聚合信息,对聚合组的信息达成一致,而不是完全依赖单端配置。与手工聚合相比,对聚合的控制更加准确、有效。在具体配置时,建议优先选择静态聚合。

手工聚合模式由用户手工创建聚合组,增删成员端口,不运行链路聚合控制协议 LACP,一般只有当对方站点不支持 LACP 协议时才采用手工模式。根据端口物理状态(Down 和 Up)来确定是否进行聚合。与静态聚合相比,该模式对聚合的控制不够准确、有效。手工聚合要求两端对接设备的端口按照端口号的顺序对接,这种模式下,某成员链路发生单向故障(如断纤),发端不能检测到这一故障,业务会受影响或中断。

(2)保护对象:以太链路保护,如 PTN 核心节点与 RNC 设备之间的链路保护。

(3)技术优势:技术成熟,现网应用广泛。

(4)技术局限性:负载分担方式下无法对 Qos 提供很好的保证;手工聚合方式发端不能检测单链路故障。

(5)配置建议:优先选择静态聚合;负荷分担方式无法提供良好的 QOS 保证,建议应用在用户侧,而不要应用在网络侧。

3.3 ML-PPP 保护技术

(1)ML-PPP(Multilink-PPP)点对点多链路捆绑,与 LAG 技术较类似,区别在于 ML-PPP 在 PTN 网络中主要用于 E1 端口的保护,而 LAG 主要应用于以太口的保护。

(2) 保护对象:E1 链路, 即 Packet over E1 中 ML-PPP 组里面的 E1 链路。

(3)技术优势:MP-PPP 可在多重数据链路上传送数据包的分片,并重组和排序,对于该技术可利用分片来降低时延,适合对时延要求比较高的业务,并可提高语音类、视频类业务在低带宽网络环境下的传输质量;通过链路负荷的动态分配,可以有效提高带宽利用率。

(4) 技术局限性:ML-PPP 不能承载以太网专网业务;不能承载 MPLS Tunnel 1+1 和 1:1 保护;不能承载 FRR 保护。

(5)配置建议:较大报文业务建议使用 LSNFF 长序列号分片格式; 较小报文业务建议使用 SSNFF 短序列号分片格式。

3.4 IAM 保护技术

IMA(Inverse Multiplexing for ATM)即 ATM 的反向复用技术,是指将 ATM 集合信元流分接到多个低速链路上来传输,在远端再将多个低速链路复接在一起恢复成与原来顺序一样的集合信元流,从而使多个低速链路灵活方便地复用起来。IMA 适用于在 E1 或其他速率链路上传送 ATM 信元。

由于 ATM 技术逐渐衰落,本文不做深入探讨。

4 网络内部保护(NNI 侧保护)

4.1 MPLS Tunnel APS 保护技术

(1)MPLS 自动保护倒换(APS,Automatic Protection Switching)是一种针对 MPLS Tunnel 的管道性保护技术。源端设备通过周期性发送 OAM 检测报文来检测工作 Tunnel 是否发生故障。如果宿端设备在 3 个周期内没有接收到检测报文, 则认为工作 Tunnel 发生故障,源、宿端设备通过 APS 协议协商将业务切换到保护 Tunnel。

(2)保护对象:MPLS Tunnel(也可理解为 MPLS 的 LSP)。

(3) 工作方式及保护原理: 与 LAG 保护技术类似,MPLS Tunnel APS 保护方式分为两类:1+1 保护、1:1 保护。按照倒换方式,又可分为双向倒换和单向倒换。

1+1 保护是指在发送方同时向工作和保护两个 Tunnel 发送业务流量, 由接收方根据 Tunnel 状态或者外部命令选择性地接收业务流量。

1:1 保护在工作 Tunnel 正常时, 源端通过工作 Tunnel 发送业务流量, 宿端从工作 Tunnel 接收业务流量。当 Tunnel 源端得知工作 Tunnel 发生故障时,通过保护 Tunnel 发送业务流量, 宿端从保护 Tunnel 接收业务流量。

单向倒换是指当一个方向的 Tunnel 出现故障后,只倒换受影响的方向,另一个方向的 Tunnel 保持不变,继续从原通道选收业务。双向倒换是指当一个方向的 Tunnel 出现故障后, 两个方向的 Tunnel 都需要倒换。业务流量要么都走工作 Tunnel,要么都走保护 Tunnel。保证两个方向的业务流量都走同样的路径,这样更便于维护。

MPLS Tunnel APS 保护原理如图 4 所示。

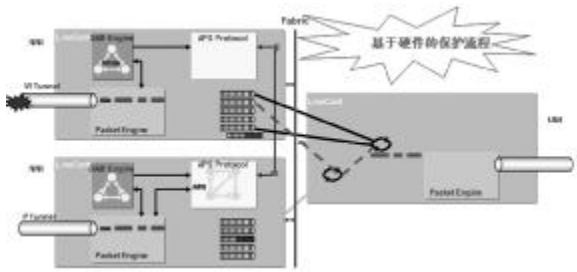


图 4 MPLS Tunnel APS 保护原理示意图

在 1:1 保护时,当工作 Tunnel 发生故障,OAM 引擎不能接收到 OAM 检测报文;在 3 个检测周期仍然没有收到检测报文后,就会触发 APS 协议;APS 协议触发保护切换,APS 协议会通告 Tunnel 源节点进行切换。1+1 保护时,切换仅由接收端进行触发即可。

OAM 检测报文有 CV 报文和 FFD 报文两种。CV 报文周期固定为 1 秒且不能改变;FFD 报文检测周期可以改变,为 3.3ms-500ms。

(4)技术优势:技术标准成熟,各厂家均支持;配置简单高效、保护全面,且可以满足 50ms 倒换要求。

(5)技术局限性:无法实现对源端、宿端设备的保护,在源端或宿端设备发生故障时,该保护技术失效,只能对源、宿端设备之间的网元故障或链路故障起到保护做用。另外,任何一点故障将导致所有业务均进行倒换,同时可能有上千条隧道或伪线发生倒换,网络影响范围较大。

(6)配置建议:由于 1+1 方式在工作、保护 Tunnel 上同时发送流量,因此对带宽要求较高;保护通道上需传送 APS 协议报文,要配置稍高的带宽,降低了带宽利用率,因此推荐使用 1:1 方式,并在保护通道上配置 100%带宽。由于双向倒换可以保证业务来回路径一致,更容易满足对时间同步要求较高的业务,且便于维护,因此推荐使用双向倒换。建议接入环与汇聚环对接时通过双节点对接,以避免工作通道与保护通道出现重路由。

4.2 MS-PW 保护技术

(1)MS-PW 保护技术通过对 Tunnel 进行分段,使故障倒换的范围有所限定;倒换仅在故障所在的小范围内发生,避免了全网震荡。

(2)保护对象:业务通道(PW)。

(3)工作方式及保护原理:1+1 保护、1:1 保护;按照倒换方式又可分为双向倒换和单向倒换。MS-PW 的保护场景如图 5 所示。

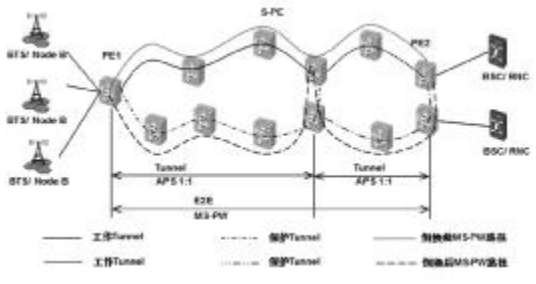


图 5 MS-PW 保护场景示意图

如图 5 所示,在 PE1 与 PE2 之间建立 MS-PW。通过 S-PE 对 PW 进行分段,分成 PE1-SPE 和 SPE-PE2 两段,并在段内部署 MPLS Tunnel APS1:1 或 1+1 保护,采用两段分别独立进行保护倒换的方式来限定倒换范围。

由此可见,MS-PW 方式下,Tunnel 是分段的,这样就可以实现故障倒换仅发生在段内而不影响段外。保护倒换后,MS-PW 作为内层标签没有发生变换,变化的仅仅是外层 Tunnel 标签。

(4)技术优势:与 MPLS Tunnel APS 技术相结合,对 Tunnel 的保护进行分段,缩小了网络故障倒换波及的范围。

(5)技术局限性:当 S-PE 节点发生故障时无法实现有效保护。

(6)配置建议:由于技术标准尚不成熟,建议先实验性部署,待技术成熟后再全网部署。

4.3 PW 双归保护技术

(1)PW 双归保护可以实现对源、宿端设备的保护,弥补了 MPLS APS 在源端或宿端设备故障时保护失效的不足。

(2)保护对象:源、宿端设备(网元级保护)和业务 PW 的保护,同时结合 LAG 技术实现了双归节点 U-NI 侧链路保护。

(3)工作方式及保护原理:1+1 保护、1:1 保护;按照倒换方式又可分为双向倒换和单向倒换。

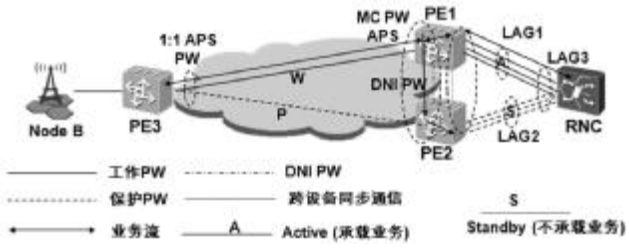


图 6 PW 双归保护场景示意图

如图 6 所示,NodeB 的业务通过 PTN 网络传送到 BSC/RNC,PE1、PE2、PE3 与 RNC 相互配合,实现业务的双归保护。

整个双归保护方案由网络侧的 1:1 MC-PW APS 保护组与双归节点 RNC 侧的 MC-LAG 组成。网络侧

的 MC-PW APS 由 PE3 设备上的 1:1 PW APS 保护组、PE1 与 PE2 设备上的 MC-PW APS 保护组组成；UNI 侧的 MC-LAG 由以下三部分组成：PE1 与 PE2 设备上的设备内 LAG（LAG1 与 LAG2）、PE1 与 PE2 之间的 MC-LAG、RNC 上的 LAG(LAG3)。

正常工作时，在网络侧，业务承载在 MC-PW APS 保护组的工作 PW 上；在 RNC 侧，MC-LAG 选择双归节点 PE1 与 PE2 中的一台设备为主用设备来转发业务(假设为 PE1，即选择 PE1 的 LAG1 承载业务)。

这种双归保护方案可以在双归节点故障、双归节点 RNC 侧链路故障或业务 PW 故障时，实现对业务的保护。

(4) 技术优势：与 MPLS Tunnel APS 技术相结合，对 Tunnel 的保护进行了分段，缩小了网络故障倒换波及的范围。

(5)技术局限性：双归保护需要与其他保护技术结合、联动，配置较复杂，且占用的网络性能资源也较多。

(6)配置建议：考虑到手工 LAG 无法识别单芯故障导致无法正常倒换，因此建议配合静态 LAG 使用。

4.4 VRRP 保护技术

(1)VRRP(虚拟路由冗余协议)是三层 IP 网络中的一种 IP 保护协议，主要是对网关设备进行保护。协议设定一个虚拟 IP 地址作为默认网关地址，两台互为主备的网关设备通过运行 VRRP 协议自动或人工推举出主用网关设备，如果主用网关发生故障(链路失效或设备宕机)，虚拟网关 IP 地址则指向备用网关设备，下挂无感知，从而实现主备网关的保护。

(2)保护对象：三层 PTN 网络中 TD-LTE 核心网元 SGW/MME 设备的主备网关和 TD-LTE 基站侧的主备网关保护。

(3)技术优势：源于 IP 网络，应用广泛，技术标准成熟。

(4)技术局限性：PTN 网络 VLAN 较多，需建立 VRRP 管理组，配置稍复杂。

(5)配置建议：VRRP 协议配置较复杂。为简化配置、方便管理，可将两台设备配置相同的 IP 和 MAC 地址；两台设备不在同一广播域，相同的 IP 地址和 MAC 地址也不会造成冲突。下挂的基站也不用与传输网内部的各种保护关联，只将对外的虚拟 IP 地址设为网关地址即可。

5 设备级保护

PTN 核心层、汇聚层设备承载着大量业务，一旦设备板卡、模块发生故障，将对大量业务产生影响，甚至导致业务中断。设备级保护就是对 PTN 设备的关键板卡、单元、模块的备份保护，如对主控单元配置 1+1 热备份。

在设备具体扩容配置时，核心层及汇聚层设备应当对主控单元进行 1+1 热备份；对接入层的设备，为节省投资，可根据具体投资规模、业务安全级别、故障影响范围，选择仅对电源模块做 1+1 热备份。

6 各种保护技术归纳总结

各种保护技术归纳总结见表 1。

7 结束语

PTN 各种保护技术均有其适用的场景、优缺点、局限性。在网络保护方案部署时，应当注意各种技术的相互结合、取长补短，有针对性地选择部署。鉴于部分 PTN 保护技术的标准尚不成熟、配置过于复杂，还有待于进一步优化完善，其保护效果仍需通过实践检验，所以在具体部署时应当先做小范围试验性部署。

参考文献

1 王磊，叶雯，李晗等.中国移动 PTN 网络规划和部署策略.移动通信，2010(17)
2 中国移动通信集团公司.中国移动分组城域传送网技术体制
3 张俊华，夏楠菲.3G 背景下城域传送网 PTN 部署方案.通信管理与技术，2010(1)
4 Draft ITU-T Recommendation G.8132/Y.1382(2008), T-MPLS Shared Protection Ring (TM-SPRing)

表 1 各种保护技术归纳总结表

类别	技术名称	工作方式	保护对象	优点	局限性	配置建议
网络边缘保护（UNI）	LMSP线性复用段保护技术	单向倒换 1+1; 双向倒换 1+1/1:1	SDH链路及端口,多用于 NodB 与 BSC 的接口链路	技术标准成熟,各厂家均支持;配置简单高效	-	由于多用于语音业务的保护,建议选择 1+1 双发选收单向倒换,提高故障收敛速度。
	LAG 链路聚合	手工聚合、静态聚合;负载分担、非负载分担	用于以太链路保护,如 PTN 落地设备与 RNC 设备之间、异厂家 PTN 设备互联的链路保护	技术成熟,现网应用广泛	1、负载分担方式下无法对 Qos 提供很好的保证; 2、手工聚合方式发端不能检测单链路故障	1、优先选择静态聚合;2、负荷分担方式无法提供良好 QOS 保证,建议应用在用户侧,不要应用在网络侧
	ML-PPP 点对点多链路捆绑	-	E1链路	非常适合对时延要求较高的业务	不能承载以太网专网业务;不能承载 MPLS Tunnel APS 保护;不能承载 FRR 保护	较大报文业务建议使用 LSNFF 长序列号分片格式;较小报文业务建议使用 SSNFF 短序列号分片格式
网络内部保护（NNI）	MPLS Tunnel APS	单向倒换 1+1 双向倒换 1+1/1:1	MPLS Tunnel	1、技术标准成熟,各厂家均支持; 2、配置简单高效,保护全面	1、无法实现对源、宿端设备的保护; 2、任何一点故障将导致所有业务均进行倒换	1、推荐使用 1:1 方式,并在保护通道上配置 100%带宽;2、推荐使用双向倒换;3、避免工作通道与保护通道出现重路由
	MS-PW	单向倒换 1+1 双向倒换 1+1/1:1	业务通道(PW)	与 MPLS Tunnel APS 技术相结合,对 Tunnel 的保护进行了分段,缩小了网络故障倒换波及的范围	1、技术尚不成熟; 2、当 S-PE 节点发生故障时,无法实现有效保护	建议目前实验性部署,待技术成熟后再进行全网部署
	PW 双归保护	-	源、宿端设备网元级保护、业务 PW的保护,同时结合 LAG/LMSP 技术,实现了双归节点 UNI 侧链路保护	实现了对源、宿端设备的网元级保护	1、需要与多种技术结合、联动,配置非常复杂;2、占用网络资源较多	手工 LAG 无法识别单芯故障,导致无法正常倒换,因此建议配合静态 LAG 使用
	VRRP 保护	-	SGW/MME设备的主备网关和 TD-LTE基站侧的主备网关保护	源于 IP 网络,应用广泛,技术标准成熟	PTN网络 VLAN 较多,需建立 VRRP 管理组,配置较复杂	1、设备配置相同的 IP、MAC 地址;2、结合 BFD 技术,实现故障的快速检测
设备级保护	对关键板卡、单元、模块的保护(如主控板、电源板、交叉板、风扇单元等关键部件的 1+1 或 1:N 保护)					

IT系统虚拟化实施率评估模型研究

李伟霄

（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:本文首先分析了虚拟化实施率评估模型的研究背景,总结了虚拟化实施率评估表,通过给出实施率、实施偏差的公式以完成实施率测算,最后建立了 IT 系统虚拟化实施率评估模型。

关键词:虚拟化 评估模型 实施率 实施偏差

1 引言

在全球企业不断实施各种层次虚拟化的大背景下,中国移动集团及各省分公司也在大力发展云计算和虚拟化技术。虚拟化技术在优势显现的同时,各种问题也随之而来。必须有效解决 IT 系统虚拟化实施情况的评估问题,才能更为准确、全面地进行 IT 系统运维和管理。

鉴于目前 IT 系统虚拟化正处于投资建设阶段,实际的虚拟化实施情况和系统建设规划不完全一致,IT 运维团队需要根据实际情况分析并测算工作量,现阶段运维实际工作量如图 1 所示。

图 1 现阶段运维工作量示意

由图 1 可以看出,IT 系统运维团队在虚拟化实施初期,测算工作量需要统计原有硬件中不可实施虚拟化的数量集,并加上纳入虚拟化与虚拟化新增硬件之和。对于 IT 系统运维,硬件虚拟化整合实现资源池,主要得益于虚拟化的动态资源调配,简化了系统调优的资源评估和测算,有效缩减了维护量。但面对 IT 系统复杂的硬件投资情况,IT 运维团队需要通过测算虚拟化的实施率来统计实际工作量,以有效管理人力成本。

2 虚拟化实施率评估表

虚拟化实施率的评估，可以通过对 IT 系统各方面的虚拟化实施情况进行评估,根据评估结果来反映整个 IT 系统的虚拟化程度,从而为 IT 系统虚拟化程度和 IT 运维工作量统计提供重要参考。

对 IT 系统虚拟化实施率的评估主要包括五个步骤:

(1)明确评估清单;

(2)计算当前系统的实施率;

(3)计算当前系统的实施偏差;

(4)计算成熟度得分;

(5)进行成熟度级别评估。

表 1　评估清单

序号	分类	权重(%)	子项	赋权	已实施
1	维护工具平台	10	监控系统	5	
			资源管理	5	
			维护工具整合	5	
			知识库	5	
			日志管理	5	
			灾备	5	
			合计	30	
2	桌面虚拟化	5	客户端管理	5	
			客户端定制	5	
			软件管理	4	
			脱网运行	3	
			终端脱离	3	
			桌面安全	5	
			合计	25	
3	网络	5	VDM支持	3	
			OpenFlow支持	3	
			IRF支持	4	
			带宽管理	4	
			IO管理	5	
			虚拟网络设备	5	
			虚拟网络分层	5	
			合计	29	
4	主机	15	集中管理	5	
			虚拟化产品支持	5	
			资源自动调配	5	
			模板定制和管理	4	
			Cluster	5	
			自动部署	5	
			迁移及变更	4	
			整机克隆	5	
			软件分发与管理	5	
			合计	43	
5	灾备	10	客户端集中管理	5	
			增量备份	4	
			快照备份	4	
			镜像备份	4	
			虚拟卷	5	
			合计	22	
6	存储	10	自动调配	5	
			集中管理	5	
			Fabric支持	5	
			合计	15	
7	监控	20	自动发现	5	
			变更发现	5	
			自动匹配	5	
			性能监控	5	
			主机监控	4	
			网络监控	4	
			应用监控	4	
			存储监控	4	
			备份监控	4	
			告警与预警	5	
			合计	45	
8	安全	25	虚拟防火墙	4	
			虚拟防病毒	5	
			安全审计	5	
			安全防护	5	
			安全控制	5	
			日志分析	5	
			用户管理	5	
			合计	34	
权重		100	总计	243	

3　实施率

实施率指通过已实施子项条目数和预期实施子项条目数进行对比,根据实施率来评估系统虚拟化的实施情况。具体按照公式(1)计算。

$$\xi = \sum^{n} \bar{a}_i \cdot \lambda_i, \left(\lambda_i \in [0,1] \cap \sum^{n} \lambda_i = 1 \right) \quad (1)$$

式中:n_i 为每个分类的子项条目数;

i_i 为所有实施的子项条目数;

s_i 为每个分类包含的子项条目数;

p_i 为每个子项条目的实施率。即 $p_i=i_i/s_i$

$\bar{a}_i$ 为每个虚拟化分类的所有子项平均实施率; $\bar{a}_i = \frac{\sum_{i=1}^{n} p_i}{n_i}$。

n 为所有分类总数,n=8;

λ_i 为分别为个分类分配权重,所有分类权重合计为 1;

ε 为虚拟化实施率。

4　实施偏差

实施偏差指计算已实施子项条目数与各个分类中子项的平均实施比率, 根据实施偏差来评估 IT 系统虚拟化指标在各个分类中是否均衡,避免出现个别项目分值高而其它项目偏低、但无法在评估结果中体现的情况。具体按照公式(2)计算。

$$\sigma = \frac{\sum_{i=1}^{n} (P_i - \bar{P})^2}{n} \quad (2)$$

式中:I_i 为所有实施的子项条目数,其中代表子项数;

s_i 为每个分类包含的子项数;

p_i 为每个分类的实施率,即 $P_i=I_i/S_i$。

n 为所有分类总数,n=8;

$\bar{p}$ 为平均实施率, $\bar{P} = \frac{\sum_{i=1}^{n} P_i}{n}$;

σ 为实施偏差程度。

5　实施率测算

实施率的计算总体反映了系统的虚拟化实施情况。具体按照公式(3)计算。

$$M = \xi \cdot (1-\sigma) \cdot 100 \quad (3)$$

式中:M 为成熟度;

ξ为虚拟化实施率;

σ为实施偏差程度。

6 IT 系统虚拟化实施率评估模型

虚拟化的成熟程度体现了系统的具体可控情况，从而为客户满意度、系统可用率等信息化系统运维关键指标考核工作提供了重要保证。通过对虚拟化实施内容的分析、评估，综合分析结果，提出了四级成熟度模型；通过对 IT 系统虚拟化的实施情况进行成熟度评估，充分认识当前虚拟化的程度，为做好运维工作、提高各项运维指标提供了指导、参考。具体内容如表 2 所示。

表 2 虚拟化实施率评估表

序号	虚拟化等级	虚拟化率	虚拟化实施情况
1	I 初始级	0-50	虚拟化的程度不能得到保证，IT 系统虚拟化处于初始阶段，且系统运行随时可能出现异常，客户满意度和系统可用率基本无法得到保障。
2	II 已定义	51-70	虚拟化指标得到实施，但资源池的自动化程度不高，支撑工具不齐全。
3	III 可管理	71-85	虚拟化的主要技术指标都已经实施，虚拟资源的调配与调度可自动完成，支撑工具对资源池的支撑有了很大改善，系统异常情况可以得到全面控制和有效解决，客户满意度和系统可用率已经达到客户要求。
4	IV 优化级	86-100	虚拟化的所有技术指标都已经基本覆盖，系统运行稳定，客户满意度和系统可用率较高。运维团队对于虚拟资源的实现可控、可管，全面实现安全防护和调度控制，实现了对系统的精细化分析和管理，可以通过自身持续的改进、优化，不断提高各项运维指标。

7 结束语

本文提出的 IT 系统虚拟化实施率评估模型，已在省级移动公司 IT 运维项目中得到应用，研究成果对管理信息系统的虚拟化运维工作具有指导意义。评估模型中评估清单可以根据不同项目的评估需求制定不同分类，灵活定制，具有较强适应性。

(上接第 11 页)

(2)将物理服务器、存储磁阵划入不同的安全等级区域，针对虚拟机在业务平台中担任的角色不同，为虚拟机分配运行时所在物理服务器的区域、存储磁阵的区域。

(3)在业务上，制定虚拟机之间的访问控制策略。业务部署之初，通过调研部署模块的访问关系，制定虚拟机之间的访问控制规则，使得虚拟机在运行阶段具备监控是否有未经授权的修改和违规活动的能力。

4.2.3 定期风险评估

定期进行安全风险评估分析，是云平台持续提供安全服务的保障。安全风险存在于云平台的每一个层面，定期风险评估是一个动态管控体系。

主要评估项目包括：日志审计、漏洞扫描、渗透测试、配置核查、镜像文件一致性核查等内容。这些评估项目在传统 IT 环境中已经存在，所不同的是需要针对虚拟环境的特殊性进行相应调整。

5 结束语

云平台的安全防护，要从规划和部署阶段就开始考虑。虚拟化安全问题还需要不断跟踪研究，根据实际业务应用不断提出新的安全需求，逐步建立起比较完善的虚拟化安全需求参考模型。

全业务运营下综合业务接入区划分方法研究与实现

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:本文介绍了一种全业务运营背景下综合业务接入区的划分方法和步骤,旨在提出科学有效的规划思路,做到划分方法步骤清晰、划分工具简单便捷,并具有一定的可行性和指导性。

关键词:综合业务接入区 业务汇聚点 Google Earth

为提升全业务运营背景下的市场竞争力,解决面向移动综合业务接入的实际问题,本文介绍了一种综合业务接入区的划分方法和步骤。

1 综合业务接入区划分前的准备

综合业务接入区是指为满足 2G/3G、WLAN、集团客户、家庭客户等的业务接入需求,根据城市自然区划和路网结构,将城市划分成的多个能独立完成业务汇聚的区域。

1.1 确定业务区划分标准

大中型城市内的金融、行政等高度集中的功能区,工业园区,高密度住宅区等区域应根据功能区域划分,可按照 2 平方公里左右进行规划;商户聚居区、普通商业区、普通住宅区、写字楼区及其他业务密集区可按照 2-5 平方公里进行规划;非密集城区、县城和发达乡镇等区域可按照 5-10 平方公里进行规划。

1.2 选择合适的划分工具

传统无线网络或光缆线路的规划工具一般使用 MapInfo,但在规划综合业务接入区时存在一定局限:无法显示地形、小区覆盖方向的地理环境;对于地级市或县城而言,道路名称不准确或更新不及时;使用 MapInfo 需要购买注册码,成本很高。

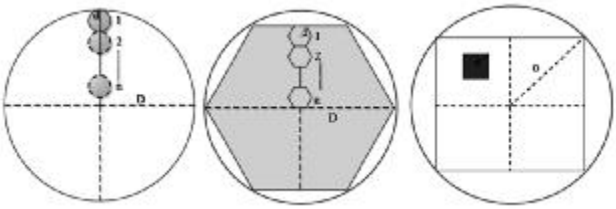
另外一种常用方法是将高精度地图扫描至电脑并导入 CAD 中使用，但规划综合业务区时无法自动导入上千个客户位置信息,显然不能使用。

在划分综合业务接入区方面,Google Earth 使用起来方便很多,显示直观,地形地貌明显,城区各目标点位置准确;更新及时的免费版 Google Earth 可以满足规划所需功能，如根据经纬度进行客户接入点导入、图层编辑、多样化图标设置等。

另外,Google Earth 可导入的文件是 kml 文件,已知经纬度信息的客户文件(excel 格式)是无法直接导入 Google Earth 的。因此，为配合 Google Earth 的使用,在划分综合业务接入区时还需要 kml 文件转换工具。

1.3 测算综合业务区划分数量

综合业务接入网建设对业务、技术、成本要求十分敏感,投资大,建设周期长,存在一定经济风险。利用较少投入获得较大收益回报,是建设单位关注的重点。因此,应从投资角度确定科学合理的业务区数量,从而使方案更具说服力。利用高等数学中的数学建模思路,可以对业务区进行简单的建模分析。如图 1 所示,D 表示规划区域内的范围;N 表示区域内的用户数量;P 表示区域内的用户密度;d 表示某业务区半径。



模型一 模型二 模型三

图 1 覆盖区域模型

如图 1,区域覆盖一般为圆形、正六边形、正方形。由于现实覆盖区域多是根据主干道路、管道分布进行分割,所以大多数接入区呈正方形,故据此计算综合业务接入网投资。

(1)光缆投资 C_1

光缆很少直接相连,一般是从机房沿街道走折线或者曲线到用户,设折线系数为 K_1。 假设机房位于区域内几何中心位置,如图 2 所示。

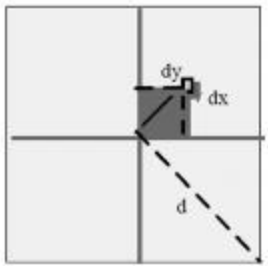


图 2 光缆投资模型图

所有用户直线距离和由式(1)计算。

$$S_0= 4\times\int_0^{d/\sqrt{2}}\int_0^{d/\sqrt{2}}\left(\sqrt{x^2+y^2}\right)\times P\times dxdy \quad (1)$$

所有用户接入光缆距离由式(2)计算。

$$S=S_0/K_1 \quad (2)$$

业务接入区内所有用户数由式(3)计算。

$$N_0= 2d^2\times P \quad (3)$$

区域内单用户平均光缆长度由式(4)计算。

$$L=S/N_0=S_0/(K_1\times N_0)$$
$$= 4\times\int_0^{d/\sqrt{2}}\int_0^{d/\sqrt{2}}\left(\sqrt{x^2+y^2}\right)\times P\times dxdy/(K_1\times 2d_2\times P)$$
$$= K_2 d/K_1 \quad (4)$$

设 K_3 为单公里光缆造价, 光缆投资计算公式见公式(5)。

$$C_1=N\times L\times K_3= N\times d\times K_2\times K_3/K_1 \quad (5)$$

经计算可知,正方形时 K_2=0.54,现实网络中 K_1 根据经验一般取值 0.8。

(2)机房投资 C_2

设 K_4 表示机房单价,机房投资与机房造价及数量有关。

$$C_2= K_4D_2/d_2 \quad (6)$$

(3)局端接入设备投资 C_3

设 K_5 表示机房设备单位用户造价, 局端接入设备投资与覆盖用户数量有关,与区域覆盖半径无关。

$$C_3= K_5\times N \quad (7)$$

(4)用户侧投资为 C_4

K_6 表示用户侧 ONU 综合造价,用户侧投资与用户数量有关,与区域覆盖半径无关。

$$C_4= K_6\times N \quad (8)$$

综合业务接入网建设综合造价由式(9)计算。

$$C= C_1+ C_2+ C_3+ C_4$$
$$= N\times d\times K_2\times K_3/K_1+ K_4D_2/d_2+ K_5\times N+ K_6\times N \quad (9)$$

上式中对 d 求导可知,在 $d=\sqrt[3]{(K_1\times K_4/(K_2\times K_3\times P))}$ 时, 综合业务接入网投资有最小值,d 与用户密度 P 有关。确定了每个业务区的平均半径,在划分面积既定情况下,就可以计算出业务区的数量,此数值是具体划分业务区时的重要参考。

2 综合业务接入区划分实例

下面以某省二线地级市市区为例,介绍综合业务接入区的划分步骤。

(1)区块划分

以城市的铁路、河流、湖泊、公园、绿化带、主要街道及其他妨碍光缆线路穿行的大型障碍为界,对城市进行网格状区块划分。如图 3 所示,以南环、北环、东环和西环划定行政区界,以铁路、河流及东西方向 3 条(东西路 1、2、3)和南北方向 1 条(南北路)贯穿市区的主干道路为界,将市区划分成若干个区块。区块是综合业务接入区的最初形态。

(2)收集整理基础信息资料

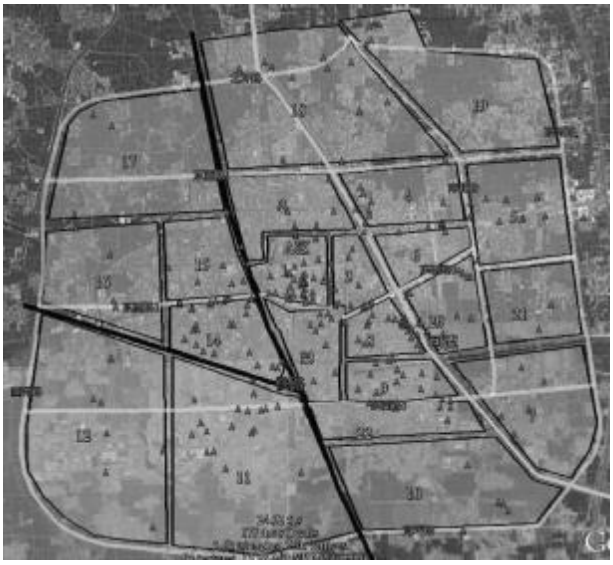
此步骤与(1)同步进行。基础信息资料的来源,主要是客户的网管信息平台、基础资源管理平台、施工单位竣工材料反馈及网络维护人员的日常维护资料。所有基础资源如机房、光交、管线等均要有经纬度信息,据此进行地图位置定位。这些材料是进行综合业务接入区划分的重要依据和参考, 准确度要求很高。为便于查看、使用,针对不同的信息需要使用不同的图层区分。

(3)客户需求分布调查

客户的分布是进行综合业务接入区划分的另一重要依据,主要来源于自上而下的调研和自下而上的上报需求。运营商自上而下的机构设置完善,利于调研表的分发及最终结果的反馈;有强烈接入需求的客户会上报其具体位置信息。

(4)勘察

对于网管平台无法获取的基础资源信息、不准确的资源信息以及调查后无法定位的客户位置进行实地勘察。勘察是获取各方面信息的最准确途径,目的是查缺补漏。勘察点越多,综合业务区划分结果的准确性越有保证。最终将所有的包括勘察核实后的客户位置定位到 Google Earth 中, 如图 3 所示。



注:图中粗实线代表铁路,细实线代表业务区边界,浅色代表主干道路或河流

A 表示客户分布位置,图中未显示次干道路

图 3 客户位置分布及综合业务接入区划分

(5)测算划分区域的业务区合理数量

利用公式 $d=\sqrt[3]{(K_1\times K_4/(K_2\times K_3\times P))}$ 以及从现有信息中确定的 K_1~K_4 和 P 值(P 值按固定值考虑)进行粗略计算得知, 业务区的平均半径 d 约为 1.6 公里、面积约为 5 平方公里时,综合业务区建设的投资接近最小值。但在实际划分中,不同区域的用户密度 P 有很大不同, 因此 5 平方公里是个基准数字,每个业务区根据 P 值的不同在 5 平方公里范围内浮动。若城区面积为 100 平方公里左右,则最终划分为 20 个综合业务接入区时建设投资接近最小值。对于愈来愈重视投资回报的运营商来说,20 这个数字对于评估最终的划分结果有着重要的参考意义。

(6)区块裂变、调整,形成最终方案

在业务区划分的总原则下,根据客户密度划定密集区域和非密集区域,决定现有区块是进行裂变还是在现状基础上稍做调整或保持现状;根据管线资源分布情况对由主干道路决定的区块边界进行重新界定,保留管线分布较少的主干道路边界,管线分布密集的主干道路可以不作为边界;根据次干道路、光交等信息进行区块裂变后的精细化修正。最终的划分数量最好接近 20,以使方案投资接近最小值。

参看图 3 的 A 区块(北至东西路 1,东至河畔,西至铁路沿线,南至东西路 2,面积约 7 平方公里),为客户密集分布区,区内管线分布密集,管孔资源丰富(图中未画出)。以 A 区块中的次干道路为界,按照 2 平方公里左右为单位划分,A 区块裂变调整为综合业务接入区 1、2、3。按照同样思路,整个市区共划分为 22 个综合业务接入区,其中,业务区 1-6、8、9、13、14、20、21 为用户密集区或预测未来会有较多用户发展的区域,按照 2-5 平方公里划分,剩余每个业务区域的面积约为 5-10 平方公里。同时,数值 22 与总投资最小值时计算出来的数量(20)接近,证明结果较为合理。

3 结束语

本文介绍了综合业务接入区的概念,业务区的划分原则、步骤、方法和工具,其中以利用数学建模思路确定科学合理的业务区数量最为关键,据此提供了综合业务接入区划分实例。

综合业务接入区网络结构的重要特性是分层分区,应达到“层次清晰、布局合理、调度灵活、管理方便”的目标,从而满足网络可持续发展的需要。每个综合业务接入区的覆盖范围一旦划分确定,应保持一定时间的稳定、不要再随意变动,以利于区内网络建设,但也可根据业务实际发展情况进行适当的分拆、归并或调整。

拉远 RRU 基站动力环境监控的实现

邹玉明 刘述佳

（中国联通威海市分公司,威海 264200）

摘 要:本文介绍了拉远 RRU 基站动力环境监控的实现原理,为大量建设拉远 RRU 基站提供了参考。

关键词:拉远 RRU 基站 动力环境监控 BBU+RRU DB15

1 引言

随着 WCDMA 网络建设的展开，某市本地网拉远 RRU 基站数量日益增加,随之而来的是拉远 RRU 基站由于没有实现动力环境监控,因市电、光缆中断等问题不能及时上报而导致基站退服的情况较多。为提高基站的运行可靠性,2013 年 1 月起,某市电信公司组织力量，将拉远 RRU 基站全部实现了动力环境监控。

2 研究背景

拉远 RRU 基站因其节省建网费用和机房面积、可快速部署、便于升级、节省能源等优点,所以得到了规模应用。近端基带 BBU 部分实现监控比较容易,出现故障后可以及时判断、处理;但拉远端 RRU 部分,因为拉远端设备一般放置在楼宇弱电井、室外抱杆等处而在监控范围之外。当网管上报拉远设备(RRU)断站后，无法迅速判断是电源原因还是光缆故障引起,需要维护人员现场进行逐项测试,耗费人力、物力,故障得不到及时修复。而 RRU 设备覆盖用户对信号的需求都较强烈,故障修复时间越长,用户感知度越差,容易引发大量投诉。利用现有传输资源,低成本实现拉远 RRU 站点的动力环境监控，是一个亟待解决的课题。

3 拉远 RRU 基站动力环境监控的实现

现网中，部分室外拉远 RRU 宏站及室内分布系统由于 BBU 是集中放置，与 RRU 不在同一位置,所以无法将 RRU 的停电告警、门磁告警上报至综合网管，导致这些室外 RRU 基站的市电停电、蓄电池欠压、门磁等信息都无法及时上报。蓄电池电量放完后直接出现的 RRU 退服和基站断站，无疑会影响维护指标和用户感知度。

传统 2G、3G 基站的动力环境监控系统，一般采用逐级汇接的拓扑结构。在传送承载上,某市电信公司主要有两种方式：

(1)在 2G、3G 共站的情况下,利用传统 2G 基站 BTS 设备与基站控制器 BSC 设备之间的 SDH 业务电路完成。

(2) 在只有独立 3G 基站的情况下，将基站 NODEB 设备空闲 FE 端口与机房内监控设备相连,利用 3G 基站的路由转发功能,通过 NODEB、IP 承载网和 RNC,将基站监控数据转发至监控中心服务器。

而拉远 RRU 基站采用的是 BBU+RRU 分离的组网方式,其技术特点是将基站分成近端机即无线基带控制(BBU)和远端机即射频拉远(RRU)两部分,二者之间通过光纤连接;其接口是基于开放式 CPRI 或 IR 接口,可以稳定地与主流厂商设备进行连接。BBU 安装在配套齐全的机房内；而 RRU 则安装在基站现

场(天线端)附近,往往只有一个一体化电源柜。拉远 RRU 不能提供传输 2M 以传送监控参量,不能提供从 2G 基站 2M 电路中提取 1 个 64K 时隙的方法来传送监控参量，也不具备 3G 基站空闲 FE 端口来转发监控参量,且厂商没有提供其他明确或标准的动力系统监控接入方式，所以拉远 RRU 暂无法实现动力环境监控。

现网 BBU+RRU 的组网图如图 1 所示。

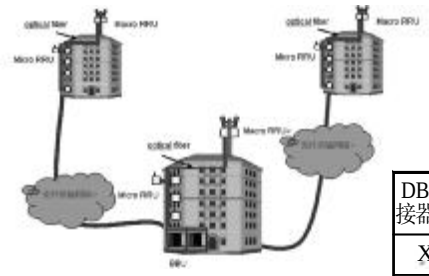


图 1 拉远 RRU 基站组网图

鉴于上述情况,2013 年 1 月,某市电信公司尝试建设拉远型基站监控系统,最终找到了最佳方案。

3.1 深入分析,制定方案

经过深入分析,结合现网实际,该公司提出了通过拉远 RRU 监控通道进行开发的方案。对比发现,某设备厂商的交流 RRU 都能上报基站停电告警，而直流 RRU 则无法上报。对比 RRU 结构(图 2)可知:交流 RRU 比直流 RRU 多了整流模块和 DB15 成品监控线。

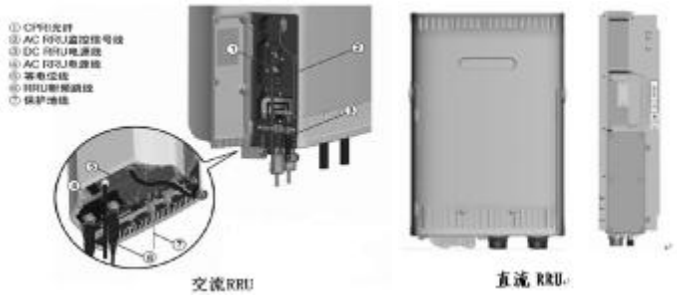


图 2 RRU 结构对比图

查阅厂商设备手册,可知交、直流 RRU 均支持 2 路开关路告警的上传,所以,交流 RRU 能上报停电告警，直流 RRU 因没有整流器进行干节点告警上报而无法上报告警。设想:通过直流 RRU 的 DB15 接口引入各种监控参量,利用 RRU 进行上报。

DB15 连接器结构图如图 3 所示。

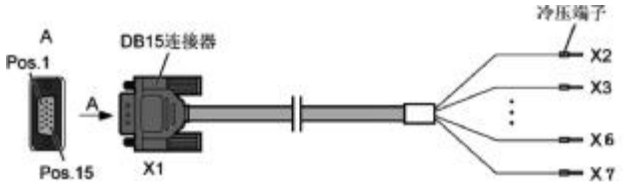


图 3 DB15 连接器结构图

DB15 连接器线缆表见表 1。

表 1 DB15 连接器线缆表

DB15连接器芯脚	DB15连接器信号名称	芯线颜色	芯线类型	冷压端子	线缆标签	干节点告警	告警名称
X1.2	SWITCH_INPUTO+	白 / 蓝色	双绞线	X2	SWITCH_INPUTO+	第 1 路	门禁开关
X1.3	GND	蓝色		X3	GND		
X1.6	SWITCH_INPUT1+	白 / 橙色	双绞线	X6	SWITCH_INPUT1+	第 2 路	交流停电
X1.7	GND	橙色		X7	GND		

3.2 分步实施,稳妥实现

(1)方案实施前的准备

由于华为 2G/3G RRU 硬件、软件结构基本类似,因此下面主要讲解拉远直流 3G RRU。方案实施前,必须先改造现有网络结构：将直流 RRU 告警接口连接 DB15 监控线,将监控线另一端与开关电源、门禁等动力环境设备相连。完成后，按图 4 制作好 DB15 公头并接入直流 RRU;螺丝拧牢,盖上 RRU 的盖板。

图 4 RRU 与电源柜接线图

(2)网线另一端分别与需监控设备连接,实现物理对接

以该公司某站点为例，对拉远 RRU 基站的开关电源停电告警和门禁实现接入。

将 DB15 监控线的 X6、X7 两根线缆与电源柜第 1 路输出干节点相连,调节电源柜设备,将第 1 路输出干节点设置为电源柜交流停电检测。X2、X3 两根线缆与电源柜第 2 路输出干节点相连，调节电源柜设备,将第 2 路输出干节点设置为电源柜门禁检测。

交流停电为常闭型告警。市电正常时,输出干节点为通;市电停电时,输出干节点为断。所以,X6 线缆接 GND,X7 线缆接输出干节点常闭接点(NC)。

开关电源门禁告警也为常闭型告警。门开时,输出干节点为通;门关时,输入干节点为断。所以,X2 线缆接 GND, X3 线缆接输出干节点常闭节点(NC)。

(3)相关告警数据的添加

以上操作只完成了拉远基站 RRU 与需监控设备的物理连接;要实现监控参量在网管系统中的正确上报,需进行相关告警数据的添加。

1)打开 RRU 外部告警客户定义开关

SET ALMPORT: CN=0, SRN=80, SN=0, PN=0, SW=ON, AID=65033, PT=BOOL, AVOL=HIGH

SET ALMPORT: CN=0, SRN=80, SN=0, PN=1, SW=ON, AID=65034, PT=BOOL, AVOL=HIGH

2)设置 RRU 的环境告警参数

SET ENVALMPARA: ALMID=65033, ANM="RRU 掉电 ", ALVL=CRITICAL, ASS=POWER

SET ENVALMPARA: ALMID=65034, ANM="门磁告警 ", ALVL=CRITICAL, ASS=POWER

3)M2000 上设置 65033 告警名称为 “RRU 掉电”,65034 告警名称为“门磁告警”

需要从 M2000 上定义新增加的告警，以便从 M2000 上能够监视到此告警。打开 M2000 的客户端,在“监控”的“告警设置”里面找到“网元告警设置”,如图 5 所示。

图 5 M2000 新增告警的设置

点击打开,可以看到“用户自定义告警”里面的“告警定义”;点击右下角的“增加”选项,如图 6 所示。

图 6 M2000 自定义告警的设置

通过以上步骤,完成了拉远基站中停电告警和门禁告警的上报。网管终端上报门磁及停电情况如图 7、图 8 所示。

图 7 门磁及停电告警的上报

图 8 门磁及停电告警的恢复

(下转第 36 页)

GSM数字光纤直放站在胶济客运专线中的应用

于 强 王晓蓉

(中国联通潍坊市分公司,潍坊 261061)

摘 要:本文介绍了在胶济客运专线高密段采用 **GSM** 数字光纤直放站专网覆盖方式,解决了高速移动环境下 **GSM** 网络存在的高掉话、接入失败、数据速率低等问题,并总结了应用结果。

关键词:GSM 数字光纤直放站 高速铁路 次强邻区

1 引言

胶济客运专线全长 362.5 公里, 最高时速可达 250 公里。运行车型以 CRH5 为主,CRH2 和 CRH3 为辅;CRH5 的车体损耗明显高于另外两种,可达 24dB 左右。由于 CRH 动车特别是 CRH5 速度快、车体密封性好、无线信号穿透损耗高等原因,列车内 GSM 场强弱、接入成功率低、数据速率低,导致用户感知很差。专线高密段全长 33 公里,地形为平原,是行车速度最快的路段之一。高密段 GSM 网络为摩托罗拉设备,由于老化严重,造成性能严重降低、故障率高,且基站密度也很低, 不少站点与铁路间的直线距离超过 1 公里,现有网络不能满足动车模式下的覆盖和重选切换需求。由于无法通过宏站现网调整和宏站专网方式解决现有问题,我们采用了数字光纤直放站建设光纤专网方式。

2 光纤直放站专网覆盖的特点

现阶段高速铁路通信解决方案中,包括利用现网覆盖和建设专网覆盖。建设专网又可分为基站专网和光纤专网两种方式。利用数字光纤直放站建设专网覆盖高铁,在单扇区覆盖范围内可大大降低切换次数和掉话风险,明显改善用户感知。

光纤直放站分为模拟光纤直放站和数字光纤直放站。数字光纤直放站采用先进的数字信号处理技术和数字信号光纤传输技术,可以实现多载频信号的远距离传输和大容量、大动态范围的信号覆盖,实现单小区长距离专网覆盖。相比传统的模拟光纤直放站,数字光纤直放站有如下特点:

(1)很好地解决了上行噪声抑制功能,在带 24 个远端时引入的噪声不超过 -130dBm (带宽为 200KHz),可以确保链路平衡不受任何影响,保证基站的接收灵敏度和覆盖范围。

(2)输出功率可达 60W。

(3)可自动测量、调整远端的传输时延,保证各个远端的时延一致,防止重叠覆盖区的时延色散干扰。

(4)可实现近端和远端实时监控。

3 光纤专网覆盖的实现

3.1 手机在车厢内的最低信号强度需求

根据公式计算移动台接收机要求的输入电平:

SSreq=MSsens+RFmarg+IFmarg+Bloss (1)

式中,MSsens 为手机接收机灵敏度, 取值为 -104dBm;RFmarg 为瑞利衰落(快衰落)余量,取值为 5dB;IFmarg 为干扰余量, 取值为 4dB;BLoss 为人体损耗,取值为 5dB。

因此,SSreq =-88dBm。

而根据实际优化经验，在高速铁路模式下,GSM 手机能有效发起、建立呼叫并保持时的最低电平为 -85dbm。因此，以下讨论中 SSreq 统一取值为 -85dbm。

3.2 手机在车厢外的最低信号强度需求

手机在车厢外的最低信号强度要求,即设计电平值:

SSdesign=SSreq+LNFmarg+LPL (2)

式中,LNFmarg 为慢衰落储备，取值 3db;LPL 为穿透损耗,取值 24db。则 SSdesign=-85+3+24=-58dbm。也就是说,需要车厢外信号强度达到 -58dbm 时,车厢内的信号强度才能达到要求。

3.3 不考虑重叠覆盖区时的站间距估算

假设有效全向辐射功率 EIRP 为 53dBm(考虑了大多数基站的发射功率、馈线及跳线损耗,天线增益为 21dBi),则最大允许的路径损耗为:

Lpathmax =EIRP-SSdesign=111dB (3)

根据 Okumura-Hata 模型传播公式:

$$Lp = 69.55 + 26.16\lg f - 13.82\lg hb - \alpha(hm) + (44.9 - 6.55\lg hb)\lg d \quad (4)$$

式中,Lp 为路径损耗;f 为信号频率,取 900MHz;hb 为基站天线高度,取 25m;hm 为手机天线高度,取 3m。考虑列车衰落严重,都以大城市为基准,移动台高度修正因子 $\alpha(hm) = 3.2(\lg 11.75hm)^2 - 4.97$,有:

$$111dB = 69.55 + 26.16\lg f - 13.82\lg hb - [3.2(\lg 11.75hm)^2 - 4.97] + (44.9 - 6.55\lg hb)\lg d$$

$$111 - 69.55 - 4.97 = 26.16\lg 900 - 13.82\lg 25 - 3.2(\lg 11.75*3)^2 + (44.9 - 6.55\lg 15)\lg d$$

$$36.48 = 77.28 - 19.32 - 7.66 + 37.2\lg d - 13.82 = 37.2\lg d$$

$$0.425 = d$$

即:覆盖距离为 425 米,则市区站间距为 850 米。根据 Okumura-Hata 传播公式采用郊区模型计算后,郊区站间距约为 1550 米。

3.4 重叠区域距离计算

手机在服务小区的信号强度衰落到一定程度,会触发小区重选(idle 模式)或者切换(专用模式)过程,因此必须保证在手机顺利进入新小区之前,当前小区的信号不会进一步衰落到门限值以下,否则空闲的手机可能脱网、通话模式的手机可能切换失败而导致掉话。所以,需要控制重叠区域的大小,以保证重选或者切换的完成。

小区重选的时间要比切换慢,因此切换带只需要满足小区重选即可满足切换需求。

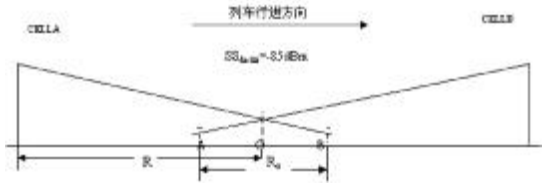


图 1 重选与切换重叠区示意图

如图 1 所示,手机在从 CELLA 往 CELLB 移动的过程中,一直在测量二者的信号强度,并计算各自 C1、C2 值。根据小区重选规则,若 C2B>C2A 超过 5 秒,则重选到 CELLB。在 O 点,C2B=C2A。因此重叠区域的定义就是：列车从 O 点向 CELLB 行进 5 秒到达 B 点时的距离的两倍(需考虑反方向)。另外,还需要 C1A 大于 0 才不会脱网。当然,由于在 O 点的电平为 -85dbm,这种情况就不存在了。则重叠覆盖区距离 Ro=2*OB=2* (200 公里 / 小时) /3600*5=556 米。

3.5 考虑重叠覆盖区的站间距

由于重叠覆盖区域的存在，使得站间距有所下降,以郊区为例,最终的站间距为 1550-556=994 米。但由于是直放站,除分界点之外的基站间都是同源信号,不需进行重选和切换,只要保证信号的连贯性即可,故在实际工程中可采用站间距 1300 米左右。

3.6 站点规划的其它要求

考虑到列车内部的空间损耗,要求站点沿铁路线呈“之”字型分布,以保证列车内信号分布均匀。由于直放站采用高增益天线,水平波瓣较窄,基站距铁路的直线距离在 100~200 米之间最为合适。

3.7 网络容量需求

CRH5 的标准配置为 8 节车厢,额定载客人数为 604 人;双联车 16 节车厢,双向会车用户人数可达到 2416 人。按照目前联通 GSM 移动客户 20%渗透率和每用户 0.02ERL 计算,将带来 9.66ERL 话务。查 ERL B 表(2%呼损)可知需要 16 个 TCH。考虑到 EDGE 业务配 4 个静态 PDCH, 专网小区至少配置 3 个载频。高密城区段由于有专网与公网的出入口,故配置 4 个载频。

3.8 邻区配置及参数设置

由于是直放站专网覆盖,不再专门设置与公网间的重选、切换参数,只是在车站和直放站两端设置与公网的重选、切换关系。

按照传统方式, 在车站一般会添加室内分布系统,作为专网和公网之间的缓冲区域,完成用户在两者之间的重选、切换工作。但是由于种种原因,未能在车站建成室内分布系统,只能进行公网和专网之间的直接切换、重选。通过前期测试分析,发现在站台上公网信号是很强的,即使开通直放站专网,只要添加了邻区关系,就有可能导致列车上的客户切入公网而掉话(公网在铁路上的覆盖较弱)。为解决这一难题,我们设计了“次强邻区”,如图 2 所示,即:在直放站专网与其公网间的次强邻小区设置正常的双向重选、切换关系,而原先最强的邻小区去掉邻区关系,这样既保证了手机客户进出火车站的顺利切换和重选,又成功解决了站台列车上的手机客户占用公网信号的问题(由于是次强小区, 其在站台的信号强度远弱于专网信号)。

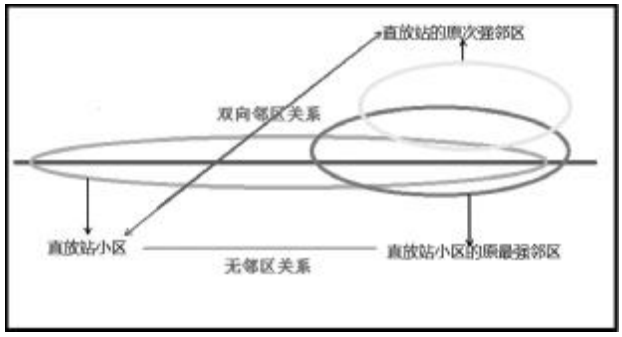


图 2 火车站邻区关系设置示意图

设置邻区关系时必须避免同频同 BISC 的情况,但是直放站专网的覆盖距离过长, 通常是 5-10 公里,很容易疏忽掉那些不加邻区的同频同 BISC 强信号,造成切换到不该去的小区。另外,邻区设置时要注意:所添加邻小区的 BCCH 是否与直放站沿线无邻区关系而物理上又相邻的强信号的 BCCH 相同,如图 3 所示。

图 3 邻区设置示意图

假设直放站小区 A 与公网小区 B 存在重选邻区关系(即 BA1 表内存在),而在 A 小区覆盖范围内存在 C 小区,该小区与 B 小区同频,都为 100,且 C 小区的信号又很强,手机空闲态经过 C 小区附近时发现强信号 100,又发现 BA1 表中存在 100,在达到重选条件的前提下会重选到 C 小区, 这样用户就出了专网。反过来说,公网用户也有可能重选到专网又切不出来,造成专网拥塞和公网用户投诉。因此,专网的邻区关系设置一定要严谨慎重。

而在两端与公网交界处,通过重选、切换参数设置,使手机在从公网向专网段行驶时优先重选、切换到专网即可。

主要参数设置如下:

(1)TA 限制及最大允许时间提前量

(Ms_Max_Range)均设为最大值 63,因为传输线路在铁路两侧绕来绕去,TA 值会变得很大。

(2)由于在设计中制定了列车内手机电平信号强度 -85dBm,因此 ACCMIN 值定为 -95dBm。

(3)专网小区关闭上、下行的功率控制。

(4)开启信令信道切换允许。

以直放站信源高密铁路火车站为例,需要特别注意的参数、邻区设置见表 1。

表 1 直放站信源主要参数、邻区设置

项目	设置
最大时间提前量	63
MS最小接收信号等级	15
上行功率控制允许	否
下行功率控制允许	否
信令信道切换允许	是
次强邻区设置	高密的福广场 1 小区

3.9 频率规划

由于采用直放站方式覆盖,频率规划上存在较大困难。尤其是 900M,频率资源本就较紧张,如今再拿出 3 个频点做长距离覆盖,困难较大。经过分析,最后拿出 96、98 和 100 号频点给直放站使用,同时将铁路沿线频率规划困难区域的 900M 公网站点在保证覆盖的前提下,有选择性地替换为 1800M 设备,这样就解决了频率规划问题。县城城区段直放站由于采用 1800M 进行覆盖, 频率规划较简单, 选取 662、664、666、668 作为信源频点。

4 站点设置

全线共设置 25 个直放站物理点, 平均站间距为 1.3 公里,分为西段(农村)、中段(县城)和东段(农村);每段 1 个信源,东、西段都是 900M 的 3 载波配置,中段是 1800M 的 4 载波配置,如图 4 所示。

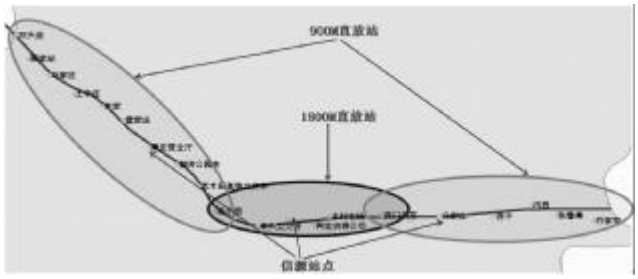


图 4 直放站站点分布图

直放站之间采用并联方式,而不是原先的串联方式,这样即使其中一个直放站出现了故障,也不会影响下面的直放站,如图 5 所示。

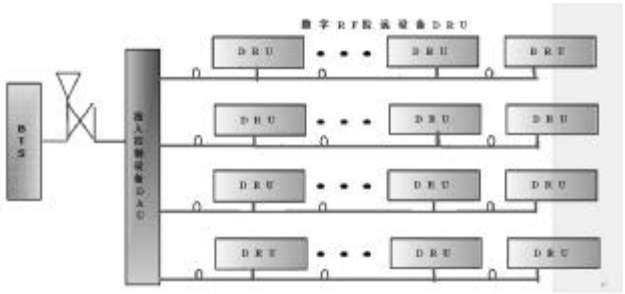


图 5 光纤直放站连接示意图

5 方案效果

方案实施效果较为理想,常规指标都达标。全程切换次数只有 3 次(含两端出入口),掉话为 0。表 2 为高密段原覆盖方式和光纤专网覆盖方式的比较。

表 2 光纤专网实施前、后指标对比

指标	原覆盖方式	光纤专网方式
接通率	90.2%	100%
掉话率	1.8%	0
RxLevelSub>=-80	83.46%	94.9%
切换尝试次数	23	3
单位里程切换请求次数	0.674	0.078
Rxqual>=4	95.15%	97.73%
C/I>=12	94.88%	100%
话音拥塞率	0	0
下载速率	18.6k/s	87.1k/s

通过表 2 可以看出，专网和公网的覆盖基本相当,但是专网的切换次数要远低于公网,因此减少了切换不及时造成的风险,同时专网的话音质量和载干比也高于公网。

6 结束语

通过在胶济客运专线潍坊高密段实施光纤直放站专网覆盖,大大改善了高速铁路覆盖效果,减少了切换和重选次数,测试指标完全达到预期。特别是通过设置“次强邻区”,解决了火车站公网与动车专网的重选、切换问题。同时,1800M 作为直放站信源覆盖动车线也是可行的。高速铁路专网方案是高铁通信保障的首选,本文介绍的光纤专网方式应用对高铁场景网络建设和优化具有较好的参考价值和指导性。

参考文献

1 华为技术有限公司.GSM 无线网络规划与优化,2008

2 高健,罗华斌.直放站的原理与应用.中国无线电,2005(07)

(上接第 31 页)

4 实施效果

拉远基站在移动无线网中将越来越多。新型网络节点出现后,因为设备内部协议的变更、厂商提供附加功能的空白,导致原有的基站动力环境监控实现面临新的课题。某市电信公司在不影响现专业网络原有设备性能、功能的基础上,以很少的投入实现了拉远基站动力环境监控。方案充分考虑了网络演进趋势,为企业创造了可观的维护效益和经济效益。功能测试结果见表 2。

表 2 功能测试对比表

性能	信号	直流 RRU				交流 RRU			
		实测值	监控中心显示值	反应时间	测试结果	实测值	监控中心显示值	反应时间	测试结果
实时参数准确性	交流停电告警	掉电	交流掉电告警	------	合格	掉电	交流掉电告警	------	合格
	电池欠压告警	电池欠压	欠压告警	------	合格	无	无	------	合格
	门禁	门开	门禁告警	------	合格	门开	门禁告警	------	合格
告警传送及时性	停电	------	------	3s	合格	------	------	3s	合格
	门磁	------	------	4s	合格	------	------	3s	合格
设备运行稳定性		测试期间因 RRU 光缆传输原因导致监控系统异常 1 次				测试期间监控系统未发生异常			
告警判断		退服后能判断出停电或光缆断				退服后能判断出停电或光缆断			

(1)增强了网络安全性,提升了网络运行质量,维护管理更加精确化。

通过安装拉远 RRU 基站监控,当基站退服后,能及时、有效地判断退服原因,进而提高派单准确率,大大缩短故障修复时长,明显提升用户感知度。

(2)性价比优势突出,节省投资可观

方案以较少的投入实现了拉远 RRU 基站的动力环境监控(停电、欠压、门禁等),性价比优势突出,节省投资可观;再考虑减少网络调整等维护工作量的因素,其效益更为明显。

(3)可复制性强,具有较高推广价值

方案不仅填补了设备厂商的功能空白,也成为了专业融合的成功案例,为兄弟地市解决此类问题提供了范例。可复制性强,具有较高推广价值。

5 结束语

通过挖掘现网潜力,某市电信公司创新实现了拉远 RRU 基站动力环境监控系统。随着 3G 网络建设、优化的深入,该方案将不断得到丰富、完善。

基于 CDMA 智能手机共享访问企业专网的设计与实现

邢 星 刘志建 刘铁民

(中国电信东营分公司,东营 257000)

摘 要:本文结合 VPDN 技术与智能手机的热点共享功能,用另一种方式为企业实现了多终端的移动办公。详细介绍了组建 VPDN 移动办公专网并通过手机共享的实现过程,分析了该方式的可行性以及为企业带来的经济效益。

关键词:CDMA VPDN 热点共享 移动办公

1 引言

随着信息时代的到来,企业对内部通信的稳定性、便捷性、保密性要求越来越高,企业需要一张内部办公专网。同时,企业对移动办公的需求也日益突显,随时随地访问企业专网势在必行。3G网络为解决“内部专用”和“随时随地”之间的矛盾提供了解决方案,即以 VPDN 方式接入内部专网,即“VPDN 拨号上网”。

另一方面,人们拥有的移动终端种类越来越多。预计到 2020 年,每名企业员工将平均有 6 种移动设备与企业专网相连。这么多终端都通过 VPDN 拨号方式接入专网,每台设备都要支持 3G 插卡,需办理大量 3G 上网卡,企业支出巨大。怎样才能既兼顾多终端使用 VPDN 又尽量节约企业支出呢?答案就是利用智能手机建立 VPDN 连接,然后通过手机自带的热点共享功能共享整个 VPDN 网络,使移动终端都能通过 wifi 网络接入企业专网,即“VPDN 共享上网”。

2 VPDN 组网及手机共享的设计

VPDN 组网示意图如图 1 所示。

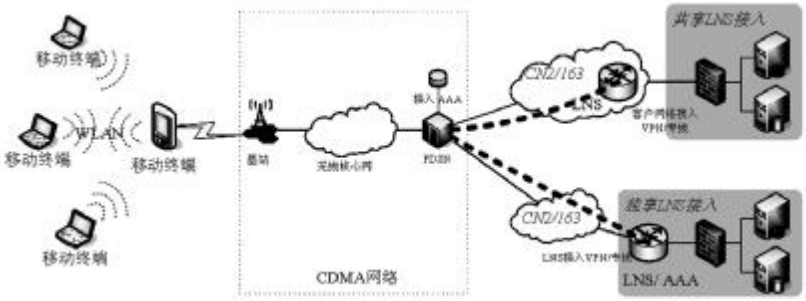


图 1 VPDN 组网示意图

2.1 VPDN 组网

中国电信 CDMA 网络已有成熟的 VPDN 解决方案。通过核心网 PDSN、AAA 与企业 LNS 路由器建立二层隧道连接,CDMA 网络与企业专网之间建立桥梁,用户移动终端通过电信 AAA 认证后直接接入企业专网。

根据企业规模,推荐小型企业使用运营商共享 LNS 路由器,企业不需自建 LNS 路由器,节省企业建设、运营成本;推荐大型企业使用独享 LNS 路由器,企业自建 LNS 路由器并自行维护,拥有 LNS 路由器的全部资源。

2.2 手机拨号及共享

支持新建 APN 的手机终端可以通过新建 APN 方式直接拨入企业内网,拨号成功后会在屏幕顶端显示 3G 连接标志。

新版本的安卓和 iPhone 智能手机都支持热点共享功能。启用热点共享功能后,手机成为 wifi 路由器,周围的笔记本电脑、平板电脑都可以通过 wlan 网络与手机组建无线局域网,共享通过手机接入的企业专网。

有些型号的手机热点共享时,会中断新建的 APN 连接、自动拨入互联网,这与手机的底层系统有关。具体型号需要在使用前测试,以确保用户使用正常。

3 VPDN 组网及手机共享的实现

3.1 VPDN 组网实现

以独享 LNS 接入方式为例,LNS 路由器选用华为 2811 路由器,ETH0/0 作为上联口接入电信互联网,ETH0/1 接入企业专网,在路由器上做如下主要配置:

(1)配置接口地址

```
interface Ethernet0/0
ip address 222.174.*.*  255.255.255.248
interface Ethernet0/1
ip address 192.168.1.1  255.255.255.0
```

(2)配置二层隧道与电信 PDSN 互联

```
l2tp-group 1                          // 隧道设置
// 强制 LNS 与用户端之间重新进行链路控制协议的协商
mandatory-lcp
allow l2tp virtual-template 1 remote SHDLAC
// 隧道密码,与电信 PDSN 端一致
tunnel password simple ******
```

(3)配置 AAA 认证

```
radius scheme VPDN                    // 新建验证方案
// 认证服务器设置 公网接入的为 *.*.*.*
primary authentication *.*.*.* 1645
// 计费服务器设置 公网接入的为 *.*.*.*
primary accounting *.*.*.* 1646
// 认证密码设为 123456
key authentication 123456
// 计费密码,一般和认证密码一样 123456
key accounting 123456
```

(4)配置域名

```
// 域名,vpdn 帐号 @ 后面的部分,不同用户域名不一样
domain dylsyh.vpdn.sd
// 该域所使用的 RADIUS 验证方案
scheme radius-scheme VPDN
// 根据实际情况修改,该地址池用于分给拨号终端
ip pool 1 192.168.2.2 192.168.2.254
```

(5)配置虚模板

```
interface Virtual-Template1
ppp authentication-mode pap
// 虚拟接口,无线终端的网关,根据实际情况修改
ip address 192.168.2.1 255.255.255.0
remote address pool 1
```

(6)配置默认路由

```
ip route-static 0.0.0.0  0.0.0.0  222.174.*.*  preference 60
```

配置完成后,需要与电信 PDSN 侧的二层隧道密码、AAA 密码一致,可以通过 display l2tp session 命令查看二层隧道状态。无论共享或是独享 LNS 接入方式,都需要运营商与企业协商,在企业防火墙上指向 LNS 路由器一段专网 IP 地址, 运营商将这段专网 IP 地址通过 AAA 平台分配给授权拨入专网的移动终端,此时授权接入专网的移动终端就成为企业专网内的一个终端了。

3.2 手机拨号及共享实现

以安卓智能手机为例,配置如图 2 所示。

图 2 APN 设置界面

如图 2 所示,打开手机“设置”,找到“移动网络”,选择“接入点名称(APN)”,进入 APN 设置界面,系统自带 ctnet 和 ctwap 两个 APN,这是正常使用中国电信 CDMA 网络必须的两个 APN, 按菜单键选择“新建 APN”。

图 3 新建 APN

如图 3 所示,在“修改接入点”界面,按照图 3 所示填写必要部分。“名称”和“接入点名称”按自己喜好填写,“用户名”和“密码”按照运营商分配的填写,“PPP 拨叫号码”填写“#777”,按菜单键保存后,出现了新增的 APN—vpdn。这时,可以通过选中该 APN 实现手机直接访问企业专网的目标。

图 4 开启热点共享

如图 4 所示,打开手机“设置”,找到“移动热点”,进入移动热点设置界面, 首先选择 “配置 WLAN 热点”。配置完成后,勾选“便携式 WLAN 热点”。如此操作后,手机即成为无线热点,所有支持 WIFI 的设备均可通过搜索 SSID 为“AndroidAP”的设备连接该企业专网。

4 实际效果测试

经过实际测试,VPDN 共享方式与 VPDN 直拨方式相比,下载速度有一定差距,时延和丢包率较直拨方式差距较大,打开企业内网网页的速度相当,能够支持一般的网络访问。具体对比如表 1 所示。

表 1 网络对比测试

测试项目	VPDN共享上网测试	VPDN直拨上网测试
下载速率	150 Kb/s	195Kb/s
至内网互联地址丢包率	7%	1%
至内网互联地址时延	233ms	98ms

5 优势对比

与传统的终端直接拨号发起 VPDN 连接方式相比,共享 VPDN 方式可以有效节约企业成本。以一个移动商务办公常用场景为例,一名出差人员,配备智能手机、iPad、笔记本电脑三种移动终端,花费对比如表 2 所示。

表 2 费用对比明细

连网设备	VPDN共享上网	VPDN直拨上网
3G智能手机	2000元	2000元
iPad	16GWifi版 3688 元	16GWifi+3G 版 4688 元
笔记本电脑	约 6000 元	笔记本 + 上网卡约 6000+250 元
上网套餐	189 元 / 月	(189 +50+50)元 / 月
合计	11688+189 元 / 月	12938+289 元 / 月
办公成本差距	一次性投入差距 1250 元	月投入差距 100 元

由此可见,使用 VPDN 共享上网方式,在每名员工拥有三个终端的情况下,一次性投入节约 1250 元,个人每月话费节约 100 元,合计一年节约 2450 元。在一家大型企业 500 人配备移动终端的情况下,一年可以节约 120 多万元。

企业可以基于专用 VPDN 网络,开发移动终端的 OA 软件,在 VPDN 企业专网环境下实现简单的手机移动办公,同时可以用手机作为热点,共享整个企业专网给其他移动终端, 从而有效节约企业运营成本,提高移动办公效率。

6 结束语

本文介绍了智能手机共享 VPDN 上网的实现过程,对企业和运营商而言,技术简单、实现门槛低,且经济价值显著。该方案对智能手机的要求较高,除了手机的硬件配置尽可能高之外,还要对备选手机进行测试,因此选择手机时要特别注意。

参考文献

1 敖绮.全面认识 CDMA-VPDN .中国新通信,2006(11)
2 罗建平.浅析 VPDN 技术.中国数据通信,2003(12)
3 高辉,王均.CDMA VPDN IMSI 号认证与 IP 地址绑定解决方案.通信世界 B, 2007(6)

微波通信规划设计探讨

张嘉智[1] 王 奕[2]

(1 山东省邮电规划设计院,济南 250031
2 中国联通济南市分公司,济南 250002)

摘 要:本文介绍了浙江某通信运营商微波通信网络规划设计,总结了微波通信规划设计的步骤及注意事项。

关键词:微波通信 规划 设计

1 引言

浙江某地岛屿众多,地形复杂,光缆网络建设难度很大,而海底光缆建设成本高且周期长。因此,采用微波通信传输无疑是最好的选择之一。

2 浙江某通信运营商微波通信现状及问题

浙江某通信运营商现存微波数量较多,包括汇聚层和接入层。汇聚层微波传输网络目前共有 10 个微波站,7 条微波传输路由,全部为 SDH 方式;接入层网络有 80 个微波站,48 条传输路由, 其中 4 条采用 SDH 方式、44 条采用 PDH 方式。

从微波现状分析,主要存在以下问题:

(1)部分微波划归另一家运营商,对该运营商以后的网络发展会有一定影响。

(2)地方经济发展迅速,通信需求量日渐增大,部分 PDH 微波需进行扩容改造。

(3) 城市建设中存在原路由出现障碍物的情况,造成微波传输信号的极大衰减。

(4)目前微波路由主要以链状形式存在,安全性不高,无法满足业务量大且重要的站点的安全需求。

鉴于上述问题,应对该公司微波网络进行全面规划。

3 微波通信规划

微波通信规划主要包括三部分:路由规划、频率规划和设备选型。

3.1 路由规划

微波通信的路由选择应本着目前和长远需要相结合的原则,做到既符合国家的通信规划,又能满足本地区当前通信任务的实际需要。

(1)由于地面对电波传播的影响,线路应尽量避免跨越水面和平坦的开阔地面,以防强反射造成信号深衰落;

(2)为保证可靠通信,站距不应太长;

(3)每一中继段要有合理的余隙;

(4)应避免越站干扰;

(5)应避免其它微波电路的干扰;

(6)具体站址的考虑还应兼顾投资、施工和维护方便以及运行成本。尽量利用原有地形地物,选择交通方便、供水供电可靠的地方。

3.2 频率规划

在进行频段规划时, 应根据系统传输信道数量、通信网络规划,并结合已建通信线路状况和当地条件

综合考虑。遵循以下原则:

(1)波道频率配置采用集中排列方式;

(2)克服越站干扰,相邻的第四个微波站站址不要选在第一、二两站的延长线上;

(3)一条链路上,高、低站应相间排列,不允许一个站既有高站又有低站的情况存在;

(4)设计频率配置时,优先使用 7/13/15 G 频段;

(5)枢纽站多方向发送时,如果频率有相同的情况,应采用不同的极化方向,以减少干扰。

本案微波频率的分配办法完全符合 ITU-R 和我国有关的频段分配、频道配置的建议、规定,如图 1 所示。

ITU-R频率规划:

频段	4G	L6G	U6G	7G	8G	11G	13G	15G	18G	23G	26G	38G
频率范围	3.6~4.2	5.9~6.4	6.4~7.1	7.1~7.7	7.7~8.5	10.7~11.7	12.7~13.2	14.5~15.3	17.7~19.7	21.1~23.6	24.5~26.5	37.0~39.5

图 1 ITU-R 频率规划

3.3 设备选型

微波网络规划中,设备配置是在路由方案确定之后进行,主要工作内容包括:选定微波工作频段、天线的大小、馈线的长度、分集天线等。

选定微波工作频段:工程方案确定后,站址、微波天线的工作方向也就确定了。在满足前述组网要求的前提下,结合局方要求即可选定微波工作频段。

选定天线的大小:在站址位置、天线高度确定后,在同一个站点,根据传播距离选择适合的天线型号。

选定分集天线:粗略估算电路传输指标后,如果误码率不能满足要求,就要考虑采用分集措施。(实际在做电路配置方案时就应确定,并考虑天线的分集间距。)

4 微波通信勘察

微波通信的勘察的目的,是准确掌握工程现场情况,收集相关信息。

4.1 制定勘察计划

(1)确定勘察范围、目标、日程、参与人员等;

(2)制定勘测行程路线,尽量减少重复行程;

(3) 预先联系所去微波站的管理部门或业主,准备机房开门钥匙等;

(4)如去偏远地区,需联系向导。如微波站附近无住宿设施,勘察当日无法返回、需在机房或野外过夜,要预先购置睡袋、帐篷、药品、食品等。

在确定勘察计划时,一定要与业主达成一致并获得支持,要有业主方的相关人员一起参与勘察,以保证现场勘察数据的准确有效。

4.2 需要准备的工具

(1)GPS 同步卫星定位系统:用于勘测现场定位;

(2)接地电阻测试仪:用于测定新建站(局)点的大地电阻率;

(3)轻便的森林罗盘仪:用于站(局)点至通信方向上的障碍物、目标物和行进方向的定位;

(4)频谱分析仪(可选项):必要时用于确定定位点环境干扰频率和电平测量;

(5)便携式红外线测距仪:用于小范围空间尺寸的测量;

(6)数码相机:记录现场情况;

(7)工程覆盖区域范围的城建规划图,有经纬度的五万分之一或更大的地形地貌图。

4.3 勘察任务

现场勘察工作一般由微波设计人员 1—2 人,建设单位微波设计 1—2 人,相关土建、铁塔、电源、地质等部门设计人员组成。重点完成以下工作:

(1)现场视通情况的确定;

(2)对视通无法确定的传输接力段,如站距过长、现场无法看到对端站,且缺少地图资料或通过读图无法确定视通情况(如城市内传输)的,需组织建设方进行路由电测,或选择备用路由方案;

(3)对于确定无法视通的微波接力段,需重新规划路由,选取中继(有源中继、无源中继)站址,或制定备用路由方案;

(下转第 44 页)

服务质量差距模型在热线满意度提升中的应用

史燕

（中国移动通信集团山东有限公司客服一中心，济南 250022）

摘　要：本文借助服务质量差距模型，结合呼叫中心运营实际，搭建了热线满意度差距模型，借此发现一线与客户、后台与一线及部门之间存在的三大差距，制定针对性措施以提升客户满意度。

关键词：服务质量差距模型　客户满意度　热线满意度提升

1　引言

为实现对客户满意度的实时分析与监控，借助服务质量差距模型，结合呼叫中心运营实际，搭建了热线满意度服务质量差距模型，旨在有效缩小客户感知差距，提升热线满意度。

2　服务质量差距模型理论

服务质量差距模型是一种直接有效的管理工具（图 1），用于指导管理者发现引发质量问题的根源，发现服务提供者与客户在服务观念方面存在的差距。通过制定、实施针对性措施，以提升客户满意度。

图 1 服务质量差距模型

客户感知差距（差距 5）即客户期望与客户感知的服务之间的差距，这是差距模型的核心。客户感知差距主要由公司内部运营的四个差距叠加而成：不了解顾客的期望（差距 1）；未选择正确的服务设计和标准（差距 2）；未按标准提供服务（差距 3）；服务传递与对外承诺不匹配（差距 4）。

3　服务质量差距模型在热线满意度提升中的应用

客户不会明确指出具体差距，也分不清是业务问题、公司问题还是协作问题，只是以结果为导向，表现出“满意”或“不满意”。那么呼叫中心应该如何缩小差距、提升客户满意度呢？借助 5GAP 服务差距模型，结合呼叫中心运营实际，搭建热线满意度服务质量差距模型（图 2），包括热线服务的感知差距、体验差距、交付差距和协作差距等四个关键差距，对症下药，以有效弥补客户感知差距，提升热线服务品质。

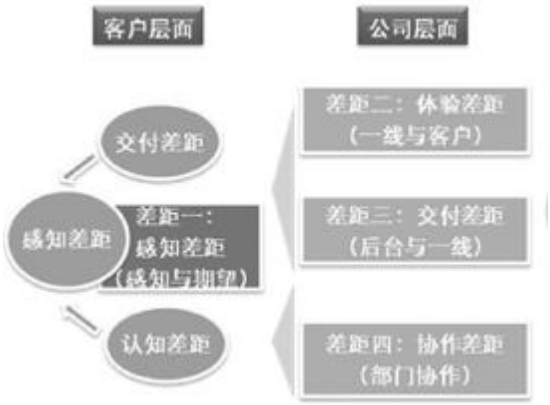


图 2 热线满意度差距模型

3.1 差距 1:感知差距,即顾客期望和管理者感知的差距

客户对热线服务的期望是“又快又好地解决问题”,但客户期望与企业提供的服务感知存在一定差距。鉴于此,实施相应策略以持续缩小差距,提升客户感知。

(1)做好热线客户满意度调查,掌握客户期望

为全面掌握客户满意度情况,定期采取满意度回访、问卷调查、模拟拨测、投诉分析等方式,开展客户满意度调查提升工作。围绕影响客户感知的各要素,提取客户感知数据,搭建热线满意度量化管控体系,进一步定位客户“体验落差”。通过客户感知指标和内部运营指标之间的关联性研究,准确定位客户关注度高、对客户感知影响大的内部运营指标,通过改善内部运营指标以提升客户感知。

(2)持续做好各项服务策略的执行,满足不同客户需求

实现普席与专席之间的无缝衔接,加大对自有专席资源的倾斜力度,优化专席业务范围,不断深化专席一体化运营。在品牌差异化服务方面,重点做好全球通客户、TD 客户的快速接入及服务人员工作能力的提升。加强对特殊客户群服务策略的分析,提高应对的有效性。继续做好夜间服务模式的分析、推进工作,提高服务资源利用率。全面实现忙天 / 忙时简单业务查询办理的自助引导,充分利用 IVR 语音、短信主动推送等方式做好渠道分流宣传。

3.2 差距 2:体验差距,即客户感知和服务质量标准的差距

一线人员对服务规范流程的执行情况和服务技巧,直接影响客户的体验感知,导致出现一线服务传递与客户体验之间的差距。基于此,找出问题根源,实施针对性提升措施。

(1)开展“来电必复”,弥补服务承诺差距

针对多次拨打人工热线未能接通的客户,热线提供留言(预约回复)服务,实施“来电必复”业务流程梳理、系统支撑需求申请及运营跟踪等工作,并设置专岗确保对客户进行 100%回复;对预约回复质量、及时性进行跟踪通报。流程上线以来,预约回复量达到 112.8 万例。针对可能出现的话务突发状况,制定保障方案,成立应急虚拟小组,以确保客户感知。

(2)开展客户关系修复,弥补服务体验差距

组建“客户关怀团队”,制定科学合理的不满意客户追访工作流程;通过数据收集分析,定位服务短板,建立从不满意客户定位—客户深度分析—客户关怀—效果评估的闭环管理流程。

2012 年企业将热线易接通、热线业务办理便捷性、话务人员三个要素确定为服务短板,利用 PDCA 原则开展质量改进工作;遵循 SMART 原则制定改进措施,使改进过程及效果可监控、可测量,保证了改进的有效性。

(3)强化个体差异的改进,弥补服务感知差距

在员工质量改进方面,运用正态分布及长尾理论,重点关注长尾员工,通过案例分析、专题培训、经验分享等形式,提高其综合能力、服务水平。将标杆管理与正向激励相结合,强化标兵示范作用,借助正向行为分析(SPSD)模型,发掘、复制最佳实践经验,及时进行全员推广,促进员工个体差异改进。

3.3 差距 3:交付差距,即服务质量标准和实际提供服务之间的差距

后台能否有效支撑一线做好服务的传递至关重要,支撑不足则导致交付差距。公司业务日趋复杂多样,业务知识、服务技能、系统支撑直接影响客服代表的服务质量和效率。通过加强后台支撑,可有效缩小交付差距。

(1)统一、明确应对口径,确保服务感知一致性

随着业务复杂程度的加深、客户咨询热点的变化,针对夜间服务模式调整、高频专席上线、服务密码验证等关键时刻,后台人员提前梳理应对口径,加强宣贯,并拨测、抽查执行情况,确保前台人员应对方式统一,保证热线服务的一致性。

(2)制定服务流程地图,确保流程执行一致性

根据客户需求适时优化服务流程,建立客户导向的服务流程地图;优化话务预测分析制度、客户投诉预防流程、专席转接规范性等服务流程,确保每个接触点执行统一规范;定期进行流程拨测,确保流程执行的一致性。

(3)创新培训、知识库,确保业务答复一致性

打破传统培训模式,量身定制培训方案,实现薄弱业务、员工的精准定位;广泛征求一线员工意见、建议,以简单易用、快捷查询为原则,对知识库的设计、维护、系统支撑等进行优化,为话务员工作做好业务支撑。

3.4 差距4:协作差距,即实际提供的服务和外部沟通的差距

客户希望"营销宣传清晰、业务使用便捷、资费返还透明、疑难投诉响应"。鉴于此,客服部门与市场部门、业务支撑部门之间要加强协作,前向规避可能影响客户感知的隐患点,后向改进不符合客户期望的问题点。

(1)协同处理话务突增,确保客户问题快速解决

规范话务量突增预警及处理流程,建立涵盖预警目标、预警方式、应急流程、预警信息发布及处理的闭环处理投诉预警机制,按照黄色、橙色、红色、黑色预警四级预警流程,使省、市公司相关部门能够及时了解客户反映的问题,并促进问题的有效解决。

(2)传递"客户之声",确保感知短板快速解决

从"提升现场解决能力,减少地市派单"、"加大电子渠道宣传推广力度, 提高业务办理便捷性感知"两方面入手,加强与省、市公司的协作,从宣传、支撑、服务等角度深入分析服务短板; 针对地市公司业务、营销活动,优化服务口径,保证服务承诺契合服务水平,有效开展对外宣传。

4 结束语

客户满意度管理是一种差值管理,受客户体验值与客户期望值的双重影响,而服务质量差距模型正是解决差距的一种有效管理工具。借助该模型,可以发现公司层面的一线与客户、后台与一线及部门之间存在的三大差距,逐一制定针对性措施,有效提升客户满意度。

(上接第41页)

(4)丈量微波站点室内尺寸,绘制站点机房平面图。确定馈线电缆、电源电缆、接地线的走线方式、所需长度。确定微波设备的安装位置及接口设备的相对位置;

(5)丈量铁塔、机房相对位置,绘制站点平面图。确定新装天线安装塔臂; 确定馈线孔入机房位置;确定现有天线挂高、口径及朝向。确定新装天线可安装位置;

(6)确定各微波站现有电源系统状况;

(7)在新建微波站、铁塔位置设立显著标记,用数码相机拍下周围地形、地貌特征;

(8)记录机房内现有运行微波设备的频段(如果有)。

4.4 微波传输电路电测

在微波通信工程设计中, 电路设计是至关重要的。要获得合理、可靠的电路设计结果,必须准确获得电路设计所需各项参数。由于自然地理条件的复杂性以及电波在实际传播过程中的一些特殊物理现象,微波传输工程的现场勘察设计是微波通信设计的基础。对于城市、居民聚居区等建筑物众多的地区以及在地图上无法确定视通情况的新建微波路由,现场勘察尤为重要, 其目的主要是确认路径能否满足使用要求,是否存在阻挡、损耗等。

5 结束语

微波通信作为光纤通信的补充,在现有通信网络中扮演着不可或缺的角色。虽然近年来由于多种原因,微波通信建设遇到了一定困难,但是凭借自身优势、随着技术的发展,微波通信将始终是通信网络中的一种重要通信手段。

参考文献

1 刘仲明. 微波传输设计一例. 移动通信,1998(6):49-51
2 张旭. 微波路由设计和天线挂高计算的探讨. 信息技术,2007(3):35-36
3 范传立. 微波技术. 北京:电子工业出版社,1994

两种不同的 TD-LTE 初期语音解决方案

1 引言

由于 TD-LTE 采用全 IP 化的网络体系，只有 PS 域可提供高速的数据业务,但对语音业务的支持考虑不足。相比较而言,传统的 TD-SCDMA/GSM 网络已经成熟，可提供高质量的语音业务支持。而且 TD-LTE 的网络建设是一个渐进的过程,为保证语音业务的连续性，需要具备 TD-LTE 与传统 TD-SCDMA/GSM(GPRS)网络间进行业务转换的能力。同时,为保证 TD-LTE 能为大家所认可,TD-LTE 手机提供良好的话音业务就变得非常迫切。有鉴于此,根据终端形态不同,业界提出了两种不同的 TD-LTE 初期语音解决方案:CSFB 方案和双待机方案。无论哪种方案,语音业务均由现有的 2G/3G 网络提供。CSFB 方案以数据业务优先,工作在 TD-LTE 模式,发起语音业务时触发终端转换到 2G/3G 模式工作；双待机方案能够在 TD-LTE 和 2G/3G 网络下同时待机,提供及时的数据和语音业务支持,获得更好的用户体验。

2 单卡多模双待方案技术架构

2.1 终端芯片组成

TD-LTE/TD-SCDMA/GSM(GPRS)多模双待机手持终端是由支持 TD-LTE 的终端芯片，和支持 GSM(GPRS)/TD-SCDMA 的终端芯片共同组成的。其中,支持 GSM(GPRS)/TD-SCDMA 的终端芯片为多模单待终端芯片,同一时间只工作在 GSM(GPRS)模式或 TD-SCDMA 模式，支持 TD-SCDMA HSPA 功能;支持 TD-LTE 的终端芯片既可以是单模芯片,也可以是 TD-LTE 多模芯片,但仅工作在 TD-LTE 模式。

2.2 技术架构及特性

TD-LTE/TD-SCDMA/GSM(GPRS)多模双待手持终端根据业务类型自动选择不同的通信模块:语音业务选择注册 / 建立在 GSM (GPRS)/TD-SCDMA 双模单待模块，数据业务优先选择注册 / 建立在 TD-LTE 模块。若多模双待手持终端离开 TD-LTE 覆盖区,或 TD-LTE 模式无法提供正常数据业务支持,则选择在 GSM(GPRS)/TD-SCDMA 双模单待模块注册 / 建立 / 重建数据业务。

此多模双待终端的(U)SIM 卡与普通单模终端相同,双待的两个模式依据各自的流程操作同一(U)SIM 卡的相应参数区。当两个模式同时操作(U)SIM 卡时,终端控制两个模块顺序操作,以避免冲突。当一个模式操作某参数区时,若该参数区为两个模式共享参数区,终端能够控制一个模式的操作不影响另一模式下的数据。

TD-LTE/TD-SCDMA/GSM(GPRS)多模双待手持终端能够支持 GSM (GPRS)/TD-SCDMA 和 TD-LTE 模式分别独立通信和同时通信。

3 多模双待终端模式选择过程

3.1 开机选网和注册过程

终端开机后,同时启动 TD-SCDMA/GSM(GPRS)

和 TD-LTE 两个模式分别搜索网络。

(1)TD-SCDMA/GSM(GPRS)模式的开机选网和注册流程,与现在的 TD-SCDMA/GSM(GPRS)双模单待终端一致。终端优先选择 TD-SCDMA 网络,若 TD-SCDMA 无法提供服务,按普通双模单待终端流程选择 GSM 网络,正常驻留后,发起 CS 域注册流程,完成后进入 TD-SCDMA/GSM(GPRS)待机状态。

(2)TD-LTE 模式的开机选网流程与单模 TD-LTE 终端搜网机制一致,选择合适的 TD-LTE 小区正常驻留后,发起 PS 域注册流程,完成后进入 TD-LTE 待机状态。

PS 和 CS 域注册完成后,终端在 TD-SCDMA/GSM(GPRS)模式和 TD-LTE 模式同时待机,并分别依据 TD-SCDMA/GSM (GPRS) 双模单待终端和 TD-LTE 终端的技术规范,完成两种模式空闲状态下的移动性管理。

3.2 TD-LTE 丢失覆盖过程

当处于空闲状态的终端离开 TD-LTE 网络覆盖区,或 TD-LTE 网络无法提供正常 PS 域业务支撑时,终端将分组域转移到正在待机的 TD-SCDMA/GSM(GPRS)网络下注册。同时,终端控制 TD-LTE 模式进入慢搜索状态,或在判断 TD-LTE 无网络或异常情况下关闭 TD-LTE 模块。

因多模双待终端两个模式同时工作,耗电比普通单待机终端高,且此时 PS 域业务可以在 TD-SCDMA/GSM(GPRS)上进行,TD-LTE 模式关闭或进入慢搜索状态后,可以利用 TD-SCDMA/GSM(GPRS)模式下获取的 TD-LTE 邻区信息来重新唤醒 TD-LTE 模块进行搜索,这样可以及时发现 LTE 的覆盖区域,同时又能避免在无覆盖区进行无谓的搜索,达到省电和提高服务质量的双重目的。

3.3 终端业务建立过程

终端发起业务时,首先判断该业务属于 CS 还是 PS 域;选择在相应 PS 或 CS 域注册成功的通信模式上发起业务建立。

在双待机或 TD-SCDMA 单待机状态(TD-LTE 丢失覆盖)下,终端支持 CS 和 PS 域业务的并发建立 / 通话过程。在 GSM 单待机状态(TD-LTE/TD-SCDMA 丢失覆盖)下,终端对 CS 和 PS 域并发业务的支持,取决于终端和网络是否支持双传输模式(DTM)。

3.4 终端菜单和人机界面显示

TD-LTE/TD-SCDMA/GSM(GPRS)多模双待手持数字移动终端的菜单中,应包括模式选择菜单和开机默认模式菜单。其中,模式应至少包括多模双待模式,还可包含 TD-LTE 单模模式、TD-SCDMA/GSM(GPRS)双模单待模式等。包含多种模式时,用户可任意选择工作模式并在不同的工作模式间切换。

此类型终端工作在多模双待模式时,会分别显示当前的电路域和分组域的工作模式为何种无线接入技术及对应的信号强度。譬如,PS 在 TD-LTE 模式注册,CS 在 TD-SCDMA 模式注册。待机状态下,界面显示 TD-LTE 模式(L)及其信号强度 RSRP,并指明 PS 域工作在该模式下;同时显示 TD-SCDMA 模式(H)及其信号强度 RSCP,并指明 CS 域工作在该模式下。

4 多模双待终端业务过程

4.1 PS 域数据业务

TD-LTE 正常待机状态下,终端优先选择在 TD-LTE 模式上发起 PS 域数据业务。业务保持过程中,若 TD-LTE 网络覆盖不好或丢失覆盖,数据业务在 TD-LTE 模式上中断,终端应将 PS 域转移到 TD-SCDMA/GSM(GPRS)双模单待模式上注册,成功后在该模式上重建 PS 域数据业务连接。同时,终端控制关闭 TD-LTE 模式或进入慢搜索状态。

TD-SCDMA/GSM (GPRS) 单待机状态(TD-LTE 丢失覆盖或无法提供正常 PS 服务) 下,终端选择在 TD-SCDMA/GSM(GPRS)双模单待模式实现数据业务。业务保持过程中,若 TD-LTE 网络恢复正常覆盖

或服务能力,终端应在现有网络完成业务或根据需要中断该数据业务连接，将 PS 域转移到 TD-LTE 模式上注册,成功后在 TD-LTE 模式上重建连接,恢复该数据业务。

4.2 CS 域语音和短消息业务

因多模双待方案针对的 TD-LTE 网络目前不支持语音业务，所有 CS 域业务只能在 TD-SCDMA/GSM(GPRS)双模单待模式上进行,业务流程及行为同普通双模单待终端。

4.3 CS 域 VP 业务

终端发起 VP 业务时，判断此时 CS 注册的网络模式。若为 TD-SCDMA,则在该模式上发起 VP 业务;若为 GSM 模式,则提示用户不支持该业务。

VP 业务保持过程中,若 TD-SCDMA 覆盖不好、无法支撑 VP 业务，则依据双模单待终端的行为方式,将 VP 业务回退为语音业务继续进行。

5 单卡多模双待技术面临的挑战

在终端技术实施方面，因采用单卡方案,(U)SIM 卡部分与普通单模或双模单待终端相同,并且(U)SIM 卡模块通常都已具备冲突处理机制,可以防止出现两个模式同时访问(U)SIM 的情况。双待机通信模块采用双芯片方案,各模式芯片本身较独立,不涉及主要芯片级的改动。

在网络改造方面,因目前网络系统架构 CS 域和 PS 域工作网元相互独立，能够实现以不同的业务域触发不同模式的待机和工作,不需对网元做复杂的升级或改造。

但此方案终端性能方面的表现,很大程度上依赖于终端的具体实施，主要性能挑战在于以下几个方面:

(1)终端耗电性能

1)双待机状态:两种模式同时与两个网络保持同步,除终端底电流外,两种模式的芯片和射频模块耗电叠加。

2)PS 或 CS 域单业务保持状态:一种模式进入通话状态,另一种模式保持待机,此时待机模块电流相对通话状态可忽略不计,耗电无明显增加。

3)PS 和 CS 域业务并发保持状态:两种模式同时工作与网络保持交互,通话电流为两种模式的叠加。

(2)终端射频性能

1)双待机状态:两种工作模式按照各自的 DRX 周期非连续接收网络下行数据,两种模式在同一时刻接收数据的概率较低,干扰影响基本可忽略。

2)PS 或 CS 域单业务保持状态:一种模式连续接收 / 发送，另一种模式仅非连续接收网络下行数据,干扰影响不明显。

3)PS 和 CS 域业务并发保持状态:两种模式同时接收 / 发送数据,一方的发送会对另一方的接收产生干扰,影响解调性能,从而严重影响 PS 或 CS 的业务质量。尤其是 TD-LTE 模式工作在 2.3GHz,而 TD-SCDMA 模式工作在 2GHz 或 GSM 工作在 800MHz(3 倍频干扰)时,因频段间隔窄,干扰影响不能忽视,需要通过计算和测试验证进行分析。

6 结束语

单卡多模双待机方案结合 TD-LTE 新技术和传统成熟 2G/3G 的网络覆盖优势，在提供高速数据业务的同时，提供高质量的语音业务，能够解决在 TD-LTE 发展初期仅支持 PS 域业务的问题。多模双待终端是 TD-LTE 向全网 IP 发展过程中多样化 TD-LTE 终端形态中的一种,其在业务体验、网络改造和实施、产品可商用时间等方面具有较强的优势。在 TD-LTE 商用部署初期,尽早推动多模双待终端的实施和验证,有利于确保获得满意的用户体验。

——摘自“中国 IC 网”