2026 年朝阳区人口大数据监测（联通手机信令数据）合同

本合同由以下双方根据平等自愿原则，协商一致在北京市朝阳区签订：

甲方：北京市朝阳区数据局

地址：北京市朝阳区日坛北街 33 号

授权代表人：冯峻

邮编：100020

联系电话：65099913

传真：65094287

乙方：中国联合网络通信有限公司北京市分公司

营业执照注册号：911100008016572721

地址：北京市西城区骡马市大街 9 号

负责人：陈海波

联系电话：18611469090

账户名称：中国联合网络通信有限公司北京市分公司

开户银行：中国建设银行北京分行新华支行

公司账号：11001014600053002706

本《2026 年朝阳区人口大数据监测（联通手机信令数据）合同》（以下简称**本合同**）经甲、乙双方友好协商签订，双方达成以下合同内容。

第一条　　服务内容与服务标准

本合同所涵盖的各项服务内容与服务标准详细内容见附件三《单一来源文件技术应答部分》。

第二条　　服务期限

自【2026年9月25日至2027年9月24日】止。本项目成交结果可作为两次合同续签的依据，经采购人同意，且年度资金保障、乙方履约考核合格、服务内容与价格维持原成交标准不变的前提下，甲方与乙方可就新的自然年度续签合同（每次续签合同服务周期不超过12个月，累计续签上限为 2 次）。

第三条　工作检查

甲方有权按本合同第一条约定的服务内容和标准对乙方工作进行工作检查，经甲方工作检查不合格的，甲方有权要求乙方在指定期限内采取弥补措施，乙方采取弥补措施之后再次提交甲方进行检查。经乙方【三】次弥补仍未能经甲方检查合格的，甲方有权单方解除合同，不予支付剩余合同价款。

第四条　合同总价款及结算

1、本合同总价款为人民币【1302000】元（大写:【人民币壹佰叁拾万零贰仟元整】），该费用已包含本合同项下全部费用，包括但不限于税费、人工费、交通费、服务费、保修费等。除此以外，乙方无权要求甲方因本合同支付其他任何费用。

本合同生效后【15】个工作日内甲方支付合同首款【781200】元（大写:【柒拾捌万壹仟贰佰元】），支付中期款，即人民币【260400】元（大写:【贰拾陆万零肆佰元】），剩余合同价款，即人民币【260400】元（大写:【贰拾陆万零肆佰元】），经甲方验收合格后支付。甲方付款前，乙方应向甲方提供合法、有效的税务发票。

2、本项目如根据甲方要求提前终止部分服务内容的，应由甲乙双方协商一致后签署书面补充协议。甲方剩余价款支付金额以乙方提供的实际服务内容和服务时间综合核算结果为准。

第五条　乙方义务

1、乙方需安排专人负责与甲方对接本合同约定的相关工作，确保乙方按时保质完成工作，乙方安排人员未经甲方书面同意，不得随意更换。

2、乙方保证所有项目符合国家标准以及行业标准。

3、乙方严格遵守中华人民共和国法律、法规及合同对有关技术资料及技术的要求。

4、乙方确保其提供的本合同项下的所有服务所涉及的产品、技术、资料不会侵犯第三方的知识产权或所有权，否则由此造成的损失，由乙方承担全部责任。乙方安排人员在甲方服务期间，因故意或过失给甲方造成相应损失的，乙方应承担相应的赔偿责任。

第六条　知识产权

1、乙方保证乙方提供的服务不存在任何侵犯第三方知识产权的情形。如果第三方声称乙方向甲方提供的服务侵犯其知识产权，并已就此对甲方或乙方提起（包括威胁提起或很可能提起）法律诉讼程序或知识产权行政执法程序（简称侵权诉讼），则知悉上述事项的一方应立即通知合同对方，甲方有权：（1）暂停履行对侵权诉讼所涉服务的采购或支付义务直至侵权诉讼完全解决，并要求乙方自担费用向甲方提供与该第三方协商、诉讼、和解所需的一切协助（包括但不限于向甲方提供证明侵权不存在的各类证据、安排人员参加协商、诉讼或会谈等）；（2）甲方有权选择与该第三方达成和解，并由乙方支付和解协议所约定的全部费用以及甲方因侵权诉讼而遭受的全部损失或费用（包括但不限于诉讼/仲裁费、律师费、交通费、通讯费、差旅费、对第三方的损害赔偿金、行政处罚罚款、获取该服务相应使用许可的费用、因停止使用或修改、替换侵权威胁所涉及的服务而遭受的损失等）。如果甲方选择继续参加侵权诉讼法律程序，乙方应当赔偿甲方因侵权诉讼及履行生效法律裁判而需支付的费用或遭受的损失，但生效法律裁判认定乙方服务不存在侵犯第三方知识产权情形的除外。

2、甲方在乙方提供的服务基础上开发、研制形成的技术成果（包括但不限于程序、文件、资料等）的知识产权归甲方所有。

3、不论本合同是否解除或终止，本合同项下第六条独立适用。

第七条　保密义务

1、乙方应对其知晓的甲方的商业、技术、市场、管理、人事、财务

等任何方面的信息和资料予以保密，未经甲方事先书面同意，乙方不得披露、使用或以任何方式处置上述信息、资料，并应促使其员工、关联方承担相同保密义务，如果乙方员工、关联方违反上述保密义务，视为乙方违反保密义务并适用本条第 2 点的约定。

2、乙方违反保密义务的，应当对甲方因此所遭受的损失承担赔偿责任。如果乙方在本合同有效期内违反保密义务，甲方有权单方提前终止本合同。

3、不论本合同是否解除或终止，本合同项下第七条独立适用。

第八条　不可抗力

1、由于发生不可抗力事件（如战争、暴动、严重火灾、水灾、台风、地震、政府行为和禁令等事件），致使合同任一方不能履行合同义务时，遭受不可抗力事件影响的一方负有在不可抗力事件发生之日起 15 日内尽快通知合同对方以减轻可能给对方造成的损失，并应当在合理期限内提供证明。

2、遭受不可抗力事件影响的一方在履行前述义务后免除违约责任，但其合同义务不因此免除。经合同双方协商同意，合同履行时间可合理延长，延长时间相当于因事件发生受到影响的时间。

第九条　违约责任

1、乙方违反本合同约定义务的，甲方有权要求乙方在指定期限内采取弥补措施，乙方未能弥补的，视为乙方违约，乙方应向甲方支付相当于合同总金额【百分之三】的违约金。

2、乙方延期履行的，每延期一日，按合同总金额【千分之三】向甲方支付延期履行违约金。

3、因乙方过错造成甲方或第三方损失的，乙方应赔偿甲方或第三方全部损失。

4、甲方有权直接在未支付的合同总金额中扣除本条约定的违约金及赔偿金，不足部分由乙方补齐。

第十条　争议管辖

本合同项下发生的争议，由双方当事人协商解决；协商不成的，任

何一方均有权向甲方住所地人民法院提起诉讼。

第十一条 本合同自双方法定代表人或授权代表人签字并加盖公章或合同专用章之日起生效。本合同壹式肆份，双方各执贰份，具有同等法律效力。本合同的任何变更、补充或修改，应由双方协商一致并签署书面协议。

第十二条 **通知与送达**

任何一方根据本合同规定向另一方发出的通知应以书面形式作出，并以邮寄/快递、传真、专人送达方式发送。如以邮寄/快递方式发送，以邮寄/快递回执上注明的收件日期为送达日期。如以传真方式发送，收到传真机发出的确认信息后，视为送达。如专人送达，被送达人签署后，视为送达。各方联系信息以本合同首部所列为准，一方联系信息变化后，该方应在联系信息变化之前将变化情况书面通知其他方，否则该方应自行承担相应的风险、责任和后果。

第十三条 本合同中出现的“日”，除非明确写明为工作日，否则为自然日。

第十四条 本合同附件作为本合同内容的一部分，与本合同具有同等法律效力。

第十五条 如甲方因为机构调整变更主体，由变更后的主体继续履行本合同项下的内容。

附件一：《验收标准》

附件二：《合作伙伴廉政协议》

附件三：《单一来源文件技术应答部分》

（本页为签署页）

甲方：北京市朝阳区数据局

（公章）

授权代表人（签字）：

【2026】年【 9 】月【 7 】日

乙方：中国联合网络通信有限公司北京市分公司

（公章）

法定代表人或者授权代表人（签字）：王特

【2026】年【 9 】月【 7 】日

附件一：《验收标准》

一、数据监测范围

本项目人口数据覆盖范围涵盖朝阳区全境、43 个行政街乡、81 个重点区域（项目服务过程中根据实际情况进行调整，重点和个性化区域监测数量不少于 81 个）、50 个重点村、12 个商圈和 24 个旅游景区及临时新增区域。

二、数据验收要求

数据监测指标要求

针对客户实施过程要求，提供监测统计数据服务，数据监测指标包括但不限于以下内容：

1）实时活跃用户数量

2）月度居住用户、工作用户数量及流入流出情况，流入人口来源地及流出人口去向地

3）实时客流量、客流停留时长（商圈、旅游景区）

数据报告指标要求

针对客户实施过程要求，按月提供数据分析报告编写支撑，监测分析指标包括不限于以下内容：

1）统计口径及指标说明

2）朝阳区本月街乡及重点区域居住用户、工作用户分析

3）全区及分街乡居住时段（02 点）和工作时段（14 点）用户数据统计

数据交付时间要求

1）月度人口统计数据按月提供，次月 10 日前提供当月的月度监测相关数据。

2）月度人口分析报告按月提供，次月 15 日前提供当月的月度人口洞察报告。

3）统计数据交付格式为 csv，分析报告交付格式为 word。

数据安全性要求

1）本项目数据服务内容要求的汇总统计及结果数据。

2）通过本地数字传输专线，统计结果以 FTP 格式输出。

附件二：

合作伙伴廉政协议

为共同维护商业活动公平竞争秩序，保证双方在业务交往活动中做到诚信、廉洁、高效和共赢，特订本协议如下：

1、双方在合作过程中，自觉遵守国家法律、法规，按照《中华人民共和国反不正当竞争法》、《中华人民共和国招标投标法》、《关于禁止商业贿赂行为的暂行规定》以及其他相关法律规定开展商业交易活动。

2、在供应商资格预审、投标、开标与评标等过程中，做到公平、公正、公开，禁止暗箱操作。甲方监察部门或其授权人员按照规定对招投标项目实施监督，对于乙方有关招投标的投诉和举报，监察部门认真调查，秉公处理，及时回复。

3、双方相关工作人员及其亲属，不得收受对方馈送的现金、贵重物品、有价证券等，不得要求或接受对方为其住房建修、婚丧嫁娶、出国等提供资助，不得介绍亲友从事与双方合作有关的业务活动，不得收受回扣，不得参加影响公正执行公务的高档娱乐、宴请、健身或旅游活动，不得由对方报销应由本人支付的费用。

4、双方相关工作人员不得为谋取私利私下就材料供应、数量变化、材料质量问题处理等进行私下商谈或者达成默契。

5、不做违反商业道德、扰乱正常竞争秩序、有损双方形象的事情，不围标、串标，不泄露双方机密，不排挤其他经营者的公平竞争，不在预决算、招投标和商务报价中弄虚作假或恶意高估冒算。

6、双方人员发现对方人员有受贿或索贿行为以及徇私舞弊、滥用职权、严重渎职等情况时，有义务向对方监察或相应部门举报。

7、乙方若违反廉政协议将被列入廉政黑名单，甲方将视情节轻重，停止该项目或类似项目的合作，一至三年内不再邀请其投标或比选，不再开展新的业务合作。

8、甲方人员若违反廉政协议，造成公司重大损失或恶劣影响的部门和人员，将按照相关规定进行处理，对于涉嫌犯罪的，按照有关程序移送司法机关。

甲方举报渠道

电话：65099922

乙方举报渠道

电话：84122024

附件三：《单一来源文件技术应答部分》

15 单一来源采购文件要求提供或供应商认为应附的其他材料

15-1 供应商信息采集表

供应商名称	供应商所属性别	外商投资类型
中国联合网络通信有限公司北京市分公司	男	内资

注：1.供应商如为联合体，则应填写联合体各成员信息。

2.供应商所属性别请填写“男”或“女”，指拥有供应商 51%以上绝对所有权的性别；绝对所有权拥有者可以是一个人，也可以是多人合计计算。

3.外商投资类型请填写“外商单独投资”、“外商部分投资”或“内资”。

15-2 技术服务方案

乙方可以根据项目需要，将部分工作内容委托给中国联通专业子公司或具备资质的合作伙伴实施，乙方对中国联通专业子公司及具备资质的合作伙伴向甲方承担连带责任。

1.项目背景

根据《关于贯彻落实《京津冀协同发展规划纲要》的意见》，明确了人口发展目标和加强人口调控的具体要求，要求疏解非首都功能，加强人口数据的动态监测。人口资源环境与首都城市战略地位相协调，让市民的工作和生活更加便利。持续贯彻纲要精神，如何有效摸清人口规模、精确掌握人口流向、及时预警区域人口发展趋势将成为全市人口工作的重点和难点，也凸显了大数据人口动态监测工作的必要性。

《朝阳分区规划(2017 年—2035 年)》指出保持人口规模适度，引导人口合理分布，坚持综合施策、标本兼治、重点突破、以点带面，全面加强人口调控。

朝阳区“十五五”规划明确要求加强人口变化动态研判，强化数字化支撑，持续提升超大城市现代化治理水平。

充分运用手机用户等数据，分析可能存在的人口聚集风险点，及时采取措施加强防范，结合实际认真对比核实。大数据应用更加丰富、人口动态检测更加精细，对社会数据需求大幅增加，需要在原有基础上进一步扩大人口监测的口径和范围，优化人口监测模型，提高人口监测的准确性，提升人口动态监测的精准度。

2.项目总体要求

为落实相关文件及领导指示精神，做好人口动态监测分析工作，大数据应用更加丰富、人口动态监测更加精细，对社会数据需求大幅增加，需要在已有基础上进一步扩大人口监测的指标和范围，提高人口监测的准确性。通过基站与用户间不间断的海量信令信息可以获得每个用户比较准确的实时位置，是描述城市人口数量和空间分布的高效数据。采集手机原始信令数据和手机网络基础数据，利用匿名、聚合、外推的网络数据，进行过滤、分析、计算，经过高度自动化和深度降噪处理，加上多维度的统计分析，可实现对用户的时空准确画像，全面地反映人口的特征与流动分布情况。有效解决传统统计方式时效性不高的问题，大大提高朝阳区人口调控能力。基于大数据的人口动态监测分析将实现朝阳区用户的行为分析，为政府的决策提供科学有效的信息支撑。当前，大数据作为城市发展的新引擎，基于手机通信大数据分析的人口动态监测分析应用，将对朝阳区政府在创新政府服务管理和疏解调整非首都核心功能等方面发挥至关重要的作用。

根据本项目要求我司向北京市朝阳区数据局提供连续 12 个月数据监测和分析服务。具体描述如下。

2.1.业务统计指标

根据采购文件需求，在全域范围内，分别对区、街镇、重点监测区等三个空间单元，以工作用户、居住用户、日活跃用户、瞬时人流量四个指标等进行统计分析。对商圈和景区以实时客流量、客流停留时长、客流日流量三个指标进行统计分析。

为满足项目对数据实时性和准确性的要求，我公司对数据服务性能能够提供的情况如下：

1.实时数据接口传送频率不低于计划内时间，如每 30 分钟一次的接口数据，在本 30 分钟内完成传送。

2. 日度人口统计数据分析结果集在 t+3 日前完成统计。

3. 月度人口统计数据分析结果集能够在次月 10 日前完成统计。

2.1.1.标签画像

将人口、位置、城市通过“场景”联系起来，创建一套场景驱动的人口时空结构与多维画像模型，从年龄、号码归属地、居住用户识别、就业用户识别、职住同地用户识别、居住地、就业地、常住用户等维度对朝阳区人口进行标签画像，本次项目交付所涉及标签内容如下：

（1）居住用户标签

一个月内有 15 天及以上，每天在北京市停留 10 小时及以上的用户中每日 21:00 至次日 07:00 之间停留时长最长的区域为其居住地;所有能找出的符合上述条件且居住地位于属于朝阳区内的用户为“居住用户”。

（2）工作用户标签

一个月内有 15 天及以上，每天在北京市停留 10 小时及以上的用户中工作日每日 7:00 至当日 19:00 之间停留时长最长的区域为其工作地;所有能找出的符合上述条件且工作地属于朝阳区内的用户为“工作用户”。

2.1.2.项目成果物清单-实时数据

根据采购文件需求，每 30 分钟提供数据集一套，包括如下数据指标维度：

序号	监测区域	监测指标	时间粒度	交付物

1	朝阳区、43 个街乡镇、81 个重点区域	实时人流量	30 分钟	每 30 分钟提供数据集一套
2		实时人流量归属地		
3		实时人流量性别		
4		实时人流量年龄		
5		瞬时流入流出		
6		瞬时流入流出归属地		
7		瞬时流入流出性别		
8		瞬时流入流出年龄		
9		瞬时实有进区人群结构（归属地）		
10	朝阳区	实时人口栅格分布		
11	12 个商圈、24 个景区	实时客流量		
12		实时客流量归属地		
13		实时客流量性别		
14		实时客流量年龄		

输出表格样例如下：

表 1：实时人流量/客流量表

sd_date	areaid	sd_total
2026XXXXXX	XXX	XXX
2026XXXXXX	XXX	XXX
2026XXXXXX	XXX	XXX
……	……	……

表 2：实时人流量/客流量归属地表

sd_date	areaid	attrid	sd_total
2026XXXXXX	XXX	XXX	XXX
2026XXXXXX	XXX	XXX	XXX

2026XXXXXX	XXX	XXX	XXX
……	……	……	……

表 3：实时人流量/客流量性别表

sd_date	areaid	gendertype	sd_total
2026XXXXXX	XXX	2	XXX
2026XXXXXX	XXX	1	XXX
2026XXXXXX	XXX	4	XXX
……	……	……	……

表 4：实时人流量/客流量年龄表

sd_date	areaid	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5	sd_total6	sd_total7	sd_total8	sd_total9	sd_total10	sd_total11	sd_total12	sd_total13	sd_total14	sd_total15	sd_total16
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

表 5：瞬时流入流出表

sd_date	areatype	areaid	areaid2	sd_total
2026XXXXXX	in	XXX	XXX	XXX
2026XXXXXX	in	XXX	XXX	XXX
2026XXXXXX	out	XXX	XXX	XXX
……	……	……	……	……

表 6：瞬时流入流出归属地表

sd_date	areatype	areaid	attrid	sd_total
2026XXXXXX	in	XXX	XXX	XXX
2026XXXXXX	in	XXX	XXX	XXX
2026XXXXXX	out	XXX	XXX	XXX
……	……	……	……	……

表 7：瞬时流入流出性别表

sd_date	areatype	areaid	gendertype	sd_total
2026XXXXXX	in	XXX	2	XXX
2026XXXXXX	in	XXX	1	XXX
2026XXXXXX	out	XXX	4	XXX
……	……	……	……	……

表 8：瞬时流入流出年龄表

sd_date	areaty	areai	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5	sd_total6	sd_total7	sd_total8	sd_total9	sd_total10	sd_total11	sd_total12	sd_total13	sd_total14	sd_total15	sd_total16

	pe	d																
2026XXXXXX	in	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXXXX	in	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXXXX	out	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……

表 9：瞬时实有进区人群结构（归属地）表

sd_date	areaid	attrid	sd_total
2026XXXXXX	XXX	XXX	XXX
2026XXXXXX	XXX	XXX	XXX
2026XXXXXX	XXX	XXX	XXX
……	……	……	……

表 10：实时人口栅格数据表

sd_date	areaid	grid_x	grid_y	sd_total
2026XXXXXX	XXX	XXX	XXX	XXX
2026XXXXXX	XXX	XXX	XXX	XXX
2026XXXXXX	XXX	XXX	XXX	XXX
……	……	……	……	……

2.1.3.项目成果物清单要求-日度数据

根据采购文件需求，每日提供数据集一套，包括如下数据指标维度：

序号	监测区域	监测指标	时间粒度	交付物
1	朝阳区、43 个街乡镇、38 个重点区域	天实有进区人群结构（归属地）	日度	每日提供数据集一套
2		14 天实有进区人群结构（归属地）		
3		工作人口		
4		工作人口归属地		
5		工作人口性别		
6		工作人口年龄段分布		
7		居住人口		
8		居住人口归属地		
9		工作用户流入流出明细		
10		居住用户流入流出明细		
11		居住人口性别		
12		居住人口年龄段分布		
13	12 个商圈	客流停留时长		
14		客流来源地		
15		客流日流量		
16		商圈关联分析		
17		客流人群性别		
18		客流人群年龄		
19	24 个景区	游客停留时长		
20		游客日流量		
21		游客归属地		
22		游客性别		
23		游客年龄		

输出表格样例如下：

表 1：日度天实有进区人群结构（归属地）表

sd_date	areaid	location	sd_total
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
……	……	……	……

表 2：日度 14 天实有进区人群结构（归属地）表

sd_date	areaid	location	sd_total
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
……	……	……	……

表 3：日度工作/居住用户表

sd_date	areaid	sd_total
2026XXXX	XXX	XXX
2026XXXX	XXX	XXX
2026XXXX	XXX	XXX
……	……	……

表 4：日度工作/居住用户性别表

sd_date	areaid	gendertype	sd_total
2026XXXX	XXX	2	XXX
2026XXXX	XXX	1	XXX
2026XXXX	XXX	4	XXX
……	……	……	……

表 5：日度工作/居住用户年龄表

sd_date	areaid	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5	sd_total6	sd_total7	sd_total8	sd_total9	sd_total10	sd_total11	sd_total12	sd_total13	sd_total14	sd_total15	sd_total16
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……

表 6：日度工作/居住用户归属地表

sd_date	areaid	attrid	sd_total

2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
……	……	……	……

表 7：日度工作/居住用户流入流出表

sd_date	datatype	areaid	attrid	sd_total
2026XXXX	in	XXX	XXX	XXX
2026XXXX	in	XXX	XXX	XXX
2026XXXX	out	XXX	XXX	XXX
……	……	……	……	……

表 8：客流停留时长表

sd_date	areaid	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……

表 9：客流来源地表

sd_date	areaid	attrid	sd_total
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
……	……	……	……

表 10：客流日流量表

sd_date	areaid	sd_total

2026XXXX	XXX	XXX
2026XXXX	XXX	XXX
2026XXXX	XXX	XXX
……	……	……

表 11：商圈关联分析表

sd_date	areaid	areaid2	sd_total
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
2026XXXX	XXX	XXX	XXX
……	……	……	……

表 12：客流人群性别表

sd_date	areaid	gendertype	sd_total
2026XXXX	XXX	2	XXX
2026XXXX	XXX	1	XXX
2026XXXX	XXX	4	XXX
……	……	……	……

表 13：客流人群年龄表

sd_date	areaid	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5	sd_total6	sd_total7	sd_total8	sd_total9	sd_total10	sd_total11	sd_total12	sd_total13	sd_total14	sd_total15	sd_total16
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
20	X	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX

26XXXX	XX	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
2026XXXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……

2.1.4.项目成果物清单要求-月度数据

根据采购文件需求，每月提供数据集一套，包括如下数据指标维度：

序号	监测区域	监测指标	时间粒度	交付物
1	朝阳区、43 个街乡镇、58 个重点区域	工作用户	月度	每月提供数据集一套
2		工作用户性别		
3		工作用户年龄		
4		工作用户归属地		
5		工作用户流入流出		
6		居住用户		
7		居住用户性别		
8		居住用户年龄		
9		居住用户归属地		
10		居住用户流入流出		
11		职住 OD		
12		通勤半径		
13		通勤时间		
14	12 个商圈	工作用户		
15		工作用户性别		
16		工作用户年龄		

17		工作用户归属地		
18		工作用户流入流出		
19		职住 OD		
20		通勤半径		
21		通勤时间		

输出表格样例如下：

表 1：月度工作/居住用户表

sd_date	areaid	sd_total
2026XX	XXX	XXX
2026XX	XXX	XXX
2026XX	XXX	XXX
……	……	……

表 2：月度工作/居住用户性别表

sd_date	areaid	gendertype	sd_total
2026XX	XXX	2	XXX
2026XX	XXX	1	XXX
2026XX	XXX	4	XXX
……	……	……	……

表 3：月度工作/居住用户年龄表

sd_date	areaid	sd_total1	sd_total2	sd_total3	sd_total4	sd_total5	sd_total6	sd_total7	sd_total8	sd_total9	sd_total10	sd_total11	sd_total12	sd_total13	sd_total14	sd_total15	sd_total16
2026X	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX

X																	
2026XX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……	……

表 4：月度工作/居住用户归属地表

sd_date	areaid	attrid	sd_total
2026XX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX
……	……	……	……

表 5：月度工作/居住用户流入流出表

sd_date	datatype	areaid	attrid	sd_total
2026XX	in	XXX	XXX	XXX
2026XX	in	XXX	XXX	XXX
2026XX	out	XXX	XXX	XXX
……	……	……	……	……

表 6：月度职住 OD 表

sd_date	work_areaid	live_areaid	sd_total

2026XX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX
……	……	……	……

表 7：月度通勤半径表

sd_date	areaid	areaid2	sd_total1	sd_total2	sd_total3	sd_total4
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……

表 8：月度通勤时间表

sd_date	areaid	areaid2	sd_total1	sd_total2	sd_total3	sd_total4
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
2026XX	XXX	XXX	XXX	XXX	XXX	XXX
……	……	……	……	……	……	……

2.2. 数据需求及接口规范要求

根据采购文件需求，按照三网融合平台建设项目的数据需求及技术规范，配合输出提供所需的统计级标准数据，对采集到的人口数据通过模型算法和结果汇总，形成多维度的分析结果。其中，针对 50 个重点村进行的月度居住人口、工作人口监测仅以数据分析报告形式出具。

针对数据融合开展合规处理与质量管控，通过标准化流程完成数据归集、校验、规整及运维监控。

进行数据归集入库：严格规范统计数据接收入库流程，归集人口、客流等数据。进行数据交叉校验：依托汇总数据开展交叉核验，排查修正单网数据偏差、异常及误差问题。进行数据规整对齐：针对数据格式、口径差异开展规整对齐，消除数据输出偏差与格式混乱问题。进行运维监控：对数据处理全流程动态监控，及时排查处置数据缺失、断更等异常情况。

相关数据需求及接口规范描述如下，可根据项目实际情况进行调整：

1. 辖区及定制区域实时活跃用户数量，(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	实时人流量		
统计口径	每 30 分钟间隔步进进行统计，统计在每个区域下的人数		
统计区域	朝阳区、街乡、重点区域		
统计粒度	30 分钟	**输出实效**	延迟 40 分钟内
输出名称	rtarea202311011030.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出

2. 月度居住人口、工作人口数量，(朝阳区、43 街乡、81 个重点区域)；

- 居住人口数据需求：

指标名称	居住人口		
统计口径	用户 21 点-7 点（第二天）在某区域停留时长超过 360 分钟的区域为该用户的日居住地，取一个月内用户停留最多的日居住地为该用户的月居住地，统计月居住地区域下的居住人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthlive202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出

- 工作人口数据需求：

指标名称	工作人口		
统计口径	用户 7 点-19 点在某区域停留超过 480 分钟的区域为该用户的日工作地，取一个月内用户停留最多的日工作地为该用户的月工作地，统计月工作地区域的工作人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthwork202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析结果集，Word 格式电子版

3. 区域及定制区域的 30 分钟流入、流出人口数量，(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	瞬时人口流入流出		
统计口径	用当前加工后的数据集与 30 分钟前的数据集取差集； 1. 当前数据集包含，30 分钟前的数据集不包含的为流入用户，当前数据集中流入用户的所在地为流入区域，统计流入区域的流入用户人数。 2. 当前数据集不包含，30 分钟前的数据集包含的为流出用户，30 分钟前的数据集中流出用户的所在地为流出区域，统计流出区域的流出用户人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	30 分钟	**输出实效**	延迟 40 分钟内
输出名称	inout202311011030.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areatype	流动类型	N

	areaid	区域标识	N
	areaid2	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出

4. 月度职住信息统计：包括工作人口的居住地统计，及月度居住人口的工作地统计，(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	职住 OD		
统计口径	用户 7 点-19 点在某区域停留超过 480 分钟的区域为该用户的日工作地，21 点-7 点（第二天）在某区域停留时长超过 360 分钟的区域为该用户的日居住地。取一个月内用户累计停留最多的日工作地居住地为该用户的月工作居住地，统计不同的月工作地居住地之间的职住人数		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthod202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	work_areaid	工作地标识	N
	live_areaid	居住地标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析结果集，Word 格式电子版

5.月度居住人口流向情况，(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	居住用户流入流出明细
统计口径	用当前月居住用户明细的数据集与上个月的月居住用户明细数据集取差集； 1.当月数据集包含，上月的数据集不包含的为流入居住用户，当月数据集中流入居住用户的所在地为流入区域，统计流入区域的

	流入居住用户人数。 2.当月数据集不包含，上月的数据集包含的为流出居住用户，上月的数据集中流出用户的所在地为流出区域,统计流出区域的流出居住用户人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthliveinout202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	datatype	流入流出类型	N
	live_areaid	居住地标识	N
	attrid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析结果集，Word 格式电子版

6.月度工作人口流向情况，(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	工作用户流入流出明细		
统计口径	用当前月工作用户明细的数据集与上个月的月工作用户明细数据集取差集； 1. 当月数据集包含，上月的数据集不包含的为流入工作用户，当月数据集中流入工作用户的所在地为流入区域，统计流入区域的流入工作用户人数。 2. 当月数据集不包含，上月的数据集包含的为流出工作用户，上月的数据集中流出用户的所在地为流出区域，统计流出区域的流出工作用户人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthworkinout202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	datatype	流入流出类型	N

	work_areaid	工作地标识	N
	attrid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析结果集，Word 格式电子版

7. 居住用户中外来人口比重：按照身份证户籍情况统计分析(朝阳区、43 街乡、81 个重点区域)

- 数据需求：

指标名称	居住人口归属地		
统计口径	用户 21 点-7 点（第二天）在某区域停留时长超过 360 分钟的区域为该用户的日居住地，取一个月内用户停留最多的日居住地为该用户的月居住地，统计月居住地区域下不同号段归属地的居住人数		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthliveattr202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	attrid	归属地标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析报告，Word 格式电子版

8.月度居住用户、工作用户流入流出情况，分析流入人口来源地及流出人口去向地。(朝阳区、43 街乡、81 个重点区域)；

- 数据需求：

指标名称	居住用户流入流出明细
统计口径	用当前月居住用户明细的数据集与上个月的月居住用户明细数据集取差集；1. 当月数据集包含，上月的数据集不包含的为流入居住用户，当月数据集中流入居住用户的所在地为流入区域，统计流入区域的流入居住用户人数。2. 当月数据集不包含，上月

	的数据集包含的为流出居住用户，上月的数据集中流出用户的所在地为流出区域，统计流出区域的流出居住用户人数。		
统计区域	朝阳区、街乡、重点区域		
统计粒度	月	**输出实效**	延迟 10 天内
输出名称	monthliveinout202301.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	datatype	流入流出类型	N
	live_areaid	居住地标识	N
	attrid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式平台输出；数据分析结果集，Word 格式电子版

9.商圈实时客流量(输出 12 个商圈)；

- 数据需求：

指标名称	商圈实时客流量		
统计口径	每 30 分钟间隔步进进行统计，统计在每个商圈区域下的人数		
统计区域	商圈		
统计粒度	30 分钟	**输出实效**	延迟 40 分钟内
输出名称	rtbusiness202311011030.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式

10.商圈客流停留时长(输出 12 个商圈)；

- 数据需求：

指标名称	商圈客流停留时长

统计口径	统计每天在商圈区域不同停留时长的用户人数		
统计区域	商圈		
统计粒度	日	**输出实效**	延迟 4 小时内
输出名称	businessstay20230123.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total1	0-60 分钟统计人数	N
	sd_total2	60-120 分钟统计人数	N
	sd_total3	120-240 分钟统计人数	N
	sd_total4	240-480 分钟统计人数	N
	sd_total5	480 分钟以上统计人数	N

- 输出形式：csv 格式

11.商圈客流日流量(输出 12 个商圈)；

- 数据需求：

指标名称	商圈客流日流量		
统计口径	统计每天在各商圈区域客流的总人数		
统计区域	商圈		
统计粒度	日	**输出实效**	延迟 4 小时内
输出名称	business20230123.csv		
输出结果	**字段名**	**字段释义**	**是否为空**
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式

12.景区实时客流量(输出 24 个旅游景区)；

- 数据需求：

指标名称	景区实时客流量		
统计口径	每 30 分钟间隔步进进行统计，统计在每个景区区域下的人数		
统计区域	景区		
统计粒度	30 分钟	输出实效	延迟 40 分钟内
输出名称	rtly202311011030.csv		
输出结果	字段名	字段释义	是否为空
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

- 输出形式：csv 格式

13.景区游客停留时长(输出 24 个旅游景区)；

- 数据需求：

指标名称	景区游客停留时长		
统计口径	统计每天在景区区域不同停留时长的用户人数		
统计区域	景区		
统计粒度	日	输出实效	延迟 4 小时内
输出名称	dailyLYstay20230123.csv		
输出结果	字段名	字段释义	是否为空
	sd_date	时间	N
	areaid	区域标识	N
	sd_total1	0-60 分钟统计人数	N
	sd_total2	60-120 分钟统计人数	N
	sd_total3	120-240 分钟统计人数	N
	sd_total4	240-480 分钟统计人数	N
	sd_total5	480 分钟以上统计人数	N

- 输出形式：csv 格式

14.景区游客日流量(输出 24 个旅游景区)。

- 数据需求：

指标名称	景区游客日流量		
统计口径	统计每天在各景区区域出现过的游客总人数		
统计区域	景区		
统计粒度	日	输出实效	延迟 4 小时内
输出名称	dailyLY20230123.csv		
输出结果	字段名	字段释义	是否为空
	sd_date	时间	N
	areaid	区域标识	N
	sd_total	统计人数	N

输出形式：csv 格式

2.3. 数据需求结果交付

按照监测指标要求，分小时、日度、月度提供数据分析服务。具体如下：

实现对朝阳区及 43 个街乡镇、81 个重点监测区、12 个商圈、24 个景区人口动态监测及临时新增区域的 4G、5G 用户的实时、日度、月度等时间维度的实时人流量、瞬时流入流出、日度工作/居住用户、日度客流、日度实有进区、月度工作/居住用户，及归属地、性别、年龄、通勤等多维度动态监测，分别每 30 分钟、每日、每月等提交相应数据集。

具体交付数据涵盖如下表格：

实时人流量/客流量表、

实时人流量/客流量归属地表、

实时人流量/客流量性别表、

实时人流量/客流量年龄表、

瞬时流入流出表、

瞬时流入流出归属地表、

瞬时流入流出性别表、

瞬时流入流出年龄表、

瞬时实有进区人群结构（归属地）表、

实时人口栅格数据表、

日度天实有进区人群结构（归属地）表、

日度 14 天实有进区人群结构（归属地）表、

日度工作/居住用户表、

日度工作/居住用户性别表、

日度工作/居住用户年龄表、

日度工作/居住用户归属地表、

日度工作/居住用户流入流出表、

客流停留时长表、

客流来源地表、

客流日流量表、

商圈关联分析表、

客流人群性别表、

客流人群年龄表、

月度工作/居住用户表、

月度工作/居住用户性别表、

月度工作/居住用户年龄表、

月度工作/居住用户归属地表、

月度工作/居住用户流入流出表、

月度职住 OD 表、

月度通勤半径表、

月度通勤时间表。

3.服务内容及技术解决方案

结合本项目要求，我司通过对运营商手机用户数据在朝阳区域内进行连续、大规模抽样采集并结构化，汇总到区指定平台，供相关单位分析朝阳区人口流动、人口结构、人口流动的数量及变化特点等。

为了能够提供满足客户服务内容需求，我司从信令数据采集、处理、建模、沙箱环境搭建，提供整套解决方案。

3.1.数据资源准备服务

我司提供涵盖覆盖朝阳区及43个街乡镇、81个重点监测区、50个重点村、12个商圈、24个景区及临时新增区域的4G、5G用户的网络信令数据结果。按照采购人的要求对数据进行脱敏、清洗、加工、监控，保证数据使用的安全和有效。具体包括以下几个方面：

3.1.1.数据准备

我司建立内部数据标准和机制，协调完成内部的计算、存储资源的准备工作，协调中国联通手机在朝阳区行政区域内的信令数据接入，完成数据融合工作。保障本项目数据供给的完备性与及时性。

信令数据处理计算云平台提供了日报、周报、月报所需的集群环境，持续更新日度用户数据，用于各种维度模型的运算。

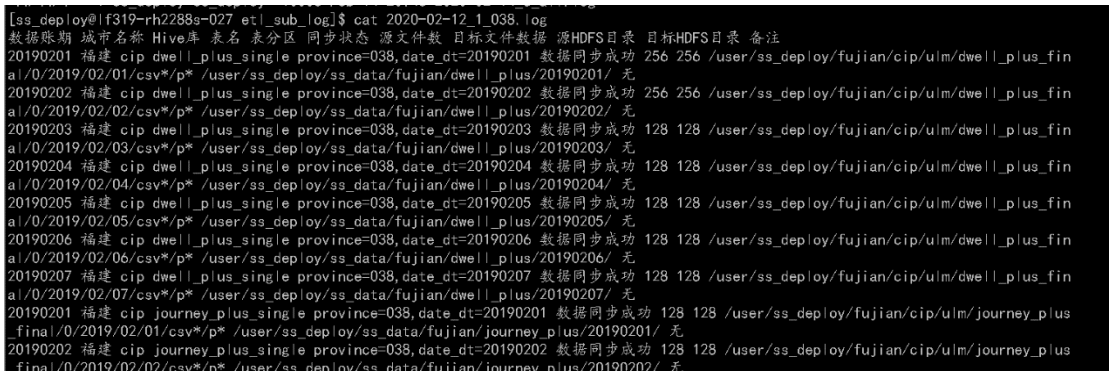
信令数据进行清洗、脱敏、降噪、关联等加工处理和计算后，推送至计算云平台中，这一过程将产生两级日志。

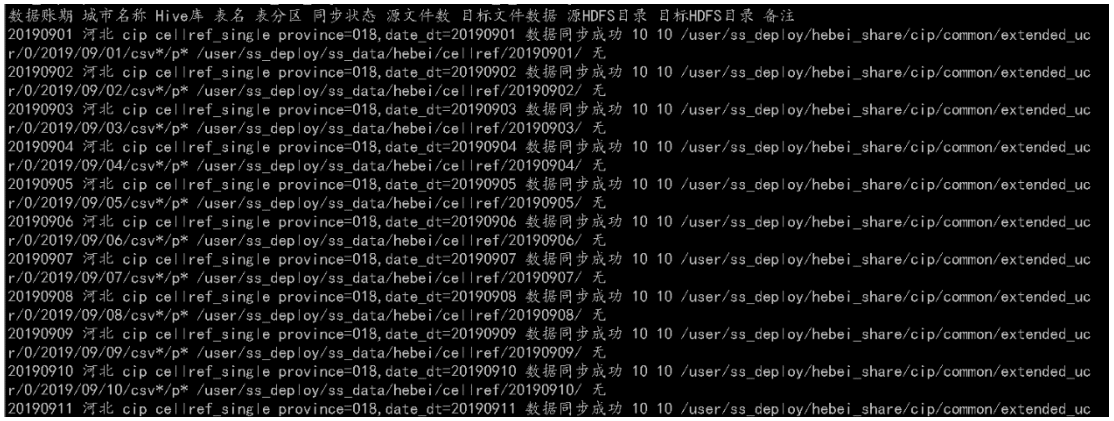
第一级日志数据导入成功截图：

开始时间	结束时间	城市	任务状态	总任务数量	成功任务数量	失败任务数量	ETL开始时间	ETL结束时间	备注
20190101	20190103	内蒙古	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:18:03	无
20190101	20190103	北京	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:18:03	无
20190101	20190103	天津	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:18:02	无
20190101	20190103	山东	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:18:03	无
20190101	20190103	河北	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:17:53	无
20190101	20190103	山西	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:05	无
20190101	20190103	安徽	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:14	无
20190101	20190103	上海	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:25	无
20190101	20190103	江苏	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:18	无
20190101	20190103	浙江	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:16	无
20190101	20190103	福建	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:15	无
20190101	20190103	海南	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:21:05	无
20190101	20190103	广东	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:23:49	无
20190101	20190103	广西	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:24:00	无
20190101	20190103	青海	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:23:53	无
20190101	20190103	湖北	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:23:53	无
20190101	20190103	湖南	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:24:03	无
20190101	20190103	江西	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:24:00	无
20190101	20190103	河南	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:23:59	无
20190101	20190103	西藏	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:26:58	无
20190101	20190103	四川	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:27:06	无
20190101	20190103	重庆	任务成功	3	3	0	2019-11-26_15:51:22	2019-11-26_16:27:12	无

第二级日志，朝阳区及北京市数据导入成功截图：

第二级日志，其他 30 省市数据导入成功截图：





数据导入完成后，大数据分析师将创建的日报、周报、月报模型部署到计算云平台，运行模型，并获取模型运行结果。

3.1.2.数据采集

我司根据北京市朝阳区数据局的数据采集要求，完成相关数据的采集工作。数据能满足北京市朝阳区数据局开展人口流动、人口结构、人口流动的数量及变化特点等业务以及人口定位、监测指标优化等工作。供应商应按照三网融合平台建设项目的数据需求及技术规范，配合输出提供所需的统计级标准数据，对采集到的人口数据通过模型算法和结果汇总，形成

多维度的分析结果。

数据范围主要包括设备对象信息（包含且不限于用户信令数据、用户驻留/出行信息数据、朝阳手机用户漫出数据等）、基站对象信息（包含且不限于工参信息数据等）、特征标签信息（包含且不限于用户标签数据）、其他辅助位置信息（用户上网行为数据等）。

2、3、4、5G 信令数据结果示例如下：


原始数据检查

数据账期：2019-12

CS域数据(2G/3G)　LTE数据(4G)　Cell数据(2G/3G/4G)　Crm数据　市场份额

省份	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
内蒙古(G)	48	49.8	49.6	42	41.3	45.3	49.7	48.4	49.4	48.7	47.8	46.2	49	47.9	47	47	46.7	46.8	46.2	47.1	46	45.1	48.3	51.3	51	51.1	52.7	51.9	50.3	52.1	53.7
北京市(G)	34.1	37.5	37.5	37.9	37.5	37.6	34.9	33.3	36.8	37.5	36.5	37.4	38.5	34.5	33.2	35.8	31.9	33.8	36.7	36.7	33.3	32.4	35.8	35.9	35.6	35.7	36.3	32.9	32.1	35.6	35.7


原始数据检查

数据账期：2019-12

CS域数据(2G/3G)　LTE数据(4G)　Cell数据(2G/3G/4G)　Crm数据　市场份额

省份	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
内蒙古(G)	326.4	331.8	322.2	370.4	375.8	392.7	402.4	401	405.5	396.2	385	362.1	398.1	395.7	375.9	376.6	385	390.5	382.4	397.2	365.3	370	397.3	400	413.9	401.6	409.2	407.2	386.8	399.2	403.9
北京市(G)	407.3	461.1	473.9	472.5	475.4	470.3	445.1	421.2	467.5	477	451	467.3	474.5	438.5	420.8	453	390.4	406.6	470.7	475.8	432.5	418.5	461.3	465.3	455.6	455.1	479.3	438.3	422.7	438	472.5

日度规模数据结果示例如下：

day	district_id	all	fuwu
20191231	110101	920744	826007
20191231	110102	1100296	979962
20191231	110105	3292571	2925379

day	village_id	all	fuwu
20191231	110115012	171243	149392
20191231	110115013	41202	36587
20191231	110101001	147736	134136

日度用户画像结果示例如下：

day	district_id	age_id	all	fuwu
20191231	1.1E+08	13	3084	2986
20191231	1.1E+08	7	4846	4683
20191231	1.1E+08	12	3711	3580

day	district_id	gender_id	all	fuwu
20191231	1.1E+08	3	20285	8211
20191231	1.1E+08	1	29992	29019
20191231	1.1E+08	2	30800	30121

day	district_id	location	all	fuwu
20191231	1.1E+08	410000	553	525
20191231	1.1E+08	640000	63	63
20191231	1.1E+08	520000	107	103

day	district_id	native	all	fuwu
20191231	1.101E+11	110000	6655	4428
20191231	1.101E+11	410000	1688	1616
20191231	1.101E+11	350000	125	105

周度规模数据及画像结果示例如下：

week	district_id	stable_use	live_user	work_user
201952	110101	371838	318294	436807
201952	110102	458402	399652	536717
201952	110105	1878562	1729949	1995695

week	village_id	stable_use	live_user	work_user
201952	1.1E+08	42113	28480	63579
201952	1.1E+08	12489	10620	13437
201952	1.1E+08	12627	11130	13062

周度用户画像结果示例如下：

week	district_id	age_id	all	fuwu	stable	day	night
201952	1.1E+08	14	1341	1257	213	230	198
201952	1.1E+08	9	21804	20935	2670	2962	2300
201952	1.1E+08	14	8212	7804	1879	1867	1726

week	district_id	gender_id	all	fuwu	stable	day	night
201952	1.1E+08	3	17187	7208	1521	1486	1285
201952	1.1E+08	2	133316	127906	12246	19821	9137
201952	1.1E+08	3	29184	5663	1062	1037	885

week	district_id	location	all	fuwu	stable	day	night
201952	1.1E+08	130000	12012	11375	1358	1593	1155
201952	1.1E+08	640000	190	181	35	40	28
201952	1.1E+08	540000	19	17	4	1	3

week	district_id	native	all	fuwu	stable	day	night
201952	1.1E+08	320000	4637	4173	710	750	633
201952	1.1E+08	220000	2590	2474	239	291	193
201952	1.1E+08	120000	2948	2699	235	237	207

月度规模数据结果示例，以稳定、居住、工作数据为例如下：

month	district_id	all_user	stable_user	live_user	work_user
201912	110101	4303740	287832	259543	360689
201912	110106	5376592	905132	879486	814125
201912	110115	4873520	721228	699587	664488

月度用户画像结果示例，以稳定、居住、工作数据为例如下　　：

month	district_id	age_id	all_user	stable_use	live_user	work_user
201912	110101	1	285	15	15	13
201912	110101	2	314	60	53	57
201912	110101	3	1788	221	210	274

month	district_id	gender_id	all_user	stable_use	live_user	work_user
201912	110101	1	2556712	166444	149829	207595
201912	110101	2	1577747	113845	103076	145104
201912	110101	3	169281	7543	6638	7990

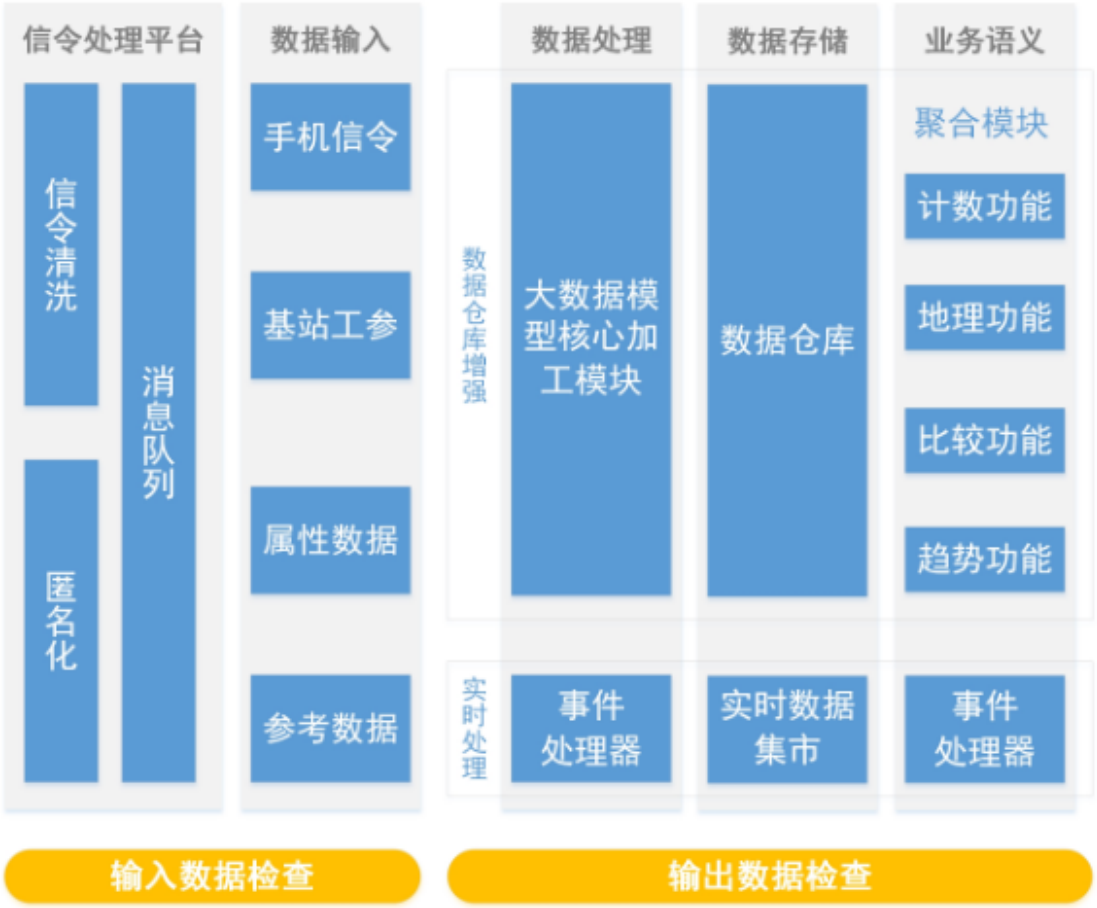
month	district_id	location_id	all_user	stable_use	live_user	work_user
201912	110101	110000	2672802	228243	207464	287754
201912	110101	120000	85325	2566	2091	3443
201912	110101	130000	360334	11013	9431	13557

month	district_id	native_id	all_user	stable_use	live_user	work_user
201912	110101	110000	1044612	112983	105258	129789
201912	110101	120000	66610	3116	2690	4158
201912	110101	130000	689905	33248	28637	45130

3.1.3.数据标准化处理

我司根据北京市朝阳区数据局的要求，对采集的数据进行脱敏、清洗和加工处理，形成格式统一规范的标准化数据。

通过输入数据处理、输出数据梳理对采集的数据进行脱敏、清洗和加工处理，形成格式统一规范的标准化数据（数据脱敏信息包括但不限于手机号码、身份证号码、IMSI、IMEI等）。数据输入处理：主要完成中国联通信令数据的接入、脱敏和清洗，以及不同来源数据（信令数据、基站工参等）之间的数据关联处理工作；输出数据处理：主要基于数据仓库，通过大数据模型处理，将历史信令数据聚合计算为网格化标签数据，以及基于 GIS 数据的路径拟合、基于预测算法的趋势分析等多种数据挖掘分析处理。



3.1.4.数据安全保障

我司建立数据安全保障机制，对软硬件环境、数据传输的各个环节进行监控，确保实施流程的合规和安全；建立风险预警机制，加强网络安全应急保障，防范数据错误和数据泄露的风险。保证数据库和其它文件只能被授权用户和播控终端访问，防止在本地存储或者网络传输的数据受到非法篡改、删除和破坏。应用系统应具有认证功能，以鉴别用户身份并验证。系统应支持访问控制、安全检测、攻击监控等一系列安全功能，应提供完整的网络安全监控、报警和故障处理功能。

传输数据均需要经过安全网关，支持 word 文件、excel 报表、csv 等多类型数据，经安全网关统一输出。并对接口进行审计，保障接口数据输出的安全。及时发现敏感数据泄露风险，在保证数据合理合规交互的同时，进一步加强数据安全的保护。项目实施过程中满足相关数据安全法要求。

3.1.5.数据质量监控

建立长效的数据质量监控机制，制定数据质量管理计划及实施办法，固化常规质量保

障流程，对监控中发现的异常数据以及北京市朝阳区数据局反馈的问题数据要及时进行校验和纠偏，并及时进行数据回补，保证数据质量的可靠。同时应完善人工核查机制，逐步从人工核查向自动化机器核查过渡，保障核查全面性、准确性与及时性。机器核查结合人工核查，保障核查全面性、准确性与及时性。

（1）对于数据稳定性保障要求：我司保障数据采集、清洗、加工、传输、存储全链路稳定，规避底层数据源波动引发的上层监测模型、统计指标异常问题，确保数据服务持续稳定输出。

（2）对于数据质量保障要求：我司确保信令原始数据可靠、统计运算口径统一、数据传入传出无缺失、无偏差。

3.1.6.信令数据情况

信令按其用途分为用户信令和局间信令两类。用户信令作用于用户终端设备(如电话机)和电话局的交换机之间，后者作用于两个用中继线连接的交换机之间。本项目中使用的信令数据是用户信令数据。

手机信令数据主要包括用户 ID，TimeStamp，Longitude，Latitude，EventID 等字段。其中，用户 ID 为手机用户的唯一标识码，能唯一地标识用户；TimeStamp 表示手机信令的发生时间；Longitude 和 Latitude 共同描述手机用户的位置，分别为用户的经度和纬度；EventID 表示事件类型。

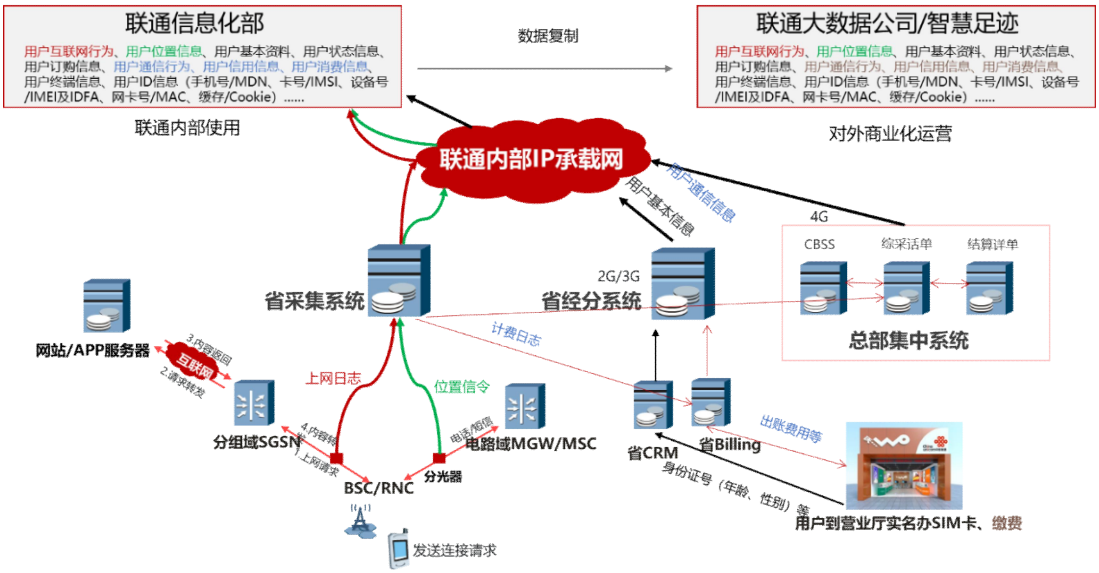
事件类型按照触发手机信令数据的方式对信令数据进行如下区分：主动事件（主叫、被叫，短信、开关机等）和被动事件（位置区切换、定时扫描等）。其划分依据为该信令产生过程是否是手机用户发起的对手机进行操作的主观行为。由于主叫、被叫、短信和开关机动作属于手机用户的对手机发起的主观行为，而位置区切换、定时扫描与手机是通信网络系统根据客户位置变化或定时更新手机用户的位置信息，不需要手机用户对手机进行任何操作。

信令数据与工参数据关联，才能确切的把握用户的时空行为信息，原因在于信令数据中只是记录了用户的 ID，信令事件触发的时间，以及当时用户所使用的基站的编号等等，不对应具体的经纬度，但基站工参信息中，蕴含了基站的编号，以及基站的经纬度信息，相比于信令数据产生的频率，工参数据的更新要缓慢的多，主要在维修、新增等情况下进行更新，工参的信息主要由运营商在设置基站时，通过实测的方式获得。为了减小由于基站工参老旧导致的误差，所搜集的基站参数信息时段应与搜集信令的时段相对应，通过基站编号将信令事件与空间位置经纬度关联起来，最终获得完整可用的记录。

手机信令数据具有采样率高、覆盖面广、置信度高等优点，不仅能反映出行需求空间分布的巨大规模人群的出行产生、出行分布、出行方式分担、出行交通分配，还能对单个出行者的轨迹进行跟踪。

2012 年中国联通已实现全国数据汇总，建立网络体系实时传输全国各地城市基站的信

令数据到总部数据中心集中处理。



各系统数据采集

中国联通集团大数据平台存储容量 85PB，Hadoop 集群的计算能力已近 4500 个节点，平台上集中了全国 4.1 亿多用户数据和 GPS 级的实时位置数据，建立了涵盖 9 大类，共计 3800+个用户标签体系；可轻松识别 4 亿 URL，20 万个互联网产品，约 4200 个手机品牌、10.5 万个终端型号；日处理 5480 亿条上网记录信息，670 亿条位置信息，170 亿条计费详单。每月可支撑内部各种数据查询服务过 6000 万次。

采集以下数据建立模型分析人口总数、分布、流动、迁徙等，服务于政府、商企、金融、交通等行业客户。

1）位置轨迹信令数据：连续、不间断地记录用户每天的位置信息，掌握驻留（居住地、工作地）、兴趣点（Point of Interest，POI）、兴趣路线（Journey of Interest，JOI）、出行方式

等时空特征标签。

2）上网行为日志数据：记录用户手机上网行为信息，通过 URL 分析用户浏览网站兴趣爱好，结合用户使用 APP 类型和频率为用户划分类别，形成偏好标签。

3）基础属性数据：用户基本社会属性（性别、年龄等）、通讯消费套餐资费水平等。

4）手机终端数据：用户持有手机终端的品牌、型号等。

5）第三方合作伙伴数据。

3.1.7.内部去重算法

为使联通手机用户数更好的转化为真实的人口数，制定以下用户去重规则，去重时采用 1—2—3 的顺序漏斗式进行。

3.1.7.1.按照用户属性去重

1、集团客户

集团客户中有约四分之一的用户是集团证件办卡，这部分用户结合实际情况，绝大多数还会有另外一张常用卡，将这部分用户剔除；

2、上网卡

通过查证，上网卡的用户主要都是流量卡，而非正常的用户卡，将这部分用户剔除；

3、终端类型

将无线网卡、无线固话、无线路由器、通信模块以及平板去除；

4、用户状态

将强制停机的用户去除，实际数据中，发现没有这部分用户。

3.1.7.2.按照通话情况去重

结合 1 个月，3 个月，6 个月呼出电话、呼入电话、呼出+呼入电话的情况，阈值暂定为三个月无呼出的用户剔除。

3.1.7.3.按照轨迹去重

轨迹去重目前采用的方案是：同身份证开卡的用户，工作地相同，且居住地相同的用户参与到去重的用户中，具体为：

1、同一个身份证开卡的用户，且职住分离，不去重；

2、同一个身份证开卡的用户，且职住重合，则去重。

轨迹去重的规则是我们通过数据的反复测试，以及对职住分离和职住相同用户其他点位比对得出的优化后的方案。

注：其他备选方案

1、极低用户：比如手机用户在网，且有使用语音，用户实际使用价值小于 52.8 元，且计费时长小于等于 5 分钟，且点对点上行短信小于等于 4 条，且总流量小于等于 3MB；

2、套餐情况，比如主副卡、智慧沃家等套餐。是否作为是家庭内不同用户使用而不参与去重。

3.2. 数据计算服务

我司根据北京市朝阳区数据局的业务要求，基于北京市朝阳区数据局提供的数据标准和计算模型，利用前期提取加工的基础信令数据，提供所需的计算和存储资源，计算并输出相应的人口监测指标。主要包括以下工作：

资源准备：我司提供满足模型计算输出人口监测指标所需的相关计算资源和存储资源；

数据计算：按照北京市朝阳区数据局根据人口监测模型和优化策略确定的计算模型，定期计算输出监测指标数据，符合人口规模、人口结构、人口流向、职住通勤等人口动态监测指标要求。此外，还应根据北京市朝阳区数据局的业务需求，适时开展各类专题人口监测的相关数据处理与计算工作。相关数据应能精准映射到网格，具备提供网格数据的能力。同时，针对客户临时性的个性化专题需求，对重点节假日等个性需求提供人口监测分析支撑，为人口调控提供支撑。

（1） 月度人口规模相关数据服务

我司根据北京市朝阳区数据局的数据要求，按照不同的监测周期，定期提供朝阳全区、街道（乡镇）、重点监测地区、重点村及临时新增区域的各类用户规模数据，包括且不限于:居住用户、工作用户、流动用户、实时用户等，并需配合采购人，根据业务工作开展的成熟情况，择机开展新增监测工作需求，并同步提供相关的数据计算结果。

（2） 人口流向相关数据服务

我司按月定期对朝阳全区、街道（乡镇）、重点村的工作用户、居住用户的流入、流出情况进行计算，并提供进入用户来源地、离开用户去向地分布情况应细化到地级市。

（3） 人口职住通勤相关数据服务

我司按月定期对全市、各区、各街道（乡镇）之间的职住通勤情况进行计算，提供各监测区域，工作用户、居住用户的职住通勤 OD 矩阵等相应的监测结果数据分析服务。

（4） 人口结构相关数据服务

我司针对人口流向等，附加用户特征数据，按月定期对区、街道（乡镇）、重点监测地区、重点村等的人口结构（例如流入用户来源地等）特征进行监测计算，并提供相关人口结构特征等结果数据分析服务。

3.2.1.基础数据配套服务能力

a.用户日度驻留位置数据分析服务

序号	字段	说明
1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	stime	驻留开始时间（通过信令和工参加工生成的用户驻留开始时间，格式为 TimeStamp）
3	etime	驻留结束时间（通过信令和工参加工生成的用户驻留结束时间，格式为 TimeStamp）
4	grid_id	位置网格编号（通过信令和工参加工生成的用户驻留位置）
5	poi_id	驻留位置编号（用户月度所有驻留位置的唯一标识）
6	ptype	位置驻留类型（用户月度驻留信息判断的驻留类型）
7	zone_id	驻留位置所在行政区，如朝阳区
8	is_core	是否核心用户（根据用户月度出现是否超过 10 天定义）
9	province	所属省份
10	city	所属城市
11	date	所属日期

b.用户月度驻留位置数据分析服务

序号	字段	说明
1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	poi_id	驻留位置编号（用户月度所有驻留位置的唯一标识）
3	ptype	位置驻留类型（用户月度驻留信息判断的驻留类型）
4	final_grid_id	位置网格编号（通过信令和工参加工生成的用户驻留位置）

5	stay_fre	月度驻留频次
6	weighted_centroid_lat	月度驻留信息通过多基站加权算法输出的用户位置纬度
7	weighted_centroid_lon	月度驻留信息通过多基站加权算法输出的用户位置经度
8	weekday_day_time	用户在该位置月度工作日白天总驻留时长
9	weekday_eve_time	用户在该位置月度工作日夜晚总驻留时长
10	weekend_day_time	用户在该位置月度周末白天总驻留时长
11	weekend_eve_time	用户在该位置月度周末夜晚总驻留时长
12	zone_id	驻留位置所在行政区，如朝阳区
13	is_core	是否核心用户（根据用户月度出现是否超过 10 天定义）
14	province	所属省份
15	city	所属城市
16	date	所属月份

c.用户日度出行数据分析服务

序号	字段	说明
1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	move_id	当日出行编号（用户当日所有出行的唯一标识）
3	stime	出现开始时间（通过信令和工参加工生成的用户驻留开始时间，格式为 TimeStamp）
4	etime	出行结束时间（通过信令和工参加工生成的用户驻留结束时间，格式为 TimeStamp）
5	mode	出行方式
6	start_grid_id	出行起始位置网格编号
7	end_grid_id	出现终止位置网格编号
8	distance	出行直线距离（米）
9	speed	出行平均速度（km/h）
10	time	出现总时长（秒）

11	moi_id	月度出行编号（用户当月所有出行的唯一标识）
12	is_core	是否核心用户（根据用户月度出现是否超过 10 天定义）
13	start_zone	起点所属区县
14	end_zone	终点所属区县
15	start_ptype	起点驻留类型
16	end_ptype	终点驻留类型
17	province	所属省份
18	city	所属城市
19	date	所属日期

d.用户月度出行路径数据分析服务

序号	字段	说明
1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	moi_id	月度出行编号（用户当月所有出行的唯一标识）
3	route_id	路径标识（用户该次出行的路径类型标识）
4	rn_seq	路径节点顺序（用户该次出行经过道路路网节点的顺序）
5	rn_id	路径节点编号（用户该次出行经过道路路网节点的编号）
6	time	经过相离两个节点的时间
7	is_end	是否为该次出现的终点
8	mode	交通方式
9	is_high	是否重要的道路节点（决定方向）
10	next_rn_id	下一个路径节点编号
11	province	所属省份
12	city	所属城市
13	date	所属月份

e.用户基础属性表

序号	字段	说明

1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	gender	性别
3	age	年龄
4	arpu	月通讯费用
5	area	归属地
6	brand	手机品牌
7	type	手机型号
8	weight	权重
9	gw	性别权重
10	province	省份
11	is_core	是否核心用户（本省 10 天）
12	is_local	是否本地用户（home 在本城市）
13	home_district	用户居住地（通过长期观察在全国夜间最常驻留）
14	work_district	用户工作地（通过长期观察在全国工作日白天最常驻留）
15	home_lon	home 经度
16	home_lat	home 纬度
17	work_lon	work 精度
18	work_lat	work 纬度
19	id_area	身份证号前 6 位
20	flux_all	月使用总流量（MB）
21	city	所属城市
22	date	所属月份

f.用户通话数据表

序号	字段	说明
1	uid	用户标识（采用 IMSI 脱敏加密生成）
2	incall	呼入电话数

3	outcall	呼出电话数
4	brand	所属月份

3.2.2.月度人口规模相关数据服务方案

我司根据北京市朝阳区数据局的数据要求，按照不同的监测周期，定期提供朝阳全区、街道（乡镇）、重点监测地区、重点村及临时新增区域的各类用户规模数据，包括且不限于:居住用户、工作用户、流动用户、实时用户等，并需配合采购人，根据业务工作开展的成熟情况，择机开展新增监测工作需求，并同步提供相关的数据计算结果。

3.2.2.1.人口规模统计口径

客户提供朝阳区、各街乡镇、重点监测地区及重点村域边界，经过与客户业务需求确认提供的人口规模统计口径：

日监测用户	用户口径定义
全用户	监测区域内，当月至少捕捉到一条信令位置的用户，去重后汇总计算得到全用户
服务用户	在全用户基础上剔除非自然人用户

周监测用户	用户口径定义
全用户	监测区域内，当月至少捕捉到一条信令位置的用户，去重后汇总计算得到全用户
服务用户	在全用户基础上剔除非自然人用户
白天用户	一周内累计 4 天及以上，每天在京停留 10 小时及以上的用户（ 每日 7:00 至当日 19:00 之间停留时长最长的区域为日工作地，周居住地选取 4 天及以上的区域）
夜晚用户	一周内累计 4 天及以上，每天在京停留 10 小时及以上的用户（ 每日 21:00 至次日 07:00 之间停留时长最长的区域为日居住地，周居住地选取 4 天及以上的区域）
稳定用户	月稳定用户：一个月内累计 15 个自然日（2 月份取 14 个自然日）及以上，每天在北京停留时间≥10 小时，用户在某个区域累计停留时长最长且天数最多，则为该区域的稳定用户。

	周稳定用户：一周内累计 4 天及以上，每天在京停留 10 小时及以上的用户 （当周停留最长时的区域为监测区域）

月监测用户	用户口径定义
全用户	监测区域内，当月至少捕捉到一条信令位置的用户，去重后汇总计算得到全用户
服务用户	在全用户基础上剔除非自然人用户
稳定用户	月稳定用户：一个月内累计 15 个自然日（2 月份取 14 个自然日）及以上，每天在北京停留时间≥10 小时，用户在某个区域累计停留时长最长且天数最多，则为该区域的稳定用户。 周稳定用户：一周内累计 4 天及以上，每天在京停留 10 小时及以上的用户 （当周停留最长时的区域为监测区域）
工作用户	一个月内累计 15 个自然日（二月份取 14 个自然日）及以上，每天在北京停留时间大于等于 10 小时，用户在某个区域累计 10 个工作日及以上，每日 7:00 至当日 19:00 之间停留时长最长且天数最多，则为该区域的工作用户
居住用户	一个月内累计 15 个自然日（二月份取 14 个自然日）及以上，每天在北京停留时间大于等于 10 小时，用户在某个区域累计居住天数为当月一半及以上，每日 19:00 至次日 7:00 之间停留时长最长且天数最多，则为该区域的居住用户
工作用户迁徙	监测区域上月工作用户，在本月迁徙的工作地去向矩阵上月工作用户本月最后 16 天及以上连续没有信令为本月离京工作用户，上月前 16 天及以上连续没有信令本月为工作用户的为本月进京工作用户
居住用户迁徙	监测区域上月居住用户，在本月迁徙的居住地去向矩阵上月居住用户本月最后 16 天及以上连续没有信令为本月离京居住用户，上月前 16 天及以上连续没有信令本月为居住用户的为本月进京居住用户
暂住用户	监测区域的服务用户中，排除掉稳定、居住、工作用户后，存在单次驻留超过 1 小时及以上的用户
过境用户	监测区域的服务用户中，排除掉稳定、居住、工作用户后，不存在单次驻留超过 1 小时及以上的用户

流动工作用户	一个月内，通过业务模型计算得到的北京市工作用户，但不属于任何一个街乡镇的工作用户
流动居住用户	一个月内，通过业务模型计算得到的北京市居住用户，但不属于任何一个街乡镇的居住用户
职住重合用户	一个月内，通过业务模型计算得到的特定区域居住用户且是该区域的工作用户。
职住不重合用户	一个月内，通过业务模型计算得到的特定区域居住用户但不是该区域的工作用户，或者特定区域工作用户但不是该区域居住用户。
职住矩阵	当月居住用户和当月工作用户的职住矩阵
京外居住京内工作通勤用户	一个月内，通过业务模型计算得到的北京市工作用户但不是北京市的居住用户。即：当月工作用户中，累计 10 个工作日及以上， 每天 21 点至次日 7 点，信令连续消失 6 小时以上，且消失前最后一次信令出现在北京边界（京界线 2 公里以内的区域）的用户
京内居住京外工作通勤用户	一个月内，通过业务模型计算得到的北京市居住用户但不是北京市的工作用户。即：当月居住用户中，累计 10 个工作日及以上，每天 7 点至 19 点，信令连续消失 6 小时以上，且消失前最后一次信令出现在北京边界（京界线 2 公里以内的区域）的用户
长期工作用户	通过一个月的业务模型计算得到的特点区域工作用户中，近 9 个月中有半年以上在北京是工作用户。
长期居住用户	通过一个月的业务模型计算得到的特定区域居住用户中，近 9 个月中有半年以上在北京是居住用户。
旅游用户	一个月内，旅游区域内的服务用户中，排除掉稳定、居住、工作用户后，存在单次驻留超过 1 小时及以上的用户
就医用户	一个月内，医疗区域内的服务用户中，排除掉稳定、居住、工作用户后，存在单次驻留超过 1 小时及以上的用户

3.2.2.2.样例数据

我司在日监测的基础之上，对当月不同用户的日监测情况进行累计计算，以满足北京市朝阳区数据局按月分析归纳朝阳区、各街道（乡镇）、重点监测地区的稳定用户、居住用

户、工作用户(职住不重合)、职住重合用户、流动用户、过境用户规模等数据的需求。

设计月度街道粒度规模数据 SQL 代码：

```
--全用户结果
drop table wangcl_bjfgw_jd_201907_huoyue;
CREATE TABLE IF NOT EXISTS wangcl_bjfgw_jd_201907_huoyue
ROW FORMAT DELIMITED fields terminated BY '|' Lines terminated by '\n' null defined as '
AS
select
      s.qx_name,s.jd_name,s.qx_code,s.jd_code,count(distinct s.user_id) as pop
from
      wangcl_bjfgw_jd_201907_poi s
group by
      s.qx_name,s.jd_name,s.qx_code,s.jd_code;
```

样例数据示例：

2020 年 1 月街道稳定、工作、居住用户规模统计

month	village_id	all_user	stable_user	live_user	work_user
202001	110108001	961318	59853	54847	60438
202001	110105004	820132	19202	17356	31750
202001	110105034	502719	48085	44060	37915
202001	110108022	639045	32012	27348	72356
202001	110108030	179452	21163	19475	15221
202001	110118109	28567	2107	1845	1864
202001	110108024	313169	21342	19078	25872
202001	110101001	1551525	22436	18105	43332
202001	110101006	157483	9132	8326	12017
202001	110105039	352505	46488	43550	34052
202001	110114007	215035	29648	28143	16470
202001	110105043	380182	23584	21516	30649
202001	110101009	521148	19942	17946	29591
202001	110101013	289226	19380	18050	18137
202001	110109003	41641	5531	5142	4271

202001	110118113	16444	2332	2112	1939
202001	110106007	598966	60942	57067	47787
202001	110105030	316451	29547	27715	24814
202001	110111005	43325	5388	4967	5188
202001	110106006	128509	11615	10483	13688
202001	110117101	91760	6530	5983	5405
202001	110112001	440521	18471	16762	15226
202001	110108011	668344	41635	36741	68515
202001	110106009	621605	55031	50816	47259

此外，针对景区、商圈等重点监测地区，依据北京市朝阳区数据局具体监测需求，开展旅游用户、就医用户监测工作。客户提供景区、商圈等重点监测区域范围边界。我司根据所在范围进行区域内人口监测。

2020 年 1 月街道之间通勤用户统计：

month	live_village_id	work_village_id	commute_user
202001	110101001	110101002	44
202001	110101001	110101005	51
202001	110101001	110101008	98
202001	110101001	110101011	16
202001	110101001	110101014	15
202001	110101001	110101017	11
202001	110101001	110102001	29
202001	110101001	110102007	47
202001	110101001	110102010	22
202001	110101001	110102013	11
202001	110101001	110102016	7

202001	110101001	110102019	17
202001	110101001	110105001	93
202001	110101001	110105004	48
202001	110101001	110105007	15
202001	110101001	110105010	15
202001	110101001	110105013	6
202001	110101001	110105016	21
202001	110101001	110105019	6
202001	110101001	110105022	33
202001	110101001	110105025	20
202001	110101001	110105028	15
202001	110101001	110105031	21

2020 年 1 月街道流动用户统计：

month	outflow_village_id	inflow_village_id	live_user	work_user
202001	110101001	110101001	11056	30206
202001	110101001	110101002	185	267
202001	110101001	110101003	3	28
202001	110101001	110101004	5	15
202001	110101001	110101005	16	58
202001	110101001	110101006	12	31
202001	110101001	110101007	232	342
202001	110101001	110101008	260	561
202001	110101001	110101009	12	28
202001	110101001	110101010	4	59
202001	110101001	110101011	59	91

202001	110101001	110101012	56	140
202001	110101001	110101013	25	61
202001	110101001	110101014	11	34
202001	110101001	110101015	7	36
202001	110101001	110101016	12	33
202001	110101001	110101017	4	30
202001	110101001	110102001	53	136
202001	110101001	110102003	1	30
202001	110101001	110102007	7	42
202001	110101001	110102009	6	39
202001	110101001	110102010	1	17

3.2.3.人口流向相关数据服务方案

我司按月定期对朝阳全区、街道（乡镇）、重点村的工作用户、居住用户的流入、流出情况进行计算，并提供进入用户来源地、离开用户去向地分布情况。

设计人口流向数据 SQL 代码例：

```
--街道与街道迁徙
--居住迁徙
drop table wangcl_bjfgw_jd_201907_homeod;
CREATE TABLE IF NOT EXISTS wangcl_bjfgw_jd_201907_homeod
ROW FORMAT DELIMITED fields terminated BY '|' Lines terminated by '\n' null defined as '
AS
select
      t.user_id,t.jd_code as inflow_village_id,s.jd_code as outflow_village_id
from
      wangcl_bjfgw_jd_201907_night2 t
inner join
      wangcl_bjfgw_jd_201906_night2 s
on
      s.user_id = t.user_id;
```

3.2.4.人口职住通勤相关数据服务方案

我司按月定期对全区、各街道（乡镇）之间的职住通勤情况进行计算，提供各监测区域，工作用户、居住用户的职住通勤 OD 矩阵等相应的监测结果数据。

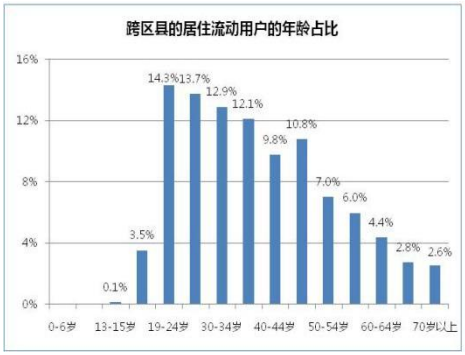
设计人口职住通勤数据 SQL 代码：

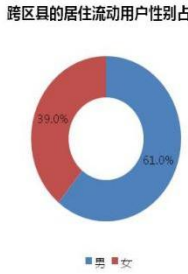
```
--街道与街道通勤
drop table wangcl_bjfgw_jd_201907_zzod;
CREATE TABLE IF NOT EXISTS wangcl_bjfgw_jd_201907_zzod
ROW FORMAT DELIMITED fields terminated BY '|' Lines terminated by '\n' null defined as ''
AS
select
      t.user_id,t.jd_code as live_village_id,s.jd_code as work_village_id
from
      wangcl_bjfgw_jd_201907_night2 t
inner join
      wangcl_bjfgw_jd_201907_day2 s
on
      s.user_id = t.user_id;
```

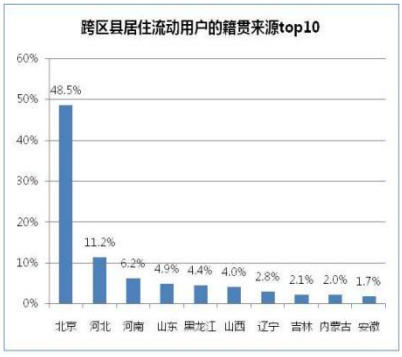
3.2.5.人口结构相关数据服务方案

我司针对人口流向等，附加用户特征数据，按月定期对区、街道（乡镇）、重点监测地区、重点村等的人口结构（例如流入用户来源地等）特征进行监测计算，并提供相关人口结构特征等结果数据。以样例数据进行说明：

通过对样例数据进行分析，跨区县的居住地变迁用户的年龄主要集中在 19-49 岁，其中 19-29 岁的占比约 28%；男性占比 61.0%；居住用户籍贯地为北京的占比 48.5%，其他较高的为河北、河南、山东、黑龙江、山西。

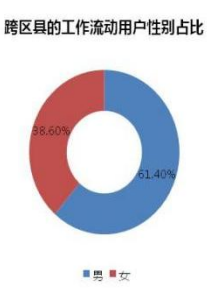






通过对样例数据进行分析，跨区县的工作流动用户的年龄主要集中在 19-49 岁，其中 19-23 岁的占比超过半数；男性占比 61.4%;工作用户籍贯地为北京的占比 45.1%，其他较高的为河北、河南、山东、黑龙江、山西。

流动人口画像分析-工作用户



3. 3. 项目实施保障及交付方案

3.3.1.基础保障能力介绍

➢全国网络链路

中国联通作为全程全网全业务的电信运营商，拥有覆盖全国的骨干光缆资源和本地通信资源，截至 2018 年 7 月全国光缆总长度 8,621,398 皮长公里，其中一级干线光缆长度 170,291 皮长公里，二级干线光缆长度 196,762 皮长公里，本地中继光缆长度 3,186,668 皮长公里，接入网长度 5,067,677 皮长公里。

中国联通拥有原网通、原联通两张覆盖全国的一干光缆网。下图为中国联通一级干线光缆示意图，对于图中涉及的所有光缆资源，中国联通都拥有全部或其中的部分产权。

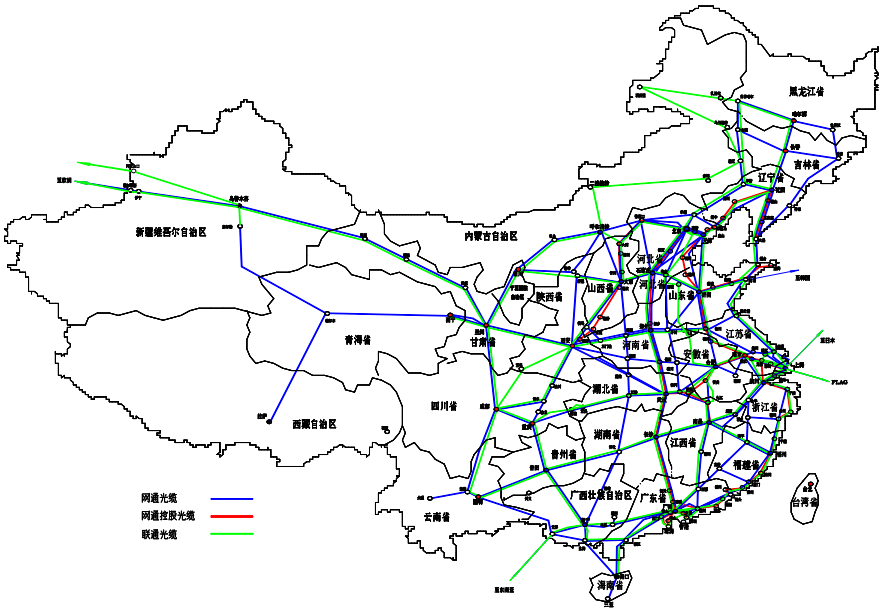


图 中国联通骨干光缆干线示意图

表 中国联通光缆长度

	全国光缆总长度	骨干网光缆长度
皮长公里	8,621,398	367053

➢北京网络资源

北京联通现有核心节点 22 个。各核心节点出局光缆路由均大于等于 3，共计 162 条，平均芯数 208 芯，共计 1708 公里，折合 33.75 万芯公里。单节点平均纤芯数为 3055、平均纤芯利用率为 48.57%。

北京联通现有汇聚节点 149 个。各汇聚节点出局光缆路由均大于等于 2，共计 1040 条，平均芯数 145 芯，共计 9432 公里，折合 121.81 万芯公里。单节点平均纤芯数为 2226、平均纤芯利用率为 47.83%。

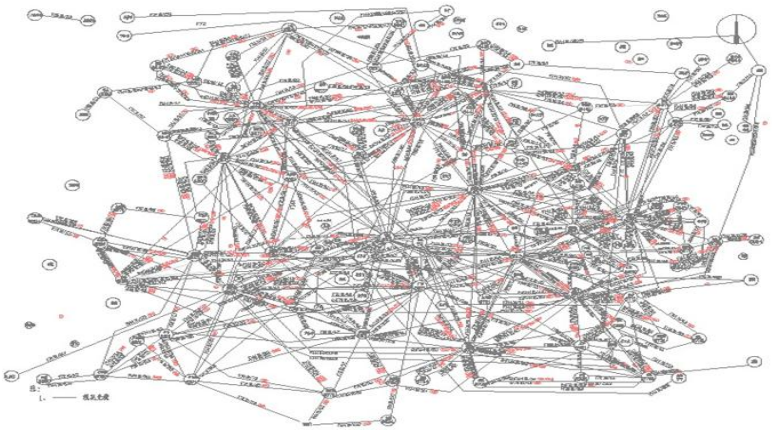


图 北京联通核心汇聚光缆拓扑图

北京联通接入层主干光缆，已达到 16532 皮长公里，折合 303 万芯公里，平均占用率为 64.55%。光交接点数量 3813 个，其中光交接箱数量 1800 个。现已完成城区 100%的综合业务区覆盖目标。城区末端业务平均接入距离 1.0 公里。城区综合业务接入区主干光缆覆盖情况（城区现有 488 个综合业务接入区，完全覆盖 225 个、覆盖不充分 263 个，完全未覆盖 0 个），部分覆盖的综合业务接入区由大局主干光缆覆盖。

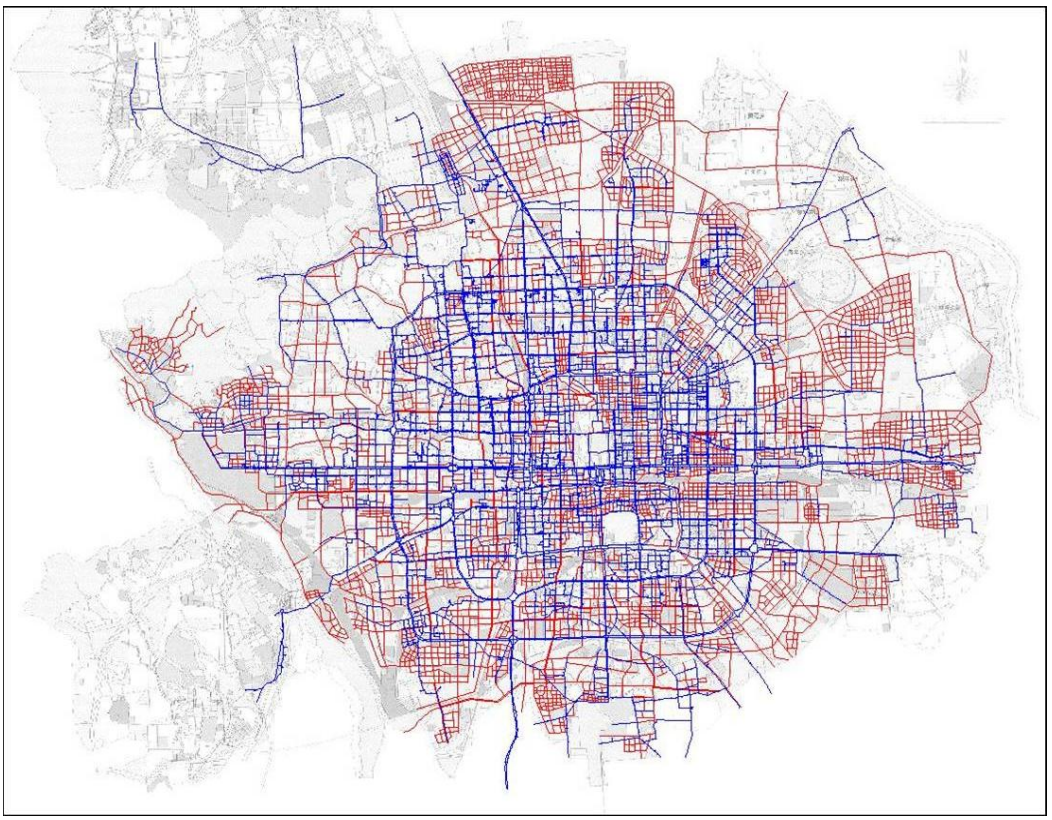


图 中国联通北京分公司城域光缆覆盖示意图

➢传输网络介绍

北京联通目前已经整合了原北京网通与原北京联通各自的城域 SDH 网络，在北京地区实现了 100%的传输网络覆盖，能为用户提供各类 SDH 专线业务。

➢北京联通 SDH/MSTP 网络

北京联通城域 SDH 网络自上世纪九十年代起开始建设，并先后建设了朗讯一网、朗讯二网（99 年）及马可尼网。进入 2000 年，传输扩容工程按照“规模建网，适度超前”的基础网络建设新思路，在进入二十一世纪的 2000-2001 年间，采用新一代的网络技术和设备建设了北京地区高速骨干环和超大交叉连接能力的大型交叉机及覆盖全网的区域环构成的 2000 年新的传输网络平台。在 2003-2004 年期间，分别和上海贝尔-阿尔卡特公司和华为公司合作，采用新一代的智能光网络技术和设备，建设了最先进的城域智能光传送网络（ASON/OSN 网络），全网支持 MSTP 技术，并可以根据需求灵活地配置电路带宽。北京联通的城域智能光传送网络可以为客户的各种业务提供最先进、最可靠、最便捷的数据传送服务。这张网是基于目前业界最先进的 ASON 和 MSTP 平台，覆盖整个北京地区，具有非常巨大的容量和可扩展性，与现有数据网络和宽带接入网络充分配合，在强大的统一网管平台管理之下，能够做到非常快速的端到端业务开通和管理。该网络不仅满足现有网通北分的业务需求，还留有足够的容量适应不断增长的语音，数据和 3/4G 业务的发展。

北京联通城域智能光传送网络由骨干、汇聚和接入三个层次组成。

（一）骨干层

骨干层共由数十个大容量骨干节点组成，其中部分核心节点采用完全 Mesh 结构，节点间以一个或多个 10Gb/s 系统连接。（完全 Mesh 网络结构是指网络所有节点与其他节点均有一个或多个线路系统直接相连）。

骨干核心节点均具备 ASON 功能。GE 和 2.5Gb/s 以上速率的上下业务由 ASON 设备解决，622Mb/s 及其以下速率的业务采用下挂 MSTP 方式解决，ASON 设备与下挂设备之间以 2.5Gb/s 光口（不同板卡 1+1）方式连接。

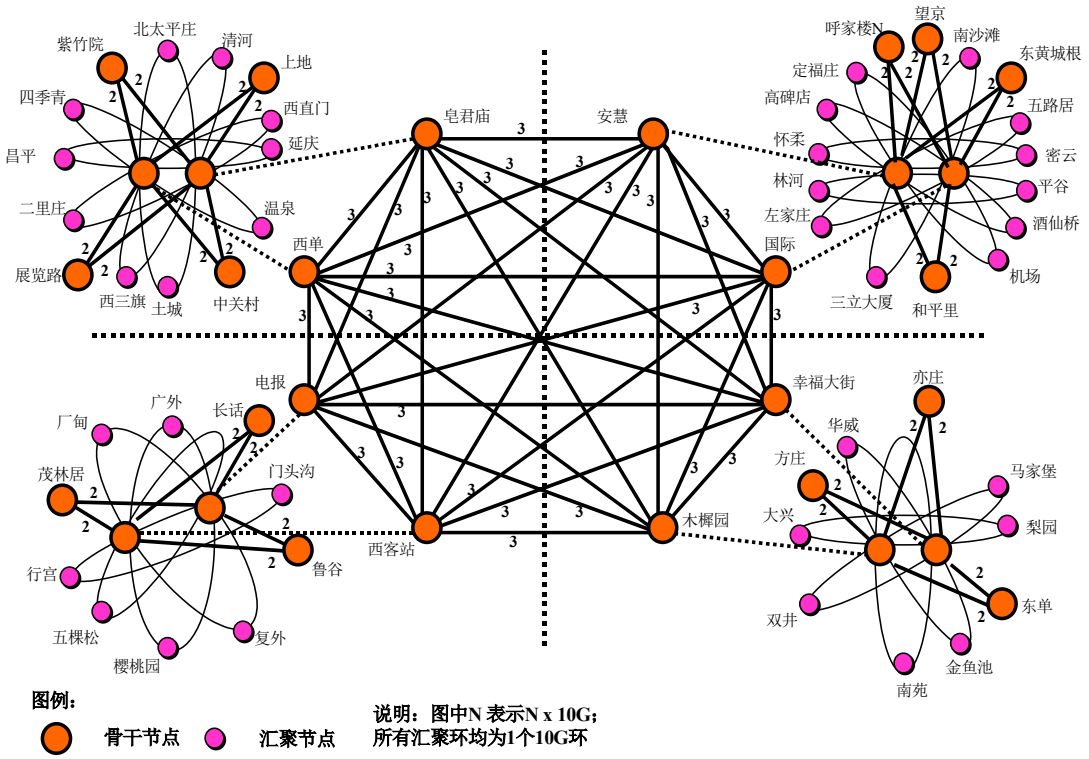
（二）汇聚层

汇聚层由数十个汇聚节点组成，采用 10G 两纤复用段保护环的方式，就近或根据业务需求与骨干节点或本汇接区其他汇聚节点连接。

（三）接入层

接入层由数百个接入节点组成，接入层设备具备 MSTP 功能。

北京联通城域 SDH 网络拓扑如下所示：



北京联通城域 SDH 智能传送网特点：

- 极高的网络可靠性、强大的多点故障生存性，保证网管信息网在任何情况下的可靠运行；
- 端到端的带宽、QoS 保证和底层业务隔离，保证网信息网的安全性和稳定性；
- 丰富的接口、多样化的接入方式，便于网快速灵活的建立、调整网管信息网；
- 不同类型、不同专业统一的物理层和数据层传送平台，便于统一管理和维护，降低运营成本；
- 专用通道的子网网管系统，方便运维人员管理和维护网管信息网。

➢移动网络介绍

北京联通公司认真贯彻落实党中央、国务院的决策部署，执行中国联通集团移动网络发展战略，以创新、协调、绿色、开放、共享发展新理念为引领，以实际行动践行网络强国战略，深入推进供给侧结构性改革，全面深入实施聚焦战略，打造匠心网络，持续提升信息通信服务能力，为用户提供更好的移动通信服务。

➢北京联通 IDC 介绍

截至 2014 年 6 月底，已建设五星级数据中心 9 个，四星级数据中心 18 个，三星级数据中心 10 个。

五星级数据中心参照 TIER Ⅲ+标准，四星级数据中心参照 TIER Ⅲ标准。已建设机房

面积约 8 万平方米，机架总数超过 2.2 万架。

黄村：工信部 4A 级绿色数据中心，DCD 大中华区“中型数据中心创新奖”

次渠：工信部 3A 级绿色数据中心

亦庄：信息安全管理系统认证、ISO/IEC 27001

支持本项目的信令大叔据处理平台部署在中国联通廊坊数据中心。

国联通基于业务发展和总部的战略部署，拟在廊坊经济技术开发区建设中国联通华北（廊坊）基地，该工程主要满足 IDC、EDC、客服等业务发展需求以及配套的运行维护、办公、住宿、餐饮等管理及辅助用房需求。初步规划廊坊基地建成之后，其业务范围将覆盖集团以及京、津、冀三省市。

A1 和 A2 数据机房楼土建工程及基础配套工程，A1 和 A2 数据机房楼 10KV 外市电，东区市政工程及其他相关配套设施。A1 和 A2 数据机房楼每栋 3.7 万平方米，合计 7.4 万平方米。

以业务需求为导向，以提升市场竞争能力为着眼点，综合考虑云计算引入、应用以及未来通信网络升级演进技术需要，提早储备，加快建设，形成资源配置合理、运营成本节约的集中化、规模化、绿色环保的新一代数据中心基地。

抓住国家发展云计算等高科技信息的政策支持机遇，积极引进国外建设大型数据通信基地的先进设计和运营理念，本着高标准、高规格、高品位、严要求的原则，建设低能耗、绿色环保、技术先进、运营稳定的信息通信基地。

- 建设标准

（1） 数据中心机房的标准遵照国标A级及B级机房（并参照UPTIME TIER Ⅲ和TIA942 Tier 3 ）标准进行规划建设，部分系统建设（尤其是供配电系统）遵照国标 A 级（并参照 TIA942 的 Tier4 的等级）规划，满足不同层级用户需求。

（2） 数据中心机房具有良好的灵活性及可扩展性，能够根据未来业务发展需求，扩大设备容量和提高用户数量及质量。

（3） IDC 单机架平均功耗将达到 4kw/机架；EDC 单机架平均功耗将达到 5kw/机架以上，支持部分设备可扩展到高功率密度。

（4） 在建筑设计、设备选型、日常维护等各方面进行高可靠性设计和建设，避免出现单点故障。采用相关软件技术获得较强的管理机制、控制手段和事故监控与安全保密等技术措施，提高安全可靠性。

（5） 贯彻基地“模块化、标准化”设计理念，采用“大平面、少楼层”的设计方案，具备弹性发展空间，在协调相关专业功能的情况下，提升机房面积占用比例。充分考虑新业务、新技术设备对机房面积和空间的要求，满足机房维护管理体制的需要，按少人或

无人值守和集中管理的原则进行设计。

（6） 采用切实有效的措施来充分体现节能、环保、减排的要求，建设绿色数据中心基地，选择低能耗、低运维成本的产品，并充分考虑产品的维保成本。

- IDC 定位

以集团战略为指引，以业务需求为导向，以国家发展云计算等高科技信息及地方政府政策支持为契机，本着高标准、高规格、高品位、严要求的原则，打造中国联通集团 EDC 主数据中心、区域 IDC 及云计算运营中心、区域呼叫服务中心，创建低能耗、绿色环保、技术先进、运营稳定的国际领先、国内一流、适用于不同客户群的大型综合信息服务基地。

中国联通集团 EDC 主数据中心：建设企业级云平台，承载信息化支撑系统，具有完整的运营管理体系；

京津冀及环渤海地区 IDC 运营中心：主要服务于消费能力强、有影响力的知名传媒网站等互联网企业、国家级和省级机关单位、金融证券、大中型企业集团等战略客户；

云计算运营中心：以中小型企业、中小型软件开发企业为主要客户，同时承载联通自有的云计算业务；

3.3.2.个性化模型服务方案

北京联通长期优化校准基站位置采集信令数据，建立信令数据处理模型算法，持续提升用户定位的精准度，对用户定位结果进行验证与修正保证精度满足 250M*250M 及 100M*100M 栅格。根据客户需求除去现有人口统计，进一步丰富用户标签体系。

依托我司提供的沙箱建模环境，对于客户个性化需求建立模型，并提供实现在沙箱模型的部署、测试、验证及个性化调整等基础维护和管理服务。

3.3.2.1.优化定位模型服务

我司在项目服务过程中持续提升用户定位的精准度，对用户定位结果进行验证与修正。相关优化技术举例如下。

3.3.2.1.1.个人位置定位优化技术

使用移动数据需要在准确性与连贯性间作出妥协。用户到底在哪里？它们去了哪些地方（非杂乱无章的位置）。我们基于信令数据和基站工参结合获得的位置信息，存在两种情况：

第一种，空间准确但数据杂乱，位置不连贯，分析价值小；

第二种，长时间连贯，对分析更有用，但是空间上不准确。

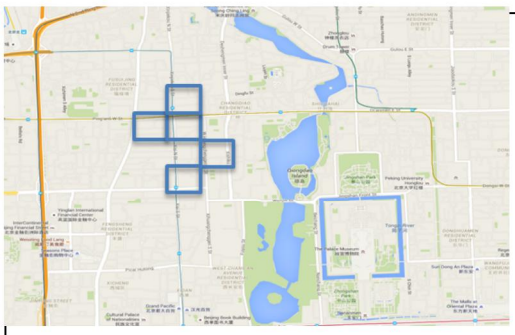


图 杂乱

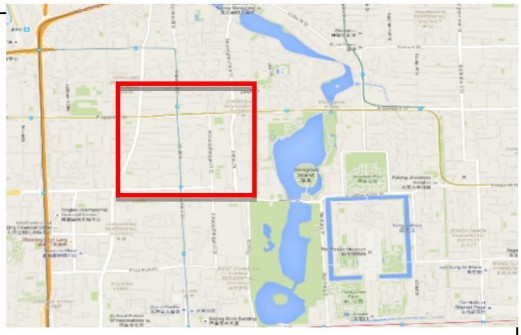


图 连贯

中国联通采用的自己的方式，这种方式可以基于历史信令数据加强用户位置的准确性和连贯性，从而获得更有分析价值的准确的用户兴趣点。

3.3.2.1.2.位置外推

手机用户可能有很多次近距离的停留，都被算作同一个位置。随着时间的推移，这就会集合成为连续的用户地点。通过对特定一个用户在一个月内的信令驻留位置判断，可以有如下图分布：

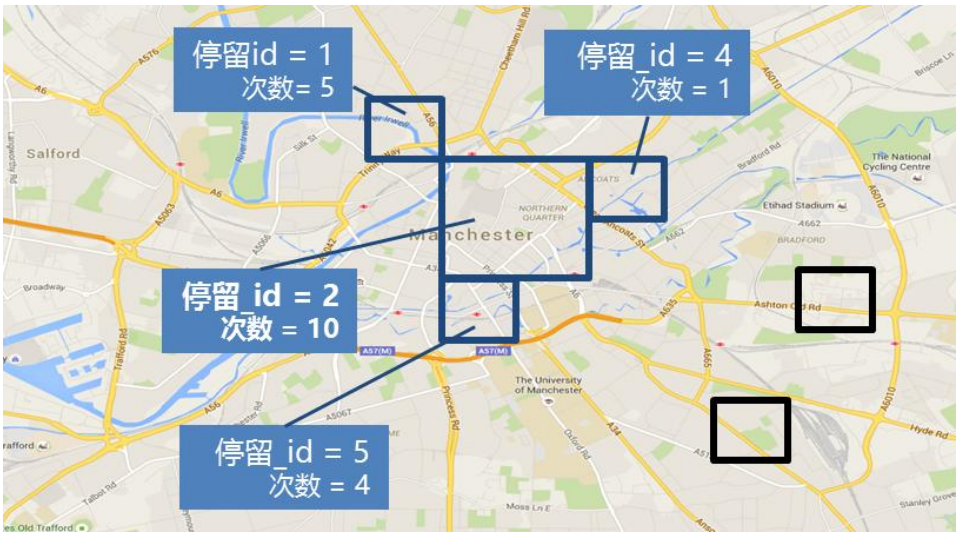


图 选取用户超过一个月驻留位置的数据

从而可以获得一个多次驻留的位置空间区域作为兴趣点，并且从长久来看，兴趣点会趋于稳定：

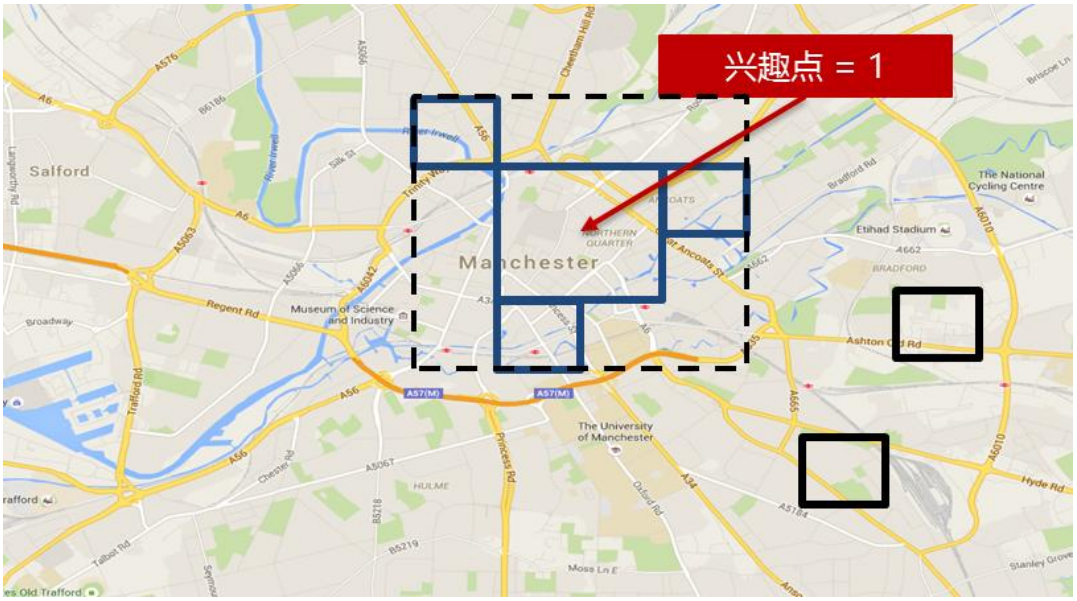


图 根据空间和接近的次数，驻留点会变成兴趣点

3.3.2.1.3.空间完善

在位置外推过程中我们获取到了一个长效意义的、较为准确的位置区域：兴趣点，接下来需要通过进一步工作使这个兴趣点的实际位置得到更加准确的优化。

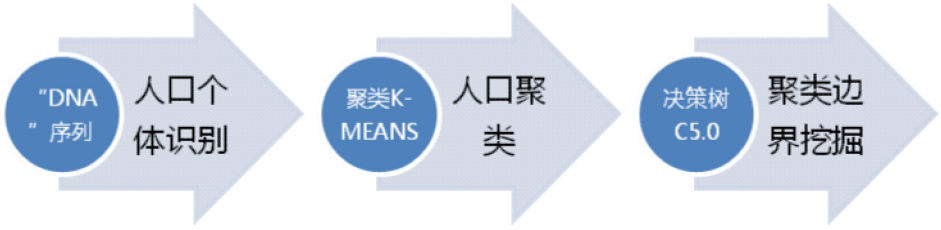
统计每个小区基站的事件量和集合的兴趣点驻留。每个基站距离兴趣点的距离、每个基站事件数量将参与 SmartSteps 独有的计算模型中，对空间质心进行合理偏移，进而计算得到加权质心的位置。

相比于兴趣点，加权质心进一步地考虑了信令发生频度、基站覆盖范围、信号衰减等多方面因素，位置更加的准确，尤其适合区域内存在不同密度人口的情况（例如一个栅格内既有公园又有写字楼，加权质心一般会更加偏向写字楼方向）。

最终得到的完善的兴趣点位置栅格，是基于分析每个小区基站纪录的事件得出。

图 完善的兴趣点位置栅格

3.3.2.1.4.人口识别模型算法



（1）人口个体识别

算法目标：由于通信规模的不断扩大以及技术的不断发展，系统设备和终端的价格在逐步下降。同时，移动运营商在面对日益激烈的市场竞争压力时，将不断降低通信资费并不断推出新的促销方式，以推动用户数量的增长,因此一人多机、一机多卡甚至多机多运营商现象日益增多,在统计中需要对用户进行个体识别。

（2）人口聚类

算法目标：需要根据用户特征识别用户的人口属性“居住人口”和“工作人口”。通过构建时间维度和空间维度上的用户驻留和行为特征，再用 K-means 聚类算法对人群进行聚类，时间维度上取分时段统计每个用户发生在对应场景区域的信令条数、停留时长、驻留天数和驻留月数，空间维度上取用户位置信息所在区域。

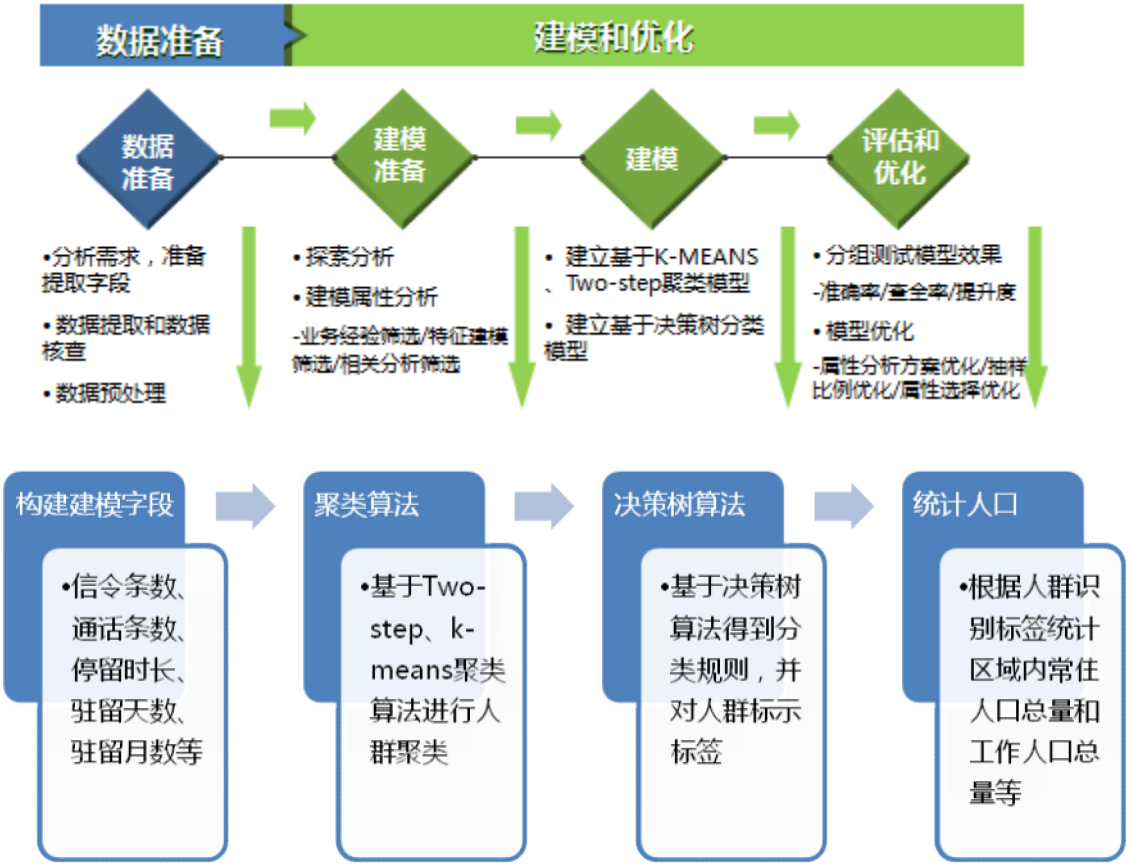
（3）聚类边界挖掘

算法目标：根据聚类结果进一步对聚类边界进行挖掘，得出“居住人口”和“工作人口”的判断规则

分类：分类是以实例为基础的归纳学习算法。它从一组无次序、无规则的元组中推理出决策树表示形式的分类规则。它采用自顶向下的递归方式，在决策树的内部结点进行属性

值的比较，并根据不同的属性值从该结点向下分支，叶结点是要学习划分的类。从根到叶结点的一条路径就对应着一条合取规则，整个决策树就对应着一组析取表达式规则。

（4）工作人口与居住人口的识别



具体步骤：

1）设定居住地时间为 21:00 点至 05:00 点（次日凌晨）。

2）设定工作地时间为 06:00 点至 20:00 点（工作日）。

3）根据用户发生通信行为所在的位置信息定位所属区域。

4）基于 Two-step、k-means 聚类算法+决策树组合算法得到居住人口和工作人口分类规则。

5）如果一个用户满足多个居住地，则以驻留月数最多的位置作为居住地。

6）如果一个用户满足多个工作地，则以驻留月数最多的位置作为工作地。

7）计算居住地和工作地区域内的人口数量。

3.3.2.1.5.驻留和出行的核心指标判定

（1）驻留核心指标判定

1）工作时段与休息时段的标准

根据我国居民通常的工作和休息习惯，定义 9:00-18:00 为工作时段，21:00-7:00 为休息时段。

2）潜在职住地点的判断

以单个用户为单位，判断用户工作时段、休息时段到访过的网格，同时还统计用户在相应网格停留的时长，以分钟计。基于每日结果，统计出单个用户在一个完整月中，工作时段和居住时段到访过的所有网格(无重复)，作为该用户潜在工作地和潜在居住地

3）居民职住地的初步确定

根据潜在居住地和工作地，选取停留时间最长的，并超过一定天数阈值的(居住地一般为研究时段天数的一半，工作地一般为研究时段工作日的一半)，作为用户的最终居住地和工作地

4）居民职住地的修正与最终确认

对上一步的结果做校核，排除物联网以及一人多卡的用户后，记录用户的最终居住地和工作地。

（2）出行核心指标判定

1）单个用户驻留地的识别

依据基站的覆盖情况划分网格单元，观察单个用户信令的时空分布，将时间上连续空间上临近的多次信令数据进行汇聚，认为是一次驻留

时间上连续（30 分钟内），空间上临近（300m 内），多次（大于 2 条）

2）单用户出行链的判定

在完成驻留判定的基础上，认为至少要超过 1 个小时，才是有效驻留。研究区域内，以天为单位，将单个用户在研究区域内的所有有效驻留，串联得到出行的区域对，排除起始地和目的地都在一个区域的部分，剩余部分作为出行的研究部分。

3.3.2.2.优化用户标签体系服务

我司提供优化用户标签体系服务，按照人口监测业务需求，进一步丰富用户标签体系。

3.3.2.2.1.用户属性标签优化

用户属性标签包括用户的性别、年龄段、消费能力（根据月度话费）、月度流量、手机终端等方面。

标签分类	标签内容（示例）
性别	男、女
年龄	0-6、7-12、13-15、16-18、19-24、25-29、30-34、35-39、40-44、45-49、50-54、55-59、60-64、65-69、>70
消费能力（月度话费）	0-50、50-100、100-160、160-200、>200（以联通通讯消费套餐月度话费数据进行定义）
月度流量	<100M、100M-500M、500M-1G、1G-2G、>2G
终端品牌	苹果、三星、华为等

3.3.2.2.2.互联网偏好标签优化

互联网偏好标签主要是商务应用类、生活服务类、娱乐休闲类、新闻资讯类、通信交流类、工具软件类等。

标签分类	标签内容
商务应用类	网上购物、金融理财、电子支付、教育培训、求职招聘、招聘、中外名酒、手机银行、商务办公、手机数码、借贷、办公
生活服务类	餐饮美食、团购打折、打车软件、母婴资讯、医疗健康、旅游出行、教育学习、汽车信息、二手车、酒店、外卖送餐、物流快递、导购、火车票、机票、公交、违章查询、时间天气、家居服务、成人、彩票、生活综合
娱乐休闲类	手机视频、电影、手机阅读、小说（不区分）、玄幻小说、中外文学、笑话、期刊杂志、漫画、手机音乐、听书、手机游戏、动作游戏、模拟经营、手机动漫、娱乐搞笑、网络电台、演出票、电影票
新闻资讯类	时政要闻、国内时政、女性时尚、体育资讯、军事资讯、科技资讯、数码、程序代码、娱乐资讯、财经资讯、房产、股票、文化教育、考试、外语、企业门户、金融业、交通运输、旅游休闲、轻工食品、建筑建材、石油化工、机械机电、医药卫生、服装纺织、环保绿化、办公文教、电子电工、玩具礼品、家居用品、社会资源、政府机构、综合资讯、自然人文
通信交流类	婚恋交友、社区论坛、交友论坛、博客空间、社交网络、通信交流
工具软件类	安全杀毒、浏览器、输入法、词典翻译、主题桌面、教育、求职、星座占卜、电子邮件、工具软件、主题壁纸

3.3.2.3.个性化业务分析服务

我司提供个性化业务分析服务，满足突发性的人口监测业务需要，例如重大节假日等特殊时期。

针对春节、国庆等重大节假日及重大或突发事件情况下，我司根据采购人需求，开展相关人口监测工作，满足采购人对人口监测分析工作需要。

在特殊时期，我司以天作为监测周期，重点关注朝阳全区、街乡镇、重点监测地区相关的用户流入、流出情况。

3.3.3.数据质量保障服务方案

联通集团已经实现全国信令数据一点集中，全国采集统一存储、处理。为保证信令数据稳定的采集传输指定详细信令数据采集规范，保证数据质量及校核以便发现问题及时修正，搭建信令数据监测平台。

3.3.3.1.数据稳定性保障服务方案

我司保障稳定提供数据，保障数据的采集、清洗、加工以及传输等环节的稳定性，以确保运营商底层数据的稳定，不造成上层业务模型的波动。

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

[1]YD/T 1097-2001《高端路由器设备技术规范》（中华人民共和国信息产业部）

[2]3GPPTS 24.008 Technical Specification Group Core Network and Terminals;Mobile radio interface Layer 3 specification;Core network protocols(3rd Generation Partnership Project)

[3]3GPP TS 24.301 Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS) (3rd Generation Partnership Project)

[4]3GPP TS 25.413 UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling（3rd Generation Partnership Project）

[5]3GPP TS 36.413 Evolved Universal Terrestrial Radio Access Network (E-UTRAN);S1 Application Protocol (S1AP) (3rd Generation Partnership Project)

本规范为中国联通 GSM/WCDMA/LTE 网络信令 DPI 采集系统技术规范，规定了 2/3/4/5G 移动网络信令采集的接口范围、采集系统功能要求、信令解析生成话单要求、话单格式、系统接口、性能和可靠性、安全性要求等。

本规范是充分了解中国联通现有的移动网络的相关规划、建设情况，参考了相关国内行业标准、企业标准，并结合中国联通的实际情况和具体要求编制而成。

本规范规定了中国联通移动网络（GSM/GPRS/WCDMA/LTE）信令采集系统设备的功能要求、接口要求、性能要求、时间同步要求、安全要求等。

本标准由中国联通公司运维部提出。

本规范使用的缩略

缩略语	英文	中文
3G	3rd Generation	第三代移动通信
4G	4th Generation	第四代移动通信
APN	Access Point Name	接入点名称
BSC	Base Station Controller	基站控制器
CI	Cell Identifier	小区标识
CM	Configuration Management	配置管理数据
DPI	Deep packet Inspection	深度报文解析
FDR	Signal Detail Record	上网流量详单记录
FTP	File Transfer Protocal	文件传输协议
GGSN	Gateway GPRS Support Node	网关 GPRS 支持节点
GPRS	General Packet Radio Service	通用分组无线业务
GPRS	General Packet Radio Service	通用分组无线服务技术
GSM	Global System for Mobile Communication	全球移动通信系统
GSN	GPRS Support Node	GPRS 支持节点
GTP	GPRS Tunnel Protocol	GPRS 隧道协议

HSS	Home Subscriber Server	归属签约用户服务器
HTTP	HyperText Transfer Protocol	超文本传输协议
ICMP	Internet Control Message Protocol	Internet 控制报文协议
IMAP4	Internet Message Access Protocol 4	交互式数据消息访问协议版本 4
IMEI(SV)	International Mobile Equipment Identity(Software Version)	国际移动设备身份码（软件版本）
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	互联网协议
Ipv4	Internet Protocol version 4	互联网协议版本 4
Ipv6	Internet Protocol version 6	互联网协议版本 6
LAC	Location Area Code	位置区识别码
LAI	Location Area Identify	位置区识别标识
LTE	Long Term Evolution	长期演进
MGW	Media Gateway	媒体网关
MME	Mobility Management Entity	移动性管理实体
MR	Measurement Report	测量报告
MSC	Mobile Switching Center	移动交换中心
MSISDN	Mobile Subscriber International ISDN/PSTN number	移动用户国际 ISDN/PSTN 号码
NAT	Network Address Translation	网络地址转换
NTP	Network Time Protocol	网络时间协议
OMC	Operation and Maintenance Center	操作维护中心
PDN	Public Data Network	公共数据网
PDP	Packet Data Protocol	分组数据协议
PGW	PDN GateWay	PDN 网关
PM	Performance Management	性能管理数据

POP3	Post Office Protocol 3	邮局协议版本 3
RAID	Redundant Arrays of Inexpensive Disks	磁盘阵列
RNC	Radio Network Controller	无线网络控制器
RTSP	Real Time Streaming Protocol	实时流传输协议
SDR	Signal Detail Record	信令详细记录
SGSN	Serving GPRS Support Node	服务 GPRS 支持节点
SGSN	Serving GPRS Support Node	服务 GPRS 支持节点
SGW	Serving GateWay	服务网关
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
TAP		电口分路器
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据包协议
URL	Uniform / Universal Resource Locator	统一资源定位符
VLAN	Virtual Local Area Network	虚拟局域网
WAP	Wireless Application Protocol	无线应用协议
WCDMA	Wideband Code Division Multiple Access	宽带码分多址接入系统
WLAN	Wireless Local Area Network	无线局域网
XDR	X Detail Record	信令/流量详细记录

3.3.3.1.1.DPI 信令采集系统的位置和作用

随着3G网络的完善以及4G网络的建设，网络所提供的承载能力进一步增强，用户对移动网络的服务也有更高的感知体验要求，这就要求运营商在网络建设、网络维护的水平持续提升，保证网络建设投资精准性和有效性，保障网络的更优质服务。中国联通建设移动网络信令采集系统和信令分析平台，收集和分析移动信令，精细化分析和评价网络质量，衡量用户对网络的感知体验；从而指导进行高效的网络建设和优化、提升网络对用户的服务水平。

DPI信令采集系统对相关网络接口链路进行旁路分光，对链路中的数据进行实时分析并生成信令详单（SDR，针对于信令部分）和流量详单（FDR，针对于用户面流量数据），同时将信令原始码流存储下来，并将所有的详单（SDR和FDR，统称XDR）传送到总部相关系统。针对某些实时应用场景，DPI信令采集系统同时支持根据链路数据解析生成实时消息并将消息发送给总部相关系统的功能。针对某些实时性要求高的网络KPI指标，DPI采集系统按照一定的时间粒度进行计算并将计算结果的指标值按照规定格式和协议传送给总部相关系统。

移动网络中还包括从OMC/RNC上采集配置数据（CM）、话统数据（PM）、测量报告（MR）、Trace信令等，这类数据不是通过链路分光和拆包解析方式获取，由其他规范进行规定。

DPI信令采集系统位于各省分，所生成的XDR话单、实时消息、KPI指标数据等通过承载网传送到总部所需的应用系统；同时，省分采集系统提供对XDR话单和原始码流的缓存，并提供信令跟踪和信令查询接口。

在联通总部整体OSS2.0体系下，XDR话单可根据需要通过统一采集与指令适配平台（ESB）进行传送，由统一采集与指令适配平台向各相关应用系统提供XDR话单。

DPI采集系统在网络中的位置参见下图。

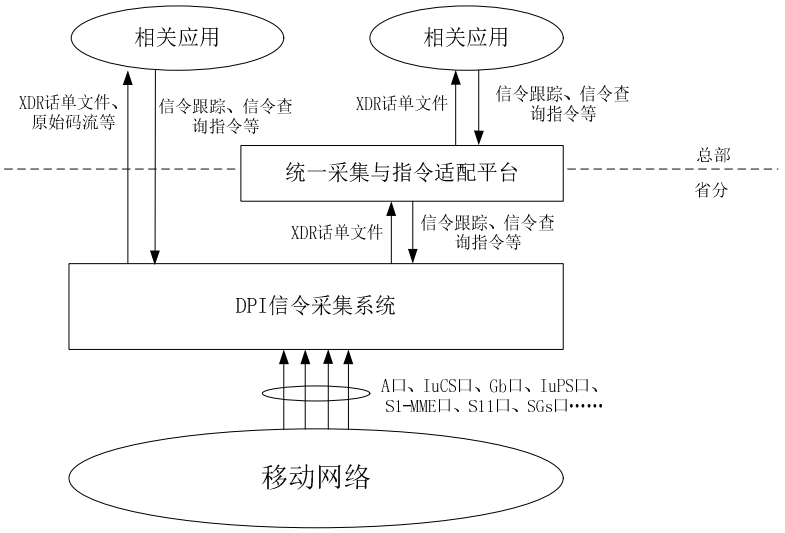


图 DPI 信令采集系统在网络中的位置

DPI 信令采集覆盖的接口范围，现阶段信令采集系统的采集范围如下表所示：

表 DPI信令采集系统涵盖的接口范围

	网络类型	接口名称	涉及网元
DPI 信令采集	GSM/GPRS	A	BSC—MSC
		Gb	BSC—SGSN
	WCDMA	IuCS	RNC—MGW
		IuPS	RNC—SGSN
		Gn	SGSN—GGSN
		Gr	SGSN-HLR
		Gp	GSN-GSN 网间漫游接口
		3G DNS	SGSN-DNS 接口
	LTE	S1-MME	eNodeB—MME
		S11	MME—SGW
		SGs	MME—MSC
		S8	SGW-PGW 漫游场景
		S6a	MME—HSS
		S1-U	S1-MME—SGW
		S10	MME—MME
		4G DNS	MME-DNS
		iDRA	国漫 DRA 设备

注1：对A口和IuCS的采集可通过Mc口进行。

注2：语音话单中涉及C\D\E口部分内容，此部分接口内容不做强制要求

3.3.3.1.2.DPI 信令采集系统功能结构

DPI 采集部分通分光旁路网络中的相关接口链路数据，对链路中的信令数据进行解码、合成、各协议关联、用户信息回填，并生成 XDR 话单，并上传话单文件到总部平台。同时，信令解析设备生成实时消息和 KPI 指标数据，并传送给总部系统（或通过文件服务器等进行指标计算和汇聚传送）。其功能结构模块见下图所示。

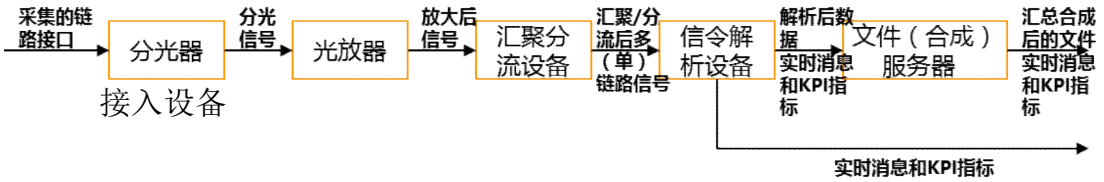


图 DPI 信令采集系统的功能结构示意图

图中整个系统包括

- 接入设备：实现对原有链路的数据的旁路、复制、汇聚分流及其他必要处理，对于不同物理接口类型，所需设备可能包括分光器、以太网分路器（TAP）、光放器、汇聚分流设备等。接入设备可依据现有情况进行利旧或共享使用。
- 信令解析设备：完成对数据包的抓取、协议解码、并进行分析、关联等，生成规定格式的XDR话单、实时消息和KPI指标，同时记录需要保存的原始信令。
- 文件服务器：对多接口的话单进行合成汇总，或进行KPI指标的计算和实时消息的汇聚，并负责将话单和原始信令FTP上传到总部平台以及实时消息和KPI指标数据的实时传送；同时对话单文件和原始信令进行缓存。并在省分提供原始信令的FTP共享。

3.3.3.1.3.DPI 信令采集系统的部署

分光DPI部分的接入设备分光器、TAP、光放器、汇聚分流设备的部署可依据省分情况进行统一规划或利旧使用，分光设备和汇聚分流设备一般可分级规划，按照业务需要预留光口/电口，保证资源的充分利用以及未来的可扩展性。

信令解析设备根据省分链路情况可将多条接口链路汇聚到省分一点集中部署，文件服务器在省内可采用集中部署方式。

3.3.3.1.4.DPI 信令采集系统技术要求

3.3.3.1.4.1.接入设备要求

3.3.3.1.4.1.1.分光器设备要求

Gn口接入设备负责将Gn链路的数据（信令数据、业务数据）全部复制，并输出到汇聚分流设备，要求不影响原链路业务传输。

由于不同物理类型的接口，需要支持不同的接入设备，即支持分光方式和电口方式（TAP）进行Gn口数据的采集。其中，分光采集方式应达到线速的数据采集，同时在光信号不足的情况下，需要提供光信号复原设备OEO，以保证数据采集的准确性和完整性。

分光接入方式的采集，需要在被监测网络的光纤链路中串接分光器，需保证不增加被监测网络的交换机负荷，保证对被监测网络不造成任何不良影响。

分光器应符合行标YD/T 1097-2001《高端路由器设备技术规范》中的性能指标要求。

3.3.3.1.4.1.2.OEO 放大器设备要求

光功率放大器用于光口链路分光后光信号光层放大，提高单跨段传输距离，可广泛应用于长距离、大容量、高速率的光纤通信系统，作为功率放大器以提高发射机的功率。

3.3.3.1.4.1.3.TAP 设备要求

TAP设备用于监测百兆电口或者千兆电口的链路，其功能是将电信号复制一份，TAP的网络口接被测链路的两端设备，TAP的监测口接信令监测系统。TAP设备失电后被测链路主通道具备链路直通的功能。

3.3.3.1.4.1.4.数据汇聚分流设备要求

数据汇聚分流模块主要实现对采集后的原始码流量进行过滤，将数据进行汇聚，根据预先设定的策略（如源IP地址段等），将数据流至采集解析设备，采集解析设备根据处理能力可以设置多台进行并行处理，实现汇聚分流与采集处理机的负载均衡，从而实现资源的最大化利用。

数据汇聚分流设备要求如下：

- 支持镜像输出的光口或者电口的流量采集；
- 支持对流量的过滤，负载均衡转发和汇聚；
- 支持对流量汇聚后再分流；

- 支持对流量按分类的复制后再输出。

3.3.3.1.4.2. 信令解析设备要求

3.3.3.1.4.2.1.总体要求

信令解析设备支持对S1-MME/S6a/S11/Gn/Gb/A/IuPS/IuCS/Gn/S1-U/Gp/Gr/iDRA/S8等各链路中的逻辑接口数据进行自动识别，完成信令数据的解码和关键信息提取，并按照标准格式生成记录XDR。

信令解析设备可根据业务过程中各接口信令过程之间的相关性，对信令处理过程进行动态实时关联，并实时获取、存储和更新GUTI-IMSI-IMEI-MSISDN-TMSI-PTMSI、真实号码与漫游号码等之间的映射关系并将无法直接从消息中获取的IMSI、MSISDN、IMEI等回填入XDR中。XDR中需要对重复信令进行剔重，并对重传数量进行统计。对于无法解析的信令消息，需留存错误记录并一并上传到文件服务器。同时信令解析设备还需要对信令原始码流进行提取并传送到文件服务器缓存。

3.3.3.1.4.2.2.XDR 话单分类

XDR话单有两大类，单接口话单和专项话单。单接口话单是针对某特定接口中的数据进行解析生成的话单，专项话单是针对特定需求、需要进行多接口关联或是进行二次处理生成的话单。对于单接口话单，按照接口的不同又分为各接口话单。

3.3.3.1.4.2.3.话单字段填写的通用要求

XDR话单文件为文本文件，填写的字段为文本字符，如话单中不加特殊说明，则通用填写规则如下：

字段内容	填写要求	填写示例
时间	YYYY-MM-DD HH:MM:SS.1234567，精确到0.1微秒	2017-06-21 15:23:37.2345167
IP地址	IPv4按照通常的10	IPv4：192.168.1.1

	进制表示形式 IPv6按照带“:“的16进制形式	IPv6： 1050:0000:0000:0000:0005:0600:300c:326b
端口号	10进制的数字形式	如：455、1024等
手机号	不加国家码等前缀的手机号码	如：18600113467
IMSI	15位IMSI码数字	如：460010912121001
IMEI/IMEISV	15位或16位数字形式	如：356869014100729
TAC、LAC、RAC、CI等小区和位置区标识等	10进制的数字形式	如：LAC为 41059
信令点码、网络类型标识、业务类型标识、Cause结果码等	10进制数字	如：Cause值为 86

3.3.3.1.4.2.4.信令原始码流封装和传送

采集解析设备接收信令链路中的原始码流，按帧进行封装，并基于 XDR ID，将其对应的原始码流组合后实时传输到文件服务器。

具体操作要求如下：采集解析设备生成 XDR 后，该 XDR 对应的原始码流按照采集时间顺序组成一个数据包，并通过 SDTP 协议实时发送给文件服务器。根据 XDR 类型的不同，原始码流的内容不同。如果是信令 XDR，则原始码流为原始信令；如果是业务 XDR，则原始码流为原始业务数据中的包头部分，并不包含 payload 部分。

文件服务器将原始码流存储成二进制文件，文件命名规则为：接口标识[字符型：同信令解析话单文件名]+分隔符（下划线）+省分代码[3 位]+年[4 位]+月[2 位]+日[2 位]+时[2 位（24 小时制）]+分[2 位]+秒[2 位]+文件序列号[5 位，从 0 开始]+信令解析设备编码[3 位]+文件后缀(.signal)。

文件中的内容格式见下表：

表 原始码流文件格式

字段	长度（Byte）	字段描述
RAT	1	RAT 类型
Interface	1	接口类型
XDR ID	16	XDR ID 信息
原始码流条目数	2	原始信令或原始业务包头总条目数 N
Length Total	4	后续原始码流总长度，单位为 Byte，包括本字段之后的信息块长度指示字段，不包括结束标志。
Payload1	不定长	信令 1 或业务包头 1 的按帧封装后的原始码流
Payload…	不定长	…
PayloadN	不定长	信令 N 或业务包头 N 的按帧封装后的原始码流

3.3.3.1.4.2.5.原始码流的按帧封装格式

原始码流的封装格式要求如下：

图 原始码流帧格式

帧格式如下：

名称	字节长度	名称	说明
Len	2	数据包长度	不包括长度本身、定界标志
Head1	12	通用包头	各种链路公用的数据包头
Head2	0	专用包头	每种链路独有的数据包头
Load	不定长	原始信令数据	采集到的原始信令数据（从 MAC 地址开始）

其中，通用包头长度为 12 字节，包含如下字段：

名称	字节长度	说明
Ver	1	包头信息版本 当前版本为 4.0；值填为 0x04
LinkType	1	承载链路类型 0x01-2M（SS7） 0x02-64K(SS7) 0x03-IPv4 0x04-ATM 0x05-Abis 0x06-LTE 软采 0x07-LTE 硬采
CardType	1	板卡类型 0x01-FE/GE 0x02-E1 0x03-ATM 0x04-STM 0x0F-其它
CardID	1	采集板卡标识 取值范围 0~255
Time	4	距 1970 年 1 月 1 日 0 时 0 分 0 秒的秒值，单位为秒
Time2	4	时间的纳秒部分，单位为纳秒

专用包头中，对于 IP 链路无专用包头。

原始信令数据中，如果是 GTP-U 数据，则只包含包头部分，不包含 payload 部分，例如对 HTTP 包，只包含 HTTP header，不包含 body 部分。

某些接口中的信令数据（S6a、GTP-C等）可能需要在多套采集解析设备之间共享（如不同接口由多个DPI厂商采集和解析的情况），此时可由信令解析设备

等按照本节的封装格式将原始码流利用SDTP协议实时传送给需要的其他采集系统（也可采用在前端由汇聚分流设备分出一路信号的方式）。

3.3.3.1.4.2.6.用户面实时消息接口功能要求

为满足某些实时业务场景需求，采集解析设备支持根据链路中的用户流量解析结果按要求生成和发送实时消息，实时消息格式和内容要求如下：

实时消息采用 UDP 协议，发送的 IP 地址和端口号可根据工程实施需求进行配置。

序号	字段	字节数	说明
1	Time	8	毫秒数，即将标准 unix 时间转成毫秒，网络字节序
2	MSISDN	16	手机号码,不足 16 字节填 0，不包含字冠如+86,0086，86
3	IMEI	16	16 位的 EMEI 号，不足 16 字节填 0
4	IMSI	16	不足 16 字节填 0
5	RAT	1	承载网络：1=3G, 2=2G,6=4G
6	LAC/TAC	2	2/3G 对应 lac，4G 对应 Tac，网络字节序
7	CI/ECI	4	2/3G 对应 ci/sac，4G 对应 eci，网络字节序
8	APN	16	超过 16 字节则截断为 16 字节
9	Longitude	8	经度，双精度浮点，网络字节序，默认值全 FF，统一转换为 GPS 坐标系
10	Latitude	8	纬度，双精度浮点，网络字节序，默认值全 FF，统一转换为 GPS 坐标系
11	FlowType	3	流量类型编码
12	坐标系	1	应用使用的坐标系 1 ： 百度坐标系 2 ： Google 地球坐标系 3 ： 墨卡托坐标系 4 ： 高德坐标系

			0：其他坐标系/未知
13	ProvinceID	3	采集省份，编码见附录 G

实时消息中所有字段的编码采用二进制编码，涉及到用户号码的，编码形式为TBCD编码。

实时消息的传输需支持：

1、对同一省份内的多台采集解析设备，支持对用户面实时消息的单点汇聚传输，即面对总部相关消息接收系统，同一个省保持一个实时消息发送IP地址

2、对于利用ESB系统进行实时消息传送的情况，向省份ESB传送实时消息时，可以是多个发送方IP地址。

3.3.3.1.4.3. 控制面信令实时消息接口功能要求

3.3.3.1.4.3.1.通话类实时消息

为满足某些实时业务场景需求，采集解析设备支持根据链路中的用户流量解析结果按要求生成和发送实时消息，实时消息格式和内容要求如下：

实时消息采用 UDP 协议，发送的 IP 地址和端口号可根据工程实施需求进行配置。

实时消息中所有字段的编码采用二进制编码，涉及到用户号码的，编码形式为TBCD编码。

1、开关机：

序号	字段	字节数	说明
1	Time	8	毫秒数，即将标准 unix 时间转成毫秒，网络字节序，业务发生的时间
2	MSISDN	16	手机号码,不足 16 字节填 0，不包含字冠如+86,0086，86
3	IMEI	16	16 位的 EMEI 号，不足 16 字节填 0
4	IMSI	16	不足 16 字节填 0
5	RAT	1	承载网络：1=3G, 2=2G,6=4G
6	LAC/TAC	2	2/3G 对应 lac，4G 对应 Tac，网络字节序
7	CI/ECI	4	2/3G 对应 ci/sac，4G 对应 eci，网络字节序

8	ServiceType	1	0：开机 1：关机
9	ProvinceID	3	采集省份，编码见附录 G

2、语音通话：

序号	字段	字节数	说明
1	Time	8	毫秒数，即将标准 unix 时间转成毫秒，网络字节序，业务发生的时间
2	MSISDN	16	手机号码,不足 16 字节填 0，不包含字冠如+86,0086，86
3	IMEI	16	16 位的 EMEI 号，不足 16 字节填 0
4	IMSI	16	不足 16 字节填 0
5	RAT	1	承载网络：1=3G, 2=2G,6=4G
6	LAC/TAC	2	2/3G 对应 lac，4G 对应 Tac，网络字节序
7	CI/ECI	4	2/3G 对应 ci/sac，4G 对应 eci，网络字节序
8	ServiceType	1	2：振铃（alert 消息） 3：接通（connect 消息） 4：挂机（disconnect）
9	MO/MT	1	0：主叫 1：被叫
10	MSISDN	16	对方号码，不足 16 字节填 0
11	Duration	8	通话时长，单位毫秒，具体含义见语音呼叫话单中的通话时长，没有填 FF
12	RingDuration	8	振铃时长，单位毫秒，Alerting 消息和下一条消息的时间差，如果没有 Alerting 消息，则填 FF
13	Cause	8	释放原因，见语音呼叫话单中的释放原因，没有填 FF
14	ProvinceID	3	采集省份，编码见附录 G

实时消息的传输需支持：

1、对同一省份内的多台采集解析设备，支持对实时消息的单点汇聚传输，即面对总部相关消息接收系统，同一个省保持一个实时消息发送IP地址

2、对于利用ESB系统进行实时消息传送的情况，向省份ESB传送实时消息时，可以是多个发送方IP地址。

3.3.3.1.4.3.2.位置类实时消息

序号	字段	字节数	说明
1	Time	8	毫秒数，即将标准 unix 时间转成毫秒，网络字节序，业务发生的时间
2	MSISDN	16	手机号码,不足 16 字节填 0，不包含字冠如+86,0086，86
3	IMEI	16	16 位的 EMEI 号，不足 16 字节填 0
4	IMSI	16	不足 16 字节填 0
5	RAT	1	承载网络：1=3G, 2=2G,6=4G
6	LAC/TAC	2	2/3G 对应 lac，4G 对应 Tac，网络字节序
7	CI/ECI	4	2/3G 对应 ci/sac，4G 对应 eci，网络字节序
8	ServiceType	1	5：位置变化（位置更新、切换、路由区更新、跟踪区更新、IuPS 重定位信令情况时生成该消息）
9	MSC/VLR GT	10	更新后的 MSC GT，没有填 FF
10	RoamType	1	见 A/IuCS 接口话单中的“RoamType” 1=本地用户 2=省内漫游 3=国内漫入 4=国际漫入 5=国内漫出 6=国际漫出 无法判断漫游情况则填 0
11	ProvinceID	3	采集省份，编码见附录 G

实时消息中所有字段的编码采用二进制编码，涉及到用户号码的，编码形式为TBCD编码。

实时消息的传输需支持：

1、对同一省份内的多台采集解析设备，支持对实时消息的单点汇聚传输，即面对总部相关消息接收系统，同一个省保持一个实时消息发送IP地址

2、对于利用ESB系统进行实时消息传送的情况，向省份ESB传送实时消息时，可以是多个发送方IP地址。

3.3.3.2.数据质量保障服务方案

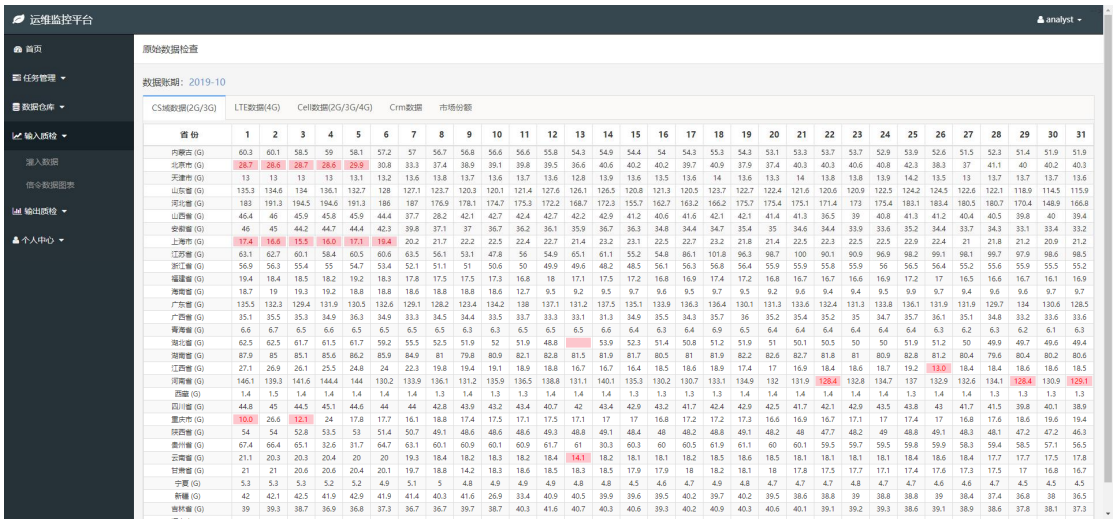
我司在项目服务过程中保障数据一致性；保障信令数据的准确性；保障数据传入与传出的完整性。

每月月中，灌入上月工参数据进行数据量统计。对于工参的检查，主要统计工参总数及2/3/4/5G分类别工参个数及不可使用的工参测试，不可使用的工参定义为经纬度未填或为0的。工参后续进行增量更新，并保存至其他目录中供后续使用。若工参有问题时，将采取多种方式进行工参获取，并做核查，无误后上传平台，对原有工参进行技术修补，从而固化常规数据质量保障流程。以下为数据传输处理、数据质量监控系统监测平台截图：

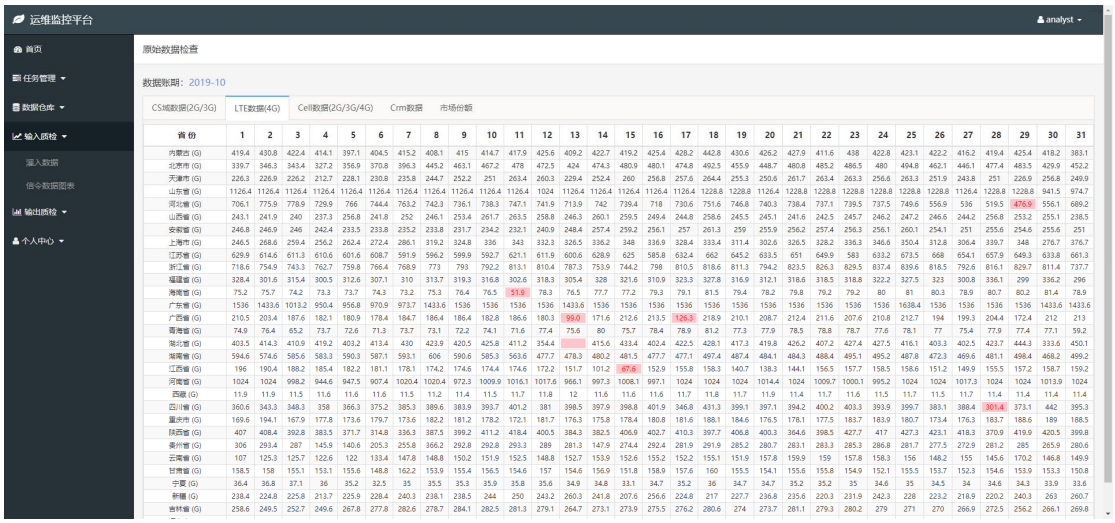
每天18点前原始信令数据传输至信令大数据处理云平台均会进行环比、同比，如发现数据包大小偏差大于10%则触发报警，并在4小时之内进行人口排查解决相关问题。

日传输数据包大小偏差在10%~20%之间为一般问题，解决时间为一个自然日；偏差在20%~40%之间为重大问题，必须进行数据链路、基站工参、原始信令数据采集设备等相关排查、补录数据，解决时间为三个自然日。

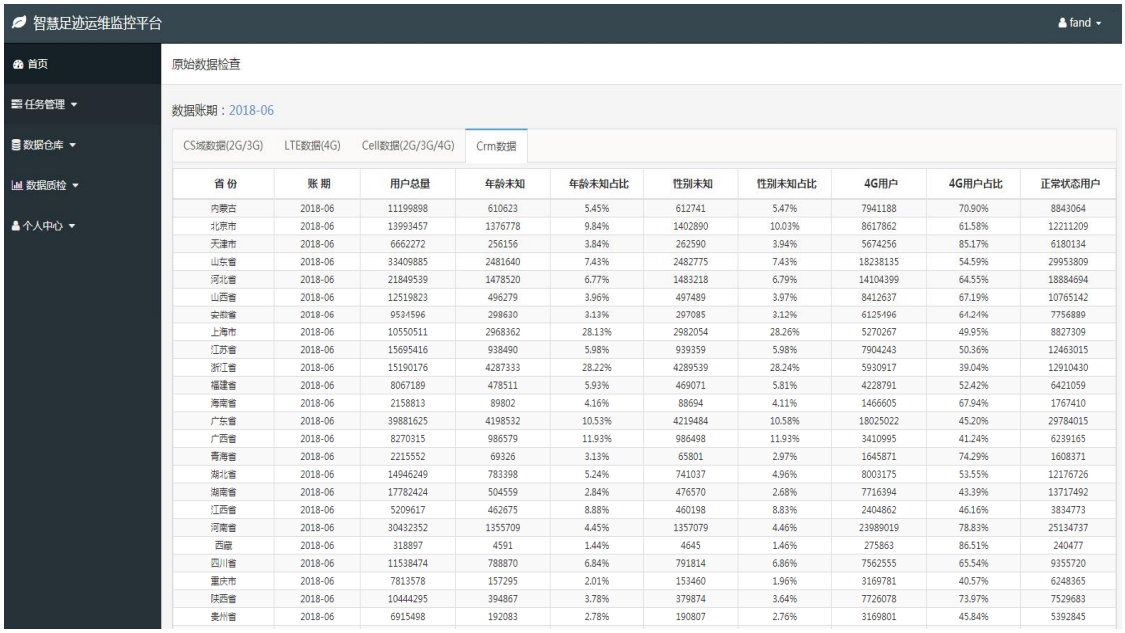
2019 年 10 月全国 CS 域数据



2019 年 10 月全国 LTE 域数据

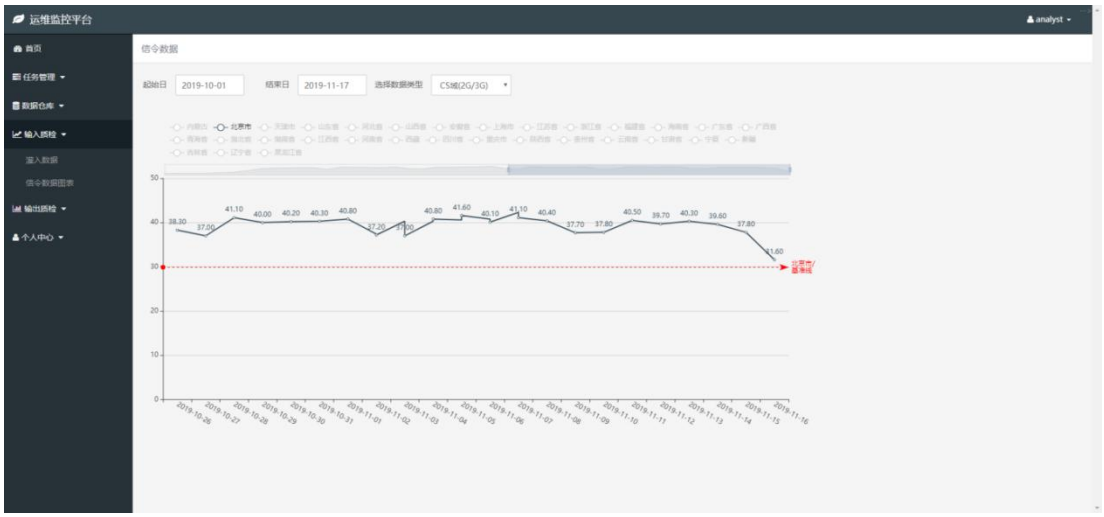


2018 年 6 月全国 CRM 数据

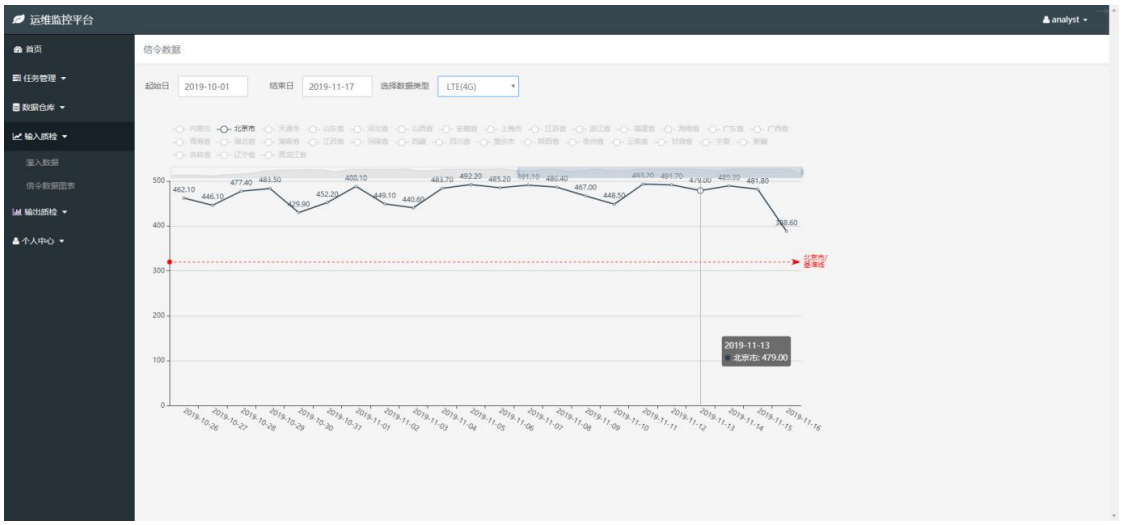


省 份	账 期	用户总量	年龄未知	年龄未知占比	性别未知	性别未知占比	4G用户	4G用户占比	正常状态用户
内蒙古	2018-06	11199898	610623	5.45%	612741	5.47%	7941188	70.90%	8843064
北京市	2018-06	13993457	1376778	9.84%	1402890	10.03%	8617862	61.58%	12211209
天津市	2018-06	6662272	256156	3.84%	262590	3.94%	5674256	85.17%	6180134
山东省	2018-06	33409885	2481640	7.43%	2482775	7.43%	18238135	54.59%	29953809
河北省	2018-06	21849539	1478520	6.77%	1483218	6.79%	14104399	64.55%	18884694
山西省	2018-06	12519823	496279	3.96%	497489	3.97%	8412637	67.19%	10765142
安徽省	2018-06	9534596	299630	3.13%	297085	3.12%	6125496	64.24%	7756889
上海市	2018-06	10550511	2968362	28.13%	2982054	28.26%	5270267	49.95%	8827309
江苏省	2018-06	15695416	938490	5.98%	939359	5.98%	7904243	50.36%	12463015
浙江省	2018-06	15190176	4287333	28.22%	4289539	28.24%	5930917	39.04%	12910430
福建省	2018-06	8067189	478511	5.93%	469071	5.81%	4228791	52.42%	6421059
海南省	2018-06	2158813	89802	4.16%	88694	4.11%	1466605	67.94%	1767410
广东省	2018-06	39881625	4198532	10.53%	4219484	10.58%	18025022	45.20%	29784015
广西省	2018-06	8270315	986579	11.93%	986498	11.93%	3410995	41.24%	6239165
青海省	2018-06	2215552	69326	3.13%	65801	2.97%	1645871	74.29%	1608371
湖北省	2018-06	14946249	783398	5.24%	741037	4.96%	8003175	53.55%	12176726
湖南省	2018-06	17782424	504559	2.84%	476570	2.68%	7716394	43.39%	13717492
江西省	2018-06	5209617	462675	8.88%	460198	8.83%	2404862	46.16%	3834773
河南省	2018-06	30432352	1355709	4.45%	1357079	4.46%	23989019	78.83%	25134737
西藏	2018-06	318897	4591	1.44%	4645	1.46%	275863	86.51%	240477
四川省	2018-06	11538474	788870	6.84%	791814	6.86%	7562555	65.54%	9355720
重庆市	2018-06	7813578	157295	2.01%	153460	1.96%	3169781	40.57%	6248365
陕西省	2018-06	10444295	394867	3.78%	379874	3.64%	7726078	73.97%	7529683
贵州省	2018-06	6915498	192083	2.78%	190807	2.76%	3169801	45.84%	5392845

2019 年 10 月 1 日至 2019 年 11 月 17 日北京 CS 域数据

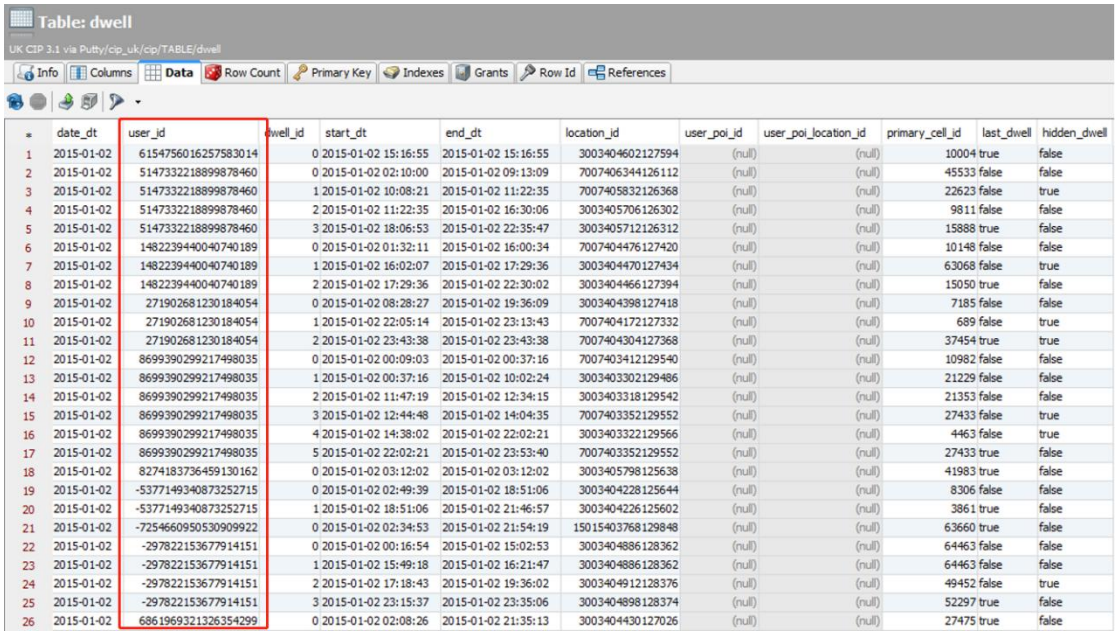


2019 年 10 月 1 日至 2019 年 11 月 17 日北京 LTE 域（4G）数据



3.3.3.3.数据安全性保障方案

北京联通针对用户数据进行严格保密，进行统一脱敏、加密，保障数据的安全性。不提供用户手机号、身份证号、设备号等能代表个人信息的明文数据，采用 MD5 不可逆算法实现用户 ID 加密。



*	date_dt	user_id	dwell_id	start_dt	end_dt	location_id	user_poi_id	user_poi_location_id	primary_cell_id	last_dwell	hidden_dwell
1	2015-01-02	61547560162575830 14	0	2015-01-02 15:16:55	2015-01-02 15:16:55	3003404602127594	(null)	(null)	10004	true	false
2	2015-01-02	51473322188998784 60	0	2015-01-02 02:10:00	2015-01-02 09:13:09	7007406344126112	(null)	(null)	45533	false	false
3	2015-01-02	51473322188998784 60	1	2015-01-02 10:08:21	2015-01-02 11:22:35	7007405832126368	(null)	(null)	22623	false	true
4	2015-01-02	51473322188998784 60	2	2015-01-02 11:22:35	2015-01-02 16:30:06	3003405706126302	(null)	(null)	9811	false	false
5	2015-01-02	51473322188998784 60	3	2015-01-02 18:06:53	2015-01-02 22:35:47	3003405712126312	(null)	(null)	15888	true	false
6	2015-01-02	14822394400407401 89	0	2015-01-02 01:32:11	2015-01-02 16:00:34	7007404476127420	(null)	(null)	10148	false	false
7	2015-01-02	14822394400407401 89	1	2015-01-02 16:02:07	2015-01-02 17:29:36	3003404470127434	(null)	(null)	63068	false	true
8	2015-01-02	14822394400407401 89	2	2015-01-02 17:29:36	2015-01-02 22:30:02	3003404466127394	(null)	(null)	15050	true	false
9	2015-01-02	27190268123018405 4	0	2015-01-02 08:28:27	2015-01-02 19:36:09	3003404398127418	(null)	(null)	7185	false	false
10	2015-01-02	27190268123018405 4	1	2015-01-02 22:05:14	2015-01-02 23:13:43	7007404172127332	(null)	(null)	689	false	true
11	2015-01-02	27190268123018405 4	2	2015-01-02 23:43:38	2015-01-02 23:43:38	7007404304127368	(null)	(null)	37454	true	true
12	2015-01-02	86993902992174980 35	0	2015-01-02 00:09:03	2015-01-02 00:37:16	7007403412129540	(null)	(null)	10982	false	false
13	2015-01-02	86993902992174980 35	1	2015-01-02 00:37:16	2015-01-02 10:02:24	3003403302129486	(null)	(null)	21229	false	false
14	2015-01-02	86993902992174980 35	2	2015-01-02 11:47:19	2015-01-02 12:34:15	3003403318129542	(null)	(null)	21353	false	false
15	2015-01-02	86993902992174980 35	3	2015-01-02 12:44:48	2015-01-02 14:04:35	7007403352129552	(null)	(null)	27433	false	true
16	2015-01-02	86993902992174980 35	4	2015-01-02 14:38:02	2015-01-02 22:02:21	3003403322129566	(null)	(null)	4463	false	true
17	2015-01-02	86993902992174980 35	5	2015-01-02 22:02:21	2015-01-02 23:53:40	7007403352129552	(null)	(null)	27433	true	false
18	2015-01-02	82741837364591301 62	0	2015-01-02 03:12:02	2015-01-02 03:12:02	3003405798125638	(null)	(null)	41983	true	false
19	2015-01-02	-53771493408732527 15	0	2015-01-02 02:49:39	2015-01-02 18:51:06	3003404228125644	(null)	(null)	8306	false	false
20	2015-01-02	-53771493408732527 15	1	2015-01-02 18:51:06	2015-01-02 21:46:57	3003404226125602	(null)	(null)	3861	true	false
21	2015-01-02	-72546609505309099 22	0	2015-01-02 02:34:53	2015-01-02 21:54:19	150154037681298 48	(null)	(null)	63660	true	false
22	2015-01-02	-29782215367791415 1	0	2015-01-02 00:16:54	2015-01-02 15:02:53	3003404886128362	(null)	(null)	64463	false	false
23	2015-01-02	-29782215367791415 1	1	2015-01-02 15:49:18	2015-01-02 16:21:47	3003404886128362	(null)	(null)	64463	false	false
24	2015-01-02	-29782215367791415 1	2	2015-01-02 17:18:43	2015-01-02 19:36:02	3003404912128376	(null)	(null)	49452	false	true
25	2015-01-02	-29782215367791415 1	3	2015-01-02 23:15:37	2015-01-02 23:35:06	3003404898128374	(null)	(null)	52297	true	false
26	2015-01-02	68619693212363542 99	0	2015-01-02 02:08:26	2015-01-02 21:35:13	3003404430127026	(null)	(null)	27475	true	false

加密传输

1）数据访问控制

用户管理和授权机制，能够提供面向角色的用户操作行为授权和管理范围授权。系统提供用户日志记录功能。从用户登录系统至用户退出系统中的所有操作内容、操作时间、登录终端地址等都会被详细记录。系统还提供了日志查询统计功能，以便在必要时及时搜索到有用的审计信息。除了应用软件层面的安全访问控制外，系统还可以借助成熟的操作系统和

数据库系统安全访问控制机制保证所有对操作系统和数据库的访问和操作都是得到授权的。利用移动机房进出管理制度和相关技术手段，保证物理安全。

2）数据加密传输

传输文件加密：基于 openssl 网络通信安全及数据完整性协议，实现基本的传输层资料加密功能。把明码的话单文件用加密算法转换成加密的文件以实现数据的保密，加密的过程需要用到密钥来加密数据然后再解密。没有密钥，就无法解开加密的数据。

3）数据存储加密

针对敏感数据的存储，采用可逆加密算法进行存储，同时定期更换加密密钥。

管理维护权限控制

提供用户权限管理，其权限设置分角色、用户、权限管理；针对敏感功能，其查询、保存、定制、配置、删除等均为权限分配单元；系统提供新增用户、修改用户信息和删除用户的操作功能；针对角色管理，系统提供角色新增、修改和删除操作功能，并提供角色赋权功能。

系统能对用户名密码的设置进行限制，符合密码复杂度和密码生存期限限制。口令至少由 8 位及以上大小写字母、数字及特殊符号等混合、随机组成，密码生存期限可配置。

1）帐号

系统支持自动的帐户密码策略，实现对密码长度，复杂度，可用时间，修改频度等参数的控制，并根据配置实现对用户修改密码等账户管理行为的自动控制，并留下日志记录，便于审计。

2）权限

系统可以通过功能控制点和角色的方式来实现权限控制。权限按照最小化权限的原则，尽量实现细粒度划分，除一般的系统登录、目录访问、文件操作之外还实现模块、进程操作级别的权限控制，并进行日志记录。

3）角色

由若干功能控制点构成一定的操作权限定义为角色。角色是系统用户操作类型的集合。

4）接口安全

系统的客户端及主机进行通信时，使用安全接口或进行加密，保证信息不被窃取及篡改，并增加客户端及主机之间的认证信息，对客户端及主机身份进行校验，禁止未经允许的客户端或假冒客户端访问系统，防止认证平台受到攻击。

系统建设时，仅仅允许与存在明确互联需求的系统互联，系统验收时需建立细化到连接双方的 IP、端口、承载信息、信息敏感性等内容在内的网络连接信息表。

任何业务接口（包括 FTP、webservice 等）采取认证手段，防止未授权的业务连接，用户名密码复杂度满足公司安全要求，不得写死到程序中，可以在需要时进行修改。

在跨网络传送客户信息等敏感数据时，不得使用协议的默认端口，采取 1024 以上的端口传送。

5）端口管理

加强工程建设期间对设备服务端口管理，每一个端口用途有明确说明，对于无用的端口要关闭。项目验收时提供确切的项目端口与服务列表。不是给用户提供服务的对外开放服务端口，使用 1024 以上的端口。禁止使用默认端口。

3.3.3.4.数据校核服务方案

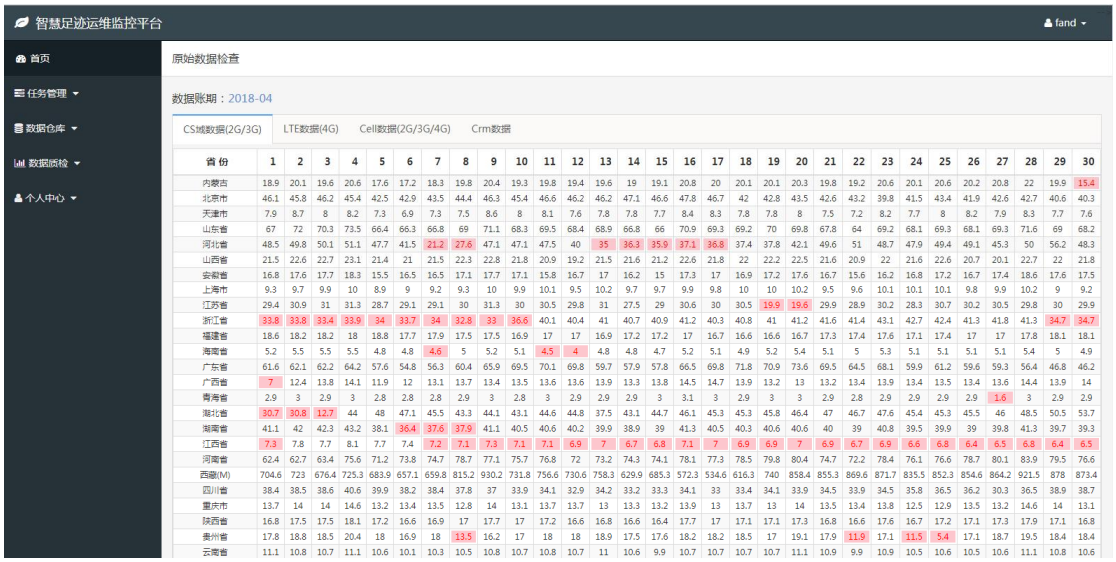
我司对输出的各项人口监测指标提供数据校核服务，并提供对异常情况修正的服务。

通过信令数据监测平台可查看北京市数据已经导入并正常进行处理，在数据处理过程中实现监测，如发下问题及时调整优化，保证数据结果的准确性。

在信令数据处理过程中如发现数据异常出发报警，并在 4 小时之内进行人口排查解决相关问题。

与历史数据相比异常幅度高于 10%为一般问题，解决时间为一个自然日；高于 20%为重大问题，必须进行数据资源、模型代码、口径定义等相关排查，解决时间为三个自然日。

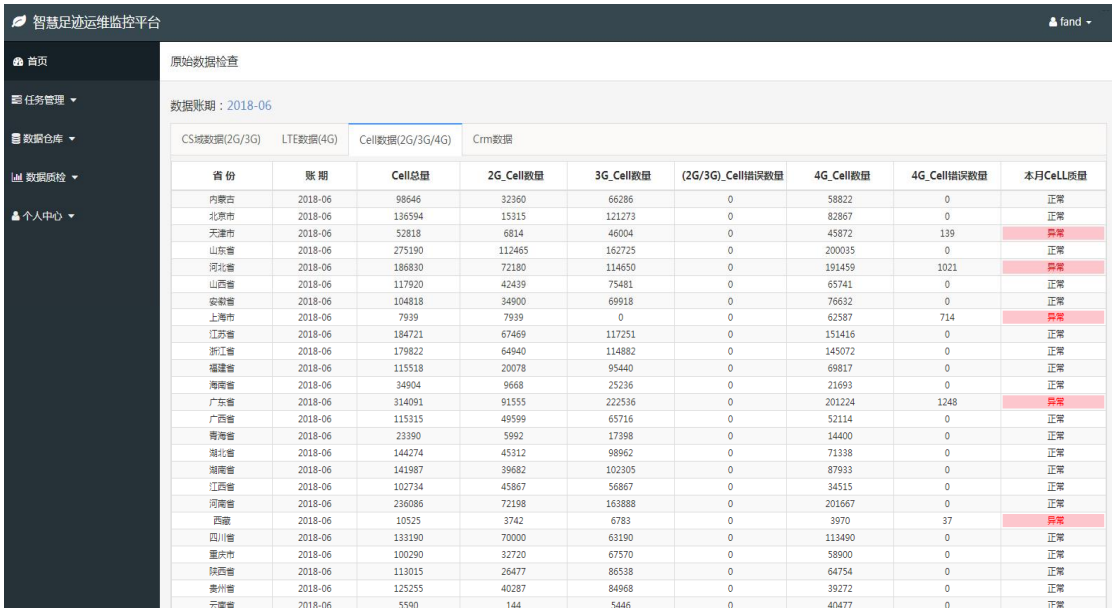
每日对前一日信令数据进行检查，检查内容为数据的容量大小值，并对检查内容进行留存。信令检查包含对 2/3/4/5G 信令检查等部分。若某省信令数据量低于阈值，该日的单元格将突出显示。



手机信令数据校验图

（2）基站工参、CRM 数据校验

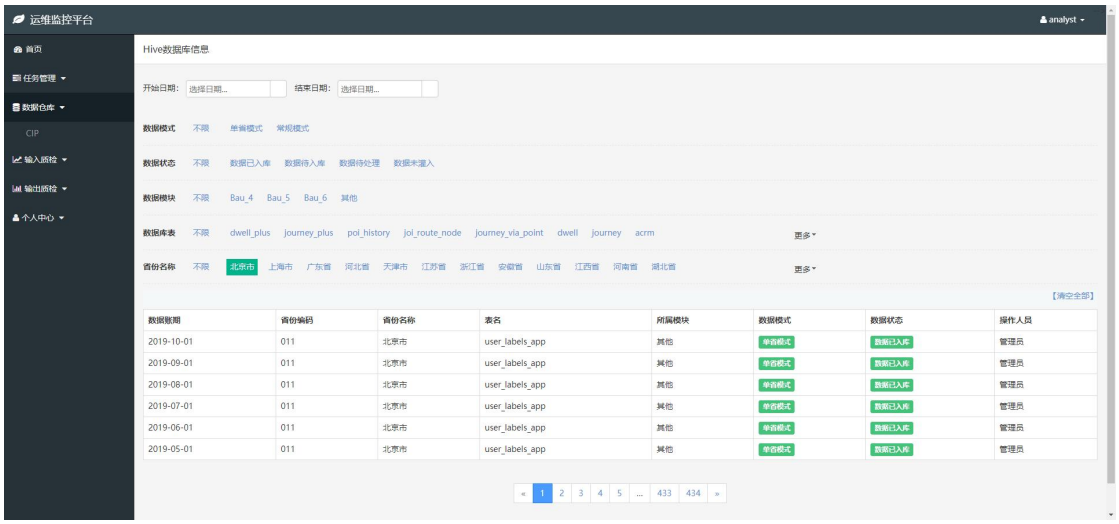
每月月中，灌入上月 CRM 和工参数据，对于 CRM 数据，主要进行数据量统计。对于工参的检查，主要统计工参总数及 2/3/4/5G 分类别工参个数及不可使用的工参测试，不可使用的工参定义为经纬度未填或为 0 的。工参后续进行增量更新，并保存至其他目录中供后续使用。若工参有问题时，将采取多种方式进行工参获取，并做核查，对原有工参进行技术修补。



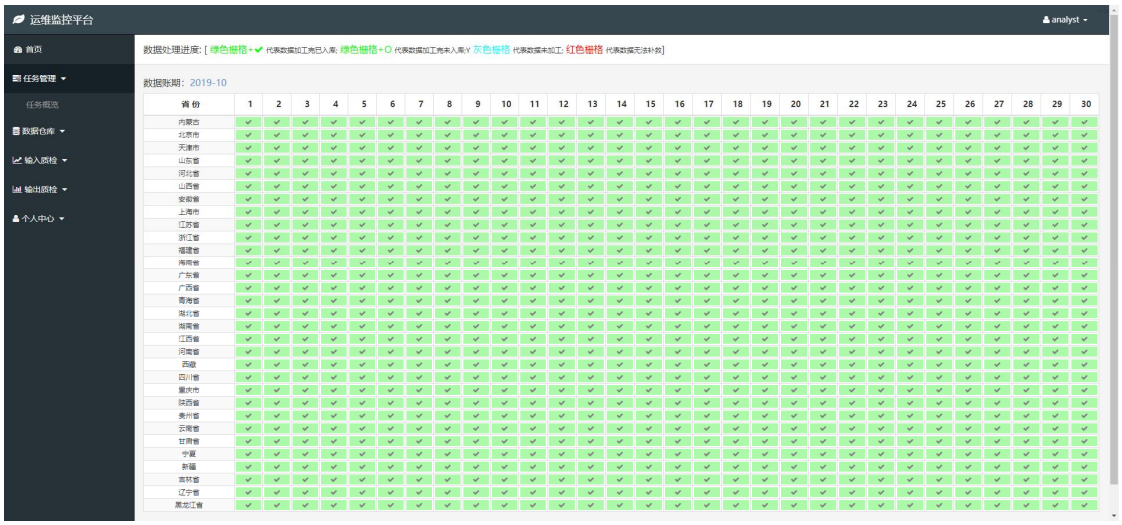
省 份	账 期	Cell总量	2G_Cell数量	3G_Cell数量	(2G/3G)_Cell错误数量	4G_Cell数量	4G_Cell错误数量	本月CeLL质量
内蒙古	2018-06	98646	32360	66286	0	58822	0	正常
北京市	2018-06	136594	15315	121273	0	82867	0	正常
天津市	2018-06	52818	6814	46004	0	45872	139	异常
山东省	2018-06	275190	112465	162725	0	200035	0	正常
河北省	2018-06	186830	72180	114650	0	191459	1021	异常
山西省	2018-06	117920	42439	75481	0	65741	0	正常
安徽省	2018-06	104818	34900	69918	0	76632	0	正常
上海市	2018-06	7939	7939	0	0	62587	714	异常
江苏省	2018-06	184721	67469	117251	0	151416	0	正常
浙江省	2018-06	179822	64940	114882	0	145072	0	正常
福建省	2018-06	115518	20078	95440	0	69817	0	正常
海南省	2018-06	34904	9668	25236	0	21693	0	正常
广东省	2018-06	314091	91555	222536	0	201224	1248	异常
广西省	2018-06	115315	49599	65716	0	52114	0	正常
青海省	2018-06	23390	5992	17398	0	14400	0	正常
湖北省	2018-06	144274	45312	98962	0	71338	0	正常
湖南省	2018-06	141987	39682	102305	0	87933	0	正常
江西省	2018-06	102734	45867	56867	0	34515	0	正常
河南省	2018-06	236086	72198	163888	0	201667	0	正常
西藏	2018-06	10525	3742	6783	0	3970	37	异常
四川省	2018-06	133190	70000	63190	0	113490	0	正常
重庆市	2018-06	100290	32720	67570	0	58900	0	正常
陕西省	2018-06	113015	26477	86538	0	64754	0	正常
贵州省	2018-06	125255	40287	84968	0	39272	0	正常
云南省	2018-06	5590	144	5446	0	40477	0	正常

基站工参、CRM 数据校验图

通过信令数据监测平台可查看北京市数据已经导入并正常进行处理。



数据账期	省份编码	省份名称	表名	所属模块	数据模式	数据状态	操作人员
2019-10-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员
2019-09-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员
2019-08-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员
2019-07-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员
2019-06-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员
2019-05-01	011	北京市	user_labels_app	其他	单省模式	数据已入库	管理员



根据北京每天的信令数据建模分析用户驻留的数据结果监测发现十一期间用户驻留相比较上月同时有偏差。

点击时间查看北京市 16 城区这天信令数据的用户驻留信息，发现集中在石景山区、顺义区、昌平区这三个行政区。数据分析师会对这三个行政区重点进行原始信令数据传输、工参数据排查，如发现问题及时做数据补录、修正，如没有问题则查看真是情况是否人员增加或减少，并作详细说明。

3.3.3.5.应急支撑响应方案

对于应急支撑响应要求，我司提供应急支撑服务，针对临时性报告、紧急数据报告等紧急工作任务提供服务，对紧急数据及时响应提供：

1）在原有监测指标的基础上增加监测区域、基于现有的监测指标数据出具分析报告等；可实现 24 小时内响应；

2）新增监测指标（包括新指标新区域）、或在新指标的基础上出具分析报告，结合需求复杂度评估。

3.3.4.本项目交付成果方案

我司提供连续 12 个月的数据监测和分析服务。

（1）按月进行月报数据分析服务提交上月的月报数据，涉及朝阳区、区内 43 个街乡镇、81 个重点监测区、50 个重点村，12 个商圈、24 个景区及临时新增区域，内容主要包括：人口规模、人口流动人口特征、职住流向等相关监测指标。

（2）次月 10 日前完成人口监测的结果数据情况分析，并提供数据分析结果集。

统计颗粒度	统计指标	统计口径	统计区域
实时	实时人流量	每 30 分钟间隔步进进行统计，统计在每个区域下的人	朝阳区、43 街乡、81 重点区域

	瞬时人口流入流出	用当前加工后的数据集与30分钟前的数据集取差集； 1. 当前数据集包含，30分钟前的数据集不包含的为流入用户，当前数据集中流入用户的所在地为流入区域，统计流入区域的流入用户人数。 2. 当前数据集不包含，30分钟前的数据集包含的为流出用户，30分钟前的数据集中流出用户的所在地为流出区域，统计流出区域的流出用户人数。	朝阳区、43街乡、81个重点区域、50个重点村
	商圈实时客流量	每30分钟间隔步进进行统计，统计在每个商圈区域下的人数	12个商圈
	景区实时客流量	每30分钟间隔步进进行统计，统计在每个景区区域下的人数	24个旅游景区
日度	商圈客流停留时长	统计每天在商圈区域不同停留时长的用户人数	12个商圈
	商圈客流日流量	统计每天在各商圈区域客流的总人数	12个商圈
	景区游客停留时长	统计每天在景区区域不同停留时长的用户人数	24个旅游景区
	景区游客日流量	统计每天在各景区区域出现过的游客总人数	24个旅游景区
月度	居住人口	用户21点-7点（第二天）在某区域停留时长超过360分钟的区域为该用户的日居住地，取一个月内用户停留最多的日居住地为该用户的月居住地，统计月居住地区域下的居住人数。	朝阳区、43街乡、81个重点区域
	工作人口	用户7点-19点在某区域停留超过480分钟的区域为该用户的日工作地，取一个月内用户停留最多的日工作地为该用户的月工作地，统计月工作地区域的工作人数。	朝阳区、43街乡、81个重点区域
	职住OD	用户7点-19点在某区域停留超过480分钟的区域为该用户的日工作地，21点-7点（第二天）在某区域停留时长	朝阳区、43街乡、81个重点

		超过 360 分钟的区域为该用户的日居住地。取一个月内用户累计停留最多的日工作地居住地为该用户的月工作居住地，统计不同的月工作地居住地之间的职住人数	区域
	居住用户流入流出明细	用当前月居住用户明细的数据集与上个月的月居住用户明细数据集取差集； 1. 当月数据集包含，上月的数据集不包含的为流入居住用户，当月数据集中流入居住用户的所在地为流入区域，统计流入区域的流入居住用户人数。 2. 当月数据集不包含，上月的数据集包含的为流出居住用户，上月的数据集中流出用户的所在地为流出区域，统计流出区域的流出居住用户人数。	朝阳区、43 街乡、81 个重点区域
	工作用户流入流出明细	用当前月工作用户明细的数据集与上个月的月工作用户明细数据集取差集； 1. 当月数据集包含，上月的数据集不包含的为流入工作用户，当月数据集中流入工作用户的所在地为流入区域，统计流入区域的流入工作用户人数。 2. 当月数据集不包含，上月的数据集包含的为流出工作用户，上月的数据集中流出用户的所在地为流出区域，统计流出区域的流出工作用户人数。	朝阳区、43 街乡、81 个重点区域
	居住人口归属地	用户 21 点-7 点（第二天）在某区域停留时长超过 360 分钟的区域为该用户的日居住地，取一个月内用户停留最多的日居住地为该用户的月居住地，统计月居住地区域下不同号段归属地的居住人数	朝阳区、43 街乡、81 个重点区域

3.3.4.1.项目服务周期

项目服务期限满足采购文件要求，项目服务期限为2026年9月25日-2027年9月24日。

项目进度安排：

（1）合同签订之日起15日内，完成需求调研分析和手机信令人口数据制作技术规定编制工作。

（2）合同签订之日起1个月内，出具朝阳区大数据人口动态监测相关数据集，并每月更新。

（3）项目服务期限截止1个月内，完成所有人口动态监测大数据制作工作，进行项目验收。

3.3.4.2.朝阳区街乡镇清单

朝阳区全区及43个街乡镇清单如下：

	areaid	areaname	parentid	areatype
1大区 43街道	110105	朝阳区	110	3
	110105001	建外街道	110105	4
	110105002	朝外街道	110105	4
	110105003	呼家楼街道	110105	4
	110105004	三里屯街道	110105	4
	110105005	左家庄街道	110105	4
	110105006	香河园街道	110105	4
	110105007	和平街街道	110105	4
	110105008	安贞街道	110105	4
	110105009	亚运村街道	110105	4
	110105010	小关街道	110105	4
	110105011	酒仙桥街道	110105	4
	110105012	麦子店街道	110105	4
	110105013	团结湖街道	110105	4
	110105014	六里屯街道	110105	4

	110105015	八里庄街道	110105	4
	110105016	双井街道	110105	4
	110105017	劲松街道	110105	4
	110105018	潘家园街道	110105	4
	110105019	垡头街道	110105	4
	110105021	南磨房乡	110105	4
	110105022	高碑店乡	110105	4
	110105023	将台乡	110105	4
	110105024	太阳宫乡	110105	4
	110105025	大屯街道	110105	4
	110105026	望京街道	110105	4
	110105027	小红门乡	110105	4
	110105028	十八里店乡	110105	4
	110105029	平房乡	110105	4
	110105030	东风乡	110105	4
	110105031	奥运村街道	110105	4
	110105032	来广营乡	110105	4
	110105033	常营民族乡	110105	4
	110105034	三间房乡	110105	4
	110105035	管庄乡	110105	4
	110105036	金盏乡	110105	4
	110105037	孙河乡	110105	4
	110105038	崔各庄乡	110105	4
	110105039	东坝乡	110105	4
	110105040	黑庄户乡	110105	4
	110105041	豆各庄乡	110105	4
	110105042	王四营乡	110105	4
	110105043	东湖街道	110105	4

	110105400	首都机场街道	110105	4

3.3.4.3.重点区域清单

朝阳区 81 个重点区域清单如下：

表 人口大数据 81 个监测重点区域范围

81 个重点和个性化区域		
CBD 核心区	原管庄乡-郭家场村	十八里店乡-十八里店村
CBD 中心区	原管庄乡-咸宁侯村	原石各庄村
奥林匹克公园	原管庄乡-小寺村	首都儿科研究所附属儿童医院
奥林匹克森林公园-北园	广渠快速路	首都经济贸易大学
奥林匹克森林公园-南园	合生汇中心	四海官鑫日用品市场
奥林匹克森林公园-廉洁奥运主题文化园	黑桥公园	四合庄村
奥林匹克公园中心区	定辛庄安置房区域	松榆里市场
北京盛华宏林批发市场	弘善家园	孙河乡地区
北京第二外国语学院	原花车展览区域	天丰利生活用品市场
北京工业大学	温榆河公园区域温榆河公园（原黄港片区）	规划绿地（市场群已疏解）
北京望京医院	金瀛农贸市场	望京电子城西区北扩
北京朝阳医院	来广营村	萧太后河滨水绿色休闲廊道
北郎东	来广营乡城锦苑小区	小红门乡 65 号院
长安街沿线二	原奶西村	亚星香园农副产品市场
长安街沿线一	南磨房乡-广华新城	国家文创实验区（CBD-定福庄国际传媒走廊）
大柳树市场	农光里农贸市场	育慧南路及周边
大望京	农展北路集贸市场	朝京金旭菜市场
大洋路农副产品市场	潘家园旧货市场	朝阳公园

道尔泰农贸市场	平房乡-平房村	原朝阳区-崔各庄乡-南皋村
原定辛庄东村	温榆河公园（原前苇沟片区）	原朝阳区-黑庄户乡-定辛庄西村
东坝乡欣和园小区	三里屯	原朝阳区-黑庄户乡-苏坟村
豆各庄乡青荷里南山园小区	温榆河公园（原沙子营片区）	中国传媒大学
对外经济贸易大学	温榆河公园（原上辛堡片区）	中国科技馆
垡头街道双合家园小区	芍药居北里	中国医学科学院肿瘤医院
高碑店乡泰和园小区	原十八里店十里河市场一条街市场群	中日友好医院
国家会议中心	国家体育馆	国家游泳中心
香江北岸	国家速滑馆	中国残疾人体育运动管理中心

3.3.4.4.重点村清单

朝阳区 50 个重点村清单如下：

表 人口大数据 50 个重点村范围

50 个重点村		
四合庄村	万子营东村	皮村
何各庄村	大鲁店一村	西村
马泉营村	原定辛庄东村	小店村
草场地村	原定辛庄西村	来广营村
东辛店村	原黑庄户村	新生村
费家村	郎各庄村	原平房村
奶东村	郎辛庄村	原石各庄村
原南皋村	双树北村	三间房西村
豆各庄村	双树南村	原横街子村
六里屯村	原苏坟村	老君堂村
八里庄村	万子营西村	原吕家营村

司辛庄村	小鲁店村	原西直河村
原郭家场村	幺铺村	小武基村
原咸宁侯村	东村	原孛罗营村
大鲁店二村	东窑村	观音堂村
大鲁店三村	黎各庄村	南花园村
王四营村	原肖村	

3.3.4.5.重点商圈及景区清单

朝阳区 12 个商圈、24 个景区清单如下：

表 人口大数据监测商圈范围

	areaid	areaname	parentid	areatype
12 个商圈	110105901	CBD 商圈	110105003	9
	110105902	三里屯商圈	110105004	9
	110105903	亚奥商圈	110105031	9
	110105904	朝青商圈	110105015	9
	110105905	燕莎商圈	110105012	9
	110105906	望京商圈	110105026	9
	110105907	双井商圈	110105016	9
	110105908	太阳宫商圈	110105024	9
	110105909	朝外商圈	110105002	9
	110105910	常营商圈	110105033	9
	110105911	东坝商圈	110105039	9
	110105912	蓝色港湾	110105012	9

表 人口大数据监测景区范围

24 个旅游景区

奥林匹克森林公园	兴隆公园	京城梨园景区
朝阳公园	将府公园	北京蓝调庄园
奥林匹克公园	大望京公园	国家体育场（鸟巢）
日坛公园	庆丰公园	北京欢乐谷
团结湖公园	北小河公园	蟹岛绿色生态农庄
红领巾公园	四得公园	中国紫檀博物馆
北京蓝色港湾	白鹿公园	中华民族园
古塔公园	斯普瑞斯奥莱旅游商业文化体验区	温榆河公园

本项目我司严格按照行政区进行划分，根据行政区域经纬度坐标实现边界测绘，并充分考虑测绘区域内覆盖的基站数量等情况，对测绘区域进行微调，以保证人口统计的准确性。项目服务过程中重点和个性化区域根据实际情况进行调整，监测数量不少于 81 个。

3.3.5.数据服务的性能需求方案

我司满足项目对数据实时性和准确性的要求，对数据服务的性能需求如下：

1. 实时数据接口传送频率不低于计划内时间，如每 30 分钟一次的接口数据，在本 30 分钟内完成传送。

2. 日度人口统计数据分析结果集在 t+3 日前完成统计。

3. 月度人口统计数据分析结果集在次月 10 日前完成统计。

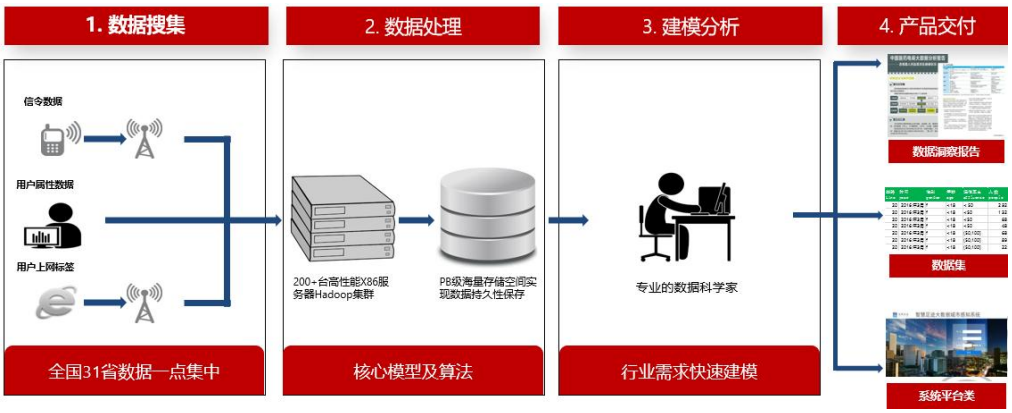
3.3.5.1.数据处理平台介绍

中国联通大数据处理平台底层采用基于 Hadoop 架构的 Spark 集群的先进大数据处理框架，搭建全国信令数分析处理的云计算平台，保证北京信令数据处理所需的计算资源、存储资源同时提供对计算云平台存储服务、计算服务以及应用服务的运行监控和管理服务等。满足对于原始信令数据采集和加工处理要求，我司需按日对 SIM 卡原始信令数据进行采集、清洗、脱敏、降噪、关联等加工处理和计算。

平台采用三层技术架构：

- 数据获取层：主要完成中国联通信令数据的接入、脱敏和清洗，以及不同来源数据（信令数据、基站工参等）之间的数据关联处理工作；
- 数据转换层：主要基于数据仓库，通过大数据模型的 6 轮 BAU 处理，将历史信令数据聚合计算为网格化标签数据，以及基于 GIS 数据的路径拟合、基于预测算法的趋势分析等多种数据挖掘分析处理；
- 数据消费层：对于数据转换层产出的数据结果，提供外部 API 访问、可视化平台展现和地图服务等多角度、多场景的应用

3.3.5.2.数据处理流程介绍



对应平台技术架构，数据处理和应用分析流程包括五个步骤：

●数据收集：数据来源包括手机信令数据、基站工参数据、以及用户属性数据和用户上网标签数据等。信令数据包括 CS 域信令数据和 PS 域信令数据，均为记录级脱敏

数据。

●降噪及加工：Spark 下的数据加工处理。清洗信令数据中的噪声，将信令数据和基站工参进行关联从而获得信令产生位置；分析数据质量；通过平台独有算法跑出以250m*250m 网格为单位区域的位置标签数据和其他相关联的属性标签数据。

●数据存储：采用数据仓库多维模型存储产出的标签数据，OLAP 模型便于数据的快速查询和主题扩展。

●建模分析：由分析师完成。主要工作为：对平台产出数据进行初加工和扩样；根据统计区域在 GIS 上绘制分析范围；筛选区域内的基站及网格；根据需求和条件进行数据分析工作和结果验证工作。

●产品交付：分析师按需提交的脱敏数据集和区域洞察报告。软件开发工程师将数据封装为接口数据文件供 API 调用。

3.3.6.数据服务的系统安全性能方案

为满足数据服务的安全性，要求系统平台在专网进行网络传输，只能传输统计级数据，并在数据传输过程中全程进行数据加密，以保证关键数据在传输过程中不被监听，避免敏感数据外泄，避免被未授权者操控。对数据服务的系统安全性能需求如下：

应用安全：应用系统应具有认证功能，以鉴别用户身份并验证。用户管理、权限管理应充分利用操作系统和数据库的安全性，软件运行时须有完整的日志记录，不允许以明文方式保存用户密码或系统使用的各类密码。

数据安全：保证数据库和其它文件只能被授权用户和播控终端访问，防止在本地存储或者网络传输的数据受到非法篡改、删除和破坏。

网络安全:系统应支持访问控制、安全检测、攻击监控等一系列安全功能，应提供完整的网络安全监控、报警和故障处理功能。

传输数据均需要经过安全网关，支持 word 文件、excel 报表、csv 等多类型数据，经安全网关统一输出。并对接口进行审计，保障接口数据输出的安全。及时发现敏感数据泄露风险，在保证数据合理合规交互的同时，进一步加强数据安全的保护。项目实施过程中满足相关数据安全法要求。

国务院《促进大数据发展行动纲要的通知》将网络和大数据安全保障作为十大工程之一，明确要求健全大数据安全保障与评估体系，强化安全支撑，在数据采集、业务开发及系统集成等各个阶段均有专门针对数据安全的技术方案，最大程度的保障数据安全，实现多方共赢。

（1）数据对接阶段：

- 运营商数据不出局，所有的数据和分析平台均在运营商内部，仅对外提供数据结果，客户要求提供数据，数据处理平台使用运营商内部资源，随时监控
- 数据加密脱敏，原始信令加密，手机号、IMEI 加密
- 数据严格审计，对输出至客户侧的信令数据严控输出范围，对输出至分析平台数据进行抽查

（2）业务开发阶段：

- 针对个人的服务必须首先遵守运营商相关个人隐私规定，明确此类合作开展的原则
- 管控合作，考虑到数据敏感性，严格审核客户和外部合作客户的外资、行业背景

（3）系统集成阶段：

- 内容安全：设计清晰的应用安全架构，对发布的内容信息将进行合规性检查，并对发布权限管理，防篡改、定期巡检等进行一下安全管理。
- 网络安全：采用应用服务器与数据库分开部署，从而保障数据安全，服务器具备硬件防火墙，应用系统已关闭与业务无关的服务和端口，实现服务端口最小化。

3.3.6.1.安全管理措施

3.3.6.1.1.应用系统安全管理

此系统具备完善的安全管理设置，如下：

✓系统内置完善的用户权限管理机制，根据角色定义分为主任、管理员、普通用户三个级别，不同用户级别有不同的操作权限，可针对各个应用模块进行分别设置访问权限。

✓只有主任级别可以添加删除用户，授予用户权限。

✓系统登录要求用户名、密码验证，密码长度要求 6 位以上，并且强制要求定期修改。

✓系统可设置对于要查询用户号码的黑白名单机制，黑白名单机制与用户权限机制互相配合，比如：

●主任级别用户不受黑白名单限制

●管理员级别用户对于处于黑名单中的用户信息禁止查询详细信令消息及呼叫记录，

●普通用户对于所有用户信令消息及呼叫记录的查询都受限。

✓系统内置完善的用户日志管理机制，可针对用户使用系统的所有行为进行日志记录，并可后续查询检索。日志的内容包括但不限于：用户名、登陆时间、使用功能模块、使用功

能模块时间、ＩＰ地址、查询的用户号码，操作行为等

3.3.6.1.2.数据安全方案

随着近年来互联网的迅猛发展，各企业网络规模日益扩张，众多分支机构的不断接入，企业的发展对信息化网络的需求也在不断地增加。然而，伴随着网络规模的扩张，网络用户数的膨胀，互联网络的网络环境开始变得不安定：病毒泛滥成灾；网络攻击猖獗；黑客无孔不入；垃圾邮件成堆；用户电脑行政管理越来越繁琐。由于管理手段和措施的缺乏，企业网络的的网管人员也力不从心，网络用户大部分情况下还不知情，首先成为不安定的网络环境的受害者，继而变成网络环境的破坏者。

网络病毒、网络攻击、黑客行为等破坏行为大多是利用了操作系统或者应用程序的系统安全漏洞，Windows 平台的各种漏洞很多，用户大都是使用 Windows 平台上网。解决系统漏洞的问题，计算机的安全问题解决了 50%，另外的 50%直接与用户行为相关，得依靠相关工具协助。

此系统因为涉及到大量的用户业务和位置信息等隐私数据，并且与外部系统的互联互通非常开放，所以良好的系统安全方案是系统搭建的必要前提。

3.3.6.1.3.数据安全建设原则

以“统一规划、重点明确、合理建设、逐步强化”为基本指导原则。

全面规划逐步实施原则

安全保密系统的建设，必须从一个完整的网络系统体系结构出发，全方位、多层次的综合考虑信息网络的各种实体和各个环节，运用信息系统工程的观点和方法论进行统一的、整体性的设计，将有限的资源集中解决最紧迫问题，为后继的安全实施提供基础保障，从解决主要的问题入手，伴随信息系统应用的开展，逐步提高和完善信息系统建设。

适度安全原则

在安全保密系统的建设中，要尽量考虑安全机制的合理性，对重点信息资源，一定要实现重点保护。在保证安全的前提下，应尽量减少安全机制的规模和复杂性，使之具有可操作性，避免因过于复杂而导致安全措施难以执行。

经济合理原则

安全保障系统的建设，要以实际安全保密需求作为设计依据，在不影响安全保密效果的前提下，应尽可能体现经济性原则，特别加强对安全保密重点部位的保护，使有限的资源发挥重要的作用，使最小的投入获取最大的效益。

保障系统运行性能

安全保障系统应最大限度地服务于系统业务的高效运行，要最大限度保护系统的可靠

性、稳定性、可用性；保证数据流动的真实性；保证访问者身份的真实性；保证数据交互和访问的合法性。

技术与管理相结合

任何一个信息系统的安全，都包括了产品、过程、人等多方面因素，必须在考虑技术解决方案的同时，充分考虑法律、法规、管理等方面的制约和调控作用，坚持技术和管理相结合。

安全子系统可扩展性

随着技术发展和网络应用的开展，系统必然面临着不断改进、扩展的需求。在安全保密建设过程中，必须考虑到信息系统应用及安全需求的扩展，安全保密系统应具有较强的扩充、升级兼容能力，以满足业务高速发展的需要。

3.3.6.1.4.网络连接和防火墙设置

整个系统分为底层数据接口平台，上层应用平台，用户访问信令处理系统是通过客户端连接的方式与上层应用服务器间进行通信。整个系统唯一开放给用户级访问的接口是应用服务器，在应用服务器前放置防火墙和用户行为审计子系统。应用服务器内置完善的用户权限管理、日志管理对系统使用情况进行监控和限制。防火墙采用高性能，安全配置策略灵活的的产品，主要完成流量控制、端口限制、服务限制、IP 地址绑定等功能。

核心网络汇聚设备的安全建议

面对现在网络环境越来越多的网络病毒和攻击威胁，核心汇聚设备必须提供强大的网络病毒和攻击防护能力，局方所选用的网络产品不仅应提供基于 SPOH 技术的 ACL 功能，而且还支持防源 IP 地址欺骗（Souce IP Spoofing）、防 DOS/DDOS 攻击（Synflood，Smurf），防扫描（PingSweep）等能力，从设备本身的功能即可保证网络安全。

因此对于系统内网中，建议如下部署：在核心汇聚部署支持防源 IP 地址欺骗（Souce IP Spoofing）、防 DOS/DDOS 攻击（Synflood，Smurf），防扫描（PingSweep）等设备。

防扫描攻击

众所周知，许多黑客攻击、网络病毒入侵都是从扫描网络内活动的主机开始的，大量的扫描报文也急剧占用网络带宽，导致正常的网络通讯无法进行。为此，在汇聚层交换机上建议提供了防扫描的功能，用以防止黑客扫描和类似“冲击波病毒”的攻击，并能减少三层交换机的 CPU 负担。

目前发现的扫描攻击有两种：

1）目的 IP 地址变化的扫描，我们称为“scan dest ip attack”。这种扫描是最危害网络的，不但消耗网络带宽，增加交换机的负担，更是大部分黑客攻击手段的起手。

2）目的 IP 地址不存在，却不断的发送大量报文，我们称为“same dest ip attack”。这种攻击主要是针对减少交换机 CPU 的负担来设计。对三层交换机来说，如果目的 IP 地址存在，则报文的转发会通过交换芯片直接转发，不会占用交换机 CPU 的资源，而如果目的 IP 不存在，交换机 CPU 会定时的尝试连接，而如果大量的这种攻击存在，也会消耗着 CPU 资源。当然，这种攻击的危害比第一种小得多了。

以上这两种攻击，汇聚交换机都可以在每个接口上调整相应的攻击阀值、攻击主机隔离的时间等参数（通过汇聚或者核心交换机的 system guard 功能），以便管理员最细化的管理配置。

防 DOS/DDOS 攻击

近年来，各种 DoS 攻击（Denial of Service，拒绝服务）报文在互联网上传播，给互联网用户带来很大烦恼。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。攻击报文主要采用伪装源 IP 以防暴露其踪迹。

针对这种情况，RFC2827 提出在网络接入处设置入口过滤（IngressFilting），来限制伪装源 IP 的报文进入网络。这种方法更注重在攻击的早期和从整体上防止 DoS 的发生，因而具有较好效果。使用这种过滤也能够帮助 ISP 和网管来准确定位使用真实有效的源 IP 的攻击者。ISP 应该也必须采用此功能防止报文攻击进入 Internet；企业（校园网）的网管应该执行过滤来确保企业网不会成为此类攻击的发源地。

网络交换机采用基于 RFC2827 的入口过滤规则来防止 DoS 攻击，这种过滤是通过自动生成特定的 ACL 来实现，该过滤采用硬件实现而不会给交换机的网络转发增加负担。

接入安全控制

在接入部署 ACL，对冲击波、蠕虫等病毒进行防范以及生成树 BPDU 攻击、MAC 攻击等二层攻击，使有害数据包在接入就被过滤。我们建议配备至少全千兆安全智能型交换机，其上应该具备完善的 QoS 以及强大的安全接入控制能力。具体特点如下：

二至四层线速转发，二至七层智能识别：集团采用的全千兆智能型交换机应可以硬件全线速实现 ACL、QOS、带宽限制，以提升网络体验；

硬件实现端口与 MAC 地址和用户 IP 地址的绑定：集团采用的全千兆智能型交换机应能够通过设定访问交换机上某个端口的用户 MAC 地址和 IP，就可硬件实现严格控制对该端口的用户输入，以防止非法用户的接入。

有效杜绝非法组播源：集团采用的全千兆智能型交换机支持 IGMP 源端口检查功能，以及支持 IGMP 源 IP 检查功能，有效地杜绝非法的组播源播放非法的组播信息，更好地提高了网络的安全性。

极灵活的基于流的带宽控制能力：集团采用的全千兆智能型交换机可以基于交换机端

口、MAC 地址、IP 地址、协议、应用组合进行带宽限速，限速粒度：1Mbps（128KB）粒度/百兆端口、8Mbps（1024KB）粒度/千兆端口。

完善的 QoS：集团采用的全千兆智能型交换机支持完善的 QOS，包括丰富的流分类能力包括基于交换机端口、MAC 地址、IP 地址、TCP/UDP 协议、应用组合的流分类，802.1P 和 DSCP 的数据标记、SP 和 WRR 的队列调度机制队列调度。

强大的安全接入控制能力：集团采用的全千兆智能型交换机硬件本身即可实现端口与 MAC 地址和用户 IP 地址的绑定，另外和配合厂商提供的认证计费管理系统可实现用户帐号与 IP、MAC、交换机 IP、端口、Vlan ID 多元素的复合绑定。保证用户身份的合法性和唯一性，以有效的避免 IP 地址冲突、帐号盗用等问题发生。

通过 PVLAN 即可隔离用户信息互通：集团采用的全千兆智能型交换机采用保护端口（即将该端口设为保护端口）实现端口之间相互隔离，不必占用 VLAN 资源。采用保护端口即保证用户信息安全，又节约 VLAN 资源，同时不必再修改 VLAN 配置，以提高维护效率。

多端口同步监控 MSPAN：集团采用的全千兆智能型交换机应能通过一个端口同时监控多个端口的数据流，可以只监控输入帧或只监控输出帧或双向帧，有效提高监测效率。

防病毒广播泛洪

多种交换机可实现广播报文的计数累计功能，往往一台主机受病毒时会发出大量的广播报文，交换机可实现对与进入报文的计数累计，广播病毒一般会在短时间内产生大量的广播包，通过可设置广播包的阀值，当达到一定的广播保文的数量时端口可是直接关闭，确保网络的安全、稳定。

网络硬件防病毒建议

现在网络病毒对网络的冲击影响已经越来越大，如非常猖狂的红色代码（codered）、冲击波（MS Blaster）等网络病毒，所以有必要对网络病毒继续有效的控制。

防网络攻击建议

网络中针对交换机的攻击和必须经过交换机的攻击有如下几种：

•MAC 攻击

•DHCP 攻击

•ARP 攻击

•IP/MAC 欺骗攻击

•STP 攻击

•DoS/DDoS 攻击

•IP 扫描攻击

•网络设备管理安全

下面分别阐述各个攻击的应对策略：

MAC 攻击

攻击：交换机内部的 MAC 地址表空间是有限的，MAC 攻击会很快占满交换机内部 MAC 地址表，使得单播包在交换机内部也变成广播包向同一个 VLAN 中所有端口转发，每个连在端口上的客户端都可以收到该报文，交换机变成了一个 Hub，用户的信息传输也没有安全保障了。

防范：利用交换机端口安全功能下的 MAC 动态地址锁/端口静态绑定 MAC，或 1x 端口下端口自动动态绑定 MAC/IP，来限定交换机某个端口上可以学习的源 MAC 数量或源 MAC 地址，当该端口学习的 MAC 数量超过限定数量时，交换机将产生违例动作。

DHCP 攻击

攻击之一：恶意用户通过更换 MAC 地址的方式向 DHCP Server 发送大量的 DHCP 请求，以消耗 DHCP Server 可分配的 IP 地址为目的，使得合法用户的 IP 请求无法实现。

防范：利用交换机端口安全功能：MAC 动态地址锁和端口静态绑定 MAC、1x 端口下的自动动态绑定用户 IP/MAC，来限定交换机某个端口上可以访问网络的 MAC 地址，从而控制：那些通过变化 MAC 地址来恶意请求不同 IP 地址和消耗 IP 资源的 DHCP 攻击。当交换机一个端口的 MAC 地址的数目已经达到允许的最大个数后，如果该端口收到一个源地址不属于端口上的 MAC 安全地址的包时，交换机则采取措施。

攻击之二：非法 DHCP Server，为合法用户的 IP 请求分配不正确的 IP 地址、网关、DNS 等错误信息，不仅影响合法用户的正常通讯，还导致合法用户的信息都发往非法 DHCP Server，严重影响合法用户的信息安全。

防范：

•控制客户端发出的 DHCP 请求报文被广播出去；

•检查和控制 DHCP 响应报文是否：是合法 DHCP Server 发出的报文。

接入交换机一般不具有 DHCP Relay 功能，收到 DHCP 请求广播报文后，并在 VLAN 内是向所有端口转发。

而接入交换机具有 DHCP Relay 功能，一旦启用 DHCP Relay 功能，并且配置了 DHCP Server 的 IP 地址，则客户端发出的 DHCP 请求，在交换机中将不以广播包的形式转发出去，而是直接到交换机 CPU，从而有效避免 DHCP 请求报文广播出去被非法 DHCP Server 收到。

交换机 CPU 处理后，以单播的形式发往指定的 DHCP Server。收到 DHCP 响应报文后（Offer，ACK，NAK 报文），CPU 会判定报文中的源 IP 地址是否为交换机中设定的 DHCP Server 的地址，从而保证 DHCP 响应报文的合法性。

这比仅仅设定交换机某个端口可以接受 DHCP 响应报文更合理和可靠。

ARP 攻击

ARP 攻击：ARP 欺骗

ARP 欺骗者：利用 ARP 漏洞，发送虚假的 ARP 请求报文和响应报文，报文中的源 IP 和源 MAC 均为虚假的，或错误的网关 IP 和网关 MAC 对应关系，扰乱局域网中各 PC 以及网关中保存的 ARP 表，使得网络中的合法 PC 正常上网、通讯中断，并且流量都可流入到攻击者手中。

防范：利用交换机端口 ARP 检查安全功能：打开 ARP 报文检查 ARP 报文中的源 IP 和源 MAC 是否和绑定的一致，可有效防止安全端口上欺骗 ARP，防止非法信息点冒充网络关键设备的 IP（如服务器），造成网络通讯混乱。

IP/MAC 欺骗攻击

MAC 欺骗：

盗用合法用户的 MAC 地址，侵入网络，使得正常用户无法上网；

IP 欺骗：

•盗用合法用户的 IP 地址，使得到合法用户的通讯得不到响应，造成 Ping of death，和 ICMP 不可达风暴；

•不断修改 IP，发送 TCP SYN 连接，攻击 Server，造成 SYN Flood。

防范：

•交换机端口安全：端口静态绑定；

•交换机整机绑定 IP 和 MAC 地址；

- DHCP 动态绑定；

- 802.1x；

检查 IP 报文中源 IP 和源 MAC 是否和交换机中管理员设定的是否一致，不一致，报文丢弃，并发送告警信息。

STP 攻击

攻击：发送虚假的 BPDU 报文，扰乱网络拓扑和链路架构，可以导致整个网络瘫痪。

防范：使用交换机具备的 BPDU Guard 功能，可以禁止网络中直接接用户的端口或接入层交换机的下连端口收到 BPDU 报文。从而防范用户发送非法 BPDU 报文。

对于接入层交换机，在没有冗余链路的情况下，尽量不用开启 STP 协议。

DoS/DDoS 欺骗攻击

攻击：占用网络带宽，占用服务器提供的服务资源，表现为合法用户的请求得不到服务的响应，被攻击方的 CPU 满负荷或内存不足。攻击报文主要是采用伪装源 IP。

防范：RFC 28227 的入口过滤规则。

IP 扫描攻击

攻击：许多黑客攻击、网络病毒入侵都是从扫描网络内活动的主机开始的，大量的扫描报文也急剧占用网络带宽，导致正常的网络通讯无法进行。

防范：防 IP 扫描：检测用户、隔离用户（发日志信息）、恢复通讯（发日志信息）

被监控的攻击主机数量、隔离用户的时间都可以根据网络实际状况设置。

交换机的网络管理问题

网络管理可以说是网络中最薄弱的一个环节，因为一旦攻击者登录交换机，那么交换机配置的所有安全防范措施则化为乌有，因此必须重视交换机管理安全。

1、一般的网络管理协议：SNMPv2，Telnet，Web 等都是明文登录和传输信息的。因此，尽量使用 SSH、SNMPv3 等秘文传输方式登录交换机，因为它们都与交换机之间都是加密传输。

2、管理 VLAN 与用户 VLAN 分开。

3、交换机上不用的端口划在一个 VLAN 中，并将这些口 Shutdown，需要用时，再开启

4、限制可以管理交换机的 IP，多种网管交换机均支持 Telnet 和 Web 的源 IP 访问控制

列表。

3.3.6.1.5.安全网关、接口审计

数据安全网关系统实现了数据分发的全生命周期的安全管控：

●数据输出事前审批

建立数据分发线上审批流程，在数据分发前实现数据业务与数据安全的双重审核。

●数据输出事中检测

数据安全网关内置多种数据合规检测规则，包含敏感数据检测、文件大小检测、字段检测等，对输出的数据进行实时自动扫描，发现违规数据后，立即停止数据推送，并发送报警邮件。

●数据输出事后审计

数据安全网关输出的数据由系统备份保存，安全审计人员可随时对输出后数据进行抽查审计，确认数据内容合规、安全。

●算法管理

系统支持正则表达式、程序算法、组合字段、MD5 撞库、关键字五种算法，正则表达式和程序算法适用于较复杂的审计，组合字段适用于对多个含义字符拼成的数据进行的检测，MD5 撞库适用于手机号 MD5 加密后的识别，关键字支持手机号码、固话、身份证号、姓名、地址、邮箱等常见敏感内容检测。

系统支持算法的创建、修改、停用、删除管理。

●接口管理

接口规范是审计的依据，接口管理信息包括接口名、接口描述、输入参数、输出参数等信息的录入和管理。

●策略配置

针对每个接口配置相应的检测算法，支持一个接口对应多个检测算法。

●接口检测

将日志数据与接口规则、算法进行命中分析，发现违规的数据访问。

●文本文件检测

创建文档型文件审核任务，填写任务信息，包括任务名称、数据输入路径、是否有效、检测方式，备注以及为任务选择相应检测方式。可以添加、修改、删除、提交、查看文档型文件审核任务，检测文档(word、ppt、excel、pdf、txt)是否存在违规数据。另外，系统也支

持直接上传文件进行时时的检测。

3.3.6.1.6.软件安全设计

软件安全层次架构

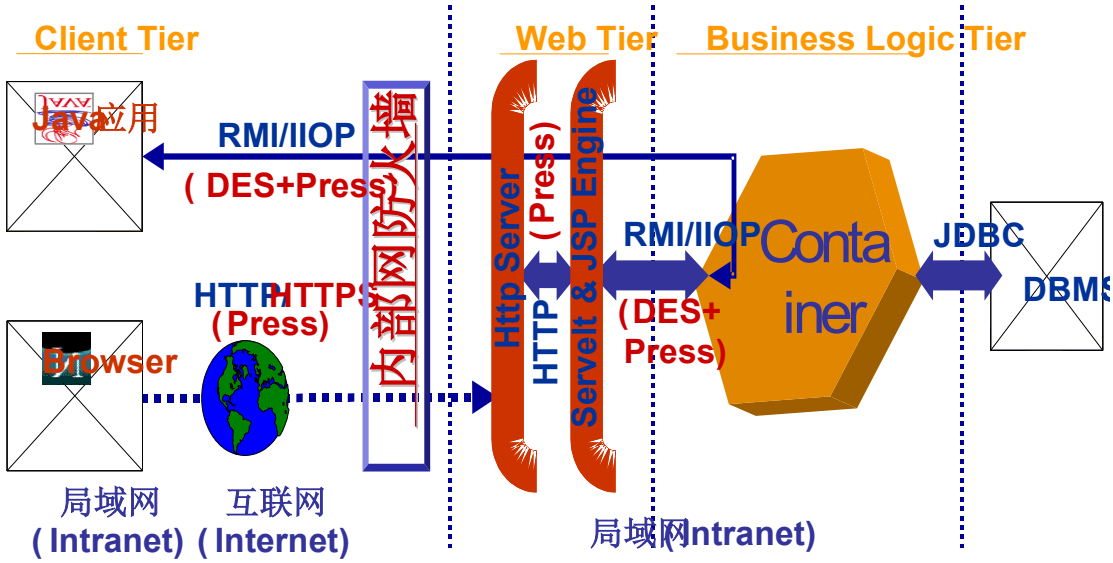
客户端接入–强大的访问控制与授权功能

系统采用“插件”式安全模型，用户能够部署自己定制的身份验证、授权和角色关系，也可以采用 OS 内部的安全机制、数字证书认证或者其它方法，并能很容易的与其它安全认证系统集成，比如指纹认证系统、数字证书认证系统、加密卡/机等等。

传输层加密–真正的安全数据传输功能

为系统运行在符合 Java EE 规范的开源或商用中间件上，所有数据都需从中间件层过滤，可以通过在中间件层对数据进行安全处理，来做到真正意义上的数据安全，从而再也不用担心底层操作系统、硬件本身具有的系统漏洞或所留的后门对数据安全带来的威胁。

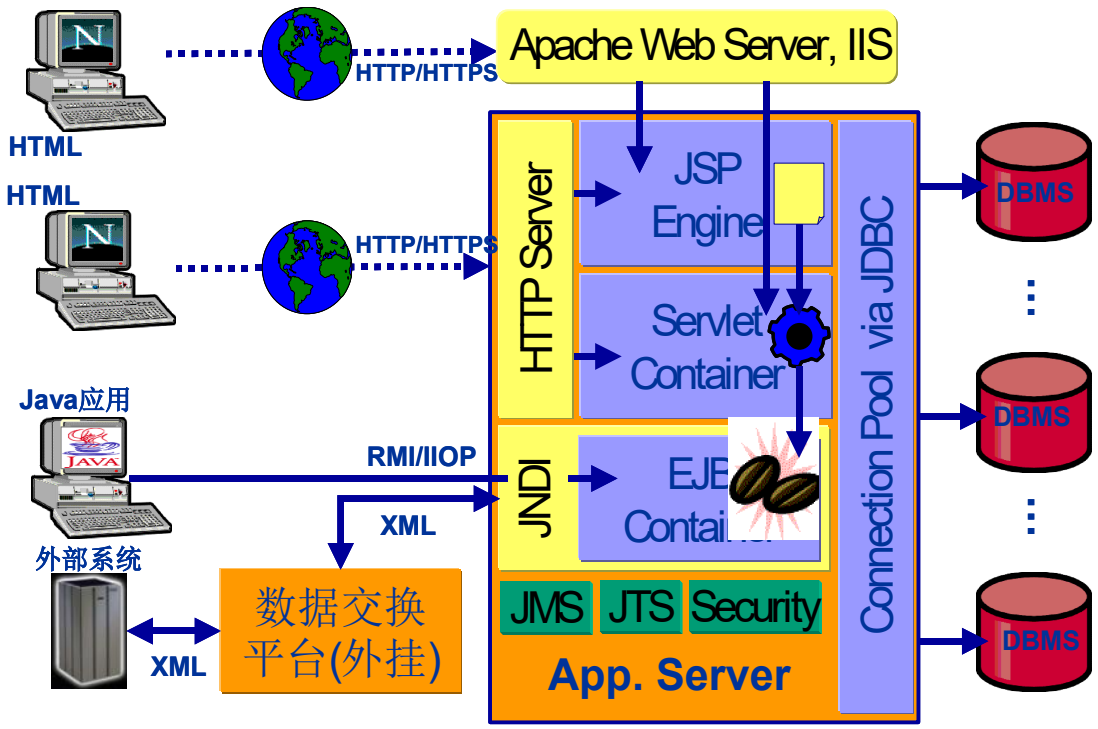
在系统中间件层中，已经对传输的数据进行了加密。算法除了一些经典的如 DES 之外，还可根据用户的需求采取具有自主知识产权的更高级别的加密算法。



服务器安全–符合 Java EE 规范的标准中间件

本系统作为电信级系统，除了能很容易的集成进用户自己的安全网络环境中外，自身已具有了强壮的访问控制功能与数据安全传输功能。

作为应用系统本身，本平台的各应用模块完全运行在符合 Java EE 规范的中间件应用服务器上，中间件本身的底层特性与健壮体系，能保证系统本身应用的高度安全性。



基于 Java EE 安全模型，本系统允许配置一个 Web 或 enterprise bean 组件，使系统资源只能由授权的用户访问；在中间件层，可实现数据的加密、压缩功能，保证数据传输的安全性等。

数据安全–安全的数据存储

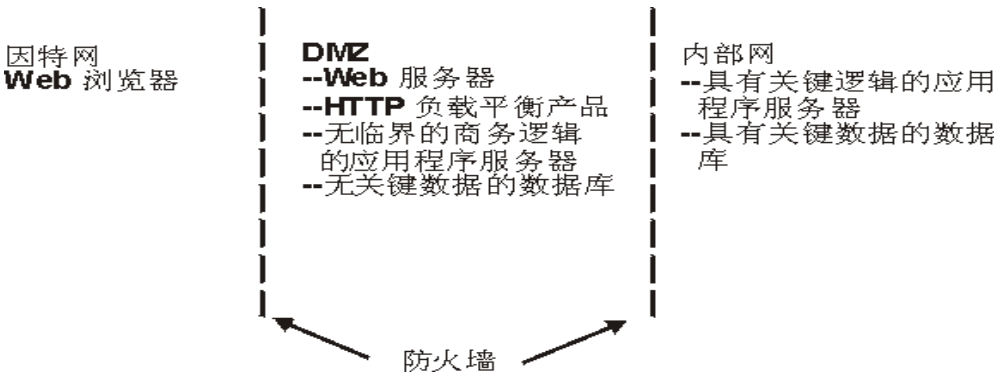
本系统对关键的数据文件可实现加密存储，因此不用担心泄密或非法访问。对于数据库中的数据，除了用户自己的安全控制之外，本系统可与数据库加密系统集成，做到只有数据库表的使用者才能读到该表的安全功能。

软件安全的扩展和整合能力

与商业中间件的整合与集成

以很容易的将本系统部署到其他商业应用 WEB 服务器和应用服务器上，从而利用这些服务器所提供的强大的安全管理与加密传输功能。比如 IBM 的 WebSphere，Oracle 的 WebLogic 等。

本系统可方便地充分利用这些商业 WEB 服务器的安全功能，同时也可以方便的集成商业中间件和应用服务器的安全功能，可利用 WebLogic 提供的安全访问、利用 WebSphere 所提供的灵活配置 DMZ 的功能等。



PKI 体系以及 CA 的应用

信息安全中存在的身份认证、安全传输、不可否认性、数据一致性等问题。完善的 PKI 体系及数字证书认证技术的应用，解决了以上问题。

数字证书是一段包含用户身份信息、用户公钥信息以及身份验证机构（也称为证书认证中心，CA）数字签名的数据。身份验证机构的数字签名可以确保证书信息的真实性，用户公钥信息可以保证数字信息传输的完整性，用户的数字签名可以保证数字信息的不可否认性。认证中心（CA）作为权威的、可信赖的、公正的第三方机构，专门负责为各种认证需求提供数字证书服务。

数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题。

根 CA 为下一级 CA 颁发签名证书，下一级 CA 再为用户颁发签名证书和密钥交换证书。

每一个用户有一个各不相同的名字，一个可信的证书认证中心给每个用户分配一个唯一的名字并签发一个包含名字和用户公开密钥的证书。

如果甲准备和乙通信，他首先必须先取得乙的证书，然后对它进行验证。如果他们使用相同的 CA，事情就很简单。甲只需验证乙证书上 CA 的签名；如果他们使用不同的 CA，问题就复杂了，甲必须从 CA 的树形结构底部开始，从底层 CA 往上层 CA 查询，一直追踪到同一个 CA 为止，找出共同的信任 CA。

证书可以存储在网络中的数据库中。用户可以利用网络彼此交换证书。当证书撤销后，它将从证书目录中删除，然而签发此证书的 CA 仍保留此证书的副本，以备日后解决可能引起的纠纷。

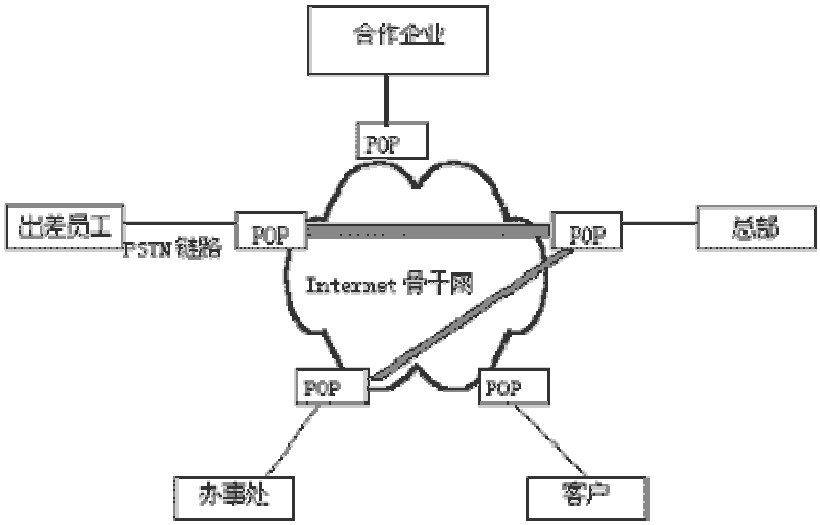
如果用户的密钥或 CA 的密钥被破坏，将导致证书的撤销。每一个 CA 必须保留一个已经撤销但还没有过期的证书废止列表（CRL）。当甲收到一个新证书时，首先应该从证书废止列表中检查证书是否已经被撤销。

数字证书可以存放在计算机的硬盘、随身软盘、IC 卡或 USB 卡中。

本系统成功地和国内外多家知名安全厂商合作，提供专业、可靠的证书认证体系。

VPN 技术的应用

在过去几年中，VPN 越来越为企业所青睐。它是一种架构在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（尤其是 IPSec）和建立在 PKI 上的加密与签名技术来获得私有性。同租用线路等方法相比，VPN 既节省开销又易于安装和使用，已经成为企业架构 Intranet 和 Extranet 的首选。

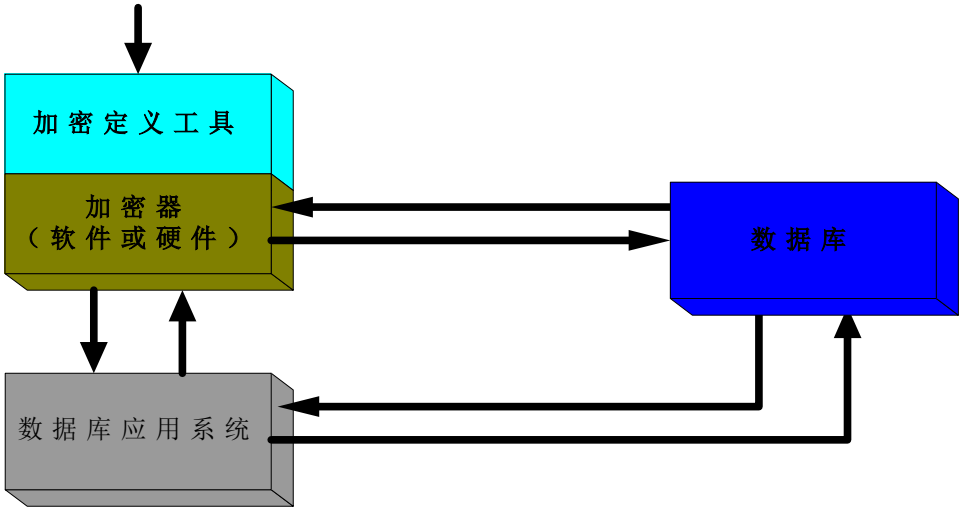


企业内部资源享用者通过 PSTN 网连入本地 ISP 的 POP（Point of Presence，指服务商通常在很大的地理范围放置多个网络设备）服务器，即可相互通信，而利用传统的 WAN 组建技术，彼此之间要有专线相连才可以达到同样的目的。

由于 VPN 需要共享公共的、存在着安全隐患的网络，如 Internet，因此安全性是一个非常重要的问题。VPN 解决方案的安全性由 3 个基本要素组成：安全认证、授权和监听。安全认证服务决定谁可以使用网络，授权服务负责分配不同资源的访问权限，而监听则确保资源的使用方式与网络的策略相符合。通过使用安全性服务，VPN 可以保证数据在传送过程中的保密性和不被篡改，并将数据正确地分配给相应的用户。

数据库加密

如果局方已不仅仅满足于一般的数据文件加密存储，而是对数据库的安全有更高的需求，要求只有表的拥有者或合法使用者才能查阅到该表的内容，其他用户、甚至是据库系统管理员也无法读到表中正确的内容。在这种情况下，可以通过在 DBMS 外层外挂数据库加密系统来实现。



数据库加密系统能够满足客户对字段加密、密钥动态管理、合理处理数据等需求，并且不影响合法用户的使用。采用这种加密方式时，加/解密运算可以放在客户端进行，其优点是不会加重数据库服务器的负载并可实现网上传输加密，缺点是加密功能会受一些限制。上图中，“加密定义工具”模块的主要功能是定义如何对每个数据库表数据进行加密，在创建了一个数据库表后，通过这一工具对该表进行定义；“数据库应用系统”的功能是完成数据库定义和操作。数据库加密系统将根据加密要求自动完成对数据库数据的加/解密。

3.3.6.1.7.信令信息采集、解码安全要求

对于信令数据输入接口来说，输出数据信息有安全考虑如下：

✓系统依据相应的存储技术规范要求，支持灵活的存储策略，支持测量报告按照不同用户、事件和区域进行抽样存储；

✓对于传输集中收敛的信令数据，系统支持采集设备灵活移动，随时调整检测。同时系统存放在可以方便移动的采集机柜内。

✓系统能对指定信息进行限制采集、限制存储或加密处理；如指定用户信令的限制采集、差异化存储，短信内容的掩码处理，信令文件的加密处理等

✓系统保证不含任何恶意代码等后门程序，定期病毒库更新提醒和升级，操作系统定期检查和升级

3.3.6.1.8.标准化的项目运作与管理

我们开发采用标准化的研发流程，并且内部针对各个系统模块实现了严格的版本配置管理和职责分工。比如系统底层的信令解码模块开发由专门的开发团队完成，而数据库的访问权限也只限制在 DBA 内部，从研发体系上保障了系统的安全性、稳定性，并且加强内部员工对于用户隐私信息的保障意识和相关责任机制。

3.3.6.2.系统安全体系建设

保密不是单靠某一个、两个安全产品来解决的，它需要系统的、立体的全方位的解决方案，从网络的设计结构角度、从物理层面、网络层面、系统层面、应用层面、数据安全层面以及安全制度体系的建设方面等多视角来设计，应该按照应用为主导，根据不同应用的特点和安全需求，综合衡量不同业务系统的重要性和所面临风险大小等因素，科学划分网络与信息系统安全等级，并依据安全等级进行安全建设和管理，提高信息安全体系的有效性。

3.3.6.2.1.安全体系建设目标

系统保密安全建设是一个系统工程，基于手机信令的大数据应用平台的安全体系建设应按照“统一规划、统筹安排，统一标准、相互配套”的原则进行，采用先进的“平台化”建设思想，避免重复投入、重复建设，充分考虑整体和局部的利益，坚持近期目标与远期目标相结合。

在实际建设中遵循以下指导思想：宏观上统一规划，同步开展，相互配套；在实现上分步实施，渐进获取；在具体设计中结构上一体化，标准化，平台化；安全保密功能上多级化。安全不可能单靠某一个、两个安全产品来解决的，它需要系统的、立体的解决。选择安全产品时，要统筹安排，满足目前，着眼扩展。超前规划，分步实施。我们认为：本次项目安全体系建设的具体目标为：

●构建可信可控的网络平台

合理划分安全域，明确不同安全域之间的信任关系，并相应地采取物理隔离、防火墙、访问控制列表等安全措施，实现不同安全域之间网络层面的访问控制和检测；

●构建安全可靠的系统平台

通过部署完善的各安全子系统及存储备份系统，并结合全面的安全服务和管理，实现系统层面的访问控制和数据的存储安全；

●构建安全有效的管理平台

在充分利用目前先进的安全技术的基础上，加强管理建设，建立有效的责任机制、人才培训机制、应急响应机制，完善安全管理制度，为基于手机信令的大数据应用平台和平台运维服务提供安全有效的管理保障。

3.3.6.2.2.安全体系建设原则

●先进性与实用性原则

在充分利用已有设备、保护先期投资的基础上，采用先进、成熟、实用的技术和设备，设计和建设网络安全防护平台，同时在满足当前应用需求的前提下，兼顾未来业务发展，使整个安全防护系统在今后几年内能保持技术的先进性，并具有良好的开放性和发展潜力，以

适应未来通信业务发展和技术升级的需要。

●灵活性与可扩展性原则

项目设计必须具有良好的灵活性与可扩展性，能够根据各单位业务不断深入发展的需要，提供扩大设备容量、增加用户数量、提高服务质量的功能，具备支持多种网络传输协议、多种物理接口的能力，提供技术升级、设备更新的灵活性。在扩容过程中对已接入网络的用户不应产生影响，且进行软件升级时不应影响用户的工作。

●标准化与规范化原则

项目的整体设计要求基于国际标准和国家颁布的有关标准，坚持统一、标准、规范的原则，为未来业务发展及设备平滑增容奠定良好的基础。

●可管理性与易维护性原则

随着信息业务的不断发展，安全管理任务必定会日益繁重，因此系统的建设必须有良好的可管理性和易维护性。所选用的设备应有统一标准的通信接口，以有效简化管理人员的日常运维工作，为整个政务网络的安全、可靠运行提供有力保障。

3.3.6.2.3.物理层面保密安全措施

我们认为，为了能够提高整体保密安全，还应该采用访问控制列表的方式来提高安全，网络层通讯可以跨越路由器，攻击可以从远方发起，因此网络层的访问控制是非常重要的安全手段。各类网络设备如交换机、路由器都可以实现一定的访问控制功能，但访问控制主要在防火墙上实现。

防火墙是近年发展起来的重要安全技术，其主要作用是在网络边界处检查网络通讯，根据设定的安全规则，在保护内部网络安全的前提下，提供内外网络通讯。防火墙是一种在信任网络和非信任网络之间实施安全防范的系统。防火墙的目的是在内部、外部两个网络之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，对进、出的内部网络服务和访问进行审计和控制。在本项目中，我们将通过防火墙设置，实现对 DMZ 区——内网的访问、运营商专线—内网进行链路控制，同时关闭其他方式的链接，保证系统的安全。

3.3.6.2.4.系统层面保密安全措施

负载均衡集群设计

业务应用服务器通过网络设备相连组成一个服务器集群，每个集群中的几台服务器都提供相同或相似的业务服务。服务器集群前端部署一台负载均衡设备，负责根据已配置的均衡策略将用户请求在服务器集群中分发，为用户提供服务，并对服务器可用性进行维护。使用负载均衡技术的优势：

低成本：按照业务量增加服务器个数即可；已有资源不会浪费，新增资源无需选择昂贵的高端设备。

可扩展性：当业务量增长时，系统可通过增加服务器来满足需求，且不影响已有业务，不降低服务质量。

高可靠性：单台服务器故障时，由负载均衡设备将后续业务转向其他服务器，不影响后续业务提供，保证业务不中断。

负载均衡技术主要实现业务服务器区业务应用负载均衡。服务器负载均衡包括三个方面，其一是将用户访问流量均衡分配到各台服务器，使服务器资源得到充分利用，提高服务器群整体的性能；其二是对服务器节点的健康检查，保证流量被负载均衡到正常工作的服务器；第三是对于需要定位到某台服务器进行访问的用户来说，采用会话保持技术来保证用户会话的持续性

操作系统安全

系统层面安全主要来自网络上运行的操作系统， 该层次的安全问题主要表现在两方面：一是操作系统本身的安全漏洞和隐患；二是对操作系统的错误配置。

通常，我们对于操作系统本身在安全方面考虑较少，而且会因为设计、编码的原因存在各种各样的安全漏洞（已知的、未知的），还可能留有隐蔽通道或后门。我们建议在日常的网络维护过程中，系统管理员应及时安装厂商公布的最新升级软件包和补丁包，减少安全漏洞和隐患。

操作人员对系统功能、系统服务、数据库管理系统等的误操作或者错误配置，也同样会给信息网络系统带来一定的安全风险。我们建议应定期检查系统配置，纠正错误的配置，比如关闭不需要的系统服务，或者采用更安全的服务等。

操作系统很容易被病毒感染，而且病毒的传播方式多种多样，如外来文件的拷贝、盗版软件、从外部站点下载的文件或应用软件的非法安装，邮件等。我们建议在日常的网络维护过程中，对所有服务器和客户端进行病毒防护；同时也针对邮件服务，对进出的邮件进行病毒查杀。

3.3.6.2.5.应用层面保密安全措施

应用系统的安全

DNS 服务为网络应用提供了极大的灵活性。几乎所有的网络应用均利用域名服务。但是，域名服务通常为 hacker 提供了入侵网络的有用信息，如服务器的 IP、操作系统信息、推导出可能的网络结构等。我们建议应在网络系统中限制 DNS 服务器提供 DNS 域的记录或全部记录传送功能，如控制对 DNS 服务器 TCP 端口 53 的访问。

数据传输过程中的安全加密

在网络办公环境下，应用系统数据将会在网络中传输，在传输的过程中可能会泄漏、丢失、篡改，由于网络本身的自由性、广泛性，数据在网络上传输，很难保证不被非法窃取和篡改，因此我们在进行系统设计时，应当提供数据传输加密的功能，保证数据在传输过程中的安全，同时，还用该提供对敏感数据采取本地加密的功能。

我们所设计的应用系统将支持 SSL 加密协议，可以保证在网络中传输的数据的安全性；同时应用系统还支持文档级的加密，利用存储在本地设备或机器上的密钥，对加密文档进行正确解码，实现数据的安全传输。

3.3.6.2.6.数据层面保密安全措施

数据安全管理的原则

对数据进行安全管理是为了保证数据的一致性和完整性，消除系统使用者和操作者的后顾之忧。不同的应用环境要求不同的解决方案来适应，一般来说，一个完善的备份系统，需要满足以下原则：

●稳定性

备份产品的主要作用是为系统提供一个数据保护的方法，于是该产品本身的稳定性和可靠性就变成了最重要的一个方面。首先，备份软件一定要与操作系统 100%的兼容，其次，当事故发生时，能够快速有效地恢复数据。

●全面性

在复杂的计算机网络环境中，可能会包括了各种操作平台，如各种厂家的 UNIX、NetWare、Windows NT、VMS 等，并安装了各种应用系统，如 ERP、数据库、群件系统等。选用的备份软件，要支持各种操作系统、数据库和典型应用。

●自动化

很多系统由于工作性质，对何时备份、用多长时间备份都有一定的限制。在下班时间系统负荷轻，适于备份。可是这会增加系统管理员的负担，由于精神状态等原因，还会给备份安全带来潜在的隐患。因此，备份方案应能提供定时的自动备份，并利用磁带库等技术进行自动换带。在自动备份过程中，还要有日志记录功能，并在出现异常情况时自动报警。

●高性能

随着业务的不断发展，数据越来越多，更新越来越快，在休息时间来不及备份如此多的内容，在工作时间备份又会影响系统性能。这就要求在设计备份时，尽量考虑到提高数据备份的速度，利用多个磁带机并行操作的方法。

●维持业务系统的有效性

实时备份对业务系统的性能将会产生一定的影响，有时会很大。如何采取有效的技术

手段避免备份对服务器系统、数据库系统、网络系统的影响，将是非常重要的。

●操作简单

数据备份应用于不同领域，进行数据备份的操作人员也处于不同的层次。这就需要一个直观的、操作简单的图形化用户界面，缩短操作人员的学习时间，减轻操作人员的工作压力，使备份工作得以轻松地设置和完成。

●实时性

有些关键性的任务是要 24 小时不停机运行的，在备份的时候，有一些文件可能仍然处于打开的状态。那么在进行备份的时候，要采取措施，实时地查看文件大小、进行事务跟踪，以保证正确地备份系统中的所有文件。

数据备份策略管理

在数据安全方面，我们认为数据备份则是非常重要的环节，数据备份可以采取如下的备份测略。

■ 全备份

每次备份定义的所有数据，优点是恢复速度快，缺点是备份数据量大，数据多时可能做一次全备份需很长时间，并且很容易造成存储容量的资源浪费。

■ 增量备份

增量备份(Incremental Backup)，增量备份指每次备份的数据是上一次备份后增加和修改过的数据。这种备份的优点很明显：没有重复的备份数据，节省磁带空间，又缩短了备份时间。但它的缺点在于当发生灾难时，恢复数据比较麻烦，需进行多次数据恢复才能恢复至最新的数据状态。

■ 差分备份

差分备份(Differential Backup)，备份自上一次备份以来更新的所有数据，其优点是每次备份的数据量少，缺点是恢复时需要全备份及多份增量备份

对于大数据量的数据不宜采用每次全备份的方式，对于数据量小的数据，由于存储容量小，可以根据需要作多次全备份。

对于像本项目中数据量比较大的数据备份，采用频繁全备份的备份策略显然是不切实际的，无论是从磁带容量上还是从备份时间上考虑都是不理想的方式，比较好的策略是采用以上几种主流的备份策略的组合方式，根据具体应用的实际情况采用多种策略的组合，发挥每种备份策略的优势，弥补单一策略的不足，充分发挥数据备份系统的最理想的性能。

3.3.6.2.7.安全制度管理体系

用 “三分技术、七分管理”来描述网络安全系统已成为全世界的共识，这也说明网络安全中管理的重要地位。应在安全管理方面作好以下几方面的工作。

强化人才培训、强化信息安全意识

安全系统是必要的。但是人是信息安全的最终防线。调查表明，80%的网络安全事件不是由于外部的攻击，而是来自内部人员。网络遭受了黑客的入侵，病毒的传染等其原因是多方面的，但是其中一个主要的原因是思想问题，没有把信息安全的问题放在足够重要的位置上，才会发生应该防止的黑客没有防止，可以备份的系统没有备份，应该杀掉的病毒没有杀掉，可以堵住的漏洞没有堵住等等问题。主要责任人的安全意识对网络的整体安全具有决定意义，领导干部应将网络安全意识与政治意识、责任意识、法律意识、保密意识联系起来，同时，在用户内部，要加强信息安全的宣传和教育的力度，以“谁使用谁负责”为原则，培养每一个人信息网络用户的“网络安全人人有责”观念。要把网络安全纳入一个人人有责、层层负责、有第一负责人负总责的安全管理体制之中，建立正式的统计信息网的安全管理机构，把信息安全管理制度化、规范化。

健全网络信息安全管理制度

根据国家有关信息安全的法律法规以及用户内部的实际情况，健全网络安全管理制度体系，是做好网络安全管理的前提。安全管理制度主要包括以下几个方面：人事管理、场地设施安全、设备安全管理、介质安全管理、软件管理、应用软件开发安全管理、病毒防范管理、密钥与口令管理、技术文档管理、通信网络安全管理、运行安全管理、外包技术服务安全管理、安全审计、灾难恢复、应急管理。

随着工程实施的逐渐推进和深入，要不断的完善和细化管理制度，使之能够适应新的信息网络环境并向基层单位推广。

建立安全管理策略

网络的安全管理策略包括：确定安全管理等级和安全管理范围；制订有关网络操作使用制度；制定网络系统的维护制度和应急措施等。记录信息系统在不同时点的运行状况，特别是资源开销情况，遇有异常或超出系统设计指标时应按规定时间报告主管领导。

- 及时做好系统备份和系统日志备份，必要时打印系统日志；
- 建立系统安装、维护、升级记录文档；按要求配置系统参数；
- 制定应急措施，出现与安全有关的故障时，按规定时间处理的同时报安全部门和主管领导；

严格按规定程序接收应用软件；对上线的应用系统建立运行文档。

3.3.6.2.8.安全管理内容

安全方案

名称	安全策略		备注
安全方案	传输安全	SSL 加密通道传输	
	机制安全	多重校验，安全审计	
日志管理	安全审计	日志管理	可以查看操作日志

传输安全

- SSL 加密信道传输

SSL(Secure Sockets Layer 安全套接层),及其继任者传输层安全（Transport Layer Security，TLS）是为网络通信提供安全及数据完整性的一种安全协议。TLS 与 SSL 在传输层对网络连接进行加密。

SSL 协议提供的服务主要有：

1）认证用户和服务器，确保数据发送到正确的客户机和服务器；

2）加密数据以防止数据中途被窃取；

3）维护数据的完整性，确保数据在传输过程中不被改变。

运行安全

- 独立崩溃模式

对于安全性和稳定性要求都比较高的单位，采用各个服务器模块独立部署的方案，使得其中一个模块因为故障崩溃时，不会影响其他模块的正常运作。

尤其重要的是，用户不必担心引入信息系统会对原有 IT 系统的稳定性造成影响。

机制安全

- 数据存储的加密

对于需要持久的存储在平台服务器上的重要数据，平台系统采取加密安全存储，而不是直接存储系统硬盘数据。这样即使单位服务器被侵入，依旧无法取得用户存储于移动办公系统的机密文档。

- 用户帐户、手机密码和手机设备号的四重校验

一般的信息系统均是用户名密码的认证体系，平台通过与运营商和手机制造商的底层合作，可以实现用户账户和手机设备的三重绑定。即使有人获知了正确的用户名密码，也必

须使用特定的唯一手机才能登陆。

- 停用锁止

当用户因为手机丢失或其他原因需要暂停业务时，平台会锁定用户所有的数据，并阻止用户登录。保证用户的机密信息不会泄漏。

- 安全审计

平台对用户的操作进行严格的审计和报警，保证用户和管理员和用户可以查看以往的操作日志。同时也可以对日志分析，查看系统是否曾遭到攻击。

3.3.6.3.安全管理应急方案

3.3.6.3.1.安全应急响应范围

本数据系统安全应急方案适用于本项目，系统面临的主要数据安全风险有以下五种：

（1）信息篡改：针对系统服务器，未经授权将信息系统中的信息更换为攻击者所提供的信息而导致的信息安全事件，例如网页篡改等导致的信息安全事件。

（2）SQL 注入：通过系统正常开放的服务端口，提交一段特殊构造的数据库查询代码，从而越权获得系统数据或取得系统权限的攻击方法。

（3）网页挂马：是指利用系统漏洞侵入系统网站，在正常的网站内容中加入恶意代码，从达到窃取网站用户信息目的的攻击方法。

（4）拒绝服务：包括从外部发起，针对城市的拒绝服务攻击，也包括城市内部被非法控制的主机，作为傀儡机发起的拒绝服务。

（5）计算机病毒：指系统感染病毒，导致系统无法正常运行。计算机病毒是编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。

3.3.6.3.2.准备阶段

准备阶段是安全事件响应的第一个阶段，即在事件真正发生前为事件响应做好准备。

系统备份数据

核心的数据库每天增备、每周全备两次；防火墙及交换机的日志备份为每月一次；系统和应用程序的日志备份为每季一次。

预警信息的处理

在日常系统维护工作中，应按照上级主管部门要求落实各项预警信息处理工作，并及

时跟踪预警项进展，预警内容出现变化应及时上报，必要时调高预警级别并采取更严格防范措施。

3.3.6.3.3.安全事件检测

保密事件检测指系统维护人员使用技术手段进行安全事件检测，确定系统是否出现异常。

流量监控系统、入侵检测系统、执行日常安全维护作业计划检查、日常安全工单、安全预警公告、用户投诉等手段进行安全事件发现和检测。

保密应急方案启动条件

在保密事件检测过程中，如发现系统发生“安全应急响应范围”中描述的各类安全事件时，应当立即启动本应急方案开展安全事件处理。

保密事件的上报

当系统发生保密事件时，事件的上报应当遵从网络与信息安全应急预案规定的要求。

3.3.6.3.4.安全事件处理

抑制与根除

抑制是对攻击所影响的范围、程度进行扼制，通过采取各种方法，控制、阻断、转移安全攻击。

根除阶段是在抑制的基础上，对引起该类安全问题的最终技术原因在技术上进行完全的杜绝，并对这类安全问题所造成的后果进行弥补和消除。在根除阶段，采取的措施最大的风险主要是在系统升级或补丁时可能造成系统故障，所以必须作好备份工作。

恢复与跟进

恢复阶段是指通过采取一系列的步骤将系统恢复到正常业务状态。

跟进阶段是应急响应的最后一个阶段，本部分的内容主要是对抑制或根除的效果进行审计，确认系统没有被再次入侵。

网站信息篡改事件处理

➢紧急处理措施

进行系统临时性恢复，迅速关闭或恢复系统被篡改的内容；操作方法：

- 关闭该服务器的 WEB 服务（命令 ./usr/ipi/Tomcat5.0/bin/shutdown.sh 和 ./usr/ipi/Tomcatcp/bin/shutdown.sh）；

- 恢复该服务器的 WEB 服务（命令 ./usr/ipi/Tomcat5.0/bin/startup.sh 和 ./usr/ipi/Tomcatcp/bin/startup.sh）；

如果影响正常业务，将发生安全事件的设备脱网，做好安全审计及系统恢复准备；

➢抑制

1. 在必要情况下，将遭受攻击的主机上系统日志、应用日志等导出备份，并加以分析判断。

操作方法：

- 系统日志：备份路径——\bak\sys\，所需备份的文件——/var/log/目录下的 wtmp-N、secure-N、message-N、maillog-N、rpmpkgs-N、boot.log-N；
- 应用日志：备份路径——\bak\ipi_log\，所需备份的文件——(1)/usr/ipi/tomcat5.0/logs/下的 jkhd.log、ShopAssistat.log、YXT.log、Catalina.out

(2)/usr/ipi/tomcatcp/logs/下的 jkhd2WebService.log、CP.log、Catalina.out

2. 分析 web 应用日志，确认有无恶意文件上传、SQL 注入的非正常查；

操作方法：

- 在备份出来的应用日志下查询，使用 more + 相应的 WEB 门户的 LOG 日志，查看有无报错及不正常之处；

3. 分析系统日志(messages、sulog、lastlog 等)，确认主机上有无异常权限用户非法登陆，并记录其 IP 地址、登陆时间等信息；

操作方法：

- more /var/log/messages.N

输入如下命令查询日志后面指定行数： tail -1000 messages.N | more（注：其中 N 为数字，可选择具体时间对应的数字来查询，如果不填写 N，则为查询当前状态），就可查询 Linux 启动之后的处理消息，此日志为需要重要审核的日志，审核此日志时主要关注 ssh 登陆信息；

- 使用 lostlog 命令可查询系统中各用户最后一次登陆信息
- who /var/log/wtmp.N（注：其中 N 为数字，可选择具体时间对应的数字来查询，如果不填写 N，则为查询当前状态），就可查询用户历史登陆信息
- /var/log/cron 日志，查看系统中是否存在非法计划任务，并使用 crontab 命令将非法计划任务删除；

查看计划 crontab –l 查看用户计划任务，可以使用 crontab –e 进行编辑；

- 使用 history 命令查看非法用户操作命令；

4. 分析系统目录以及搜索（find 命令）整盘近期被修改的和新创建的文件，查找是否存在可疑文件和后门程序；

操作方法：

- 使用 find . -name "*.*" -mtime +7 ,可查询最近一周修改的文件，并分析其是否为可疑文件；

5. 分析系统服务，有无新增或者修改过的服务；

操作方法：

- 使用 setup 命令查看系统中是否存在非法服务，停止并删除服务；

6. 用 ps 命令检查有无可疑进程；

操作方法：

- 使用 w 命令查看 utmp 日志，获得当前系统正在登录帐户的信息及来源；如果发现有非法用户登陆，记录其 pts 终端号；使用 ps –ef|grep pts/x (x 为 pts 终端号)查看非法用户 bash 进程；使用 kill -9 bash 进程号，将非法用户踢出系统；
- 用 netstat -an 命令检查有无可疑端口；
- 使用 ps aux 和 netstat –anp 命令查看是否存在非法进程及端口，并使用 kill -9 进程号将非法进程停止；

7. 结合上述日志审计，确定攻击者的方式、以及入侵后所获得的最大管理权限和是否对被攻击服务器留有后门程序。

➢根除

1. 通过防火墙策略的配置严格限制外网恶意地址对该服务器的远程登录及访问请求；
2. 对 web 服务软件和数据库进行安全配置加固；
3. 对存在问题的 web 页面代码进行安全修改；
4. 必要情况下进行主机系统重新安装，并恢复数据库系统；
5. 根据确认的入侵方式，对防火墙进行安全策略设定，在网络层将非法入侵包拒绝；
6. 重新安装问题服务器操作系统（AS 4.0）；以及应用系统（Jdk、Tomcat、应用服务）；
7. 配置服务器运行参数（网络 IP、应用连接配置）；
8. 启动 WEB 服务，使用内网 IP 地址登陆进行测试；
9. 测试通过后，将服务器接入运营网络，进行业务验证，确定系统完全恢复；

拒绝服务事件处理

攻击者利用网络协议某些特性可能对系统发动拒绝服务攻击，比如说常用的SYN-FLOOD 就是利用 TCP 协议三次握手的特点发起的攻击。

1) 对于 SYN-FLOOD 攻击，可通过利用 netstat –an 命令（适用于 Windows/Unix 系统），能发现当前活动连接的状态中存在大量的 SYN_RECEIVED 状态包，这表明系统正受到 SYN-FLOOD 拒绝服务攻击；

2) 通过使用 SNIFFER，如果发现大量非正常网络连接，或协议的非正常分布，如 icmp 或 UDP 协议数据超过总流量的 20%；表明系统正在受到拒绝服务攻击。

3) 通过使用流量监控系统发现，网络流量异常增加，表明系统可能受到拒绝服务攻击。

- 紧急处理措施

1. 确认发起拒绝服务攻击的 IP；

2. 在防火墙上对进入流量进行过滤，比如：防火墙应该拒绝那些来自内部地址或保留地址发出的数据包，这些包通常都是拒绝服务的伪造包；

3. 在边界路由上进行外出流量过滤，边界路由器应拒绝非来自内部网络的向外的包，这些包通常是被利用来对其它目标进行拒绝服务攻击的；

4. 在边界路由器上对确认的 IP 进行封堵；

- 通过访问列表进行抑制方法举例如下：

定义访问控制列表号为 106 的 acl，允许其他任意 ip 地址的 TCP 数据包达到 192.168.0.0 网段的机器，其余没有在这条件内的数据全部丢弃，从而达到，网络中只有在定义范围内容的数据包，避免多余数据包占用了路由器的负载。然后把所定义好的 acl 绑定到做要 syn-flood 抑制端口上（如例子中的外接设备端口 eth0/2）。

```
Router(Config)# no access-list 106
Router(Config)# access-list 106 permit tcp any 192.168.0.0 0.0.0.255 established
Router(Config)# access-list 106 deny ip any any log
Router(Config)# interface eth 0/2
Router(Config-if)# description “external Ethernet”
Router(Config-if)# ip address 192.168.1.254 255.255.255.0
Router(Config-if)# ip access-group 106 in
```

- 抑制

1. 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，

确定攻击方式、类型等；

2. 给易受攻击的系统打上补丁，保持补丁的有效；

3. 调整操作系统或设备的性能设置，增强抵抗拒绝服务的能力；

- 根除

进一步采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除；

计算机病毒事件处理

- 紧急处理措施

1. 断开被感染的服务器网络；

2. 启用备用服务器；

3. 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

- 抑制

1. 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

2. 在问题主机上，确定病毒（木马）代码特征：进程、端口等，通常以 netstat –naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

3. Windows 下用任务管理器查看现有进程，Linux 下 Ps –ef 会列出系统正在运行的所有进程，一般先停止恶意进程，同时将其相关文件删除。

- 根除

1. 更新防病毒软件病毒库；

2. 更新系统补丁及漏洞修补程序；

3. 使用反病毒软件进行查杀，清除病毒（木马）；

4. 确认病毒类型后，下载专杀工具进行病毒清理；

5. 更新防火墙安全策略，将病毒网络数据包进行过滤。

6. 消除攻击源后，验证相关服务的运行情况；

7. 进行业务测试，确定系统完全恢复；

8. 病毒被完全清除后，系统上网运行。

9. 在不能确定木马是否被完全被清除的情况下，需要重新安装系统并进行加固。

SQL 注入事件处理

- 紧急处理措施

通过备份文件对系统进行修复，将网站恢复到没有被祝入前的初试状态；

- 抑制

1. 安置好取证工作环境，如再次发生攻击进行攻击分析和取证。取证采样包括防火墙日志、入侵检测日志、路由器日志等、系统日志等。
2. 通过应用漏洞扫描工具分析或人工分析，发现网站存在的 SQL 注入点；通过分析入侵检测系统日志、网站应用日志、数据库日志和 WEB 服务日志，查明 SQL 注入执行的具体方法和对业务的影响。日志包括：
1. 根据对网站 SQL 注入漏洞的分析，确定网站 SQL 注入点和攻击者注入方法，确定应用程序修补方案。
2. 进行应用程序修改，主要注意在用户输入过程中增加对用户输入非法字符的过滤，并禁止不必要的存储过程。
3. 对网页应用程序进行安全加固，修补 SQL 注入点；注意在利用表单输入的内容构造 SQL 命令之前对所有输入内容进行过滤。
4. 应用程序修改完成后，通过应用漏洞扫描工具和人工分析检查 SQL 注入漏洞是否已经得到修复。
5. 将系统安装最新安装补丁，并验证补丁的有效。
6. 修改系统和应用的全部密码。

- 根除

1. 进一步深入监控和分析业务系统、应用、防火墙等日志，观察修补后的 SQL 注入网页漏洞是否得到有效的解决。
2. 在有必要的情况下，要求第三方安全公司技术专家对修补后的网页漏洞进行进一步技术评估验证，直至确认漏洞以被修复解除。

网页挂马事件处理

- 紧急处理措施

1. 通过防病毒软件、木马专杀工具或手工方式进行木马程序杀毒，清除网页上被挂的木马程序。
2. 如果木马难以彻底清除，需要启动系统恢复，将网站恢复到没有被挂马的状态。

3. 通过各种日志系统分析网站被攻击和挂马的途径，采取防范和监控措施，避免网站被再次挂马。

➢ 抑制

1. 安置好取证工作环境，进行攻击分析，包括：取证采样（包括前一时段的防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

2. 给系统安装最新的操作系统和应用软件安全补丁，并验证补丁有效性。

3. 对网页进行安全加固，修补网页应用程序漏洞及 SQL 注入点。

4. 修改所有系统密码和应用密码；

5. 更新防病毒软件病毒库。

➢ 根除

进一步深入监控和分析业务系统、IDS、防火墙、应用程序日志，采取更准确而针对性的处置措施，然后继续观察处置措施的效果，同时进一步寻找更有效和根本的解决措施，直至确认危险解除。

计算机病毒事件处理

➢ 紧急处理措施

1. 断开被感染的服务器网络；

2. 启用备用服务器；

3. 通过在防火墙或网络设备设置访问控制策略，限制外部的访问。

➢ 抑制

1. 安置好取证工作环境，进行攻击分析，包括：取证采样（防火墙日志、入侵检测日志、路由器日志等）、流量特征分析、报文特征分析及其他分析，确定攻击方式、类型等；

2. 在问题主机上，确定病毒（木马）代码特征：进程、端口等，通常以 netstat –naple 查看进程和端口的绑定情况，分析出异常的端口或者进程；

3. Windows 下用任务管理器查看现有进程，Linux 下 Ps –ef 会列出系统正在运行的所有进程，一般先停止恶意进程，同时将其相关文件删除。

➢ 根除

1. 更新防病毒软件病毒库；

2. 更新系统补丁及漏洞修补程序；

3. 使用反病毒软件进行查杀，清除病毒（木马）；

4. 确认病毒类型后，下载专杀工具进行病毒清理；

5. 更新防火墙安全策略，将病毒网络数据包进行过滤。

6. 消除攻击源后，验证相关服务的运行情况；

7. 进行业务测试，确定系统完全恢复；

8. 病毒被完全清除后，系统上网运行。

9. 在不能确定木马是否被完全被清除的情况下，需要重新安装系统并进行加固。

3.3.6.3.5.事件总结

当安全事件应急处理完成后，应当对保密事件的发生原因、处理过程、处理方法以及调整安全策略等内容进行总结，并输出总结报告备案。

3.3.7.数据融合要求方案

本项目以联通手机信令原始统计数据为基础，围绕数据归集入库、交叉校验、规整对齐、全流程运维监控四大核心环节搭建标准化数据融合体系，覆盖朝阳区全域、43 个街乡镇、81 个重点监测区、12 个商圈、24 个景区及临时新增监测区域全空间范围，适配 30 分钟实时、日度、月度多时间粒度数据集输出要求，解决多源信令数据口径不一、数值偏差、数据断缺、格式混乱等问题，实现人口、客流、职住、通勤数据统一归集、清洗、校验、标准化输出，保障数据真实、完整、一致、可用，满足朝阳区人口大数据监测业务分析、人口调控、城市治理的数据支撑需求。

3.3.7.1.数据归集入库实施细则

1.标准化入库流程搭建

建立统一数据接收规范，针对实时（30 分钟）、日度、月度三类数据集分别设计独立入库通道，明确接口协议、文件格式、传输命名规则、推送时段约束：

o 实时数据：每 30 分钟定时推送接口报文，到达后自动触发入库程序，超时未推送自动告警；

o 日度数据：每日固定时点完成全量日度指标包推送，t+3 日内完成全量入库归档；

o 月度数据：每月次月 5 日前完成上月全量月度数据集推送，次月 8 日前完成入库，预留 2 天校验整改窗口期，满足次月 10 日前出分析成果要求。

2.全维度数据统一归集范围

归集覆盖全部业务指标：实时人流量/栅格数据、瞬时流入流出、日度实有进区人群、职住用户、客流停留时长、月度职住 OD、通勤半径/时长、人群性别/年龄/归属地标签等全部统计汇总表；同步纳入临时新增监测区域动态数据，支持采购人按需新增区域后自动纳入归集清单，无需调整底层入库架构。

3.入库完整性校验前置

数据落地存储前执行前置规则校验：校验文件完整性、数据表字段完整性、监测区域编码（areaid）全覆盖性、时间字段连续性，缺表、缺字段、区域编码缺失直接拦截入库，生成异常工单推送运维人员处理，确保入库资料齐全、收纳规范。

4.分层存储归集架构

采用分层存储架构：原始信令统计结果层、清洗中间层、标准化融合成果层，三层数据隔离存储，原始数据留存备查，融合成果单独对外提供，保障归集链路可追溯。

3.3.7.2.统计数据交叉校验实施方案

建立机器自动校验+人工复核双机制，全链路排查数值偏差、覆盖缺失、统计异常、网格定位匹配误差四大类问题，多层交叉比对保障数据合规有效。

1.多维交叉比对规则体系

o 空间维度交叉：同一时段全区总量数据与 43 个街乡镇分项汇总数据做差值校验；商圈、景区客流汇总数据同步与所属街乡镇数据交叉核对；

o 时间维度交叉：实时 30 分钟分时数据累加结果与当日日度人流量数据比对，月度数据与每日日度数据汇总结果双向校验，识别漏推送、数据回传缺失问题；

o 人群标签交叉：同一区域同一时段总人流量=各年龄段人群之和=男女人群之和=各归属地人群之和，分项求和与总量差值超限自动预警；

o 职住指标交叉：月度职住 OD 流入、流出总量与各街道工作 / 居住用户数据交叉核验，通勤半径、通勤时长数据与职住分布数据联动校验。

2.异常分级处置机制

按异常严重程度分级处置：

o 潜在缺失/偏差：实时推送运维工单，2 小时内核查底层信令数据源，若确实存在确实，当日完成数据补全、纠偏；

o 严重缺失/偏差：触发应急响应，对接联通底层基站信令源头排查，4 小时内反馈采购人问题原因，24 小时内完成数据回补重算。

3.周期性全面复核

每日完成当日日度数据全量交叉校验；每月完成上月所有月度指标人工复核,，列明异常点、修正方案、修正后数据。

3.3.7.3.统计数据规整对齐实施规范

针对多表、多粒度、多区域数据存在的字段口径、统计维度、输出格式差异问题，统一标准化规整规则，实现全数据集格式、口径、编码统一。

1.统一基础编码标准

固化全局唯一编码体系：统一 sd_date 时间编码、areaid 区域编码、grid_x/grid_y 栅格编码、attrid 归属地编码、gendertype 性别编码、年龄段分段编码，所有数据表共用一套编码字典，消除区域、标签字段不统一问题；新增临时监测区域同步更新编码字典并同步至所有数据表。

2.统一统计口径对齐规则

严格匹配采购需求中用户标签定义，统一居住用户、工作用户、瞬时客流、实有进区人群判定标准：

o 统一居住用户、工作用户判定算法口径（月度 15 天停留时长、早晚时段判定规则全链路统一）；

o 统一流入/流出判定、客流停留时长分段、通勤半径区间划分标准，实时、日度、月度数据一套口径，不存在分段规则差异；

o 统一栅格空间精度、区域边界测绘标准，按朝阳区经纬度范围统一切分网格，保证栅格数据空间对齐。

3.数据表格式标准化规整

严格按照采购需求附表模板规整所有输出数据集，统一字段名称、字段类型、排序规则、空值填充规范：缺失数据统一填充固定标识，不出现空白、乱码、自定义特殊符号；所有实时、日度、月度输出表完全匹配需求样表结构，字段顺序、字段数量、维度拆分标准完全一致，消除格式混乱。

4.历史数据兼容对齐

针对项目服务期内跨月份、跨季度对比分析需求，对历史存量数据同步执行规整对齐，保证同比、环比分析时口径统一，不存在前后数据规则变更导致的对比失真。

3.3.7.4.全流程动态运维监控保障方案

搭建数据融合全链路可视化监控平台，覆盖数据推送→接收入库→清洗规整→校验计

算→成果输出全环节，常态化监测、实时预警、闭环处置。

1.全流程状态实时监控

监控核心指标包含：数据推送到达时间、文件推送成功率、入库完成时长、校验异常数量、数据加工耗时、接口传输时延；针对实时 30 分钟接口重点监控传输时效，确保每轮数据在 30 分钟周期内完成传输入库，超时实时告警；对日度、月度数据集加工进度计时监控，保障日度 t+3、月度次月 10 日前交付时限。

2.多渠道异常告警机制

设置多级告警推送渠道：看板红色预警、邮件同步推送；监控异常类型包含：数据断更、整表缺失、单区域数据空白、数值剧烈波动、传输加密失败、接口访问超时、底层信令源波动等。

3.异常闭环处置流程

告警触发后自动生成处置工单，明确责任工程师、处置时限：

1）5 分钟内响应定位异常环节（推送端/传输链路/清洗计算/底层信令源）；

2）按分级处置要求完成修复、重算、数据回补；

3）修复完成后自动二次校验，确认数据正常后关闭工单。

4.7×24 小时运维值守保障

依托本项目配置 4 名数据治理工程师专职负责数据融合运维监控，建立 7×24 小时应急值守机制，重大节假日、大型活动期间增派专人盯守实时客流数据链路，保障突发时段数据不中断、融合流程稳定运行。

4.售后服务及承诺

为了保证项目实施后方便使用以及在使用中遇到问题及时获得响应，我司提供完善的售后服务工作并承诺：

在服务期满后，若后续供应商未能到位，将持续提供与原合同约定的相同标准的服务，直到后续供应商接续或采购人停止服务的通知止。

我司派遣一名专职客户经理，根据与招标方签订协议提供一年 7*24 小时工作日在线电话、邮件技术支持。如不能解决招标方问题可由客户经理向公司申请后台技术二线支持，如远程方式不能解决问题可由客户经理申请后台三线技术专家赴招标方现场。

为系统的稳定、安全、高效运行，应配备相应的高素质技术人员负责系统日常的运行、维护和管理工作。为了保证本项目服务的质量，应配备相应的专业技术人员，本项目施行项目经理负责制。配置项目经理 1 人，计算机专业；数据分析工程师 2 名，统计学等专业；数据治理工程师 4 名，计算机等专业。乙方可以根据项目需要，将部分工作内容委托给中国联通专业子公司或具备资质的合作伙伴实施，乙方对中国联通专业子公司及具备资质的合作伙伴向甲方承担连带责任。

我司保证 7*24 小时对紧急需求的响应，二线技术专家实现 2 小时响应，三线专家 4 小时赴现场响应。

1、在线服务

●热线服务

在我们维护中心，配有热线电话、值班手机和经验丰富的技术人员，常年 7*24 小时通过电话解答用户的技术问题和指导用户解决一般性故障。

●远程维护服务

在用户许可的情况下，对于用户出现的系统和应用软件问题，我们的维护人员将通过远程网络提供实时在线服务，为用户排除故障。

●现场紧急服务

对于突发的系统故障，如果情况紧急或不便于使用远程手段解决，我们将指派具有丰富经验的技术人员赶赴现场，进行现场技术支持服务。

如果系统在试运行阶段或缺陷责任期内发生故障，业主向承包人发出故障通知后，我方 7*24 小时响应（包括节假日），如需到客户现场，每天 8:00～18:00 期间 2 小时到达故障现场，其余时间 4 小时内到达故障现场。

2、技术支持服务

我们将根据要求，提供下列服务：

✧由技术支持部组成专门小组负责客户系统维护支持，如果需要，我公司可委派专门小组长驻现场进行支持。

✧以技术培训、交流会、合作开发、外出考察等多种形式为客户培养一支精通业务和大数据技术的队伍，并协助用户开发新的大数据应用系统。

3、故障响应及处理

（1）我司进行应用系统性能检测、效能分析，确保对问题能够事先预防，避免出现故障和问题。

（2）我司提供 7*24 小时响应服务，（包括节假日），如需到客户现场，则每天 8:00～18:00 期间 2 小时到达故障现场，其余时间 4 小时内到达故障现场。

（3）我司承诺若出现以下 2 种情况保障故障恢复时间：

✧一般故障 4 小时内解决；

✧重大故障 24 小时内解决。

（4）我司承诺在故障发生 24 小时内向甲方提供故障报告。

4、定期回访

定期回访，了解用户使用情况，解答用户疑问，排除故障。

5、定期升级

在质保期内我公司免费提供质量保证和软件升级、功能完善，并提供现场服务。质保期内我公司承诺将向招标人免费提供对系统软件有所改进、增加新功能以及为适应新标准所做修改的最新版本，供招标人使用，并保证升级后的系统能够稳定的运行。质保期内我公司承诺将根据国家有关管理要求的变化，免费对接口系统软件进行修改、调整。

6、服务档案

从项目启动开始，单独为本项目建立服务档案，包括设计、使用、维护情况等，并由专人管理，以保证提供的售后服务准确、周到、及时。