2024年度开发区宽带无线城市综合服务

委托服务合同

项　目　名　称：2024年度开发区宽带无线城市综合服务

委托方（甲方）：北京经济技术开发区营商环境建设局

受托方（乙方）：北京博大网信股份有限公司

签　订　地　点：北京经济技术开发区

委托服务合同

甲方：北京经济技术开发区营商环境建设局

乙方：北京博大网信股份有限公司

根据《中华人民共和国民法典》及相关法律、法规规定，在遵循平等、自愿、公平和诚实信用的基础上，甲、乙双方经协商一致，就乙方为甲方提供本合同项下相关服务事宜达成如下协议：

第一条 项目名称、服务内容及要求

（一）项目名称：2024年度开发区宽带无线城市综合服务

（二）服务内容：

提供5大类不少于50处场景,AP热点总量不少于3000点的公共Wi-Fi 网络服务，服务期内按需新增的场景公共Wi-Fi网络服务、综合运营管理平台服务及数据对接服务。室内及室外无线AP支持Wi-Fi 6技术标准及服务。

（三）服务标准要求：

乙方应配合经开区管委会制定项目服务流程和操作规范，以保证各项服务内容实行流程化管理，服务过程操作规范，确保服务质量满足北京经济技术开发区要求；具备详细的服务管理文档和服务操作文档，确保各项服务活动可追踪、服务效果可验证；根据北京经济技术开发区公共 Wi-Fi 发展现状,建立经开区宽带无线城市网络管理资料库与数据库，并以数字化形式进行展现。

服务具体内容和要求详见合同附件一《项目实施方案》。

第二条 履行期限、进度与地点

（一）合同履行期限：自合同签订生效之日起6个月内完成项目整体建设并通过甲方开通确认，开通确认后服务期一年（开通确认后正式启动本项目服务工作开始计算服务期）。

（二）具体进度要求如下：

1. 本合同生效后【15 】日内，乙方应按照甲方要求和合同约定，制定并向甲方提交《项目实施方案》(附件一)。乙方按照甲方审核确认后的项目实施方案组织项目实施。前述经甲方确认后的项目实施方案将作为甲方验收的依据之一。

2. 公共 Wi-Fi 网络整体架构搭建要求自签订本项目服务合同2个月内实现。

3. 公共 Wi-Fi 热点服务开通进度要求自签订本项目服务合同2个月内实现20%热

点AP数量；4个月内实现 50%热点 AP 数量；6个月内实现 100%热点 AP 数量。

4. 综合服务管理平台要求自签订本项目服务合同2个月内部署调试完成。

5. 【2026】年【4】月【20】日前：乙方应依约完成履约验收目标，提出履约验收申请，甲方按照项目管理和合同要求进行履约验收。

6. 【2026】年【4】月【20】日前：对项目实施情况进行总结，并形成报告提交甲方。

（三）履行地点：北京经济技术开发区。

第三条 合同成果、交付及其验收

（一）合同成果包括：

包括但不限于周报、月报、设备巡检表、报修记录表、系统故障记录表、绩效报告、满意度、年度总结。

（二）合同成果交付

1. 期限：合同签订之日至服务开通确认后服务期满一年止。

2. 地点：北京经济技术开发区。

3. 方式：提供项目纸质和电子版最终验收文档。

（三）合同成果验收

1. 验收将依据合同及其附件、国家相关规范、标准，如无国家、行业标准，则应以合理满足本合同及附件的约定，且以甲方事后认可为达到本合同质量要求的依据，由甲方或甲方委托的第三方按甲方确定的时间和方式进行验收。

2. 具体验收标准和流程：

（1）达到最终验收标准。

（2）符合国家及部颁法规及规章规定要求和本合同约定，乙方在项目服务期内服从项目监理的管理。

（3）乙方应依据本合同规定的时限出具服务成果，并及时通知甲方进行验收。如服务成果未能通过甲方的验收，则乙方应依据甲方的意见进行限期重新调整，在限期内重新调整后及时通知甲方进行再次验收，并保证不因此而延误服务成果的交付日期，因重新调整产生的全部费用均由乙方承担。如服务成果通过甲方的验收，应按照《开发区信息化项目管理办法》签署验收报告；如仍未通过验收的，乙方应依约承担违约责任。

本项目服务周期内进行两次验收，第一次验收时间为完全具备服务条件后进行，第二次验收时间为服务周期结束后进行，乙方提交本项目运行服务验收材料。甲方确定服务AP数量、平台能力、互联网接入服务情况，出具验收意见。

3. 乙方应提交的验收资料：包括但不限于周报、月报、设备巡检表、报修记录表、系统故障记录表、绩效报告、项目考核指标、满意度（公众满意度评价、市民投诉及处理率）、年度总结。

4. 验收合格的，由甲方或甲方委托的第三方出具项目验收证明。验收不合格的，乙方应依约承担违约责任。

第四条 合同价款与支付

（一）本项目合同价款：人民币【大写：捌佰玖拾伍万伍仟】元整（【￥8955000】元）。

前述合同价款业已包含劳务费、人工管理费、税款、加班费等乙方为履行本合同项下义务所应当获得的所有报酬和费用，以及甲方为此项目所有应当支出的费用。除本合同中上述明示的价款外，乙方无权再向甲方额外申请支付其他任何报酬或税费。

（二）支付方式：

双方同意甲方按下列第【 1 】项约定的方式支付合同价款：

1. 分期付款

（1）合同签订生效，乙方依约提交项目实施方案，且甲方收到乙方提供符合要求的合法有效发票后【10】个工作日内，甲方向乙方支付【70】%合同价款，即人民币【大写：陆佰贰拾陆万捌仟伍佰】元整（【￥6268500】元）；

（2）全部服务履约验收合格，且甲方收到乙方提供符合要求的合法有效发票后【10】个工作日内支付【30】%合同价款，即人民币【大写：贰佰陆拾捌万陆仟伍佰】元整（【￥2686500】元）。

2. 一次性付款

甲方于项目履约验收合格，且收到乙方提供符合要求的合法有效发票后【10 】个工作日内一次性向乙方全额支付合同价款。

（三）乙方应向甲方提供符合甲方要求的合法发票及乙方的账户信息，并保证该账户合法、有效、可用，否则甲方有权拒绝支付合同价款，且不承担任何责任。如乙方向甲方提供的发票不符合本合同约定或法律规定，因此给甲方造成的一切损失由乙方承担。

乙方账户信息：

户　名：北京博大网信股份有限公司

开户行：中国银行北京自贸试验区高端产业片区支行

账　号：319 456 027 891

（四）价款明细详见附件二。

第五条 双方的权利义务

（一）甲方权利义务

1. 甲方有权对《项目实施方案》提出修改意见和进行确认，确定项目主要工作内容和目标，审批项目计划与进度，制定项目验收标准并组织项目的验收。

2. 甲方有权要求乙方严格履行合同义务，配合查询项目资金使用情况；有权向乙方提出具体工作要求，乙方不得以任何理由拒绝或拖延执行。

3. 甲方有权监督、随时审查乙方的服务内容和质量，要求乙方提交符合要求的工作成果，有权对不符合合同规定的内容提出整改意见或更换不合格工作人员，乙方应遵照执行，若不予改正或改正后仍未符合要求的，甲方有权提前解除本合同，乙方应退回甲方已支付的全部款项，并依约承担违约责任。

4. 甲方发现乙方提交的合同成果有违反国家法律法规，不符合政治性、科学性，有低俗内容或出现质量问题的，甲方有权提前解除合同，乙方应退回甲方已支付的全部款项，并依约承担违约责任。

5. 甲方有权组织或委托第三方对乙方实施项目进行评估、项目验收；若乙方未通过评估或验收，乙方应在限期内补充完善或予以改正。否则，甲方有权提前解除合同，乙方应退回甲方已支付的全部款项，并依约承担违约责任。

6. 本合同项下成果的所有权、知识产权及其他相关权利均归甲方所有。乙方除为履行本合同项下义务外不得使用。

7. 按本合同约定向乙方支付合同款。

（二）乙方权利义务

1. 乙方应独立完成合同规定的服务内容，按时提交符合要求的工作成果，严格按照相关文件、项目实施方案开展工作，保证工作内容和质量符合国家法律法规、主管部门标准和甲方的要求。

2. 乙方按照合同约定和项目具体情况派出服务团队人员（详见附件三），不得随意更换服务团队人员，若确需更换需事先征得甲方书面同意，且接替人员的职位、资历应当与被调换的人员相当。乙方指定【于光】为项目负责人，联系电话：15001335155。

3. 在甲方指导下进行项目实施工作，接受甲方或甲方委托第三方开展的项目监管、检查调研、中期评估、项目验收等，配合甲方完成相关工作计划调整。

4. 乙方保证其在提供服务和形成资料的过程中所使用的文件、资料、软件、背景

音乐及其他物品均可合法用于本项目的执行。乙方保证其服务与资料、交付的成果合法、合规且不侵犯任何第三方的知识产权或其他合法权益，不存在任何与此相关的争议，否则一切后果由乙方承担。

5. 乙方须保证其履行本合同项下义务的合法性，并保证甲方不会因此而遭到任何第三方的索赔或陷入任何法律纠纷，否则，相关责任和后果均由乙方自行承担，且乙方亦应承担甲方因此而遭受的任何损失、支出及索赔（包括但不限于法律费用）。

6. 乙方对其因履行本合同所知悉的与本项目相关的信息以及甲方其他未公开的信息，应当采取适当有效的方式予以保密。

7. 本合同规定的任务不得以任何形式转包。

第六条 违约责任

（一）任何一方未履行或未完全履行本合同项下的义务，均构成违约。违约方应赔偿因违约给对方造成的一切损失。

（二）乙方未按本合同约定按期提供本合同下任一项成果的，每逾期一日，乙方须向甲方支付本合同价款总额 0.1%的违约金。每项违约行为可以单独计算违约金；逾期达 10 日的，甲方有权解除合同，乙方应向甲方支付合同总价款 30%的违约金并赔偿甲方遭受的全部损失。

（三）乙方提供本项目各成果不符合甲方要求的，乙方负责更正和修改，因此造成的所有损失和费用的增加由乙方承担，因此造成逾期交付的，按照前款内容承担逾期违约责任。

（四）因乙方侵犯第三方合法权益造成甲方涉诉或被投诉、举报的，由乙方承担全部责任，并向甲方支付相当于合同总价款 30%的违约金，赔偿甲方遭受的全部损失。同时，甲方还有权解除本合同，乙方应退还甲方已支付的全部款项。

（五）若乙方擅自解除、中止或终止本合同的，应退回已收到的合同款，向甲方支付合同总价款 30%的违约金，并赔偿甲方遭受的全部损失。

（六）因乙方违反本合同约定而须向甲方支付的任何款项（包括但不限于损失赔偿费用、违约金等），甲方均有权在应向乙方支付的合同款项中予以扣除。

（七）未经甲方书面同意，乙方将承担的工作内容转包、分包、转让或转委托，或者造成保密信息的被盗、泄露或其他有损信息保密的，甲方有权解除合同，乙方应退回已收到的合同款，向甲方支付合同价款 30%的违约金，赔偿甲方因此遭受的全部损失。

（八）本条全部损失包括但不限于诉讼费、仲裁费、律师费、调查费、第三方主张

的赔偿金以及其他因此支付的合理开支。

第七条 争议的解决

双方因本合同而发生的争议，应首先由甲乙双方协商解决。如协商不能解决的，则任何一方可以向甲方所在地有管辖权的人民法院提起诉讼。讼进行过程中，双方将继续履行本合同未涉仲裁或诉讼的其它部分。

第八条 其它

（一）本合同未尽事宜，双方应友好协商解决并签订《补充协议》。《补充协议》经双方盖章确认后，与本合同具有同等的法律效力。

（二）本合同一式【陆】份，具有同等法律效力。甲、乙双方各执【叁】份。

（三）本合同经双方签字并加盖公章或合同专用章后生效。

（四）本合同的所有附件均是本合同不可分割的组成部分，与本合同具有同等法律效力。若附件与合同正文有任何不一致，以合同正文为准。

本合同附件为：一、项目实施方案

二、项目分项报价

三、项目主要人员组成

（以下无正文）

甲方：北京经济技术开发区营商环境建设局

法定代表人/负责人：

或授权代表（签字）：

日期：2024年10月25日

乙方：北京博大网信股份有限公司

法定代表人/负责人：

或授权代表（签字）：

日期：2024年10月25日

附件一

项目实施方案

1. Wi-Fi 网络接入服务方案

1.1. 基本接入服务方案

北京经济技术开发区以“E-town”作为用户公共 Wi-Fi 服务的统一业务名称，提供 7*24 小时免费无线接入服务，每个 AP 单点不低于 4M，覆盖区域内切换无断点。接入前由开发区行政审批局委托第三方检测机构按服务规范检测，合格后方可提供服务。用户通过网络 Portal 基于手机号码完成首次注册认证登录后，可实现“一次注册、无感知认证、可追溯、可管理”，终身无感知接入。

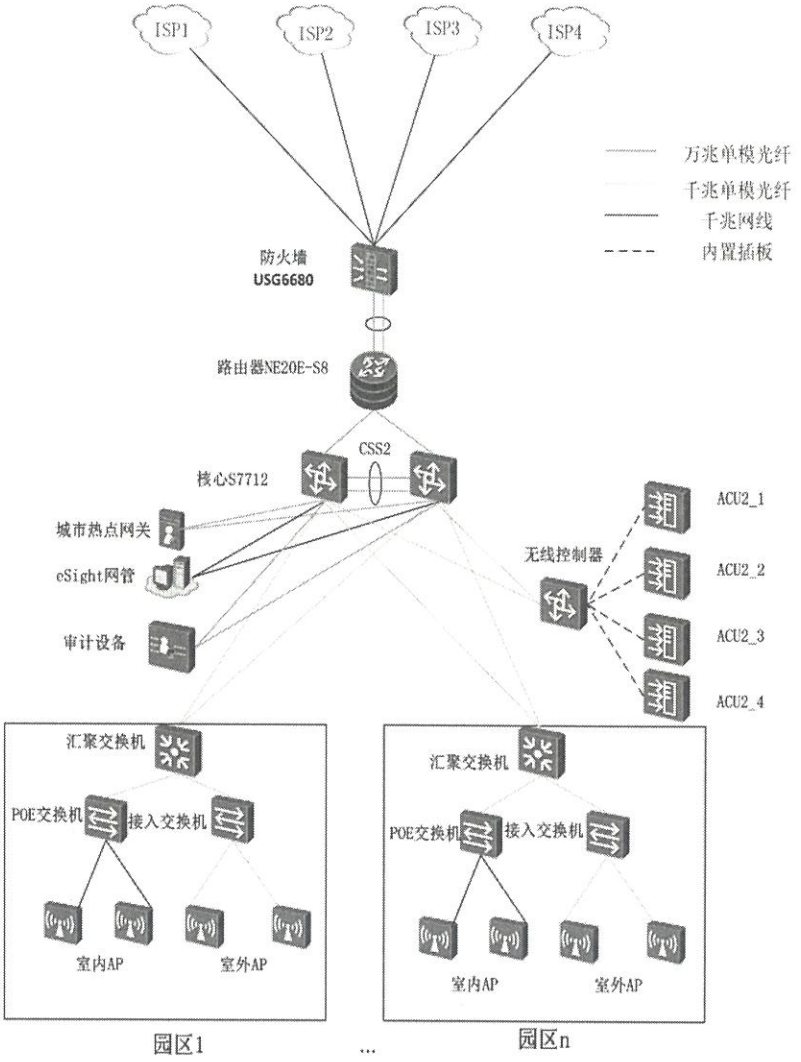
2. 网络建设服务方案

2.1. 网络设计

为满足网络安全等要求，需配置公共 WiFi 网络专用安全设备，具备基于 AP 位置的多种管理功能，相关设备还支持多种功能，如用户接入、AP 反制、应用路由等。要求按核心层、汇聚层、接入层组网，在经开区建专属机房，各层设备放于机房，流量汇聚到核心层，满足多项条件，如 WLAN 覆盖强度、带宽原则不限制、网络承载及设备需支持 Wi-Fi6，整体服务还具备动态调整、完整传输网络、可扩容及扩展等特点。

总体网络拓扑如下图所示:

网络拓扑图



核心层

2.1.1. 核心层

核心层是园区数据交换的核心，连接园区网的各个组成部分，如数据中心、汇聚层、出口区等，核心层负责整个园区网络的高速互联。实现带宽的高利用率

和网络故障的快速收敛，通常需要部署高性能的核心交换机，通常三个以上部门规模的园区网建议规划核心层，核心交换机通过万兆单模光纤上连至出口区域防火墙。

2.1.2. 汇聚层

汇聚层是接入层与园区核心骨干网之间的网络分界线，主要用于转发用户间的“横向”流量，同时转发到核心层的“纵向”流量。汇聚层可作为部门或区域内部的交换核心，实现与区域或部门专用服务器区的连接。另外汇聚层还可以扩展接入终端的数量。汇聚层交换机通过千兆单模光纤双上连至核心交换机。

2.1.3. 接入层

接入层为用户提供各种接入方式，是终端接入网络的第一层。接入层通常由接入交换机组成，接入层交换机在网络中数量众多，安装位置分散，通常是简单的二层交换机。如果终端层存在无线终端设备，接入层需要无线接入点 AP 设备，AP 设备通过接入交换机接入网络。AP 通过千兆网线上连至接入交换机，接入交换机通过千兆单模光纤上连至汇聚层。

2.1.4. 园区出口区

园区出口是园区内部网络到外部网络的边界，内部用户通过园区出口区接入到外部网络，外部网络的用户通过园区出口区接入到内部网络。园区出口区一般需要部署出口路由器和防火墙。路由器解决内外网互通的问题，防火墙提供边界安全防护能力。

2.1.5. 网络管理区

网络管理区是管理网络服务器（例如网管系统、认证服务器等）的区域。标准的网管系统通过 SNMP（Simple Network Management Protocol，简单网络管理协议）和网络设备交互，能够提供配置、管理和维护功能，例如网络拓扑和端口的显示管理、网络设备的配置管理、网络故障诊断和告警、网络性能和状态分析等。

2.2. 网络质量服务方案

符合 GB/T 21671 要求及相关发展需求，提供 7×24 小时免费 Wi-Fi，每个 AP 单点不低于 4M，统一认证，无断点切换，有监测平台报送数据，符合安全要求。

2.2.1. 自动调优

当 AP 射频环境出现恶化，某个 AP 故障或新增扩容 AP 时，可以启动射频自动调优，以增强系统的可靠性和稳定性。选择同时支持局部调优和全局调优的 AP 设备。局部调优可方便的应用于扩容新 AP、单点 AP 故障或者微波炉等局部环境变化而引起的信道环境变化场景。

2.2.2. 负载均衡

无线用户端一般会根据 AP 信号强度（RSSI）选择 AP，这很容易导致大量的客户端仅仅因为某个 AP 信号较强而连接到同一个 AP 上。由于 WLAN 是基于 CSMA/CA 机制，实现多用户接入，当单台 AP 接入用户数过多时，用户吞吐率性能会出现急剧下降且稳定性无法保证。负载均衡特性可以按照用户数量和用户流量，将用户分配到同一组但负载不同的 AP 上，从而实现不同 AP 之间的负载分担，避免出现某个 AP 负载过高而使其性能不稳的情况。

2.2.3. 干扰检测

WLAN 网络的无线信道经常会受到周围环境影响而导致服务质量变差。通过配置干扰检测，监测 AP 可以实时了解周围无线信号环境，并及时向 AC 上报告警。

2.2.4. 多层级的流量控制能力

基于 SSID 的流量控制、基于 AP 的流量控制、基于用户的流量控制，并且支持多层级的组合使用。通过这些手段，管理员可以按不同的接入区域/热点设定不同的上下行流量带宽限制，比如公共场所 AP 提供带宽小于办公场所的带宽；可以指定具体账号的带宽限制，比如公共账号提供 2M 的带宽限制，以防止恶意的带宽占用；对于部分场合可以部署多种 SSID 接入服务，比如一个是 XXXX 无线城市，一个是 XXXX 区政，为两个不同的 SSID 接入服务设定不同的带宽资源。

2.3. 网络安全服务方案

2.3.1. 技术防范及运营维护

2.3.1.1. 网络、系统安全维护

从网络的连通性、网络的性能、网络的监控管理三个方面实现对网络系统的运维管理。

设备基础性能检测：cpu、内存使用情况监测；设备日志查看；设备 snmp 状态；测试 Ping，tracert 等工具的连通性；网络安全策略应用是否正常；

Internet 带宽流量的实时监测；网络拓扑链路状态监测；异常网络数据包流量；Dos、ddos 等网络攻击情况监测；Internet 线路的误码率、丢包率监测等技术指标。

2.3.1.2. 突发事件应对策略

值班人员平时应做好应急事件的监控工作，对于突发事件应认真分析、准确判定故障发生的数据域，负责跟踪该事件直至其结束。对于不在运维中心的故障，应在第一时间内通知负责人去现场处理，密切关注事件流程及进展情况，并做好登记工作上报领导。

正常情况下，要求值班人员在 10 分钟内进行事件确认。如果属于一般事件则按照事件流程进行分派处理，否则应迅速启动《应急预案》，并严格按照《应急预案》所规定的步骤快速实施应急处置，及时汇报上级领导，掌握实时处理情况。

在处理过程中，如需其他部门去现场增援处理，应及时向上级领导部门汇报，协调沟通，尽快联系技术工程师或厂家技术支持赶赴现场援助处理。

2.3.2. 安全审计

符合《互联网安全保护技术措施规定（公安部 82 号文）》相关要求。根据国家相关标准和要求建设网络信息安全管理系统、认证系统，对用户登录、信息发布等操作行为进行严格审计，达到公安平台可控审计追溯的能力，并符合上级宣传、网信、公安等部门相关要求，确保网络信息安全。

2.3.3. 访问控制

统一权限管理系统包括统一身份、统一认证管理、统一授权与安全审计四个核心功能模块，实现人员身份管理、组织机构管理、授权管理、合规性管理、安全审计等模块功能，实现统一管理、流程规范、过程受控、备案审查的目的。

2.4. 数据安全防护服务方案

2.4.1. 组网安全建设方案

北京经济技术开发区内主干道路均布放完成通信光缆，核心机房及主要光纤链路双线接入。可快速开通新增 AP 点位，满足招标方未来扩容条件。

核心网络设备布置在位于北京经济技术开发区内，所有用户数据及带宽汇聚核心统一分配管理。利用任子行审计设备，确保所传输数据的完整性、准确定性、

合理性，并且同步至开发区审批局。网络总出口带宽设备交换容量≥7.9Tbps 支持包转发率≥960Mpps。所有场景均通过核心机房多条冗余带宽进行上网访问，多条带宽自动调配资源来满足带宽冗余接入需求，实现各 AP 点位带宽进行自动动态调整。出口设备配备防火墙，保障数据不泄露、损坏、篡改或者丢失。配置双核心交换机，保证网络数据连通性。所有原始数据均物理隔离保存，单独存放，用户认证及上网行为数据保存日期不少于 1 年。

接入层为用户提供各种接入方式，是终端接入网络的第一层。接入层通常由接入交换机组成，接入层交换机在网络中数量众多，安装位置分散，通常是简单的二层交换机。如果终端层存在无线终端设备，接入层需要无线接入点 AP 设备，AP 设备通过接入交换机接入网络。AP 通过千兆网线上连至接入交换机，接入交换机通过千兆单模光纤上连至汇聚层。

汇聚层是接入层与园区核心骨干网之间的网络分界线，主要用于转发用户间的“横向”流量，同时转发到核心层的“纵向”流量。汇聚层可作为部门或区域内部的交换核心，实现与区域或部门专用服务器区的连接。另外汇聚层还可以扩展接入终端的数量。汇聚层交换机通过千兆单模光纤双上连至核心交换机。

核心层是园区数据交换的核心，连接园区网的各个组成部分，如数据中心、汇聚层、出口区等，核心层负责整个园区网络的高速互联。网络需要实现带宽的高利用率和网络故障的快速收敛，通常需要部署高性能的核心交换机，通常三个以上部门规模的园区网建议规划核心层。核心交换机通过万兆单模光纤上连至出口区域防火墙。

园区出口是园区内部网络到外部网络的边界，内部用户通过园区出口区接入到外部网络，外部网络的用户通过园区出口区接入到内部网络。园区出口区一般需要部署出口路由器和防火墙。路由器解决内外网互通的问题，防火墙提供边界安全防护能力。

网络管理区是管理网络服务器（例如网管系统、认证服务器等）的区域。标准的网管系统通过 SNMP（Simple Network Management Protocol，简单网络管理协议）和网络设备交互，能够提供配置、管理和维护功能，例如网络拓扑和端口的显示管理、网络设备的配置管理、网络故障诊断和告警、网络性能和状态分

析等。

此次无线控制区选用一台 S7712 交换机，并且通过无线接入控制单板 ACU2 板卡实现对无线 AP 接入点的统一运维管理。管理交换机通过万兆单模光纤双连至核心交换机。无线接入控制单板 ACU2 是一块安插在交换机中用来实现 WLAN 无线接入控制器功能的单板。无线接入控制单板 ACU2 可以在大型企业以及园区中承担关键的无线服务，可灵活配置无线接入点的管理数量，最大可管理 2048 个 AP，具有良好的可扩展性。全系列 802.11n/802.11ac 无线接入点，实现大规模，高密度的无线用户接入 服务。

管理运营系统建设拟采用分层、模块化的设计技术，模块与模块、层与层之间松散耦合，为了方便日常管理，系统应采用 B/S 架构，所有操作和配置均为 B/S 界面操作完成。

2.4.2. 明确安全责任人

对重大工程项目采取分层管理方式，主要分为高层项目负责人和项目管理层两个层次，项目管理层结合具体工程项目情况又可分为多个职责明确的工作组。

3. 点位测试服务方案

3.1. 测试目的

测试的目的在于发现场景中的服务点位是否存在信号传输问题，即缺陷或错误，通过测试来确认硬件产品的质量是否满足用户的需求和期望。具体来说，测试的目的可以细分为以下几个方面：

验证服务功能：测试的首要目的是验证服务是否按照设计规格和用户需求进行工作。这包括检查服务的功能是否完整、正确，以及是否满足特定的性能要求。

发现软件缺陷：通过执行测试用例和检查软件的输出，测试人员能够发现软件中的错误、缺陷或不符合预期的行为。这些缺陷随后会被报告给开发团队进行修复。

评估硬件质量：测试有助于评估硬件的整体质量，包括其稳定性、可靠性、易用性和安全性等方面。通过收集和分析测试数据，可以对硬件的质量进行量化评估。

提供反馈和改进建议：测试过程中发现的问题和缺陷可以为开发团队提供宝贵的反馈，帮助他们改进开发流程、优化软件设计，并避免在未来的项目中犯同

样的错误。

满足用户需求和期望：最终，测试的目的是确保场景及服务点位能够满足用户的实际需求和期望，提供高质量的用户体验。

3.2. 测试场景

服务范围内已建成的AP点位共3000个及服务期内按需新增的场景的AP点位。

3.3. 测试方式

在测试场景中，采取定点和移动相结合的方式开展测试，分别对应不同的测试内容，具体详见测试内容。

对于人员密集环境采用定点测试，选取距离点位10M内距离测试，结合场景的施工图纸进行，对于热点区域内办公区、会议室等有长期驻留区域执行定点测试。

对于人员稀疏环境采用移动测试，结合场景的施工图纸进行，对于热点区域内开阔区域、过道等无长期驻留区域执行移动测试。

3.4. 测试内容

3.4.1. 信号质量测试

对无线城市热点区域开展测试，测试项目有信号强度、信噪比、统一业务名称。各指标测试方法和合格标准见下表

3.4.1.1. 信号强度

目　　的	测试规定区域内网络覆盖情况
指标定义：AP覆盖区域内的信号强度	
测试流程： 1、明确场景内网络覆盖区域 2、使用测试工具开展移动测试，同时记录信号强度 3、全部测试完成后统计平均信号强度	
合格标准： 平均信号强度值大于-80dBm	

3.4.1.2. 信噪比

目　　的	测试规定区域内网络覆盖情况
指标定义：AP 覆盖区域内的信噪比	
测试流程： 1、明确 AP 的覆盖区域 2、使用测试工具开展移动测试，同时记录信噪比 3、全部测试完成后统计平均信噪比	
建议值： 平均信噪比应在 20dB 以上，标准不作强制要求	

3.4.1.3. 业务名称统一

检查 AP 的业务名称是否符合《北京经济技术开发区宽带无线城市建设及服务规范 v1.0》中的相关要求，SSID 使用统一的名称：E-town。

3.4.2. 网络质量测试

为保证用户的体验，因此网络质量测试项目包括网络连接测试、网速测试、网站测试、视频测试共 4 个项目（包含 6 个指标）。3 个或以上测试项目满足合格标准则业务质量测试合格。

3.4.2.1. 网络连接测试

目　　的	测试网络连通性
指标定义：	$\text{ping成功率} = \frac{\text{ping成功的次数}}{\text{ping发起总次数}} \times 100\%$
预置条件： 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程： 1、终端通过测试工具 ping 内网 IP 地址：172.16.100.1 2、ping 内网 IP 地址 10 次 3、记录 ping 成功的次数	
合格标准： 成功率不小 98％	

3.4.2.2. 网络连接测试

目　　的	测试网络稳定性
指标定义：成功接入后从终端 ping 内网的时延	
预置条件： 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程： 1、终端通过测试工具 ping 内网 IP 地址：172.16.100.1 2、ping 内网 IP 地址 10 次，每个 ping 包大小为 1600 字节 3、记录 ping 成功返回的平均时间	
合格标准： 平均 ping 包时延不大于 100ms	

3.4.2.3. 网速测试

目　　的	满足用户传输需求，保障单终端 4M 网速
指标定义：从统一的服务器使用同一软件上传下载文件时的平均速率	
预置条件： 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程： 1、终端通过测试工具开始速率记录功能 2、使用三大运营商长途站点进行上传下载操作一段时间，待速率稳定后进行记录 3、测速地址：广东移动-211.136.192.6; 广东联通-202.96.128.86; 广东电信-210.21.196.6; 重复以上动作 10 次 4、记录上下行平均速率	
合格标准： 下行平均速率不低于 512KB/S，上行平均速率不低于 512KB/S	

3.4.2.4. 网站测试

目　　的	满足用户浏览需求，保障单终端访问固定网站的成功率
指标定义：	$$访问成功率=\frac{成功访问次数}{发起访问次数}\times 100\%$$
预置条件： 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程： 1、终端通过测试工具依次访问 5 个官方网站地址，等待网站返回信息 2、若返回错误信息或等待超过 20 秒，则访问失败 3、记录成功次数 4、官方网站地址包括：百度：110.242.68.3；新浪：123.126.45.205；网易：211.91.76.26；搜狐：123.125.244.111；腾讯：221.198.70.47。测试前须保证地址的有效性。	
合格标准： 访问成功率不低于 98％	

3.4.2.5. 网站测试

目　　的	满足用户浏览需求，保障单终端访问固定网站的访问时延
指标定义: 用户访问指定网页地址，记录网页地址返回时延	
预置条件: 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程: 1、终端通过测试工具依次访问 5 个官方网站地址，等待网站返回信息 2、Ping 网站 IP 地址 10 次，每个 ping 包大小为 1600 字节 3、记录网站访问地址平均时延 4、官方网站地址包括：百度：110.242.68.3；新浪：123.126.45.205；网易：211.91.76.26；搜狐：123.125.244.111；腾讯：221.198.70.47。测试前须保证网页的有效性。	
合格标准: 网站地址平均时延不大于 1 秒	

3.4.2.6. 视频测试

目　　的	满足用户影音需求，保障单终端视频业务的能力
指标定义： 用户访问指定视频地址，记录视频地址返回时延	
预置条件： 1、系统正常运行 2、测试终端通过 BSSID 成功连接指定 AP	
测试流程： 1、终端通过测试工具依次访问 3 个视频网站地址，等待网站返回信息 2、Ping 网站 IP 地址 10 次，每个 ping 包大小为 1600 字节 3、记录网站访问地址平均时延 4、主流视频网站包括：爱奇艺：111.202.74.191、央视网：110.242.21.33、党员学习：106.74.11.153。测试前须保证视频地址的有效性。	
合格标准： 视频网站平均时延不大于 1 秒	

4. 综合维护方案

4.1. 日常维护服务

4.1.1. 服务响应及 7×24 小时免费热线服务

针对本次项目所有产品提供 7×24 小时免费热线技术咨询。一般故障 20 分钟内响应，若不能解决问题，2 小时内开展远程支持，对于远程无法解决的问题，我方提供现场支持服务；重大故障（系统瘫痪或核心设备故障）发生时，2 小时内到达故障现场，4 小时内排除故障；8 小时无法排除的硬件故障，在 24 小时内提供不低于故障产品规格型号档次的备用产品，直至产品修复，确保系统最大限度地不中断运行。

服务方设有客户服务中心，提供 7×24 小时的电话、传真、网络在线技术支持服务及技术咨询服务。用户可以直接拨打项目经理或技术支持与客户服务中心负责人手机，保证客户的问题在任何时间都能得到及时的响应。

4.1.2. 设备原厂质保及升级服务

服务方应对所提供的所有软件产品、硬件产品及随机软件产品均提供1年免费原厂质保服务，当发生设备或软件升级时，服务方应将免费提供相关升级技术资料和技术支持及技术培训。在质量保证期满后，设备需维修的，只核收基本的部件成本费。

4.1.3. 设备变更服务

委办局因业务变更需要系统重组或调整时，服务方应提供详细科学的技术方案与现场指导服务。

4.1.4. 延保服务

原生产商质保期后，出现设备故障时，服务方应提供设备维修技术与协助采购人从原生产商处采购备品备件以及其它技术咨询服务。

4.1.5. 服务标准

厂商提供7*24小时现场保修和技术支持服务，提供当日上门服务。

4.1.6. 巡回检查服务

4.1.6.1. 服务原则

在维护WI-FI网络时，首先考虑到的是满足AP跟无线网卡信号的交互，以及用户可有效的接入网络。系统的覆盖规划应主要考虑为保证AP无线信号的有效覆盖，对AP天线进行选址与相关配置。在选择AP摆放位置的时候，需遵循以下几个原则：

如果在一个大厅里只安装一个AP，则尽量把AP安放在大厅的中央位置，而且最好是放置于大厅天花板上；如果同一空间安装两个AP，则可以放在两个对角上。

保持信号穿过墙壁和天花板的数量最小。WI-FI信号能够穿透墙壁和天花板，然而，信号的穿透损耗较大。应放置AP与计算机于合适的位置，使墙壁和天花板阻碍信号的路径最短，损耗最小。

考虑AP和覆盖区域之间直线连接。注意AP的放置位置，要尽量使信号能够垂直的穿过墙壁或天花板。

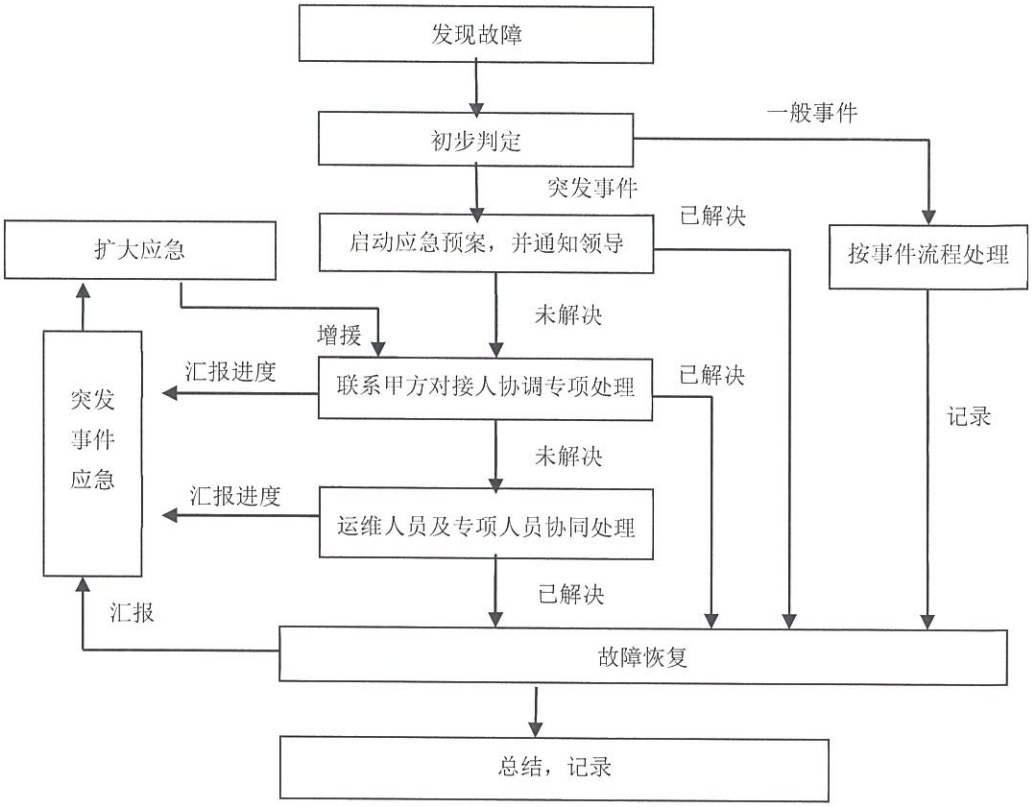
室外网桥长距离数据回传，要避免站点周围有高大建筑或山体，保证网桥两端信号的视距可达。

AP天线方向可调，安装AP的位置应确保天线主波束方向正对覆盖目标区域，保证良好的覆盖效果。

AP安装位置需远离电子设备，避免覆盖区域内放置微波炉、无线摄像头、无绳电话等电子设备。

替换及更换设备要求同品牌不限于同型号，保证互通互联。

4.1.6.2. 巡检流程及范围



巡检员每周对以下内容进行全面巡检（模板）

无限亦庄WiFi网络运维-巡检明细 (X月)

序号	目录序	区域分类	项目分类	巡检批次	项目名称	资源名称	无智慧灯杆机箱	无AP	无智慧灯杆	观感正常	表面AP不可见
1											
2											
3											
4											
5											
6											

（1）设备硬件情况检查

硬件运行状态检查工程师按照网络设备硬件巡检指导书相应标准对需要巡检的设备进行详细的硬件检查，包括设备电源插座的安装情况、交流或直流电源的供电情况、设备的接地情况、设备防尘情况、设备各个硬件模块的安装和运行情况，设备硬件系统运行正常与否的关键寄存器指标信息等，保存所有检查信息结果，据此输出设备硬件运行情况检查表。

（2）设备软件情况检查

工程师按照网络设备软件巡检指导书相应标准对设备软件的运行情况进行检查，包括软件版本情况、配置文件情况、网络流量统计情况、CPU，内存利用率的统计情况，重要网络协议运行状态的基本参数信息、重要网络协议运行过程中关键指标参数的历史记录信息、重要网络协议软件模块运行正常与否的关键寄存器指标信息、数据通讯情况、设备运行的历史日志信息，诊断信息等，保存所有检查信息结果，据此输出设备软件运行情况检查表。

（3）巡检采集信息分析

现场巡检结束后工程师需将巡检采集的所有信息带回驻场地址进行整理，技术难点需要同巡检服务专家组共同进行分析评估，专家组在2个工作日内出具相应的分析评估结果．提出注意事项和网络优化调整建议。

（4）输出巡检相关文档

网络工程师根据专家组建议，编制《故障单》、《排障明细》、《巡检明细》、《图纸效验》、《防控记录》，于3个工作日内以纸件形式提交用户，并同用户沟通其中的关键内容。巡检报告均一式两份，用户联交给用户自留，其他联需附上用户签章由工程师带回并同该电子档一起交由技术支持部进行存档。若现场用户无法签章则工程师可协调用户后期补签通过传真方式返回，工程师接收后交由技术支持部存档。

巡检内容表

巡检可包括的内容如下

编号	巡检内容		
1	硬件运行状态检查项目		
	单板状态检查	电源模块状态检查	风扇状态检查
	整机指示灯状态检查	机框防尘网检查	机房温度、湿度检查
	设备地线检查		
2	软件运行情况检查项目		
	设备运行情况检查	网络报文分析	设备对接运行状况检查
	路由运行情况检查		
3	网络整体运行情况调查		
	网络运行问题调查	网络变更情况调查	网络历史故障调查
以上巡检内容根据设备具体情况会有所不同			

4.1.7. 系统常规检查

服务方应对每一个项目在验收后定期派遣工程师对系统进行系统巡检，并对设备进行清洁服务，及时发现系统存在的故障或潜在的问题，提早消除故障隐患，确保系统安全、稳定、高效地运行。此外，我们还将同各个软硬件厂商进行协作，

将各厂商新近发现的重要问题与缺陷(Bugs)及时通知用户，使用户防患于未然。

4.2. 重要期间保障服务

4.2.1. 服务描述

重要保障期间，根据需要向服务方提出重要保障服务要求，服务方收到要求后与委办方共同制定保障方案。

4.2.2. 服务要求

重要保障期间包括重大节假日、重要活动期间等。在重点保障期间，如用户提出要求，服务方须按照双方制定的保障方案执行，此服务按照现场服务标准执行。

4.2.3. 重要时期硬件设备保障方案

4.2.3.1. 周期确定

根据相关单位下发的特殊时期通知文件，编制相应的《特殊时期服务工作安排》，明确特殊时期具体时间节点，并适当提前该周期，使相关人员体检进入准备状态。

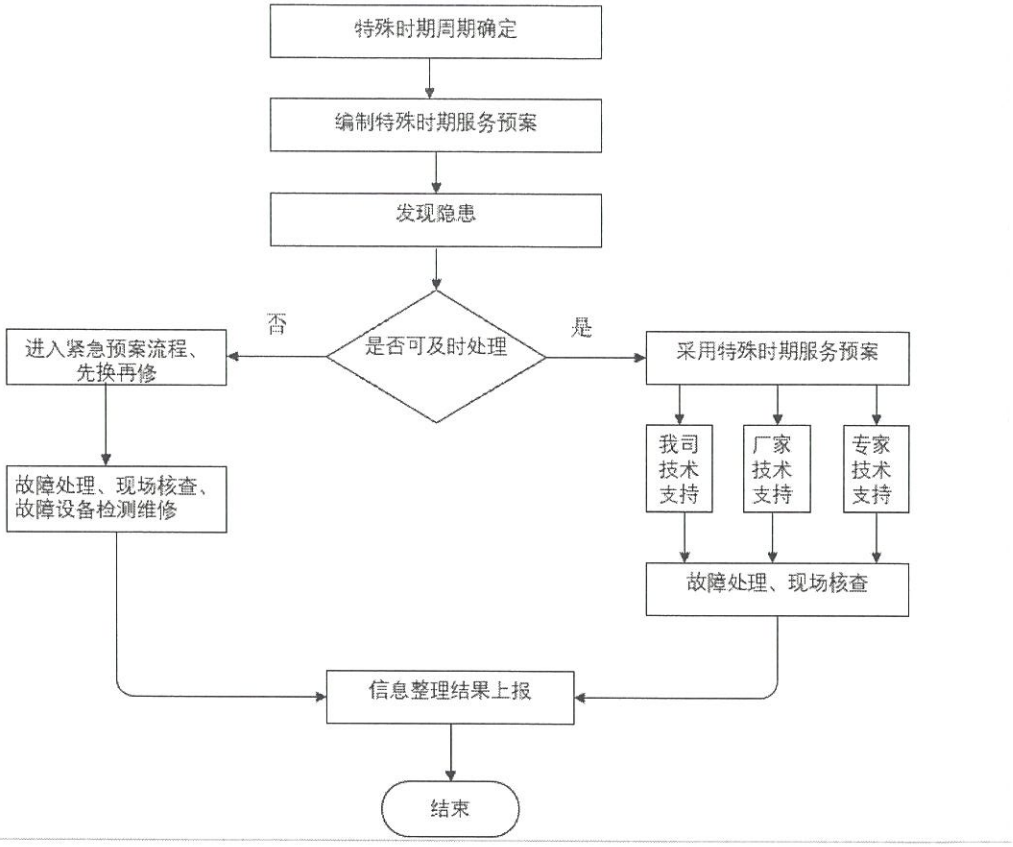
4.2.3.2. 加大巡检

根据相关单位下发的特殊时期通知文件，编制相应的《特殊时期服务工作安排》，明确特殊时期具体时间节点，并适当提前该周期，使相关人员体检进入准备状态。

进入特殊时期周期前，保障小组对政务信息网络系统进行一次全面核查，排除隐患，确保各系统各部件的正常运转，并形成安全检查总结报告备案。

特殊时期期间，对各节点间保证每日至少一次巡检，重要节点间安派驻场人员。对主要系统做到每 2 小时一次巡查。

4.2.3.3. 加快处理



巡检工程师发现系统隐患时，立即上报值班经理，并马上组织驻场技术专家、厂家技术人员展开隐患排除工作，力争在 30 分钟内解决隐患。

若无法及时处理，则直接启用应急预案，进入一级预警状态，及时调度备品备件和人员至故障地点，1 小时内完成设备的更换，保障系统稳定后再检修替换下的设备。

网络故障或者突发事件、紧急情况发生后，应立即加强对设备的运行监控，对于由网络故障或者突发事件、紧急情况引发的交换机高负荷情况和故障情况，要及时上报本单位负责网络安全的相关单位负责人，申请启动应急预案。

在资源调度时，遵循重点部分优先保障的原则。

4.2.4. 重要时期网络安全保障措施

4.2.4.1. 安全设备运行状态检查

每日 3 次（9 点、13 点、17 点）通过登陆安全设备以及查看所部署的监控软件，对防火墙等安全设备及网络出口流量进行监控。

4.2.4.2. 入侵检测安全事件监控

使用防火墙入侵检测系统，对保障期间系统访问产生的安全事件进行监控。

4.2.4.3. 互联网出口防火墙日志分析

每日分析互联网防火墙日志信息，对明显异常访问开发区内部应用的互联网IP地址进行访问策略限制。对可疑行为尽量做到抓早灭小。

4.2.5. 重要时期的人员组织

特殊时期政务信息网络保障工作实行各级维护部负责制。由保障小组组长组织调度指挥，各相关部门配合执行。

突发事件或者紧急情况发生后，保障小组可以根据需要，在事发地设立现场应急指挥部，统一进行指挥调度；特殊时期政务信息网络保障小组成员包括：

总指挥：保障小组组长

副总指挥：项目部负责人

成员：项目部技术经理、各专业运维工程师、专家团队、重要设备原厂技术人员。

负责对维保单位特殊时期政务信息网络保障工作的统一领导、指挥和协调。负责传达保障小组应急工作指令；负责特殊时期期间发生的突发事件或者紧急情况的收集、分析和评估工作；协调处理在实施特殊时期政务信息网络保障工作中的有关问题；对损失及影响进行评估；制定《特殊时期政务信息网络保障预案》并负责修订和完善；负责执行信息网络保障指令；负责修复故障设备；负责特殊时期政务信息网络保障工作中的后勤保障等配合工作。

4.2.5.1. 硬件设备现场保障人员安排计划

按照工作要求，提供7*24小时现场保障工作。现场人员如下：

职位	数量（人）	保障职责
项目经理	1	现场保障
项目副经理	1	现场保障
技术负责人	2	现场保障

4.2.5.2. 网络安全现场保障人员安排计划

专业运维服务二线应急保障人员如下：

职位	数量（人）	保障职责

领导	1	技术保障组长
技术负责人	3	专项技术负责人
信息安全工程师	2	信息安全协助服务
网络安全工程师	4	网络安全协助服务
主机安全工程师	4	主机安全协助服务
证书安全工程师	2	证书协助服务

4.2.5.3. 业务监控保障人员

针对开发区对互联网提供服务的应用系统，提供7*24小时的页面监控。确保业务系统实时检测，自动发现故障告警。监控人员确保2人在岗。

4.3. 应急响应服务方案

4.3.1. 应急响应概述

在发生应急事故时，值守人员需立即处理并记录，并尽快联系委办局管理部门相关负责人（视事件的严重程度，必要时上报部门领导），并且立刻联系故障涉及系统所属单位工程师取得技术支持，运维人员在必要时请示主管领导，组织技术力量按照下面步骤进行处理:

4.3.1.1. 识别事件

确定是否是应急事件及应急事件的类别；注意保护可追查的线索。

4.3.1.2. 缩小事件的影响范围

组织队伍立即获得事件相关信息；确定系统继续运行的风险如何，决定是否关闭系统；相关应急事件处理工作人员与网络、安全相关工作人员保持联系、协商。

4.3.1.3. 根除事件影响

确定事件的起因和症状；查找事件的源头；增强防御；查找最近的干净备份。

4.3.1.4. 恢复系统

修复系统；使系统正常；监控系统。

4.3.1.5. 系统防护

在本次故障排除后，立即着手制定相关措施，并根据故障报告和故障排除方案，制定故障解决方案。

处置结果反馈：应急事件整体处置完成后，由应急事件响应组织体系成员将应急事件的事件发生原因、事件处置过程、事件处置结果等内容，形成应急事件处置报告，以电子版或者书面形式进行备案和归档。

按照应急事件产生的初步原因，将事件分为以下三类：网络及基础设施类、网络安全类、网站应用类。

网络及基础设施类应急事件分类：

开发区政务网络出现大量服务器发布的业务系统无法被用户访问。

开发区政务网络大量用户无法正常访问互联网或内网全部业务。

管理部门机房发生空调、用电等基础设施造成较大影响的问题。

4.3.1.6. 网络安全应急事件分类

开发区政务网络内出现有害程序如计算机病毒、蠕虫、特洛伊木马、僵尸网络、网页内嵌恶意代码事件和其他有害程序对网络内终端、服务器、网络设备造成影响的事件。

开发区政务网络内出现网络攻击如拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼和其他网络攻击对网络产生影响的事件。

开发区政务网络内出现信息破坏事件如信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

4.3.1.7. 网站应用类分类：

非网络与安全问题造成的网站、网页无法打开或出现错误页面的事件。

因网站数据库崩溃等原因，导致存储数据丢失、损坏的事件。

因数据库未清理导致磁盘满继而导致的页面无法访问等问题。

4.3.2. 网络及基础设施类事件解决办法

网络故障及基础设施类事件发生的机率比其它事件发生的机率都大，因此也是保障的重点。

4.3.2.1. 服务器端故障解决办法

如果大范围服务器端不能被外网用户访问时，首先查看出口路由器及出口链路。设备故障及时恢复，保障业务系统能正常提供访问；链路故障（首信链路故障时）及时联系相应运营商，如不能及时恢复将业务系统域名解析到备用出口链路（联通链路），主用链路（首信链路）恢复后切换回正常状态。

如果大范围服务器不能被所有用户访问（内、外网所有用户）时，查看服务器端汇聚交换机、防火墙状态和链路情况。为将影响范围降到最小，首先设备故障或链路故障及时切换到备用设备或链路，首先保证业务系统的正常运行，再对设备或链路进行故障判断、解决。

如部分服务器不能被用户访问时，根据反应的情况或者发现的情况，判断出现问题的位置。首先检测目的 IP 是否可连通，连通即初步判断网络正常，然后查找其它的可能的原因，如端口、服务或者安全设备等方面的原因；如不可连通，则 tracert 目的 IP，查找中断位置，缩小故障范围，然后具体分析问题的原因。

4.3.2.2. 管理部门机房空调、用电等基础设施故障解决办法

核心机房精密空调故障，首先通过开门通风，并增加排风扇的方法对机房温湿度进行初步控制，现场工程师对精密空调做临时处理，保证空调能正常制冷，厂家工程师及时入场维修、恢复精密空调。

核心机房市电故障，能通过 UPS 对机房设备进行供电的情况下，及时通知物业部门报修，并及时跟进电力维修情况，在 UPS 电力将要使用完毕而市电不能及时供电的情况下，对机房服务器设备进行关机操作，保障设备硬件正常；UPS 主机报警导致的机房用电故障时，首先将 UPS 主机切换到旁路模式（相当于市电直接给机房设备供电，而不通过 UPS 主机对机房设备供电），及时安排厂家工程师到现场进行维修，解决故障。

4.3.3. 网络安全类事件解决办法

网络安全应急事件一旦发生，通常将涉及较大的影响或较广的范围，因此一旦发生安全应急事件应第一时间上报相关领导，组织应急事件响应组织体系成员进行处置。

4.3.3.1. 病毒事件解决办法

在计算机发生病毒感染情况的时候，马上停止所有操作，不要向外部发送任何数据，以免病毒的传播，并通知系统维护人员（必要的时候利用短信平台通知全体计算机用户）；

如果是用户计算机发生病毒感染，在用户允许后运行杀毒软件，全面检查计算机系统，将病毒彻底清除；

如果是服务器发生了病毒感染，应在负责人允许后停止服务器所运行的所有

程序和相关服务，断开染毒服务器的网络连接，防止病毒进一步扩散；

在服务器端运行杀毒软件，全面检查计算机系统，清除病毒；

如果病毒将系统破坏，导致系统无法恢复，应将感染病毒的计算机上的重要数据备份到其他存储介质，确保计算机内重要的数据不会丢失；

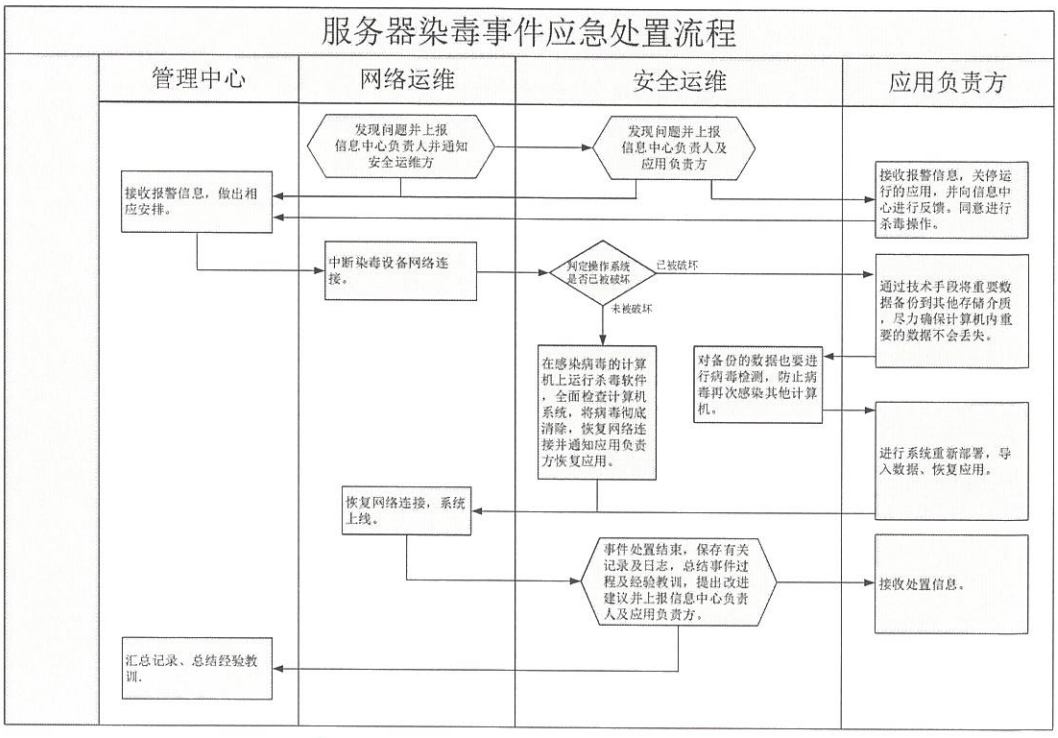
对备份的数据也要进行病毒检测，防止病毒再次感染其他计算机；

如有重要数据无法恢复，必要时可与反病毒厂家联系，由他们来协助恢复，需要保证数据信息不泄露，并作记录；如为高度涉密数据，不允许由其他单位来恢复数据；

对整个事件处理过程以及完成后均需要作详细记录；

如果发生大规模扩散的病毒，则要在重要的路由、交换机、防火墙上根据病毒的传播服务和端口，进行拦截。

服务器染毒事件应急处置流程图如下：



4.3.3.2. 网络攻击事件解决办法

发现开发区网络中断，并发现网络出口流量异常；

立即通知网络、安全运维负责人、网络运维负责人及相关人员；

逐步排查，缩小故障排查范围，判断被攻击目标位置。方式如下：登陆防火

墙，查看系统监视-端口流量，初步判断被攻击区域，根据经验通常为 DMZ 区服务器；登陆 DMZ 区接入交换机，查询端口流量，判断被攻击服务器位置；查看防火墙日志记录，寻找可疑攻击源地址及被攻击目标地址。

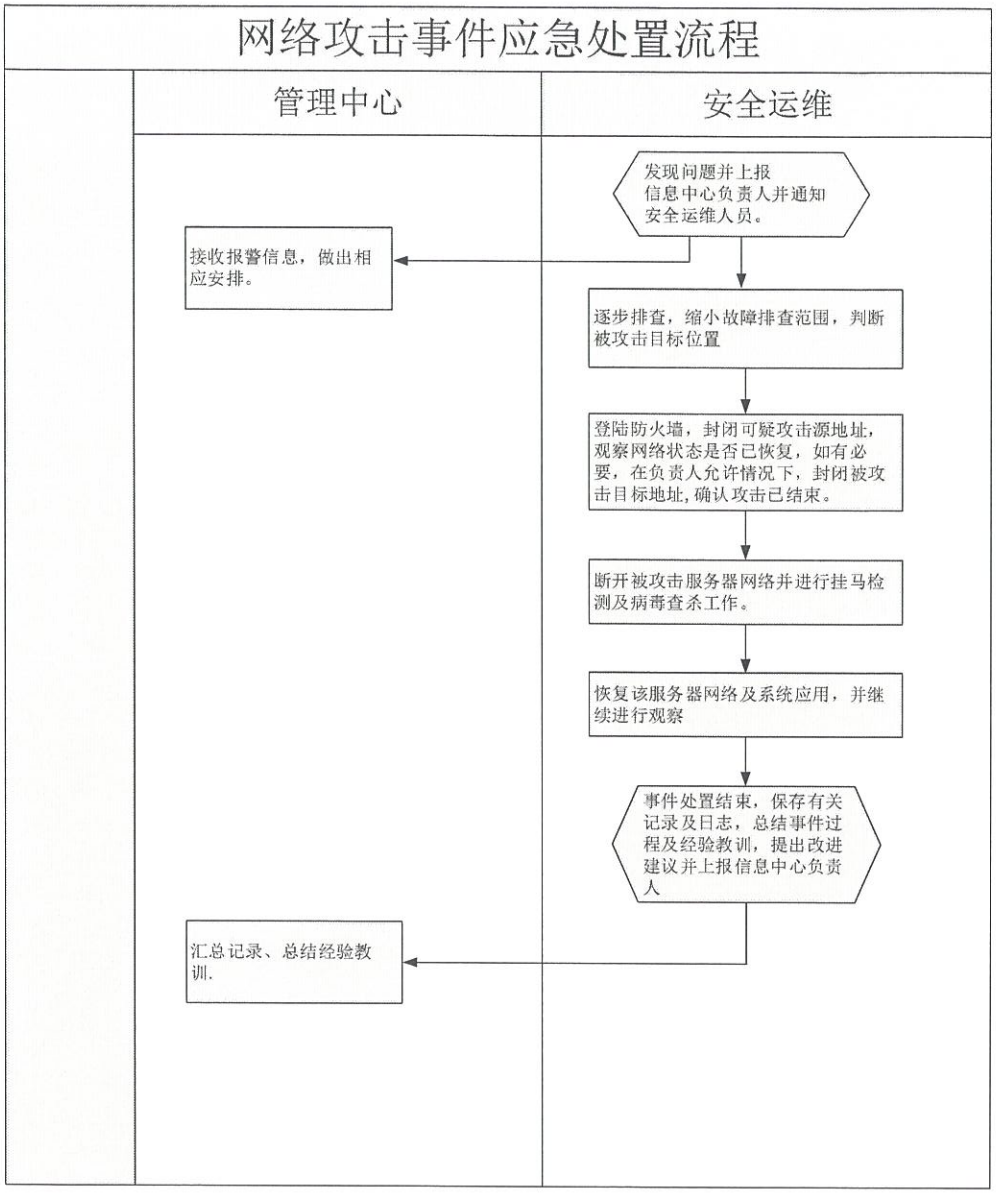
登陆防火墙，封闭可疑攻击源地址，观察网络状态是否已恢复，如有必要，封闭被攻击目标地址。确认攻击已结束；

断开被攻击服务器网络并进行挂马检测及病毒查杀工作；

恢复该服务器网络及系统应用，并继续进行观察；

整个事件处理过程以及完成后均需要作详细记录。

网络攻击事件应急处置流程:



4.3.3.3. 网站篡改事件解决办法

网络、安全、网站运维人员，通过各自监控机制发现应用系统网页被篡改，应立即通知所对应的负责人员，并通知其他运维单位。

网络运维人员立即断开该应用服务器的网线和数据库的网线，并修改映射地址，指向网站备机;

网站运维人员启用备份机，发布事先准备好的静态页面;

网站运维人员检查事故主机，将应用部署程序提供给安全运维人员；

安全运维人员，联系二线安全专家，对提供的网站程序进行挂马检测等操作，查看主机出现问题的原因；

修改主机的用户名和密码，修改应用及相关数据的密码，对主机进行加固及查杀木马病毒；

问题解决后，恢复主机的正常运行，安全运维人员通知网站运维人员，切回主机；

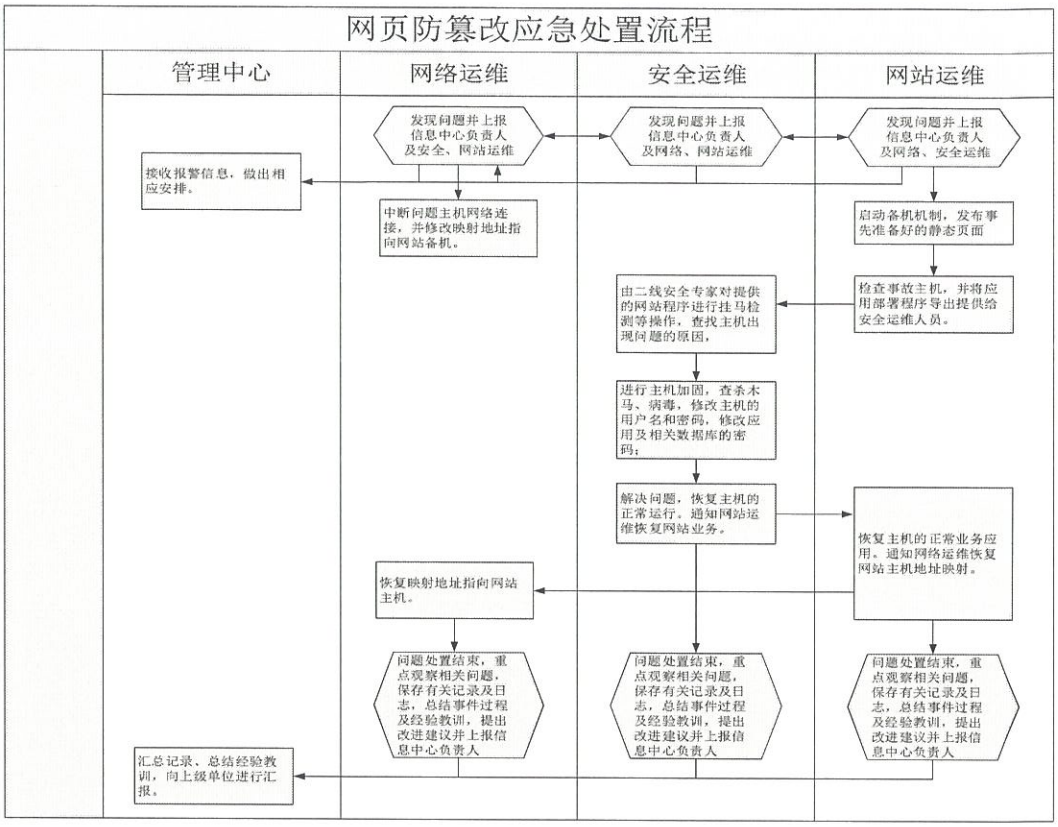
网站运维人员恢复主机相关业务应用，并通知网络运维人员，恢复主机网络连接及地址映射；

网络运维人员恢复主机网络连接及地址映射；

三方运维人员，监控主机的情况，查看运行状态；

问题处置结束，重点观察相关问题，保存有关记录及日志，总结事件过程及经验教训，提出改进建议并上报管委会管理部门负责人。

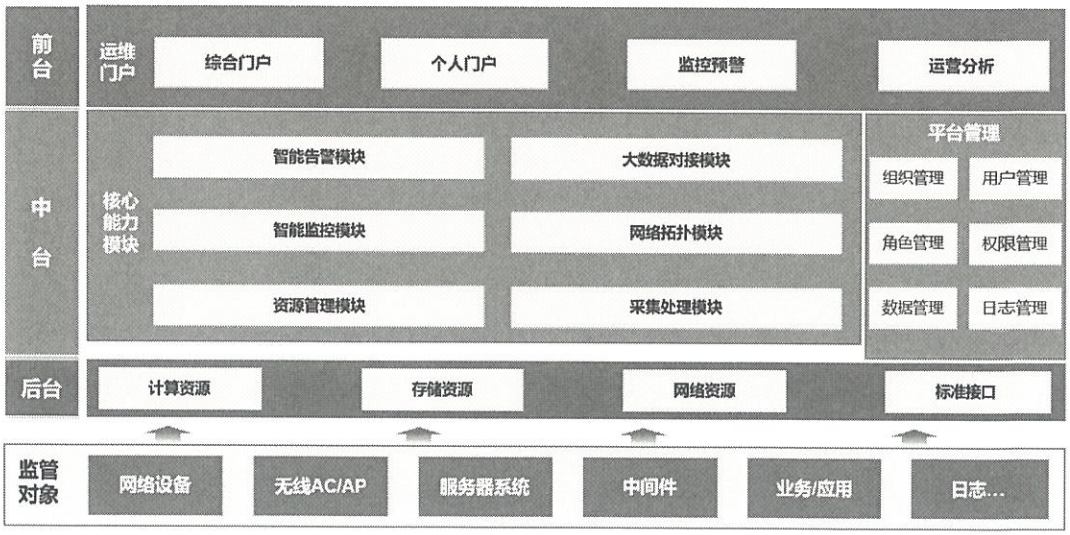
网页防篡改应急处置流程图如下:



5. 综合服务管理平台解决方案

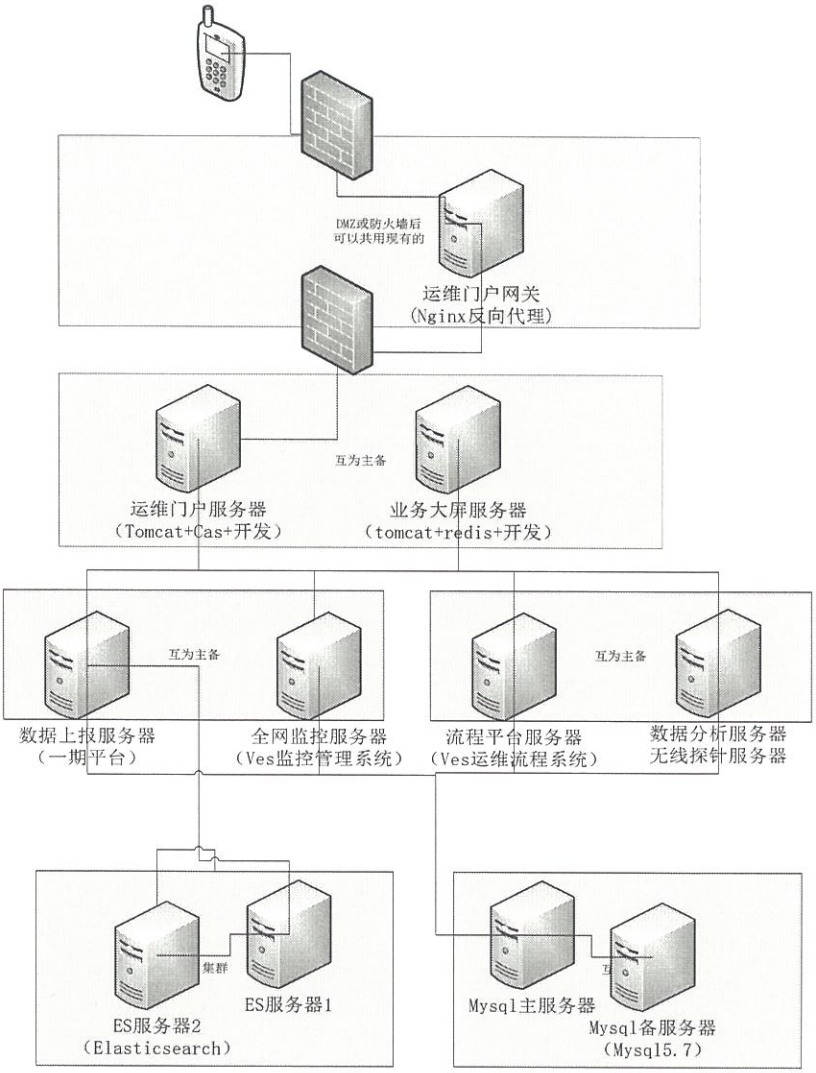
5.1. 综合服务管理平台

5.1.1. 平台架构设计



整个架构核心由基础能力平台(资源平台、采集平台、监控平台、流程平台、运管平台、消息平台)，业务中心(资源管理、监控预警、运维流程、分析)和统一门户(支持PC、大屏多端展示)。

5.1.2. 平台部署架构



部署架构如上图所示:

所有的系统及服务器部署在服务方云上，不对外开放。

5.1.3. 数据采集

平台支持对网络设备、服务器操作系统、数据库、中间件、存储等IT基础设施及虚拟化的监控管理，同时从点到面集中7×24小时的管理整个IT系统，并且监控管理具备很强的可扩展能力，方便进行功能扩展和规模扩展；平台的易用性强，方便管理人员进行日常运维工作，有效减轻运维压力，同时兼顾系统各

种层次的运维管理需求。监控管理提供对 IT 环境的性能监控及分析、故障监控、故障分析及定位、网络配置文件、资源巡检的管理。系统采用了模块化设计，全中文 Web 界面，易用性强，便于日常运维，另外还通过灵活的阈值设置衡量网络使用情况，预测潜在故障，并发出故障告警。

5.1.3.1. 资源管理

智能生态监控平台提供应用与业务系统监控、数据库监控、服务器硬件监控和各类主流操作系统监控、网络设备监控、防火墙监控、负载均衡监控、存储监控、虚拟化监控、数据报表等功能

系统能够反映用户网络系统中的各种设备的资源配备和重要参数的设置情况，能自动搜索网络系统中的所有设备的相关配置信息，识别出设备的类型、型号、生产厂家、接口等硬件配置信息。

5.1.3.2. 无线 AC/AP

系统支持国内主流设备的监控。可以监控 AC 本身的指标也支持监控 AP 的指标。

资源	指标类别	指标名称
无线 AC	可用性指标	设备可用性
	指标	网络设备 MAC 地址
		网络设备名称
		可用性
		响应时间
		系统 OID
		连续运行时间
		网络设备说明
		所有 IP 地址
		ARP 表
		FDB 表
		BasePort 表
		路由表
		IP 表
		网络接口个数
		吞吐量
		接收丢包率
		发送丢包率
		丢包率
		接收 ICMP 包率

		发送 ICMP 包率
		TCP 端口连接数
	指标	接收广播包率
		发送广播包率
		广播包率
		接收广播包数
		发送广播包数
		内存总容量
		CPU 平均利用率
		内存利用率
		内存可用容量
		内存已使用容量
		VLAN 表
		在线 ap
		离线 ap
		总 ap
		在线人数
		下行速率
		人均速率
		离线用户表
		在线用户表
AP（子资源）	指标	APIndex
		apMAC
		apSN
		可用性
		CPU 使用率
		内存利用率
		在线人数
		人均带宽
		用户粘性
		掉线率
		上线失败率
		上行速率
		上行丢包率
		下行速率
		资源名称
		IP 地址

5.1.3.3. 服务器

为了针对服务器的不同环境进行监控，系统提供不同的方式进行监控，同时系统支持对 HP-Unix、Solaris、Linux、AIX、Windows 等主流操作系统的监控。

Windows 操作系统可以通过 SNMP 和 WMI 方式获取主机设备的运行状态和性能数据，非 Windows 操作系统可以通过 TELNET 和 SSH 方式来获取数据。

系统能够管理的主机性能数据包括 CPU 利用率、DISK 磁盘容量、系统内存（物理使用内存及缓存）使用情况、磁盘利用率、文件系统、日志、关键进程、软硬件资源信息等，针对服务器相关的性能指标能够按照实际情况设定不同级别的性能阈值，对于超过性能阈值的性能指标系统能够进行故障告警或预警并通知相应的网络管理人员。并可以执行用户定义好的脚本。

系统采用图表等方式实时显示主机的 cpu 利用率、cpu 使用情况、内存利用率、磁盘信息、进程等相关信息。实时监控当前主机性能，能够根据当前系统的运行情况，提供深入的性能分析。

系统的进程分析能够实时监视系统进程的运行状况，显示进程所占用系统资源的情况。主机进程组主要为了监控主机上的应用程序，在客户的 IT 管理中心网内有很多应用，如邮件服务、DNS 服务、IIS 服务等，它们会启用多个进程，为了监视这些服务的状态，将相关的进程作为一个进程组来监控，一旦一个或者多个进程出现异常，系统就会对该进程所涉及的应用服务发出警告。

系统提供了开放式的 KPI 接口和资源模型以供用户便捷的添加自己需要的特殊 KPI，监控指标可通过页面配置或脚本修改进行快速扩展，降低了程序员的工作强度，提高了针对用户的特殊监测指标的响应速度。

Windows 系统监控指标:

资源	指标类别	所有指标
Windows 主机	可用性指标	主机在线可用性
	性能指标	CPU 平均利用率
		CPU 非空闲模式百分比
		CPU 中断时间百分比
		CPU 特权模式百分比
		CPU 用户模式百分比
		内存利用率
		内存页交换速率
		内存错页率
		硬盘平均等待队列
		硬盘平均磁盘时间
		硬盘平均写速率
		分区平均利用率
		接收和发送的 ICMP 包率

		核心内存利用率
		虚拟内存利用率
		认可用量利用率
		主机总内存容量
		主机总可用内存容量
		主机已用用内存容量
		分区总容量
		分区总使用容量
		发送的 ICMP 包率
		接收的 ICMP 包率
		页面调进速率
		页面调出速率
		硬盘平均读速率
		硬盘平均写速率
	信息指标	连续运行时间
		主机基本信息
		操作系统
		MAC 地址
		主机操作系统的 OID
		包含的 IP 地址
		系统版本
		系统 SP
		等待处理队列
		进程数
		线程数
		句柄数
		当前在线用户数
		核心内存总量
		剩余核心内存
		已用核心内存
		虚拟内存总量
		虚拟内存已用量
		认可用量总量
		已用认可用量
	配置指标	CPU 个数
		内存总容量
		硬盘个数
		硬盘总容量
		网卡个数
		网卡类型
		IP 地址
		主机名
		分区个数

		分区总容量
CPU（子资源）	性能指标	CPU 利用率
	信息指标	CPU 名称
		CPU ID 号
		CPU 型号
		CPU 频率
硬盘（子资源）	性能指标	硬盘等待队列
		硬盘磁盘时间
		硬盘读写速率
	信息指标	硬盘名称
		硬盘 ID
		硬盘容量
分区（子资源）	性能指标	分区总已用容量
		分区利用率
	信息指标	分区名称
		分区 ID 号
		分区容量
网络接口（子资源）	可用性指标	管理状态
		操作状态
	性能指标	发送利用率
		发送的丢包数
		发送的错包数
		发送速率
		接收利用率
		接收和发送利用率总和
		接收的丢包数
		接收的错包数
		接收速率
		接口带宽
	信息指标	网卡 ID 号
		接口名称
		索引
		接口类型
		接口带宽
		MAC 地址
		IP 地址

Linux 系统监控指标

资源	指标类型	指标列表
Linux	可用性指标	主机在线可用性
	性能指标	CPU 平均利用率
		CPU 平均负载(15 分钟)

		CPU 平均负载(5 分钟)
		CPU 平均负载(1 分钟)
		内存利用率
		硬盘平均写操作速率
		硬盘平均读操作速率
		硬盘平均写速率
		硬盘平均读速率
		接收和发送的 ICMP 包率
		Ping 时延
	配置指标	IP 地址
		分区总容量
		CPU 个数
		内存总容量
		硬盘总容量
		硬盘个数
	信息指标	网络接口个数
		主机说明
		连续运行时间
		主机操作系统
CPU	性能指标	CPU 利用率
	信息指标	CPU 型号
		CPU 频率
		CPU 名称（隐藏）
硬盘	性能指标	硬盘写速率
		硬盘读速率
分区	性能指标	分区利用率
	信息指标	分区名称（隐藏）
		分区已用容量
		分区容量
网络接口	可用性指标	管理状态
		操作状态
	性能指标	发送利用率
		发送的丢包数
		发送的错包数
		发送速率
		接收利用率
		带宽利用率
		接收的丢包数
		接收的错包数
		接收速率
	信息指标	索引
		接口类型
		MAC 地址

		接口带宽

5.1.3.4. 网络设备

系统可支持自动发现和手动添加两种方式监控网络设备，可支持所有满足SNMP V1/V2/V3方式的厂家路由器、交换机、安全设备、负载均衡等设备的性能指标采集和预警，系统内置了丰富的主流厂家型号及其对应指标模板，例如CPU利用率、内存利用率、Ping延时和丢包、端口状态、端口出入流量、入错误帧、出错误帧、广播入帧、广播出帧等指标。

路由器监控指标:

资源	指标类别	指标名称（67个）
Router	可用性指标	网络设备在线可用性
	性能指标	CPU平均利用率
		内存利用率
		网络设备内存池占用容量
		网络设备内存池可用容量
		总接收吞吐量
		总发送吞吐量
		吞吐量
		丢包率
		接口接收的丢包数
		接口发送的丢包数
		接收和发送ICMP包率
		发送的ICMP包率
		接收的ICMP包率
	信息指标	网络设备的OID
		连续运行时间
		网络设备说明
		交换机下的IP地址
		网络设备MAC地址
	配置指标	Cisco Config状态
		CPU个数
		内存总容量
		网络接口个数
		IP地址
		网络设备名称
CPU（子资源）	性能指标	CPU利用率
	信息指标	CPU名称
		CPU ID号
网络接口（子	可用性指标	管理状态

资源）		操作状态
	性能指标	ARP 包率
		接收的 ARP 包数
		发送的 ARP 包数
		单播包率
		接收单播包数
		发送单播包数
		发送利用率
		发送的丢包数
		发送的错包数
		发送速率
		广播包率
		接收的广播包数
		发送的广播包数
		接收利用率
		接收和发送利用率总和
		接口累计接收和发送的包数
		接口累计接收的包数
		接口累计发送的包数
		接收的丢包数
		接收的错包数
		接收速率
		组播包率
		发送组播包数
		接收组播包数
		接口带宽
	信息指标	网卡 ID 号
		接口名称
		索引
		接口类型
		接口带宽
		MAC 地址
链路（子资源）	可用性指标	链路可用性
	信息指标	链路名称
		链路 ID 号
		所属网络接口
		目标 IP

交换机监控指标:

资源	指标类别	指标名称
Switch	可用性指标	网络设备在线可用性
	性能指标	CPU 平均利用率
		内存利用率
		网络设备内存池占用容量
		网络设备内存池可用容量
		总接收吞吐量
		总发送吞吐量
		吞吐量
		丢包率
		接口接收的丢包数
		接口发送的丢包数
		接收和发送 ICMP 包率
		发送的 ICMP 包率
		接收的 ICMP 包率
	信息指标	网络设备的 OID
		连续运行时间
		网络设备说明
		交换机下的 IP 地址
		网络设备 MAC 地址
	配置指标	CPU 个数
		内存总容量
		网络接口个数
		IP 地址
		网络设备名称
CPU（子资源）	性能指标	CPU 利用率
	信息指标	CPU 名称
		CPU ID 号
网络接口（子资源）	可用性指标	管理状态
		操作状态
	性能指标	ARP 包率
		接收的 ARP 包数
		发送的 ARP 包数
		单播包率
		接收单播包数
		发送单播包数
		发送利用率
		发送的丢包数
		发送的错包数
		发送速率

		广播包率
		接收的广播包数
		发送的广播包数
		接收利用率
		接收和发送利用率总和
		接口累计接收和发送的包数
		接口累计接收的包数
		接口累计发送的包数
		接收的丢包数
		接收的错包数
		接收速率
		组播包率
		发送组播包数
		接收组播包数
		接口带宽
	信息指标	网卡 ID 号
		接口名称
		索引
		接口类型
		接口带宽
		MAC 地址
链路(子资源)	可用性指标	链路可用性
	信息指标	链路名称
		链路 ID 号
		所属网络接口
		目标 IP

5.1.3.5. 数据库

数据库是客户信息系统中的核心应用，系统提供数据库监控功能对数据库进行管理，保证数据库的安全，优化数据库的性能。

系统能够对运行在主机设备上的各种数据库的运行状态和性能数据进行统一有效的管理。系统支持 SQLServer、Oracle、Sybase、Informix、DB2、MySQL、PostgreSQL 等主流的数据库的监控管理。

Oracle 监控指标:

d	指标类别	指标名称
Oracle DB	可用性指标	实例可用性
		监听器可用性
	性能指标	系统 CPU 利用率
		Oracle DB CPU 利用率

		系统内存利用率
		Oracle DB 内存利用率
		PGA 命中率
		库缓存命中率
		高速缓冲缓存命中率
		物理读速率
		物理写速率
		数据块获取数/秒
		一致性获取数/秒
		内存排序比率
		当前连接会话数
		当前进程数
		登陆会话数/秒
		当前打开的游标数
		当前锁数量
		死锁数量
		SQL 解析次数/秒
		事务数/秒
		事务回滚率
	信息指标	资源名称
		版本
		操作系统
		主机名称
		IP 地址
		主机 Mac 地址
		连续运行时间
		实例名称
		数据库名称
		Domain 名称
		数据库大小
		Open 模式
		SQL 语句 TOP10CPUTime
		SQL 语句 TOP10DiskReads
		OracleSQLTop10BufferGets
		SQL 语句 TOP10BufferGets
		磁盘排序次数
		内存排序次数
		事务回滚数
		事务提交数
	配置指标	表空间个数
		数据文件个数
		Log 模式
		高速缓冲池

		共享池
		大型池
		Java 池
		日志缓冲池
		SGA
		PGA
		物理内存容量
表空间(子资源)	可用性指标	表空间状态
	性能指标	表空间增长率
		表空间利用率
	信息指标	表空间名称
		表空间大小
		表空间已用空间
数据文件(子资源)	可用性指标	数据文件状态
	性能指标	数据文件增长率
		数据文件利用率
		物理读速率
		物理写速率
	信息指标	数据文件名称
		数据文件 Id
		数据文件大小
		数据文件已用空间
进程(子资源)	可用性指标	进程状态
	信息指标	Oracle 实例名称(进程)
		进程名称
文件系统(子资源)	性能指标	文件系统利用率
	信息指标	文件系统名称
		文件系统已用空间
		文件类型
	配置指标	文件系统大小

5.1.4. 数据分析

数据的分析则是针对采集到的数据从运维和运营维度进行相关性的统计和分析，从中得出对管理有价值的内容，数据分析主要包括内容如下:

5.1.4.1. 运维数据统计分析

设备可用性统计和分析；设备关键数据的统计和分析。

5.1.4.2. 运营数据统计分析

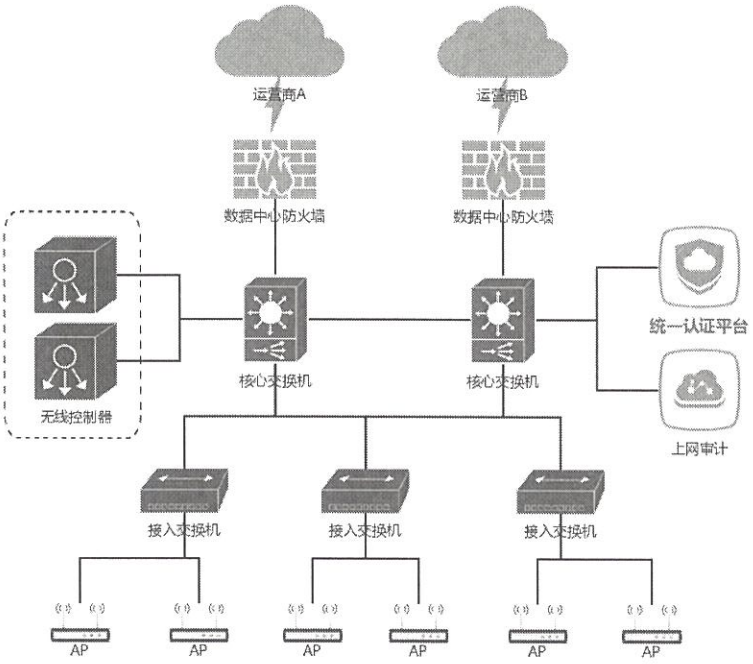
通过项目中的各类巨量数据关联分析，本次的平台建设中应在带宽、用户、趋势分析等方面快速形成有价值的信息，部分内容要通过可视化页面展示出来。

平台建设充分考虑到后期的可扩展性及与其他平台的对接，为以后在数据采集、数据存储、数据治理、数据分析、服务推送、成果展示方面做好前期的架构。

5.2. 无线认证平台

5.2.1. 无线认证平台设计方案

5.2.1.1. 认证平台设计图



5.2.1.2. 认证平台部署方式

目前项目中已经部署了无线控制器设备，为了减少预算，降低成本，在不更换已有的设备的情况下，本项目采用软件系统进行部署，将无线认证平台部署到虚拟化或物理机中，与无线控制器或安全接入网关对接的方式组网。

平台基于B/S架构设计，支持标准的Radius协议，运行在Linux系统之上，采用J2EE进行研发，内置Linux双机Keepalived部署，可进行多台集群部署，确保服务不宕机，出现问题可以第一时间实现故障转移，保证平台7*24小时的不间断运行。

5.3. 行为审计管理平台

5.3.1. 先进的系统体系结构

系统设计上采用了先进的模块化、层次化体系结构，基于面向对象的思想和插件化的并行协议栈，具有高度灵活扩展性，充分体现了资源的共享，提高了运行效率和稳定性。

5.3.2. 丰富的部署方式

基本的旁路部署，全面支持电口镜像与分路、光口的镜像与分光、电口桥接等多种线路部署方式，在复杂网络环境下的部署游刃有余，运用自如。

对于单台设备无法处理的超大流量环境，支持高扩展性的多台设备分布式部署方案，通过多台设备对超大的流量分而治之，又由统一的管理平台实现对整个网络的透明、统一的管理。

5.3.3. 高效的捕包引擎技术

使用 Intel 高性能网卡、独创零拷贝技术驱动、DMA 直接内存存取技术，使得系统在高负载下捕包分析的不稳定性与不安全性减至最小，而性能和可靠性却得到了极大提升，处理效率比传统捕包引擎提高 1 倍以上。

5.3.4. 高性能海量数据检索

独有的高性能海量数据检索引擎，在浩如烟海的审计数据查询与分析中表现出卓越的性能。

5.3.5. 审计平台功能

审计平台支持与公安网监指定平台对接，同时对无线用户和有线用户的网络行为和内容进行审计;

审计平台基于 Linux 系统，日志存储空间易扩容；提供日志空间管理功能;

产品支持包括对网页/各种在线娱乐软件/P2P 下载工具/在线视音频/流媒体/炒股软件/各种文件传输工具/IM 即时聊天软件/Telnet 等多种方式的信息收发内容记录、关键字过滤、文件传档管控、报警。

产品能够全面详实地记录网络内流经监听出口的各种网络行为，支持关于上网行为、内容、时间、用户等多种条件组合的信息审计策略和日志分析，全面监测各种网络行为，进行深度细粒审计。

内容审计既能进行无条件记录，又能通过策略指定访问者（IP 地址/帐号/

分组）、时间范围、内容关键字等有针对条件的记录管理用户需要的访问内容。

不管是行为审计还是内容审计，都具备高度的灵活性、专业性和准确性，能够为管理机构进行事后追查、取证分析提供有力技术支撑。

支持设备、源 IP、应用的总流量、流量趋势图、流量明细的查询。

支持审计设备 IP、用户 IP、用户名、发件人、收件人、访问时间等内容。

审计日志内容包括时间戳、网关设备名称、用户名、BBS 地址、贴子标题、贴子正文。

用户网络行为的 7 元组（NAT 前源 IP、NAT 前源端口、NAT 后源 IP、NAT 后源端口、NAT 后目的 IP、NAT 后目的端口、时间戳）等条目做为条件进行查询。

支持审计设备 IP 源 IP 用户名 URL 地址 URL 分类 访问时间。

支持设备 24 小时流量趋势图展示；支持 24 小时用户流量 TOP10 排行,支支持设备、源 IP、应用的总流量、流量趋势图、流量明细的查询。

5.4. 智能运维管理平台数据对接

平台具备无限亦庄项目全网设备数据的采集、清洗、转换、处理，并通过 API 接口形式与政务平台实现数据对接等一些列功能。

5.4.1. 运维数据

运维数据	
类型	数据
AP设备	MAC地址、名称、IP地址、设备厂家、设备型号、设备软件版本、室内/室外、上级设备名称、安装位置、经纬度、安装时间 用于对WLAN网络的资产关联，同时可为公众提供热点信息查询服务
AC设备	MAC地址、名称、IP地址、设备厂家、设备型号、设备软件版本、上级设备名称、安装位置、经纬度、安装时间
交换机	MAC地址、名称、IP地址、设备厂家、设备型号、设备软件版本、设备容量、上级设备名称、安装位置、经纬度、安装时间
服务器	MAC地址、名称、IP地址、设备厂家、设备型号、设备软件版本、服务器系统、硬盘容量、上级设备名称、安装位置、经纬度、安装时间

5.4.2. 设备动态数据

设备动态数据	
类型	数据
防火墙	MAC地址、名称、IP地址、设备厂家、设备型号、设备软件版本、安装位置、经纬度、安装时间
AP设备	设备状态、CPU使用率、内存使用率、在线人数、人均带宽、AP网络层级 用于WLAN网络的网络监管，可通过数据分析为用户体验、WLAN网络服务质量提供数据支撑
AC设备	设备状态、在线AP数、离线AP数、CPU使用率、内存使用率、在线人数、人均带宽
交换机	设备状态、CPU使用率、内存使用率、交换容量、出口带宽、入口带宽、各端口当前状态
服务器	设备状态、分区利用率、CPU使用率、内存使用率
防火墙	设备状态、CPU使用率、内存使用率上行流量、下行流量

5.5. 系统维护方案

5.5.1. Wi-Fi 网络运行状态监测工作

5.5.1.1. Wi-Fi 网络状态

Wi-Fi 网络状态监测工作是宽带无线城市项目基础设备日常运行保障的重要工作之一，是项目运行维护工作的信息来源和工具途径，其目的是为了减少网络故障率和缩短故障周期，监测方式通过无线城域网设备监测平台实现，包括AC 控制器平台、无限亦庄运管平台、用户行为审计平台、用户上网认证平台等。技术团队高度重视 Wi-Fi 网络状态监测工作，完善状态监测工作流程，做到对Wi-Fi 网络的监测、故障预防、故障及时处理的全面管控，实现 Wi-Fi 网络运行管理最优化。

5.5.1.2. Wi-Fi 网络运行状态检测范围和指标

	监测类别	监测事项	监测数量
1	AC 控制器状态监测	CPU 利用率	全部
		内存利用率	
		设备温度	
2	AP 性能和状	用户负载情况	全部

	态监测	用户接入失败率情况	
		用户掉线率情况	
		在线/离线状态	
		CPU 利用率	
		内存利用率	
3	射频监测	噪声强度	全网
		信道利用率	
		干扰率	
4	攻击检测	非法设备	全网
		泛洪攻击	

5.5.1.3. Wi-Fi 设备运行状态检测具体要求

每天定期登录监管平台对监测事项逐一进行指标监测，并针对异常项目进行记录并跟踪。

将问题项报项目维护组按故障维护流程处理。

针对故障项，持续跟踪故障处理进度，并将反馈的处理结果进行再次监测核对。

每月统计当月运行状态监测汇总情况。

5.5.1.4. Wi-Fi 设备运行状态检测指标详细说明

（1）AC 设备状态监测

CPU 利用率

监测标准：当 CPU 利用率超过 70%且持续时间超过 5 分钟，可认定为故障须进一步维护处理。

内存利用率

监测标准：当内存利用率超过 50%且持续时间超过 5 分钟，可判定为故障须进一步维护处理。

设备温度

监测标准：当设备温度超过 50 度且持续时间超过 5 分钟，可认定为故障须进一步维护处理。

（2）AP 设备状态监测

用户负载情况

监测标准：当单个 AP 负载数量超过 50 人且持续时间超过 30 分钟，可认定为故障须进一步维护处理。

用户接入失败率情况

监测标准：当单个 AP 用户接入失败率超过 10%，可认定为故障须进一步维护处理。

用户掉线率情况

监测标准：当单个 AP 用户掉线率超过 20%，可认定为故障须进一步维护处理。

在线/离线率

监测标准：当 AP 出现离线状态，可认定为故障须进一步维护处理。

CPU 利用率

监测标准：当 CPU 利用率超过 70%且持续时间超过 5 分钟，可认定为故障须进一步维护处理。

内存利用率

监测标准：当内存利用率超过 50%且持续时间超过 5 分钟，可判定为故障须进一步维护处理。

（3）射频监测

噪声强度

监测标准：噪声强度>-80dbm，可判定为一般性故障，且须进一步维护处理。

信道利用率

监测标准：信道利用率>70%，可判定为一般性故障，且须进一步维护处理。

干扰率

监测标准：干扰率>40%，可判定为一般性故障，且须进一步维护处理。

（4）攻击检测

非法设备

监测标准：当 AP 或用户提示状态为非法设备，可判定为安全故障，且须进一步维护处理。

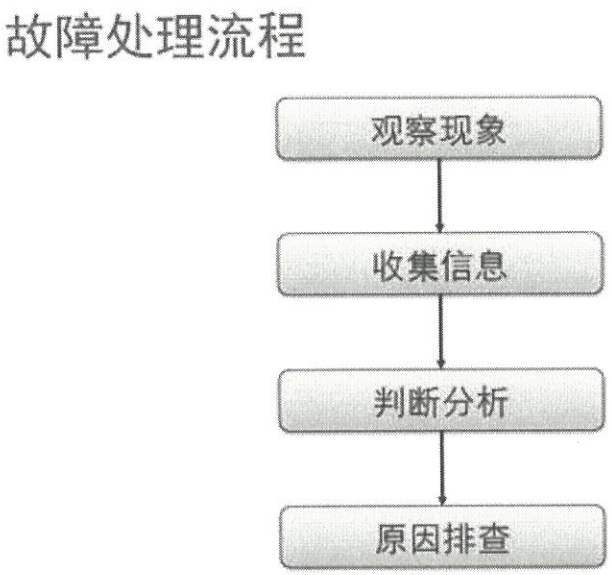
泛洪攻击

监测标准：当 AP 出现被攻击提示时，可判定为安全故障，且须进一步维护处理。

5.5.2. Wi-Fi 网络设备巡检服务情况

5.5.2.1. 巡检服务内容

网络管理维护通过网络管理平台，可以提供网络设备、非法 AP 等物理资源监控，实现故障的快速感知、定位及解决，同时通过无线相关报表及多形式分类资源统计，可以提供日常运维及网络调整提供了依据，极大提升网络管理效率。



故障处理系统化是合理地一步一步找出故障原因，并解决故障的总体原则。网络故障处理的基本步骤是观察现象、收集信息、判断分析、原因排查，其基本思想是系统地将故障的所有可能原因缩减或隔离成几个小的子集，从而是问题的复杂度迅速下降。

5.5.2.2. 网络故障记录表（模板）

北京经济技术开发区宽带无线城市项目

日常故障处理记录表

	故障发生时间	故障类型	场景类别	场景名称	故障信息	故障来源	设备编号	故障处理时间	故障时长	解决方式	处理结果	处理方式	处理人

项目经理签字：

日期：

6. 项目进度计划及保障措施

6.1. 进度计划

我公司在公共 Wi-Fi 网络整体架构搭建和综合服务管理平台自签订本项目服务合同 2 个月内实现，对本项目的网络建设工作，能够提前两个月完成全部建设工作并通过验收。综合服务管理平台要求自签订本项目服务合同 2 个月内部署调试完成并具备各项指标要求。

工作内容	第1周	第2周	第3周	第4周	第5周	第6周	第7周	第8周	第9周	第10周	第11周	第12周	第13周	第14周	第15周
现场勘察设计															
基础路由施工															
设备进场															
平台建设															
大市政路由建设															
设备安装调试															
试运行、网络优化															

6.2. 项目建设实施方案

6.2.1. 前期准备工作

场景勘察准备建设相关方案

设备采购:为保证工期和施工效果，我公司第一时间对部分采购周期较长，对工程进度影响较大的设备进行了采购。并且时时跟进采购进度，争取将采购周期缩减到最短。其他设备和材料合同签订后即纳入采购日程，将随着工程进展逐步到位。

设备到货

设备到货后我公司会派人第一时间在用户的在场情况下进行设备的到货验收和加电验收。

设备到货验收

设备到达最终用户现场后，设备到货验收在设备安装施工前进行。参加人员包括：用户方代表、华为公司方代表、项目集成方代表。设备到货验收主要进行两项工作：依照设备清单内容清点到货设备；签收设备验收报告。

设备到达最终用户现场后，进行设备开箱和清点。主要内容如下:

检查设备外包装完整性，并对设备包装箱进行拍照;

按照设备开箱单，清点设备和板卡数量，板卡外包装完整性，并对设备、板卡、资料进行拍照;

填写设备开箱报告，并记录板卡数量和序列号，记录与设备开箱单和合同设备清单中不符的内容。

设备加电验收

设备清点验收完成之后，对设备进行加电验收。

设备加电前调整板卡位置，调整板卡时带防静电手带，设备加电后利用Console线通过笔记本电脑监测设备或板卡启动情况，验收通过后集成商工程师与用户方人员共同签署验收报告，设备到货验收过程中出现问题，对货验收报告的异常情况进行记录,并报告项目经理,由项目经理与用户和设备厂商协调解决。

前期现场环境勘测

我公司已经对施工现场的情况进行了初步实地考察和调研,包括基础设施建设和设备安装条件等，为实际安装操作提供了第一手的资料。为下一步的情况分

析做准备。并逐一对各区域进行实地调研考察，包括基础安装条件，会议环境条件及网络环境条件，并对实际情况进行记录，需要改进的给予提醒和建议。

为了避免在施工过程中遇到各种不可预见的问题，在工程施工前，对本次项目进行详细调研，其中某些工作需要用户方给予密切配合。主要调研内容包括：

现有设备位置及运行状况

现场安装条件的确认，如电源、机架、电缆线等；线路情况的调研，即目前线路接入情况；其他可能影响现场施工问题的确认。

在本阶段我方将向用户方项目负责人发出书面确认函，提出需要确认内容，并由用户方给予书面确认。根据书面确认结果，若施工条件具备，由双方协商确定现场施工时间。

机房/设备间情况调研

工程施工前，我司将派工程师前往机房/设备间进行调研，检测其是否满足场地要求系数，具体的场地要求如下：

电源系统

本次工程的 220V 交流电源由交流电源架引接交流 220V 火、零、保护地线至设备集装架电源入线端，由集装架内的电源接线盒向上述设备供电。

电源机柜系统的供电系统要求支持输出功率为 7000W 以上，电源线缆的横截面积为 50 个平方毫米，能够支持 125A 的电流强度。

单个机架的设备支持：输出功率要求支持 3500W 以上，电源线缆的横截面积为 25 个平方毫米，能够支持 60A 的电流强度。

主要设备对供电系统要求：本次工程安装的设备所允许的电源变化范围为 220V（正负百分之十），单项，50Hz（正负 2Hz）。电源插头应适合在中国使用。若无此插头，则提供插座，以配合相应的插头。设备具有满足 FCC 标准第 15 部分标准或等价标准的防电磁辐射能力。

布线系统

机房内通信电缆及电力电缆应在防静电地板下布放，布防距离尽量短而整齐，排列有续，通信电缆与电力电缆应尽量分不同管线槽敷设；如同一线架布放时，距离应保证至少 100 毫米以上。

在用户方机房及各楼的施工前应检查：现有水平布线的数量和配线架的连接；

需要增加或升级改造的垂直光纤走线位置、配线架位置、跳线等；机房和各楼之间光纤的连通状况和进出节点、配线架位置。

机房环境

房间尺寸：不小于4平米；空气条件：尘埃，低于0.3mg/m3；振动：机房内部地面低于0.25G；有害气体：气体浓度不能高于危害操作员健康和机器寿命的限度；地板强度：大于等于500kg/m2(相当于一般写字楼地面)；地板表面：防静电材料、防尘封材料；楼层高度：大于等于2.2m；墙壁和天花板：防静电材料、防尘封材料、阻燃材料、吸音和隔音材料；窗户：为防止阳光对设备损害，应加窗帘、防尘和防止盐类与有害气体的腐蚀；门：最窄不小于1.2m，最高不少于2.0m；保安：能防火、防洪水与地震和操作员及设备安全；卫生条件：能防鼠患和昆虫；防火：安装自动火警装置和灭火器；电场强度：≤120dB(1V/m)，频率范围从10KHZ到1GHZ；磁场强度：≤50 Oe（显示器要求为0.015 Oe)；静电：≤6KV（试验设备的要求为150PF/3300hm)；照明：300到700流明（1uX）高于地顿85cm；温度：10¯25摄氏度；湿度：20%-80% 。

业主在机房建设时应满足以上施工条件，需要改造，知道满足国家相关标准为止。

实施前的网络系统现状调查

在项目实施开展前，需要用户方所属各物理地点的网络信息系统进行详细的调查，主要包括如下信息的调查：

业主单位各物理地点现有的状况；当前各物理地点的网络计算机规模和局域网络架构的连接状况；当前各物理地点系统管理人员的配备和职责分工信息；在本项目实施期间和未来一段时间（3-5年）各物理地点的发展与变化状况。

实施前的网络系统改变与配置分析

随着业主单位网络系统集成和网络设计的实施建设，必将对现有各物理地点的设备、系统配置带来改变，为此，在实施前必须对现有的配置信息进行分析。

总结分析调研结果

我公司组织具有丰富实际工作经验的专业工程师对调研结果进行分析和总结，将实际存在的问题和可能遇到的问题分别进行分析，找到解决方法和应对措施。能独立解决的问题，拿出解决方法；不能独立解决的问题，说明原因，同甲

方共同解决；需要甲方配合的，提前与甲方沟通。

总之就是将问题解决在最早也是影响最小的时候，做到有备无患。争取将本项目做成一个成功的项目。

实施方案的细化

在方案调整阶段，我方与甲方就本次项目技术方案和商务方案进行讨论，并针对甲方的最终需求进行方案调整。

在详细方案设计阶段，我方承担详细技术方案的设计和编写工作。在设计和编制过程中，我方与甲方技术负责人及时沟通和交流，确保设计符合甲方的要求。详细方案设计结束后，提交给甲方审核确认。本阶段编制生成《工程整体设计方案》、《工程施工方案》和《系统测试方案》等文档。

6.2.2. 网络设备的安装调试

我方在本项目安装和调试阶段，将完成以下工作。

在甲方及各节点单位技术人员的协助下，完成设备安装机房的环境检测和每个信息点连通性测试，以达到符合联网要求。

我方负责设备安装和联网调试，以及甲方工作站的接入调试，并向甲方提供一个可使用、可靠的运行网络。

设备采用先集中联调方式，由甲方提供临时地址进行集中调试。网络设备集中调试周期需要 2 天，并形成联调、测试、配置报告提交项目经理。

在集中调试结束后，开始实施设备安装计划。将提前两天为时间点，以书面和电话方式通知网络管理部门安排现场设备安装。

提供详细地项目实施计划，在项目验收及免保服务期间，参加项目实施的主要技术人员不离开该项目组并参加免保服务工作。

安装调试具体包括下列内容（但不限于）的工作:

协助使用单位细化并实施 IP 地址的规划与分配;

协调基础运营商完成线路的施工、入户与测试;

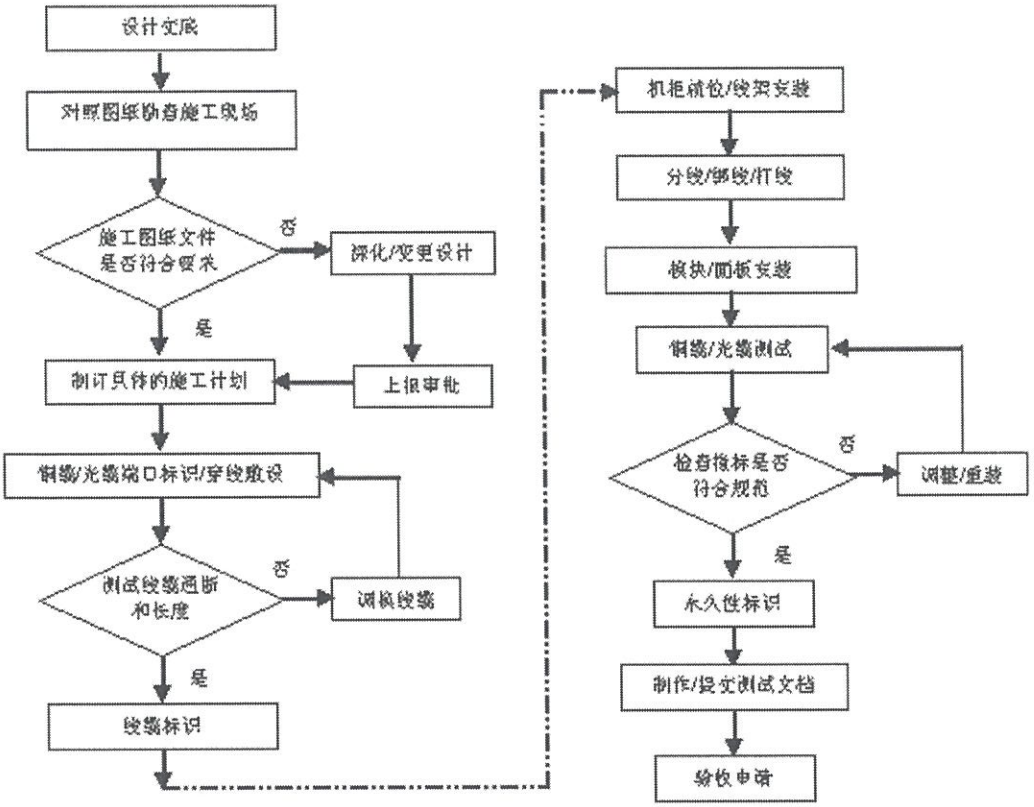
完成的所有网络产品的配置及广域与局域的连接，完成各类网络软件的安装与调试，完成所有设备的安装与设置，路由协议与广域端口参数的配置;

负责完成路由设备配置以及防火墙等安全设备的设置等，以及其它保证网络完整性的相应工程实施工作;

完成网管平台软件等安全产品的安装和设置

6.2.3. 综合布线系统实施

合布线施工工艺流程图



缆线的端接

缆线在端接前，必须检查标签颜色和数字含义，并按顺序端接。缆线中间不得产生接头现象。缆线终端处必须卡接牢固，接触良好。缆线终端须符合设计和厂家安装手册要求。对绞电缆与插接件连接应认准线号、线位色标，不得颠倒和错接。对绞电缆芯线终端须符合下列要求：端接时每对对绞线应尽量保持绞结形态。对绞线在与信息插座（RJ45）相连时，必须按色标和线对顺序进行卡接。插座类型、色标和编号须符合设计要求。对绞电缆与接线模块（RJ45）卡接时，应按设计和厂家规定进行操作。

光缆芯线终端须符合下列要求：采用光纤连接盒对光缆芯线接续、保护，在连接盒中光纤应能得到足够的弯曲半径。连接盒面板必须附加标示，按设计要求跳线。光纤接续损耗值，须符合规定。

各类跳线的端接:

各类跳线缆线和接插件间接触良好，接线无误，标志齐全。跳线选用类型须符合系统设计要求。各类跳线长度须符合设计要求，对绞电缆不得超过 5 米，光缆不得超过 10 米。

施工过程中的主要注意事项

链路与设备必须具有保护措施以防止干扰:

将所有不同的设备接到同一个保护地；使用封闭或半封闭的金属线槽；综合布线电缆与电磁干扰源(如日光灯等)保持最小 30cm 的间距。如果不可能保持这一最小间距，则需要采用封闭金属线槽。

6.2.4. 网络测试

测试过程是检验网络改造是否成功的关键环节，是检查网络实际状况是否附合设计要求的必要手段。因此，在网络改造工作完成以后，我们建议进行相应的测试过程，以保证工程质量，具体步骤如下:

在随机地选取几个终端进行内网联通性测试；通过 Traceroute 的方式检查网内路由的正确性；通过 traceroute 的方式检查到外网路由的正确性；检查内路由是否附合相关路由政策；检查防火墙配置是否正确、是否符合相关策略。

6.2.5. 应急方案

当割接步骤完成以后，若测试网络联通性及其它网络参数不成功，且在短时间内不能解决，则需要采用应急方案，将网络恢复至原有状态。应急方案的具体步骤为:

如因物理链路接入造成影响，因立即断开新设备与网络的物理连接，恢复原有设备连接，查找原因，并排除错误。

如因软件配置导致网络不通，应立即删除新配置命令，并根据错误信息进行调试，如在两小时内未排除，将恢复原有配置。

如因运营商链路切换导致网络不通，因立即通知运营墒恢复原有链路，再对网络进行检查。

6.3. 管理和协调方法

项目的管理和协调方法主要是通过定期和不定期的项目协调会议和周报、月报等方式，及时通报项目进展、解决项目中出现的各种问题、部署下一步工作内

容等。协调工作包括外部协调、内部协调。本项目采用以下项目沟通方式:

项目工作周报

向建设方、监理方提交项目本周进展报告。主要内容包括本周工作进展情况和下周工作安排，或者提出工作建议。按照“项目周报模版”格式要求编写。每周一次，每周星期一报送。报送建设方；同时抄送监理方;

项目月度汇报

向建设方、监理方报告项目本月进展情况。可以是月报方式，也可以是汇报会方式。主要内容是项目进展情况及下一步计划，项目中出现的主要问题及解决方案，希望建设方支持的内容。按照“项目月报模版”格式要求编写每月一次，每月第一周的星期一报送。报送给建设方；同时抄送监理方。

项目例会

由项目经理召集和主持，请建设方和监理方有关人员参加，对项目进展情况进行总结，讨论其中存在的一般性问题和解决办法，并对下一步工作进行部署。例会形成例会报告，及时提交给建设方、监理方。按照“会议纪要模版”格式要求编写，两周一次，向建设方报送《会议纪要》，抄送参加会议的相关方。

项目协调会

由项目协调领导小组、或建设方、或项目经理、或项目监理发起。对项目中涉及多方、需要协调解决的问题，进行研究、协调。协调会形成《会议纪要》，及时提交给各相关方。按照“会议纪要模版”格式要求编写，视需要或事件触发，向建设方报送《会议纪要》，抄送参加会议的相关方。

专题讨论会

项目经理不定期组织项目组相关成员，邀请建设方领导、相关人员、专家组成员、外部邀请专家对工程建设中遇到的技术问题进行讨论或专题讨论。

附件二

项目分项报价

分类	名称	数量	单价（元）	合价（元）	备注/说明
政府办公	党群活动中心	59	2985	176115	/
	博大大厦及食堂	248	2985	740280	/
	朝林大厦	201	2985	599985	/
	博大朝林停车场	48	2985	143280	/
	博大朝林电梯厅	14	2985	41790	/
	仲裁服务中心	36	2985	107460	/
	隆盛综合执法局	19	2985	56715	/
	荣华街道办事处	105	2985	313425	/
	荣华街道办事处9号楼	45	2985	134325	/
	经海街道办事处	64	2985	191040	/
	上海沙龙活动中心	93	2985	277605	/
	总工会职工服务大厅	31	2985	92535	/
	总工会教育服务基地	22	2985	65670	/
	亦城客厅	113	2985	337305	/
政府服务	交通队服务大厅	27	2985	80595	/
	交通队办公楼	145	2985	432825	/
	隆盛大厦交通队	22	2985	65670	/
	消防-荣华中队	55	2985	164175	/
	消防-博兴中队	58	2985	173130	/
	消防-经海中队	49	2985	146265	/

	开发区综合救援支队	46	2985	137310	/
	消防-瑞和路特勤站	114	2985	340290	/
	消防-永昌中队	96	2985	286560	/
医疗	国家康复医院	122	2985	364170	/
	振国医院	80	2985	238800	/
	东方医院	160	2985	477600	/
文教	第四幼儿园	28	2985	83580	/
	杂技团	12	2985	35820	/
体育场馆	博大永康俱乐部	4	2985	11940	/
	体育场	60	2985	179100	/
	数码庄园	15	2985	44775	/
	博大水务体育场	10	2985	29850	/
	汇龙森	9	2985	26865	/
	生物医药产业园	7	2985	20895	/
	金风科技	40	2985	119400	/
市政公园绿地	亦庄文化园	3	2985	8955	/
	凉水河景观	2	2985	5970	/
博兴街道辖下社区	博客雅苑	56	2985	167160	/
	亦城茗苑	64	2985	191040	/
	瀛海庄园	27	2985	80595	/
	中芯会馆	15	2985	44775	/
	亦园小区居委会	8	2985	23880	/
	壹中心	10	2985	29850	/
	通泰社区服务中心	16	2985	47760	/
	通泰社区	36	2985	107460	/
荣华街道辖下社区	大雄城市花园	13	2985	38805	/
	管委会宿舍	3	2985	8955	/
	上海沙龙社区	22	2985	65670	/

	一栋洋房	22	2985	65670	/
	一品亦庄	2	2985	5970	/
	永康公寓	18	2985	53730	/
	金地格林	16	2985	47760	/
	狮城百丽社区	6	2985	17910	/
	卡尔 24 小时书屋	2	2985	5970	/
商街	亦庄生活广场	15	2985	44775	/
重要科技园区	北人国际会展中心	387	2985	1155195	/
合计：				8,955,000.00	

附件三

项目主要人员组成

序号	拟承担职务	姓名	性别	年龄	学历	专业	从业资格（职称、证书等）	备注
1	项目经理	于光	男	42	本科	计算机网络	信息系统项目管理师（高级）	/
2	行政服务人员	宗 珊	女	36	本科	计算机科学与技术	政工师（中级）	/
3	系统集成工程师	甄 挚	男	38	本科	电子与通信工程	一级建造师 机电工程（高级）	/
4	系统集成工程师	李 堃	男	38	本科	计算机统信工程	通信工程师（中级）	/
5	系统维护工程师	孔祥南	男	38	本科	软件工程	电子工程计算机（中级）	/
6	系统维护工程师	陈永根	男	39	本科	信息计算机与智能系统	一级建造师 机电工程（高级	/
7	网络技术工程师	孙德俊	男	36	本科	网络工程	网络工程师（中级）	/
8	网络技术工程师	康京雷	男	30	专科	机电一体化技术	系统集成项目管理师（中级）	/
9	网络技术工程师	孙鹏	男	39	本科	电气工程与自动化	二级建造师（机电工程）	/
10	网络技术工程师	刘宇豪	男	37	本科	数字媒体艺术	系统集成项目管理师（中级）	/
11	网络技术工程师	何权	男	42	本科	工商管理	信息系统项目管理师（高级）	/

12	施工维护工程师	张华平	男	47	专科	机电一体化	建筑电气与智能化工程（中级）	/
13	施工维护工程师	杨子嵩	男	39	专科	安全工程	电气工程师（中级）	/
14	施工维护工程师	司建达	男	30	本科	工程管理	/	/
15	施工维护工程师	张皓	男	50	本科	经济管理	电气工程师（中级）	/
16	施工维护工程师	房红武	男		本科	建筑环境与能源应用工程	楼宇智能自动化（中级）	/
17	施工维护工程师	马晓峰	女		本科	计算机通信工程	系统集成项目管理工程师（中级）	/

保 密 协 议 书

甲　方：北京经济技术开发区营商环境建设局

乙　方：北京博大网信股份有限公司

为明确甲乙双方的保密责任，确保甲方国家秘密、商业秘密事项的安全，依据《中华人民共和国保守国家秘密法》以及相关保密法律法规的要求，经甲乙双方协商一致，签订本协议。

一、甲方的权利和义务

（一）甲方应指定专门的人员，配合乙方开展业务工作；

（二）甲方保密管理部门在业务范围内，有权随时对乙方的保密管理情况进行监督、检查和指导；发现问题，可书面要求乙方进行整改。

二、乙方的权利和义务

（一）乙方在履行甲方委托合同的过程中，对于了解或知悉的国家秘密和甲方的商业秘密，承担保密责任；

（二）乙方应加强对本方所有与《2024年度开发区宽带无线城市综合服务项目委托服务合同》相关人员的保密教育和管理；

（三）乙方应建立、健全本方的规章制度，并采取一切行之有效的措施，保证保密法规和要求的落实，确保不发生与委托代理协议相关的任何泄密事件；

（四）乙方应按照国家秘密载体管理的有关规定，加强涉及咨询事项资料的管理，所有资料（含电子文档）应进行编号、登记管理，涉及国家秘密的资料销毁应履行清点、审批和监销手续；

未经甲方书面同意，乙方一律不得将涉及委托代理事项的任何资料（包括书面资料和电子文档）转交任何机构和个人。

接收甲方发送的涉及国家秘密、商业秘密和单位内部事项的电子文档的，乙方只可在相应涉密等级的计算机上存储、处理，不得在互联网上发布、通过互联网发送或在连接互联网的计算机上处理。

（五）乙方应为履行甲方委托配备相应的安全保密设备；

（六）乙方在合同解除或履行完毕后，仍然负有保守国家秘密和甲方商业秘

密的义务。

三、乙方实施任何违反国家保密法律法规的行为的，应当承担相应的法律责任。同时甲方有权追究乙方的民事赔偿责任，并可在甲方与乙方签订主合同金额的范围内，追偿相应的补偿费用。

四、本协议书一式【陆】份，甲乙双方各持【叁】份，陆份协议书具有同等的法律效力。

五、本协议书作为甲方与乙方主合同的附件，与主合同具有同等法律效力；本协议自签订之日起生效，长期有效，不因主合同的中止、终止、失效或解除而失效。

甲方：北京经济技术开发区营商环境建设局（盖章）

单位负责人／授权代表：_____（签名）

2020年 10月 25日

乙方：北京博大网信股份有限公司（盖章）

法定代表人／授权代表：_____（签名）

2020年 10月 25日

廉 政 协 议 书

甲方（发包人）：北京经济技术开发区营商环境建设局

乙方（承包人）：北京博大网信股份有限公司

项目名称：2024 年度开发区宽带无线城市综合服务

合同金额（大写）：捌佰玖拾伍万伍仟元整

项　目　概　况：为开发区政府、企业、居民提供无线网络服务。提供 5 大类不少于 50 处场景，AP 热点总量不少于 3000 点的公共 Wi-Fi 网络服务、服务期内按需新增的场景公共 Wi-Fi 网络服务等无线网络服务

廉 政 协 议 书

为进一步完善监督制约机制，确保工作质量和预防职务犯罪行为以及各种不正当行为的发生，在开发区各项工作中保持党员干部的廉洁自律，根据开发区有关廉政建设的相关规定，并结合实际特订立本协议如下：

一、甲乙双方应当自觉遵守国家法律法规以及有关党风廉政建设的各项规定。

二、甲方工作人员应保持与乙方的正常工作交往，不得接受乙方的礼金、有价证券和贵重物品，不得在乙方报销任何应由个人支付的费用，不得以任何形式向乙方索要和收受回扣或变相收受贿赂。

三、甲方工作人员不得参加可能对公正执行公务有影响的宴请和娱乐活动。

四、甲方工作人员不得要求或者接收乙方为其住房装修、婚丧嫁娶、家属和子女的工作安排以及出国等提供方便。

五、甲方工作人员不得向乙方介绍亲属或亲友从事与甲方工作有关的经济活动。

六、乙方应当通过正常途径开展相关业务工作，不得向甲方工作

人员及第三方赠送礼金、有价证券和贵重物品等。

七、乙方不得为谋取私利擅自与甲方工作人员及中介机构就有关工作问题进行私下商谈或者达成默契。

八、乙方不得以洽谈业务、签订经济合同为借口，邀请甲方工作人员外出旅游和进入营业性高消费娱乐场所。

九、乙方不得为甲方单位或个人购置或者提供通信工具、交通工具、家电、高档办公用品等。

十、乙方如发现甲方工作人员有违反上述协议者，应向领导或者甲方上级主管单位举报。甲方不得以任何借口对乙方进行报复。

十一、本协议作为合同的附件，与合同具有同等法律效力。经双方签署后立即生效。

十二、本协议的有效期为双方签署之日起至该项目验收合格时止。

十三、本协议一式三份，由甲方执二份，乙方执一份。

甲方（盖章）

法人代表或委托人（签字）：

签订日期：2024年10月25日

乙方（盖章）

法人代表或委托人（签字）：

签订日期：2024年10月25日