采购需求

说明：

1.为落实政府采购政策需满足的要求

本招标文件（以下或简称为“采购文件”）所称中小企业必须符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）的规定。

2.“实质性要求”是指招标文件中已经指明不满足则投标无效的条款，或者不能负偏离的条款，或者采购需求中带“▲”的条款。

本项目“技术要求及需求”及“商务要求”凡标注“▲”的条款或要求，投标人不响应或不满足的，投标文件即作无效处理；其他标注“▲”的事项或说明，投标人投标文件不符合要求的即作无效处理。

3.投标人必须自行为其投标产品或技术服务侵犯他人的知识产权或者专利成果的行为承担相应法律责任。

4.所属行业依照《中小企业划型标准规定》（工信部联企业〔2011〕300号）及《国民经济行业分类》（GB/T4754-2017）的有关规定执行。**本项目所属行业为：软件和信息技术服务业**

5.本采购需求中技术要求所使用的标准或应用标准如与投标人所执行的标准不一致时，按最新标准或较高标准执行。

6.**评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响其服务或产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理**。

7.**本项目采购需求表中，若有要求提供的证明文件材料或承诺书的，请在《技术要求偏离表》或《商务要求偏离表》中应答时，注明相关文件材料或承诺书放置的页码。**

广西教育骨干网第二期链路租用服务项目概况及采购需求

一、项目概况

1.广西教育网要为教育数智基座建设和数据治理、推广智慧教育教学和人工智能应用

等工作构建网络基础条件。广西教育网由骨干网、各地城域网及校园网组成，是万兆主干、千兆到校、百兆到班分层管理的教育信息网络系统。骨干网按双环路设计，在广西教育数据中心、中国教育和科研计算机网络（CERNET）广西节点广西大学和广西师范大学（桂林）分别设置 3 个核心节点，租用双环主干光纤传输线路。在 14 个设区市设置共计 13 个汇聚节点（其中，南宁市设置 2 个汇聚点，钦州市、北海市、防城港市共设置 1 个汇聚节点），租用双路主干光纤传输线路。广西教育网网络中心和广西教育数据中心共址建设，一体化运维管理。

2.骨干网核心线路具备自愈环保护功能，纵向接入城域网，实现线路两端的互通。

3.本次服务采购要充分利用互联网、云计算和大数据、第五代移动通信技术（5G）、物联网（IoT）、人工智能（AI）、区块链、边缘计算等技术，构建服务全区各级各类学校、教师和学生的绿色网络空间。

4.教育部对信息化工作提出“需求驱动、应用为王”的指导思想，本次服务采购要以提高骨干网的应用率、应用水平和质量为核心目标开展工作。采购人在本次服务采购服务期内的重点工作包括但不限于：

（1）继续推进广西教育网的 IPv6 规模部署和应用，开展信息系统（网站）IPv6 单栈部署、试点应用和区域推广应用。

（2）持续提高广西教育网访问互联网、电子政务外网、中国教育和科研计算机网（CRENET）等网络教育资源的稳定性和人机体验。

（3）持续提高广西教育网网络应用的人机体验。

（4）持续提高广西教育网和广西教育数据中心的数据管理的能力和水平。

（5）持续提高广西教育网和广西教育数据中心的数据安全管理、个人信息保护、未成年人信息保护的能力和水平。

5.原广西教育网骨干网建设概况见本章附件 1 了解。

二、技术要求及需求

▲1.本次服务采购延用广西教育网组织架构和管理体系，利旧广西教育网网络中心和骨干网现有基础设备和设备系统，同时采购相关设备系统维保服务，包括并不仅限于系统软硬件故障保修、备件更换、软件升级，以及应用的技术支持服务和应急救援等。**相关技术文件属不可公开材料（包括非结构化、结构化、备份和测试等 4 套存储系统），由投标人在获取本项目招标文件后，可自愿原则按本项目规定的统一现场考察时间，到采购单位现场签定保密协议后，采购人统一提供查阅。未参加现场考察的投标人若中标，自行承担**

合同履约责任及风险（含投标报价所有成本核算）。

▲2.骨干网定级网络安全等级保护第三级。**投标人在投标文件中提交服务方案和承诺应符合相关规定和要求。**中标供应商提供的服务应符合相关规定和要求，且须无条件配合采购人开展测评和整改等相关工作，直到采购人获得公安部门认可的、有效期内的、等级测评结论为“基本符合”及以上的测评报告。

A 分标　采购预算： 764.001 万元

序号	标的名称	数量及单位	所属行业	技术要求及需求
1	广西教育骨干网第二期链路租用服务（1）	1 项	信息传输业	**（一）传输线路租用服务** ▲1.≥100G 点对点专线，3 条；≥10G 点对点专线，10 条。 ▲2.透明传输线路，上下行带宽对等，传输线路与互联网（公网）隔离。 ▲3.具备自愈环保护，具备双路由保护。 4.相关网络设备满足可平滑升级的要求。 5.传输设备要求具有全网网管监控功能，并实行 7×24 小时实时监控；用户端可实时监测线路状况，线路监控设备由中标供应商提供。所有接入设备由中标供应商提供或利旧使用采购人原有设备，所有线路经由服务商汇聚后提供给用户使用。 6.专线租用服务期间，提供专线集中管控服务。包括但不限于：专线网络拓扑、实时状态、性能指标（包括但不限于：时延、丢包率、带宽占用率等）、告警信息等端到端可视化运维管理能力，以及定期总结报告运维管理情况等服务。 7.保证网络的畅通，负责采购人本次采购传输线路租用服务涉及所有设备（即“（一）传输线路租用服务”中的设备）的运行维护且不得额外收取费用，包括但不限于：光端机、转换器等设备；培训传输知识，指导采购单位及相关服务支持单位的人员做好日常维护。 8.用户网络需要扩展或升级时，负责提供相应解决方案等技术支持，不得额外收取费用。 ▲9.网络参数要求：

				（1）全年网络阻断时长总计不超过 24 小时； （2）端到端电路的传输比特差错率(误码率)：≤1.0×10E-7； （3）端到端电路丢包率≤1%； （4）端到端电路平均网络延时≤50ms、时延抖动≤10ms。 10.未约定的其它服务质量指标，则由中标供应商按《电信服务规范》（信息产业部令第 36 号）的要求，为采购人提供相应的服务。 **（二）运维管理服务** 部署一套运维监控管理信息系统，统一纳管本项目涉及的软硬件设备系统，包括但不限于：网络设备、服务器、存储设备、安全设备、操作系统、数据库、中间件、应用服务等，并提供相应运维管理技术支持服务。 **1.系统部署服务** （1）提供本地化部署和管理、分布式部署和管理、多层级管理、数据采集负载均衡、高可用、冗余备份等能力和服务。 ▲（2）提供监控≥3000 个管理对象的能力，并支持后期扩展。 （3）可利旧原广西教育网网络中心和广西教育数据中心的算力和存储，不足部分，由中标供应商负责提供。 （4）可部署于国产服务器 （5）可部署于 Windows、linux，以及国产操作系统。 （6）可部署于国产数据库和中间件。 （7）系统独立自主研发，不存在第三方版权争议。**（投标人在投标文件中提供软件著作权证明，或第三方测试机构出具的检测报告，或投标人的声明、不存在第三方版权争议、承担版权争议责任的承诺书等，并加盖投标人公章）** **2.运维管理服务** 包括但不限于： （1）网络运维，包括但不限于：网络线路、网络拓扑、IP 地址管理、设备配置、流量分析等。能够利用多种主流网络协议进行端到端质量探测，精准测量

				关键路径的网络性能指标，实现对骨干网健康状况与服务质量的持续监控、性能评估与故障快速定位。 （2）设备纳管，包括但不限于：自动扫描添加、运行状态、性能指标等，对纳管设备支持用户灵活定义的多级资源分组管理、标签管理。 （3）业务保障，能够辅助快速查找故障，包括但不限于：业务分层、业务拓扑、运行状态、性能指标等。 （4）可视化，按管理层级和业务逻辑展示运维管理数据，包括但不限于：运维管理数据展板（包括但不限于：网络拓扑、业务拓扑、关键指标实时仪表盘等）、报表和报告等。报表生成时间≤10 分钟，支持导出 PDF/Excel 格式。拓扑图、仪表盘加载时间≤10 秒。 （5）告警提醒，能够利用手机短信、电子邮件、即时通信应用（钉钉、或企业微信、或飞书等）等方式及时提供报警信息。 （6）管理服务，提供自动巡检、巡检管理、工单管理、知识库等能力和服务。 3.提供定制开发数据对接服务 按采购人对接自治区网信、公安、数据局等第三方关于网络安全和网络运维监督管理信息系统的需要，提供数据对接服务。 **（三）骨干网运维管理人工智能应用服务** 利用大数据和人工智能技术，采集和分析广西教育网骨干网（含网络中心）和广西教育数据中心运维管理数据，挖掘分析部署于广西教育数据中心的教育部省级部署管理信息系统和自治区自建管理信息系统的数据，以及数据间的关联关系，支撑采购人加快推进本项目服务期内重点工作，助力本项目提质增效。 **1.运维管理人工智能应用服务** 提供广西教育网骨干网运维管理的人工智能应用服务，实现运维数据实时采集和智能分析，提供运维管理和业务应用的 信息咨询和信息服务。 **1.1 运维数据采集分析** 通过建立数智基座实现数据实时采集，结合运维人工智能（AI）模型实现智能分析，自动识别设备系

				统性能、流量、资源占用和应用响应等异常数据，以通知、报告和展板等多种方式提供报警信息。 （1）数据采集覆盖网络设备和安全设备（包括但不限于：端口流量、丢包率、时延等）、服务器（包括但不限于：CPU/内存/磁盘使用率、进程状态等）、应用系统（包括但不限于：响应时间、并发量等），支持≥10000 个监控对象。 （2）数据采集频率可自主选择配置，默认 1 分钟/次，关键指标（如核心链路流量、数据库 CPU）支持自定义 10 秒-30 秒/次，数据采集成功率≥99.9%。 （3）基于历史数据预测潜在故障，自动生成预警通知。 （4）识别准确率≥90%。 （5）能够利用手机短信、电子邮件、即时通信应用（钉钉、或企业微信、或飞书等）等方式及时提供报警信息。 **1.2 运维管理问答咨询** 构建基于知识库的问答系统，为运维人员、管理人员和业务应用用户提供精准高效的咨询服务。 （1）提供便捷的交互界面，支持文本输入提问。用户输入问题后，系统通过智能问答算法快速生成基于信息化设备运维、业务系统应用及相关资料的准确回答，并可展示回答依据的具体条款或资料来源，辅助用户理解和决策。 （2）为业务应用用户提供咨询服务的功能模块，应具备独立部署、提供互联网服务的能力。 **1.3 数据应用运维保障** 提高广西教育网网络应用用户人机体验，助力提高广西教育网和广西教育数据中心的数据管理的能力和水平，自动识别全区教育系统组织机构、教师、学生及其监护人基础信息数据的错漏和异常，锁定异常数据流转过程，生成报告和展板，提供数据修复建议意见和服务，支撑广西教育网用户网络接入身份认证、部署于广西教育数据中心的教育部省级部署管理信息系统和自治区自建管理信息系统单点登录的应用和运维管理。 **2.本地化≥32B 大语言模型训练和推理能力服务** **▲2.1 大语言模型服务**

				（1）对大语言模型进行全生命周期管理服务，包括但不限于：模型部署、模型测试、模型更新、模型导出、模型版本管理、模型详情查看等功能。 （2）本地部署 DeepSeek、Qwen 等多种国产主流模型。 （3）提供多种模型自由切换服务。 （4）提供通过 API 进行访问和接口调用模型服务。 （5）提供可视化工作流编排，预设模板≥5 个，可自由设计和组合各种功能模块，可以通过拖拽式界面，设计复杂的问答流程，包括条件判断、循环、模型调用等节点。 （6）提供 MCP（模型上下文协议，Model Context Protocol）工具，同时支持自定义的 MCP 工具，可在构建复杂工作流时直接调用 MCP 工具作为处理节点，实现更强大的功能组合。 **2.2 应用模型服务** （1）提供运维管理涉及应用模型服务，包括并不限于文本文档识别模型、pdf 文档识别模型、图片识别模型等，大小 5MB 及以下的文档识别处理时间≤20 秒。 （2）提供图片智能识别、智能数据分析、语音转文字等应用模型服务。 **2.3 知识库服务** （1）导入运维相关 markdown、word、pdf、txt 等常用格式文件快速构建本单位知识库，并对文本数据进行预处理、向量化和问题答案（QA）分割。包括并不限于通过 RAG（检索增强生成，Retrieval-Augmented Generation）等技术，将运维相关文档（markdown、docx、pdf、txt 等常用格式文件）快速构建为本地知识库。 （2）基于多模态大模型、OCR 模型、文本生成大模型、知识图谱等技术构建知识图谱，融合各类文本、标准条款、设备参数、故障案例等数据，通过实体链接与关系抽取技术建立知识关联。 **2.4 大语言模型训练推理能力的配套硬件服务** 选装合适模型和匹配硬件设备系统，确保推理结果的精度与稳定性。

				（1）显存能够支持不低于 32B 参数、精度为 FP16/BF16 的模型训练和推理。 （2）支持≥20 个用户并发访问。 （3）内置硬盘总容量≥32TB。 （4）内置缓存盘：≥2*3.2TB NVMe SSD。 （5）单台一体机 CPU：≥2 颗，每颗核数≥32 核；内存：≥1024GB；系统盘：≥2*480GB SATA SSD；RAID 卡：≥1 张，支持 RAID0、1、10、50、60 以及直通；网卡：GE 网卡(电口)≥2 口，≥10GE 网卡≥2 口（光口，满配多模光模块）。 ▲（6）如果需要由多台一体机组网的，须提供系统组网配套网络设备和配件。 **2.5 大语言模型通用要求** 支持自然语言对话，至少支持记忆≥6 轮互动，支持输入最大长度≥2000 token。 **3.安全要求** 部署环境应保证智能运维相关的人工智能应用和部署的大模型安全可信，实现数据安全管理。 （1）数据本地化存储。所有数据应存储在本地算力平台（系统）或用户指定的本地存储设备，不向第三方服务器传输数据。 （2）身份认证与权限控制。基于采购人组织架构，以及运维管理人员角色配置应用条件环境，可审计所有操作日志，日志留存≥6 个月。 （3）数据传输基于国产商用密码技术，确保数据采集过程中传输安全，访问用户安全可控。 **（四）骨干网城市节点和网络中心 10G 接入能力服务** 1.骨干网 13 个汇聚节点的 10G 接入能力租用服务。 2.按承担城域网接入服务需要，提供每个节点≥8 个 10G 光口的接入能力服务，总计≥148 个 10G 光口的接入能力服务。【13 个汇聚节点 10G 光口接入能力服务需求情况：广西教育数据中心（南宁）：≥8 个；广西大学（南宁）：≥8 个：广西科技大学（柳州）：≥16 个；广西师范大学（桂林）：≥20 个；梧州学院（梧州）：≥8 个；北部湾大学（钦州）：≥16 个；广西工业职业技术学院（贵港）：≥8 个；玉林师范学院（玉

				林）：≥12 个；百色学院（百色）：≥16 个；贺州学院（贺州）：≥8 个；河池学院（河池）：≥12 个；广西科技师范学院（来宾）：≥8 个；广西民族师范学院（崇左）：≥8 个；总计：≥148 个】。接入能力服务提供方式可以选择以下两种方式之一： 2.1 方式一： 通过在现网设备扩展端口方式提供接入能力服务（现网设备信息：品牌：华为，数量：26 台）。使用现网设备方式接入的，则中标供应商需要提供该设备 3 年的维保服务，涉及的服务费用由中标供应商承担。**（说明：为便于后续向原厂进行采购保修服务，投标人可通过参加采购人统一组织的现场考察或中标后向采购人查阅了解现网设备对应的 SN 码）** 2.2 方式二： 不基于现网设备扩展端口方式提供接入能力服务。 2.2.1 满足汇聚数据交换服务需要。 2.2.2 提供汇聚路由器 26 台，以及设备软硬件维保和调试服务。 （1）整机的主控及网板模块、内置交流电源和风扇等冗余设计且满配，风扇支持前后通风，所有业务板卡及电源、风扇均可热插拔。 （2）整机支持业务载板插槽≥8 个（不含主控槽位）。 （3）整机配置万兆光口≥24 个，千兆光口≥12 个，提供接口后剩余业务板槽位≥2 个。 （4）支持网络资源、隧道路径、业务路径、及业务 SLA 的可视可管。 （5）支持广域网智能调优。 （6）支持 SRv6，提供 SRv6 承载 VPN 业务能力，提供 SRv6 Policy 功能，具备网络定制化服务和差异化服务能力。 ▲2.3 投标人必须在投标文件中所提供的“《技术要求偏离表》”中明确上述方式（即“2.1 方式一”和“2.2 方式二”）中，是以哪一个方式提供接入能力服务。 3.配置万兆单模光模块≥148 个，应与所提供服务方案的光口数量匹配。所配模块应满足数据传输服

				务需要，与组网连接线路和网络运维管理要求匹配；可按实际应用需要配置不同传输距离规格模块。 **（五）骨干网存储系统维保服务** 1.服务范围包括：非结构化、结构化、备份和测试等 4 套存储系统。 1.1 非结构化存储，提供网络中心非结构化存储维保，数量 1 套。 1.1.1 主要包括存储柜 2 台，品牌：曙光；存储网桥 4 台，品牌：曙光；交换机 2 台，品牌：博科； 1.1.2 由 A、B 节点组成，配置：每节点配置双控制器，8 个 16G FC 前端端口，4*12Gb 后端 SAS 接口，缓存 128GB；两个节点共配置 192 块 2.5″ 1.2TB 10K SAS 硬盘；48 块 400GB SSD 闪存硬盘；96 块 3.5″ 4TB 7.2K NL_SAS 硬盘；最大支持磁盘数量 2880 个。 1.1.3 维保服务范围： （1）维保期内提供存储故障硬盘更换及更换操作相关服务，提供存储阵列设备季度巡检服务，除存储设备控制器硬件不在维保范围，其他硬件维保包括存储设备硬盘、存储设备电源模块、存储设备 IO 模块、存储设备内存条、交换机、网桥； （2）备件供应：年度维保期内硬盘坏件数量不超过 12 块（如所换硬盘在质保期内又发生故障的，中标供应商负责继续更换且不得额外收取费用，所换硬盘不占 12 块硬盘更换限制额度），超过 12 块（不含）另行计算费用（费用由双方协商确定）； （3）提供存储技术支持服务，配置更改支持； （4）提供容灾演练每年一次的现场技术支持。 1.2 结构化存储，提供网络中心结构化存储维保，数量 1 套。 1.2.1 主要包括存储柜 2 台，品牌：长虹；存储网关 1 台，品牌：长虹；CDP 连续数据保护 2 台，品牌：长虹； （1）2 台存储配合存储网关组成双活存储。单台配置：双引擎 4 控制器，32 个 8G FC 前端端口，缓存 1TB；两台存储共配置 168 块 2.5″ 1.2TB 10K SAS 硬盘；18 块 1.92TB SSD 闪存硬盘；最大支持磁盘数量 2880 个，配原装机柜； （2）1 套存储网关：配置 2 个引擎共 4 个节点控

				制器，每引擎72GB缓存，共144GB缓存，单集群最大支持横向扩展到4引擎8个控制器；配置前端端口数16个8Gb/s FC 接口；配置后端端口数16个8Gb/s FC 接口，满配光模块，原装机柜； （3）1套RecoverPoint CDP容灾装置：配置2台冗余容灾硬件设备，支持高可用集群配置，实现设备故障冗余切换及负载均衡;单台配置4端口8Gb FC，4个千兆以太网端口；配套CDP容灾软件，配置20TB本地连续数据保护复制许可； （4）1套Recoverpoint for Virtual Machines虚拟机版连续数据保护软件：为虚拟机提供虚拟机级别粒度的连续数据保护，虚拟机连续数据保护管理能通过插件与 VMware vCenter集成。基于VM虚拟机授权，配置30个保护许可。 1.2.2维保服务范围： （1）维保期内提供存储故障硬盘更换及更换操作相关服务，提供存储阵列设备季度巡检服务，除存储设备控制器硬件不在维保范围，其他硬件维保包括存储设备硬盘、存储设备电源模块、存储网关电源模块、存储设备IO模块、存储设备内存条。年度内提供结构化存储动态口令≥12次动态口令卡（巡检及更换备件需要动态口令码）登录存储更换备件及巡检； （2）备件供应：年度维保期内硬盘坏件数量不超过12块（如所换硬盘在质保期内又发生故障的，中标供应商负责继续更换且不得额外收取费用，所换硬盘不占12块硬盘更换限制额度）。 （3）提供存储技术支持服务，配置更改支持； （4）提供容灾演练每年一次的现场技术支持； （5）提供一次 RP4VM 容灾软件版本更新升级至最新的版本服务，CDP容灾演练测试； （6）提供RecoverPoint CDP硬件设备配置变更技术支持，容灾演练测试； （7）提供存储网关配置、变更，第三方存储接管，在线数据迁移技术支持服务； （8）提供现有存储设备监控软件部署实施，存储设备监控添加、配置； （9）年度内提供维保设备现场技术培训1次。 1.3 备份存储，提供网络中心备份存储维保，数

				量 1 套，品牌：曙光； 1.3.1 1 台曙光磁盘阵列，双控制器，8 个 16G FC 前端端口，4*12Gb 后端 SAS 接口，缓存 96GB；配置 36 块 2.5″ 1.8TB 10K SAS 硬盘；20 块 800GB SSD 闪存硬盘；120 块 3.5″ 4TB 7.2K NL_SAS 硬盘；最大支持磁盘数量 1920 个。 1.3.2 维保服务范围： （1）年度维保期内提供存储故障硬盘更换及更换操作相关服务，提供存储阵列设备季度巡检服务，除存储设备控制器硬件不在维保范围，其他硬件维保包括存储设备硬盘、存储设备电源模块、存储设备 IO 模块、存储设备内存条； （2）备件供应：年度维保期内硬盘坏件数量不超过 10 块（如所换硬盘在质保期内又发生故障的，中标供应商负责继续更换且不得额外收取费用，所换硬盘不占 10 块硬盘更换限制额度），超过 10 块（不含）另行计算费用（费用由双方协商确定）； （3）提供存储技术支持服务，配置更改支持； （4）提供容灾演练每年一次的现场技术支持。 1.4 测试存储，提供网络中心测试存储维保，数量 1 套，品牌：EMC。 1.4.1 1 台 EMC 双控统一存储阵列，全冗余模块化体系结构，配置 48G 缓存，支持 NAS、IP SAN 和 FC SAN 模式。配置 FCP/NFS/CIFS/iSCSI 协议及相关模块，配置 12 块 600GB 15000 转 6Gb SAS 硬盘；配置 15 块 2TB 7200 NL_SAS 硬盘，配置 15 块 3TB 7200 NL_SAS 硬盘；最大支持 250 块硬盘。 1.4.2 维保服务范围： （1）年度维保期内提供存储故障硬盘更换及更换操作相关服务，提供存储阵列设备季度巡检服务，除存储设备控制器硬件不在维保范围，其他硬件维保包括存储设备硬盘、存储设备电源模块、存储设备 IO 模块、存储设备内存条； （2）备件供应：年度维保期内硬盘坏件数量不超过 6 块（如所换硬盘在质保期内又发生故障的，中标供应商负责继续更换且不得额外收取费用，所换硬盘不占 6 块硬盘更换限制额度），超过 6 块（不含）另行计算费用（费用由双方协商确定）；

				（3）提供存储技术支持服务，配置更改支持； （4）提供容灾演练每年一次的现场技术支持。 **2.其他服务要求** **2.1 预防性检查维护服务要求** （1）技术支持：提供 7×24 小时的技术支持服务。 （2）备件服务：提供用户现场备件更换服务，维保期内放置一块 2.5 寸 1.2TB 10K SAS、一块 2.5 寸 1.2TB 10K SAS 硬盘、一块 2.5 寸 1.8TB 10K SAS 硬盘、一块 3.5 寸 4TB 7.2K NL_SAS 硬盘、一块 3.5 寸 3TB 7.2K NL_SAS 硬盘，坏硬盘更换后补齐现场备盘，提高现场备件响应速度；四套存储内的上述五种硬盘和非结构化存储及备份存储的 SSD 硬盘中，如某一技术参数的硬盘在年度维保期内都没出现过故障的，年度维保期结束后，中标供应商移交至少 1 块该技术参数的硬盘给用户且不得额外收取费用，该移交不含更换操作服务。非结构化存储和备份存储的更换额度可以互换。现场备盘的质保期为 6 个月，自采购人签收该硬盘之日起算。其他不入现场备件库，直接插入存储进行更换的硬盘，质保期为 6 个月，自采购人确认完成硬盘更换之日起算。硬盘入库现场备件库或插入存储完成更换后，还在 6 个月质保期内且项目维保服务期已超过的情况下，硬盘发生故障的，中标供应商负责再为采购人提供该硬盘的一次更换服务，不得收取费用，如再次更换的此硬盘又发生故障的，中标供应商有权不再进行更换该故障硬盘，但采购人有权认定中标供应商提供的硬盘存在质量问题，并将中标供应商列入黑名单。 （3）巡检服务：提供每季度一次例行巡检服务，检测设备及系统运行情况并提供巡检报告，每年提供一次 CDP 容灾演练服务。 （4）软件优化服务：提供维保期内提供 VMware vsphere 虚拟化平台升级技术支持服务，提供优化技术支持。提供一次 RP4VM 容灾软件版本升级服务，CDP 容灾演练测试。 （5）服务质量分析要求：在年度维保服务期内，应至少召开 1 次服务质量分析例会，对该阶段中标供应商所提供的服务进行总结和考核。在采购人的要求

				下，中标供应商有义务随时配合召开其他时间的例会。中标供应商对例会纪要中采购人的意见与建议部分于 7 日内进行反馈并跟踪落实。 **2.2 故障处理服务要求** （1）提供 7×24 小时的故障受理，30 分钟内故障处理响应服务。故障包含硬件、软件故障等存储设备自身相关联，导致系统不能正常运行的一切故障对象。 （2）故障服务的现场响应时间小于 4 小时，即 4 小时内有能够处理故障的技术人员携带常用有效备件到达现场，并立即投入对故障的处理。 （3）故障分析服务。中标供应商在完成排障，设备、系统恢复正常运行后，应于 3 日内向采购人提交书面报告。报告内容包括故障现象、原因，处理方法、配置变更内容、处理结果、可能存在的隐患及今后避免问题的措施等。 （4）对硬盘故障导致的不可用、生产系统宕机等重大故障提供 7×24 小时的现场支援。 （5）备件服务：供应商具有本地区主要硬盘备件库，保障在 4 小时内提供所需更换的备件，并保障备件为原产商生产的备件。 **2.3 备件更换维修服务** （1）在维护服务期限内，中标供应商为所有服务范围内设备的全部故障件的更换及维修所产生的费用均包含在投标报价中，即备件费用以及相应产生的备件送达运费、维护人员费用已经包含在总体的服务费用之中，不再以任何方式另行收取。所有更换的备件要求与原设备或模块的型号相同，各项性能规格不低于原有设备或模块。 ▲（2）当中标供应商派出的现场支持工程师到达现场并经过分析判断，认为其所随行携带的替换备件不能完全解决设备故障，需要再更换备件的，中标供应商必须再次通过其它方式发送备件到用户指定地点，再由中标供应商现场支持工程师实施维护操作，直至故障完全修复。 ▲（3）服务过程中，所有损坏的硬盘或被更换的硬盘均不得带走，必须交还采购人，并进行移交信息登记。

				2.4 技术服务要求 （1）存储容灾规划服务。结合采购人存储和业务系统的实际情况，对采购人的存储容灾规划提出合理建议与方案。 （2）培训和咨询服务。中标供应商在年度服务期内，至少组织一次不少于一天的设备及系统使用维护技能培训，并提供相关培训教材。同时有义务在维护期内为采购人提供有关技术咨询服务。 （3）扩容和升级服务支持。中标供应商需要派出专业系统和软件工程师，配合采购人完成对保修范围内设备扩容、升级以及保修和维护范围的业务应用软件的维护、升级等技术支持工作。 （4）故障排除技术支持。对在保内设备上运行的业务系统软件、中间件等系统软件出现的问题，中标供应商应积极配合分析和查找故障产生原因，并提出排除故障的建议和措施，不得推辞。 （5）提供存储技术支持服务，配置更改支持服务。提供现有存储网关双活存储部分双活数据分布式卷数据无损拆分（要求不损坏原有数据，不中断业务系统）、容灾演练服务；提供现有存储设备监控软件部署实施，存储设备监控添加、配置。 （6）中标供应商在未得到采购人许可的情况下，不得从事以下行为：在非故障处理和恢复的情况，改动设备连接和配置；随意通过系统账户进入系统；改动系统软件配置和口令；修改和删除系统内的文件；拆卸非保修范围内的设备；实施设备微码或系统、软件升级；任何业务系统数据访问操作。 ▲（7）保密要求。中标供应商必须与采购人签署保密协议，承担保密义务。中标供应商应采取有效预防措施，防止公司员工在合同执行期间将掌握的任何有关采购人的机密或专有信息透露给任何未经授权人。 ▲2.5 维保期内发生硬盘故障时，如采购人与中标供应商确认需要更换硬盘，所需硬盘不在现场备件库清单中的，中标供应商须在确认更换硬盘之日起 10 个工作日内完成硬盘更换服务。在约定时限内上述服务无法完成的，采购人有权追诉因此造成的损失。 2.6 采购人可根据存储剩余容量及未来规划，决

				定是否对双活存储进行拆分以增大存储容量。采购人可根据业务使用情况和存储负载情况，决定是否开展容灾演练。 ▲2.7 在本项目的维保过程中，如产品维护需原厂商服务支持，由此产生的费用，均由中标供应商承担。 ▲2.8 前置检验和服务地点 前置检验：为保障采购人后续工作主动，中标供应商必须在合同签订生效之日起 15 个工作日内，提供第一次存储维保服务巡检，提供 2 台结构化存储系统动态密码及维护工具访问并巡检存储，提供存储网关管理的结构化存储双活存储数据无损拆分，以实际成果检验中标供应商的履约技术能力。如中标供应商无法按时完成前置检验，采购人有权单方面终止合同。

B 分标　　采购预算：744.099 万元

序号	标的名称	数量及单位	所属行业	技术要求及需求
1	广西教育骨干网第二期链路租用服务（2）	1 项	租赁和商务服务业	**（一）传输线路租用服务** ▲1.≥100G 点对点专线，3 条；≥10G 点对点专线，10 条。 ▲2.透明传输线路，上下行带宽对等，传输线路与互联网（公网）隔离。 ▲3.具备自愈环保护，具备双路由保护。 4.相关网络设备满足可平滑升级的要求。 5.传输设备要求具有全网网管监控功能，并实行 7×24 小时实时监控；用户端可实时监测线路状况，线路监控设备由中标供应商提供。所有接入设备由中标供应商提供或利旧使用采购人原有设备，所有线路经由服务商汇聚后提供给用户使用。 6.专线租用服务期间，提供专线集中管控服务。包括但不限于：专线网络拓扑、实时状态、性能指标

				（包括但不限于：时延、丢包率、带宽占用率等）、告警信息等端到端可视化运维管理能力，以及定期总结报告运维管理情况等服务。 7.保证网络的畅通，负责采购人本次采购传输线路租用服务涉及所有设备（即“（一）传输线路租用服务”中的设备）的运行维护且不得额外收取费用，包括但不限于：光端机、转换器等设备；培训传输知识，指导采购单位及相关服务支持单位的人员做好日常维护。 8.用户网络需要扩展或升级时，负责提供相应解决方案等技术支持，不得额外收取费用。 ▲9.网络参数要求： （1）全年网络阻断时长总计不超过 24 小时； （2）端到端电路的传输比特差错率(误码率)：≤1.0×10E-7； （3）端到端电路丢包率≤1%； （4）端到端电路平均网络延时≤50ms、时延抖动≤10ms。 10.未约定的其它服务质量指标，则由中标供应商按《电信服务规范》（信息产业部令第 36 号）的要求，为采购人提供相应的服务。 **（二）运维管理服务** 部署一套运维监控管理信息系统，统一纳管本项目涉及的软硬件设备系统，包括但不限于：网络设备、服务器、存储设备、安全设备、操作系统、数据库、中间件、应用服务等，并提供相应运维管理技术支持服务。 **1.系统部署服务** （1）提供本地化部署和管理、分布式部署和管理、多层级管理、数据采集负载均衡、高可用、冗余备份等能力和服务。 ▲（2）提供监控≥3000 个管理对象的能力，并支持后期扩展。 （3）可利旧原广西教育网网络中心和广西教育数据中心的算力和存储，不足部分，由中标供应商负责提供。 （4）可部署于国产服务器 （5）可部署于 Windows、linux，以及国产操作

				系统。 （6）可部署于国产数据库和中间件。 （7）系统独立自主研发，不存在第三方版权争议。**（投标人在投标文件中提供软件著作权证明，或第三方测试机构出具的检测报告，或投标人的声明、不存在第三方版权争议、承担版权争议责任的承诺书等，并加盖投标人公章）** **2.运维管理服务** 包括但不限于： （1）网络运维，包括但不限于：网络线路、网络拓扑、IP 地址管理、设备配置、流量分析等。能够利用多种主流网络协议进行端到端质量探测，精准测量关键路径的网络性能指标，实现对骨干网健康状况与服务质量的持续监控、性能评估与故障快速定位。 （2）设备纳管，包括但不限于：自动扫描添加、运行状态、性能指标等，对纳管设备支持用户灵活定义的多级资源分组管理、标签管理。 （3）业务保障，能够辅助快速查找故障，包括但不限于：业务分层、业务拓扑、运行状态、性能指标等。 （4）可视化，按管理层级和业务逻辑展示运维管理数据，包括但不限于：运维管理数据展板（包括但不限于：网络拓扑、业务拓扑、关键指标实时仪表盘等）、报表和报告等。报表生成时间≤10 分钟，支持导出 PDF/Excel 格式。拓扑图、仪表盘加载时间≤10 秒。 （5）告警提醒，能够利用手机短信、电子邮件、即时通信应用（钉钉、或企业微信、或飞书等）等方式及时提供报警信息。 （6）管理服务，提供自动巡检、巡检管理、工单管理、知识库等能力和服务。 **3.提供定制开发数据对接服务** 按采购人对接自治区网信、公安、数据局等第三方关于网络安全和网络运维监督管理信息系统的需要，提供数据对接服务。 **（三）骨干网运维管理人工智能应用服务** 利用大数据和人工智能技术，采集和分析广西教育网骨干网（含网络中心）和广西教育数据中心运维

				管理数据，挖掘分析部署于广西教育数据中心的教育部省级部署管理信息系统和自治区自建管理信息系统的数据，以及数据间的关联关系，支撑采购人加快推进本项目服务期内重点工作，助力本项目提质增效。 **1.运维管理人工智能应用服务** 提供广西教育网骨干网运维管理的人工智能应用服务，实现运维数据实时采集和智能分析，提供运维管理和业务应用的信息咨询和信息服务。 **1.1 运维数据采集分析** 通过建立数智基座实现数据实时采集，结合运维人工智能（AI）模型实现智能分析，自动识别设备系统性能、流量、资源占用和应用响应等异常数据，以通知、报告和展板等多种方式提供报警信息。 （1）数据采集覆盖网络设备和安全设备(包括但不限于：端口流量、丢包率、时延等)、服务器（包括但不限于：CPU/内存/磁盘使用率、进程状态等）、应用系统（包括但不限于：响应时间、并发量等），支持≥10000 个监控对象。 （2）数据采集频率可自主选择配置，默认 1 分钟/次，关键指标（如核心链路流量、数据库 CPU）支持自定义 10 秒-30 秒/次，数据采集成功率≥99.9%。 （3）基于历史数据预测潜在故障，自动生成预警通知。 （4）识别准确率≥90%。 （5）能够利用手机短信、电子邮件、即时通信应用（钉钉、或企业微信、或飞书等）等方式及时提供报警信息。 **1.2 运维管理问答咨询** 构建基于知识库的问答系统，为运维人员、管理人员和业务应用用户提供精准高效的咨询服务。 （1）提供便捷的交互界面，支持文本输入提问。用户输入问题后，系统通过智能问答算法快速生成基于信息化设备运维、业务系统应用及相关资料的准确回答，并可展示回答依据的具体条款或资料来源，辅助用户理解和决策。 （2）为业务应用用户提供咨询服务的功能模块，应具备独立部署、提供互联网服务的能力。

				1.3 数据应用运维保障 提高广西教育网网络应用用户人机体验，助力提高广西教育网和广西教育数据中心的数据管理的能力和水平，自动识别全区教育系统组织机构、教师、学生及其监护人基础信息数据的错漏和异常，锁定异常数据流转过程，生成报告和展板，提供数据修复建议意见和服务，支撑广西教育网用户网络接入身份认证、部署于广西教育数据中心的教育部省级部署管理信息系统和自治区自建管理信息系统单点登录的应用和运维管理。 **2.本地化≥32B 大语言模型训练和推理能力服务** **▲2.1 大语言模型服务** （1）对大语言模型进行全生命周期管理服务，包括但不限于：模型部署、模型测试、模型更新、模型导出、模型版本管理、模型详情查看等功能。 （2）本地部署 DeepSeek、Qwen 等多种国产主流模型。 （3）提供多种模型自由切换服务。 （4）提供通过 API 进行访问和接口调用模型服务。 （5）提供可视化工作流编排，预设模板≥5 个，可自由设计和组合各种功能模块，可以通过拖拽式界面，设计复杂的问答流程，包括条件判断、循环、模型调用等节点。 （6）提供 MCP（模型上下文协议,Model Context Protocol）工具，同时支持自定义的 MCP 工具，可在构建复杂工作流时直接调用 MCP 工具作为处理节点，实现更强大的功能组合。 **2.2 应用模型服务** （1）提供运维管理涉及应用模型服务，包括并不限于文本文档识别模型、pdf 文档识别模型、图片识别模型等，大小 5MB 及以下的文档识别处理时间≤20 秒。 （2）提供图片智能识别、智能数据分析、语音转文字等应用模型服务。 **2.3 知识库服务** （1）导入运维相关 markdown、word、pdf、txt 等常用格式文件快速构建本单位知识库，并对文本数据

				进行预处理、向量化和问题答案（QA）分割。包括并不限于通过 RAG（检索增强生成，Retrieval-Augmented Generation）等技术，将运维相关文档（markdown、docx、pdf、txt 等常用格式文件）快速构建为本地知识库。 （2）基于多模态大模型、OCR 模型、文本生成大模型、知识图谱等技术构建知识图谱，融合各类文本、标准条款、设备参数、故障案例等数据，通过实体链接与关系抽取技术建立知识关联。 **2.4 大语言模型训练推理能力的配套硬件服务** 选装合适模型和匹配硬件设备系统，确保推理结果的精度与稳定性。 （1）显存能够支持不低于 32B 参数、精度为 FP16/BF16 的模型训练和推理。 （2）支持≥20 个用户并发访问。 （3）内置硬盘总容量≥32TB。 （4）内置缓存盘：≥2*3.2TB NVMe SSD。 （5）单台一体机 CPU：≥2 颗，每颗核数≥32 核；内存：≥1024GB；系统盘：≥2*480GB SATA SSD；RAID 卡：≥1 张，支持 RAID0、1、10、50、60 以及直通；网卡：GE 网卡(电口)≥2 口，≥10GE 网卡≥2 口（光口，满配多模光模块）。 ▲（6）如果需要由多台一体机组网的，须提供系统组网配套网络设备和配件。 **2.5 大语言模型通用要求** 支持自然语言对话，至少支持记忆≥6 轮互动，支持输入最大长度≥2000 token。 **3. 安全要求** 部署环境应保证智能运维相关的人工智能应用和部署的大模型安全可信，实现数据安全管理。 （1）数据本地化存储。所有数据应存储在本地算力平台（系统）或用户指定的本地存储设备，不向第三方服务器传输数据。 （2）身份认证与权限控制。基于采购人组织架构，以及运维管理人员角色配置应用条件环境，可审计所有操作日志，日志留存≥6 个月。 （3）数据传输基于国产商用密码技术，确保数据采集过程中传输安全，访问用户安全可控。

				（四）骨干网运维管理设备系统维保服务 1.服务范围包括：安全态势感知平台及其探针、防火墙、网页应用防火墙、VPN、超融合服务系统、统一身份认证系统、漏洞扫描系统、日志系统、数据库审计系统等 91（套），维保服务不少于 3 年。 1.1 安全态势感知平台维保，提供网络中心态势感知平台维保，数量 1 台，品牌：深信服；提供安全感知系统平台特征库软件，软件升级。 1.2 态势感知平台探针维保，提供网络中心 3 台千兆态势感知平台探针维保，数量 3 台，品牌：深信服；提供安全感知系统探针特征库软件，软件升级。 1.3 网络中心管理区防火墙维保，提供骨干网防火墙维保，数量 3 台，品牌：深信服；提供云智订阅软件，云威胁情报网关订阅软件，远程技术支持，软件升级。 1.4 外联区域防火墙维保，提供网络中心外联区域（互联网区、电子政务外网区、教育网区、测试区）防火墙维保，数量 6 台，品牌：深信服；提供云智订阅软件，网关杀毒升级许可，软件升级。 1.5 网页应用防火墙维保，提供网络中心网页应用防火墙维保，数量 2 台，品牌：绿盟；提供产品系统升级授权服务和远程支持服务。 1.6 VPN 维保，提供骨干网 VPN 维保，数量 2 台，品牌：深信服；提供远程技术支持，软件升级。 1.7 服务器维保，提供服务器维保，数量 45 台，品牌：深信服。 1.8 超融合管理软件维保，提供超融合管理软件维保，数量 45 套，品牌：深信服；提供软件升级服务。 1.9 计算虚拟化软件维保，提供计算虚拟化软件维保，数量 45 套，品牌：深信服；提供软件升级服务。 1.10 存储虚拟化软件维保，提供虚拟存储软件维保，数量 45 套，品牌：深信服；提供软件升级服务。 1.11 网络交换机维保，提供网络交换机维保，数量 30 台，品牌：信锐；提供软件升级服务。 1.12 一体化管理软件维保，提供一体化管理软件维保，数量 1 套，品牌：深信服；提供软件升级服务。 1.13 统一身份认证维保，提供统一身份认证维保，数量 26 台，品牌：深信服；提供软件升级服务。

				1.14 漏洞扫描系统维保，提供网络中心漏洞扫描系统维保，数量 1 台，品牌：绿盟；提供产品系统升级授权服务和远程支持服务。 1.15 日志系统维保，提供网络中心日志系统维保，数量 1 台，品牌：安恒；提供包含软件升级、规则库更新。 1.16 数据库审计系统维保，提供网络中心数据库审计系统维保，数量 1 台，品牌：深信服；提供软件升级。 **▲2.其他服务要求：** 2.1 当设备系统出现故障时，工程师需要在 1 小时内响应，3 小时提供上门检修服务。维保服务包括产品保修服务期内产品的维修和超时提供替换设备系统的服务。在收到用户提供的故障产品后 10 个工作日（不含运输时间）内修复并快运给用户；如 10 个工作日内无法修复该故障产品，中标供应商从明确无法修复之日起，5 个工作日内为用户免费提供与返修产品功能一致且性能不低于返修产品的设备系统暂时替换，直至故障产品修复。 2.2 服务过程中，所有损坏的硬盘或被更换的硬盘均不得带走，必须交还采购人，并进行移交信息登记。

三、商务要求及其它要求

▲（一）商务要求	
服务期及地点	1.服务期：自签订合同生效之日起，至项目初步验收合格之日后的 3 年内。 2.地点：广西区内采购人指定地点。
报价要求	投标人的投标报价应为人民币含税价，投标报价为总价包干，包括但不限于：服务的价格、链路租用、软硬件系统设备运输及装卸、上架安装及调试、相关技术服务、运维服务（含设备运维）、备件更换、保险、验收、招标代理服务费用和各项税金等费用，合同履行周期内采购人不支付任何合同以外的费用。
履约保证金	1.履约保证金金额：按分标中标总金额的 2%收取，于中标通知书发出之日起 30 日内提交至采购人指定账户。履约保证金被扣后，中标供应商应于 10 个工作日内补齐被扣金额。 2.履约保证金提交方式：银行转账、支票、汇票、本票或者银行、保险机构出具的保函等非现金方式。

	3.履约保证金退付方式、时间及条件：合同期满后，由中标供应商向采购人提出申请，采购人在收到申请材料后对相关违约情况进行核对，如有违约或赔偿的，涉及违约的违约金和损失赔偿从履约保证金中扣减后，剩余部分，采购人5个工作日内转账退还（无息）。如有不足部分，采购人有权从未支付的服务款中扣除。 4.履约保证金指定账户： 开户名称：广西壮族自治区教育技术和信息化中心 开户银行：工行南宁市南湖支行 银行账号：2102110009300335214
交付要求	1.服务交付时间要求。 **A分标：**中标供应商应在项目合同生效之日起120个日历日内完成交付。 **B分标：**中标供应商应在项目合同生效之日起90个日历日内完成交付（注：B分标交付时间为在利旧设备的基础上完成的时间；若A分标中标供应商采用不基于现网设备扩展端口方式提供接入能力服务而采用提供新设备的方案的，B分标中标供应商后续完成与其提供的相关设备对接的交付时间不计入承诺的交付期内）。 2.交付网络运维管理服务和骨干网运维管理人工智能应用服务时，中标供应商还应同时提供网络运维监控管理信息系统和人工智能应用涉及的软件系统的技术资料，包括并不限于：系统部署、系统运维管理和系统操作的说明书、手册、数据词典等。 3.中标供应商应在服务期满后，将所投入本项目软硬件系统设备（租用光纤线路部分除外）完好地交接给采购人，协助采购人完成设备维护的接收和交接工作，由采购人继续使用和维护。中标供应商必须确保所移交设施技术性能完好，可正常运行并达到所承诺技术要求，必须尽可能减少移交对公共产品或服务供给的影响，确保项目持续运营。 4.服务期满后，如采购人继续开展续租服务，但因政策调整等原因无法顺利开展采购工作，导致续租服务时间无法与本项目服务期正常衔接的，则合同履行期自动延长，如延长期超过30日的，采购人与中标供应商双方签订补充协议或协商以其他方式解决，中标供应商不得私自切断采购人租用的线路网络。 5.所有项目参与人员应提供具体人员名单及联系方式给采购人备案。
项目验收标准及要求	1.在项目验收过程中，采购人将同时按照政府采购合同约定、招标文件及中标供应商其投标文件承诺的条款进行逐项验收，如项目验收不合格，由中标供应商返工直至合格，有关返工、再行验收，以及给采购单位造成的损失等费用由中标供应商承担。连续两次项目验收不合格的，或发现成交供应商在投标文件中有弄虚作假的行为，或在投标文件中有

	针对技术商务条款有虚假响应情况的，采购人将不予验收，并追究中标供应商的责任，由此带来的一切损失由中标供应商自行承担。 在验收过程中发现中标人有违约问题，采购人有权不支付或暂缓资金结算且不承担逾期付款违约责任。待违约问题解决后，方可办理资金结算事宜。 2.主要参考验收依据： 招标文件、中标人的投标文件、合同书及《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》（桂财采〔2015〕22号）、《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）。 3.履约验收： （1）**验收过程中所产生的费用均由中标供应商承担。报价时应考虑相关费用**。 （2）本项目验收委托云之龙咨询集团有限公司（以下简称“代理机构”）组织实施，由验收小组对照项目招标文件、采购合同（含补充协议）的要求全面核对检验，对要求出具的证明文件的原件进行核查，如不符合要求以及提供虚假承诺的，按相关规定做退货（如有）处理及违约处理，中标供应商承担所有责任和费用，采购人保留进一步追究责任的权利。 （3）**各分标首次验收服务费，参照广西壮族自治区财政厅关于印发《广西壮族自治区本级政务信息化建设和运维项目预算支出标准》的通知（桂财建〔2023〕102号）表19第三方测试(测评/检测)费预算支出标准，按各分标采购预算金额采用直线内插法确定基本计费，乘以项目类型调整系数0.8确定首次验收费用，即：A分标按人民币104800.20元收取，B分标按人民币100819.80元收取。首次验收服务费由中标供应商在本项目中标通知书发出之日起30日内一次性向代理机构付清**。 1）验收活动开始前，中标供应商应对所有服务工作及服务内容作出全面检查和对验收文件进行整理，并列出清单，作为采购人收货验收和使用的技术条件依据。 2）中标供应商一次性通过验收的，由验收小组出具结论报告，自验收合格之日起五个工作日内由中标供应商向代理机构一次性付清验收代理服务费。 3）采购委托采购代理机构组织的验收项目，其验收时间以该项目验收方案确定的验收时间为准，验收结果以该项目验收报告结论为准。在验收过程中发现中标供应商有违约问题，可暂缓资金结算，待违约问题解决后，方可办理资金结算事宜。 4）**中标供应商验收不合格的，再次验收的验收代理服务费每次均以首次验收费用金额为基数，按 50%加收费用，由中标供应商承担并于验**

	收活动再次开始前七个工作日一次性向代理机构付清。 （4）本项目服务中，涉及投入到本项目的软硬件系统设备运送抵达指定现场后，中标供应商必须提供加盖单位公章的软硬件清单（包括货物名称、品牌、产地、规格型号、数量及产品附件等内容），采购单位或采购单位委托的第三方机构等多方组成验收小组，将同时对中标供应商承诺配备的所有软硬件进行检验和核实。 **（5）项目验收过程中，需质量监督检测机构介入的（如有），费用由中标供应商另行承担**。 （6）多次（3 次）验收后，最终验收达不到要求的不予验收，视为验收不合格，采购单位可解除双方的合同。 （7）履约验收过程中需要多方配合，投标人可根据自身的情况，对履约验收的相关内容提出相关建议及意见，以及合理化实施意见。
付款方式	1.首付款。合同签订后，采购人收到中标供应商等额发票之日起 10 个工作日内，按不超过合同总金额的 30%支付首付款。 2.进度款。自项目初步验收合格之日起，于第 1 个年度和第 2 个年度期满后，中标供应商提出申请，由采购人组织年度阶段服务验收。经年度阶段服务验收合格的，自收到中标供应商提供等额发票之日起 10 个工作日内，采购人按年度财政预算下达经费支付进度款（合同总金额的 20%）。 3.尾款。自项目初步验收合格之日起，于第 3 个年度期满后，中标供应商提出申请，组织项目最终验收。经项目最终验收合格的，自收到中标供应商提供等额发票之日起 10 个工作日内，采购人支付项目尾款（合同总金额的 30%）。 4.账户的真实性及合法性由中标供应商负责，如因中标供应商提供的账户信息错误导致无法付款、迟延付款等情形的不视为采购人违约。 5.采购人可根据每年财政拨款情况提前支付或延后支付，但最终在结算尾款时根据提前支付或延后支付的实际情况结清尾款（不超过合同金额的 100%）。若因采购人财政拨款问题导致采购人付款迟延的，采购人不承担责任。
（二）与实现项目目标相关的其他要求	
1.投标人的履约能力要求	
1.1 政策性加分条件	见本采购文件第四章“评标方法及评标标准”。
1.2 质量管理体系要求	如有，请于投标文件中自行提供。
1.3 业绩要求	如有，请于投标文件中自行提供。
2.验收标准	

2.1 本章《采购需求》有其他要求的按其要求。

2.2 合同履行过程中，由采购人根据中标人所提供服务，对照招标文件要求及中标人投标文件承诺进行检验并记录，发现中标人在投标文件中有弄虚作假的行为，或在投标文件中有针对技术商务条款有虚假响应情况的，采购人将终止合同或不予验收，并追究中标人的责任，由此带来的一切损失由中标人自行承担。

2.3 其他未尽事宜应严格按照《关于印发广西壮族自治区政府采购项目履约验收管理办法的通知》[桂财采〔2015〕22 号]以及《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》[财库〔2016〕205 号]规定执行。

3.进口产品及核心产品说明

本项目为服务类项目，无进口产品和核心产品。

4.其他要求

4.1 投标人可根据自身优势在响应本采购文件要求的基础上，结合本招标文件第四章“评标方法及评标标准”提供相关服务方案（格式自拟），包括但不限于传输线路租用服务方案、运维管理服务方案、骨干网运维管理人工智能应用服务、接入能力服务和设备系统维保服务。

4.2 为本项目投入技术服务团队，投入人员需为投标人在职人员，并具有相应的技术资格或职称，投标文件中需提供投入人员名单，并提供人员证书及投标人为其缴纳的社保证明、或劳动合同、或投标人为其发放工资的银行流水证明、或投标人代缴其个人所得税证明复印件。

4.3 如有，请于投标文件中提供包含但不限于信誉、业绩等。

5.其他说明

▲5.1 **本项目设置最高限价：A 分标：254.667 万元/年，3 年共计 764.001 万元；B 分标： 248.033 万元/年，3 年共计 744.099 万元，评审时以最高限价为依据，投标人投标报价超所投分标最高限价的作无效投标处理**。

▲5.2 投标人就本项目服务需求中全部内容作完整唯一报价，拆分服务内容投标或仅对部分内容投标报价的将导致投标无效。

▲5.3 **参加 A、B 分标投标活动的各投标人在投标时，必须在《开标一览表》中明确投入所投分标服务所使用的线路运营商信息（如：广西广电、中国电信、中国联通、中国移动）。**

5.4 A、B 分标链路租用服务不能使用同一线路运营商提供的线路，若某投标人所使用的线路被推荐为 A 分标第一中标候选人，其他与其使用同一线路运营商的投标人不再推荐为 B 分标中标候选人。

附件 1：

原广西教育网骨干网建设概况

一、原建设概况

广西教育网是万兆主干、千兆到学校、百兆到班级的，分层的教育信息网络系统，由骨干网、城域网和各级各类学校校园网组成。广西教育网的各级教育机构和各级各类学校都使用统一的数据标准进行信息传递，而且对外公开提供标准化的数据和功能接口，可以和遵守标准接口的第三方应用程序挂接。广西教育网将建成覆盖全区各级各类学校，支持各级各类教育教学信息化的，集数据、语音、视频服务于一体的，高带宽低延时的，支持 IPv6 部署和应用的，具有自主管理的，拥有统一管理公共 IP 地址的，拥有统一管理的全球域名的，满足“云、网、端”架构下开展各级各类教育教学的教育行业专用网络。

1.项目建设规模

1.1 业务领域

搭建在满足“云、网、端”架构下开展各级各类教育教学的网络环境，实现各级各类教育应用互联互通，教育资源、教育数据全网共享。

1.2 覆盖范围

纵向：包括广西教育数据中心、14 个设区市、118 个县（市、区）的各级各类学校和教育机构。

横向：涵盖学前教育、中小学教育、中等职业教育、高等教育、教育督导、教育科研、教育技术和信息化等业务部门。

1.3 用户规模

项目服务范围覆盖广西全区 1.96 万所大中小院校、18.9 万个班级、836 万名在读学生和 46 万名任课教师，广西教育网与互联网、电子政务外网、中国教育网等外部系统实现互通。

二、原项目建设要求

2.1 广西教育网由骨干网、城域网和校园网三部分构成，将各级各类教育机构和学校连接起来，为将来统一教育管理平台、管理教育大数据、推广智慧教学应用等工作，构建网络基础条件。

2.2 通过建设骨干网核心节点，组建骨干网核心环路，在各设区市建立市级汇聚节点（高校城市节点），连接至各核心节点，建成骨干网。在各设区市、县建立汇聚节点，各级学校建设校园网，连接至各设区市、县汇聚节点，形成设区市本级、县级城域网。各设区市、县级城域网连接骨干网市级汇聚节点，形成完整统一的教育基础网络。

2.2.1.网络中心

（1）在骨干网的核心及汇聚节点设立网络中心，可以与目前各节点核心机房共用，各设区市本级、县级城域网、跨县域的城域网根据情况设立不同规模的网络中心。

（2）网络中心主要用于为教育网提供运行环境和运维保障，建设内容主要包括机房运行环境、网络设备及运维系统、网络安全设备和系统等。机房运行环境主要包括机房装修，以及电力、空调、消防、门禁、监控等子系统。网络设备及运维系统主要包括路由器、交换机、身份认证、缓存加速、机柜及配套设施、网络管理运维等子系统。网络安全设备和系统主要包括入侵防御检测、防 DDOS 攻击、防病毒、上网行为管理、实名审计、实名日志等子系统。

2.2.2.骨干网

（1）骨干网是指在广西行政区域范围内，利用计算机网络技术，以光纤为传输介质的，连接全区各教育城域网、高等院校校园网、区直中等职业学校校园网的，由核心节点、高校城市节点、主干光纤传输线路组成的网络。

（2）骨干网及各端纵向接入城域网，实现与线路两端的互通。鉴于骨干网的重要性，骨干网核心线路需具备自愈环保护功能，针对线路经过的骨干核心层，采取不同路径的物理链路在骨干网节点连接形成双路由保护，如其中一条线路阻断时，另一条线路仍能正常使用，以保证业务能够正常运行，不受单条线路故障影响。

2.2.3.安全系统

（1）骨干网符合网络安全等级保护第三级要求。

（2）依据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）等标准规范要求，骨干网的网络安全保护等级定级第三级，按网络安全等级保护第三级的要求进行设计、建设、管理和运维。

（3）整个技术防护体系采取的主要安全措施如下：

1）采用防火墙系统对区域边界进行访问控制，根据业务需求，设置访问控制策略，定期进行安全策略的优化和维护。

2）采用入侵防御系统，并开启防火墙的防病毒模块（或部署防病毒网关），对网络入侵行为和网络层病毒进行检测和阻断，并进行告警。

3）采用专业抗 APT 攻击系统实现对新型网络攻击行为的检测、发现，并结合专家服务进行分析处置。

4）采用一体化终端安全管理系统、虚拟机化安全管理平台实现对物理主机、虚拟主机的安全防护，并对终端进行集中安全管控、集中病毒管理、统一补丁管理和安全审计。

5）采用 SSL VPN 实现对远程通信传输、远程终端数据的安全防护，实现基于互联网的传输加密和数据安全，并进行远程接入用户身份认证和访问控制。

6）采用堡垒机实现对设备的集中管理和运维审计，并实现运维管理日志的集中存储和安全运维。

7）应用系统开发同步考虑相关安全功能的实现，对重要的业务数据和系统鉴权数据进行加密存储。

8）采用应用身份认证服务平台实现对应用的双因素认证，并通过集成 SSL VPN 实现应用数据的传输安全。

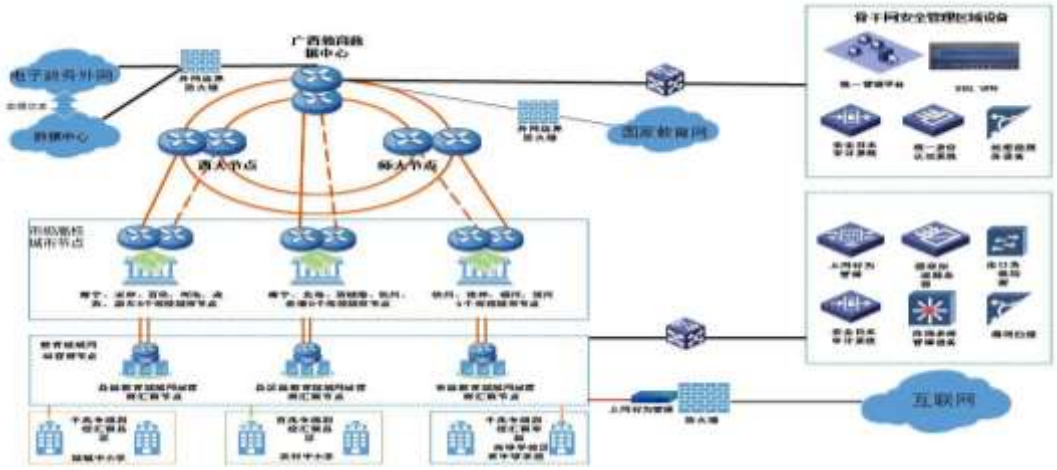
9）采用网络审计系统、数据库审计系统、上网行为审计系统、一体化终端安全管理系统的审计功能实现对用户行为审计的全覆盖，并满足远程访问和上网行为审计需求。

10）采用态势感知管理信息系统和抗 APT 攻击系统实现全网安全设备日志和安全事件的统一分析和告警，实现对高级威胁和未知威胁的发现、检测和告警，并提供安全事件报表。

11）采用防火墙集中管理，与态势感知管理信息系统联动，实现全网防火墙的自动化策略优化、下发、维护，实现策略可视化。

12）采用数字证书认证系统（教育 CA、广西政务 CA 等）进行教育网用户的身份认证，实现多因素身份认证。

三、总体网络架构



通过建设骨干网核心节点，组建骨干网核心环路，在各设区市建立市级汇聚节点（高校城市节点），连接至各核心节点，建成骨干网。在各设区市、县（市、区）建立汇聚节点，各级学校（教学点）建设校园网，连接至各设区市、县（市、区）汇聚节点，形成城域网。各城域网连接骨干网市级汇聚节点，形成完整统一的教育基础网络。

四、原架构设计

1.以 MPLS 技术为基础搭建骨干网，同时全面支持 SRv6。用 SRv6 技术实现 VPN 业务的互联互通，用 SRv6 Policy 技术实现业务的精细化管理和流量调度，用 SRv6 policy 流量统计实现隧道流量可视化。

1.1 核心环路

骨干网在广西教育数据中心（南宁）、教科网广西节点广西大学（南宁）和广西师范大学（桂林）分别设置三个核心节点。

1.2 市级节点部分

在 14 个设区市设置共计 13 个汇聚节点（其中，南宁市设置 2 个汇聚点，钦州市、北海市、防城港市共用 1 个汇聚节点）。

2.传输设计

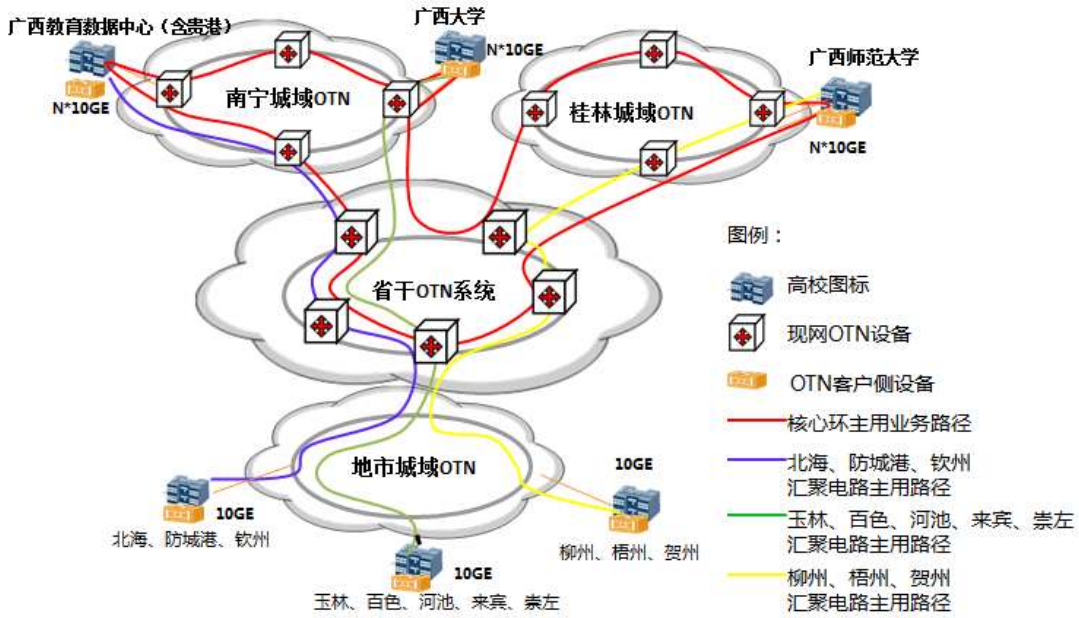
2.1 核心层

通过南宁、桂林本地 OTN 系统及省干 OTN 系统承载和调度，配置 10G/100G 波道，开通 1 个 10G 子波道，后续带宽可以平滑扩容。

2.2 汇聚层

南宁、桂林以外的节点，通过裸纤或城域 OTN 系统（优先）承载至省干 OTN 系统，再通过省干 OTN 系统调度至归属城市的城域 OTN 系统，最后通过南宁或桂林城域 OTN 系统接入骨干网核心节点。北海、钦州、防城港、贵港城市节点汇聚至广西教育数据中心，玉

林、百色、河池、来宾、崇左城市节点汇聚至广西大学，柳州、梧州、贺州业务汇聚至广西师范大学。南宁、桂林两个地市以及托管于广西教育数据中心的贵港等汇聚节点与骨干网核心节点共用机房，可通过光纤直连。骨干网线路图如下：



2.3 带宽要求

骨干网核心节点间互联设计带宽不小于 80G，首次开通带宽不小于 20G；核心节点与高校城市节点间互联设计带宽不小于 20G，首次开通带宽不小于 2G。当带宽占用率达到 70%时进行扩容，骨干网与电子政务外网互联带宽按自治区本级电子政务外网接入点的技术要求执行。

2.4 VPN 规划

2.4.1 VRF 命名

为保证 VPN 数据的独立性和安全性，PE 上每个 VPN 实例都有相对独立的路由表。为了区分不同的 VPN 实例，使用不同的 VRF 名称来进行区分。

2.4.2 RD（Route Distinguisher，路由标示符）规划原则

骨干网 RD 采用以下格式：16 位自治系统号：32 位用户自定义数字。

2.4.3 RT（router target，路由目标）规划原则

采用 RT 值的格式为：16 位自治系统号：32 位用户自定义数字。在 RT 规划时，既要能够保证各教育系统 VPN 能够各自形成，还要能够通过 RT 控制，使各教育系统 VPN 能够相互引入各自的路由，从而实现 VPN 之间的横向互访。

2.4.4 VPN 规划的原则

为适应现全区教育系统的信息资源共享的需求，教育网将在加强网络边界防护的基础上，规划设置公共域，在公共域内不设置任何访问限制，可实现各个教学单位间服务器与终端的互访。对有特殊隔离需求的网站应用，视频教学、远程教学等业务系统可单独设置 VPN 形成相互独立的虚拟专网。这些虚拟专网可根据业务需要，与公共域实现完全隔离或在采取安全

措施满足相应安全防护要求的前提下进行双向互访。

2.5 MPLS 路由设计

2.5.1 路由规划原则

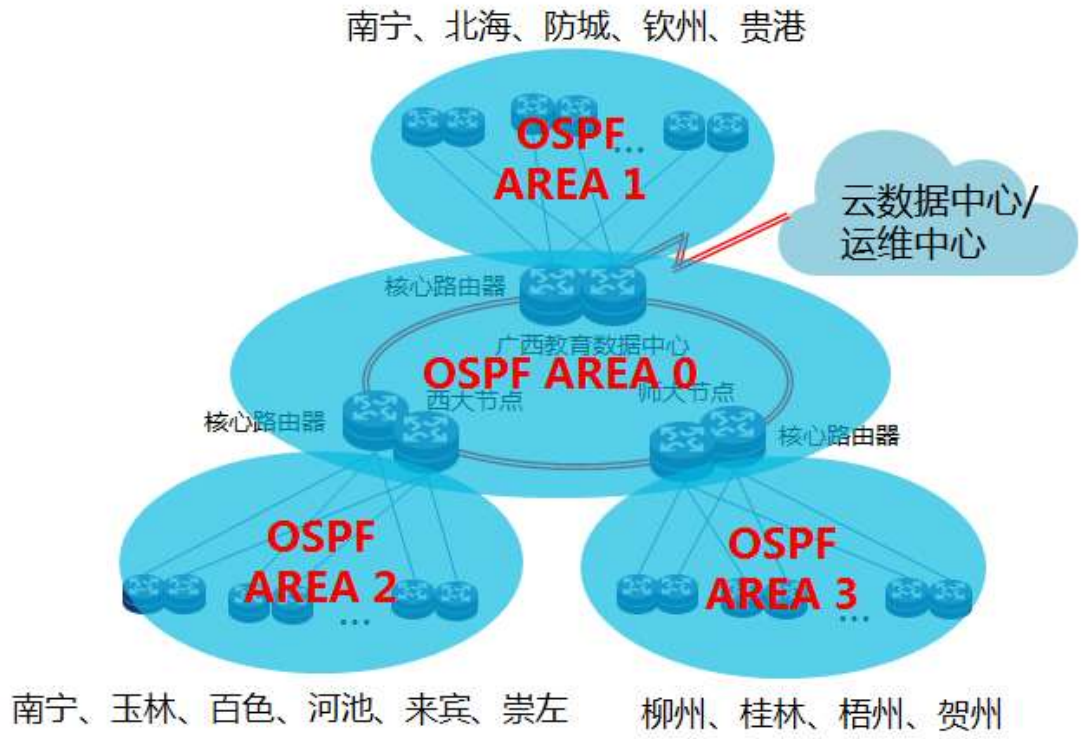
稳定性：必须考虑避免小范围（区域）的用户路由振荡引起对整个承载网大范围的路由振荡；

可控性：必须考虑能对承载网的 IGP 路由、业务路由能够进行区分、控制；

可靠性：必须考虑网络故障时路由的快速收敛、恢复，可以通过运行动态路由协议、多链路的冗余保护等手段减少对用户业务的影响。

2.5.2 路由总体设计

承载网路由总体模型如下：



整网路由协议规划

公网路由：公网路由用于所有承载网设备之间的互连地址和设备的 Loopback 地址的传递，并指导公网侧隧道的建立承载业务流量在承载网范围内的转发。

私网路由：各个不同业务各自的路由在各个 PE 之间互相传递，并指导流量传递方向。

承载路由协议（IGP）选择 OSPF 协议，该协议主要用于宣告各设备的 loopback 地址、设备间的互联地址。私网网络路由通过 MPBGP 协议承载，以保证承载网络路由与用户网络路由的隔离，确保用户网络路由的波动不会影响承载网络路由的稳定性。

2.5.3 骨干网 OSPF 规划

OSPF 作为公网路由协议，负责所有 PE 和 P 设备的互联接口和 loopback 口路由发布。指导流量在骨干网转发，并为 BGP 邻居关系建立提供路由可达条件。

在项目承载网中，所有 PE 和 P 设备接口都在骨干域：即 Area 0，负责全网进行高速、

稳定的数据包转发。承载网各 P、PE 节点设备之间的互联链路以及这些设备的 Loopback 接口地址划分到 Area 0。

2.5.4 BGP 路由规划

BGP 路由设计包括自治域设计、路由反射器，IPV4 全局路由设计以及 VPN 路由设计。自治域设计：从网络业务拓展和维护管理等各方面综合考虑，为承载网分配独立的自治域 AS 号。

路由反射器 RR（route-reflect）：

为了教育网 IBGP 的方便部署和维护，减少 BGP 对等体的数量，需要采用路由反射器 RR（route-reflect）技术。路由反射器 RR 同时为全局路由 IPv4、MPLS VPN 路由 VPNv4 提供服务。P 设备作为路由反射器，网络中心出口设备以及各单位所在 PE 设备作为 client。

如下图方式建立 MP-IBGP 邻居关系，P 节点兼做反射器（所有 PE 都和 P 建立邻居关系，包括骨干层和接入层 PE）。

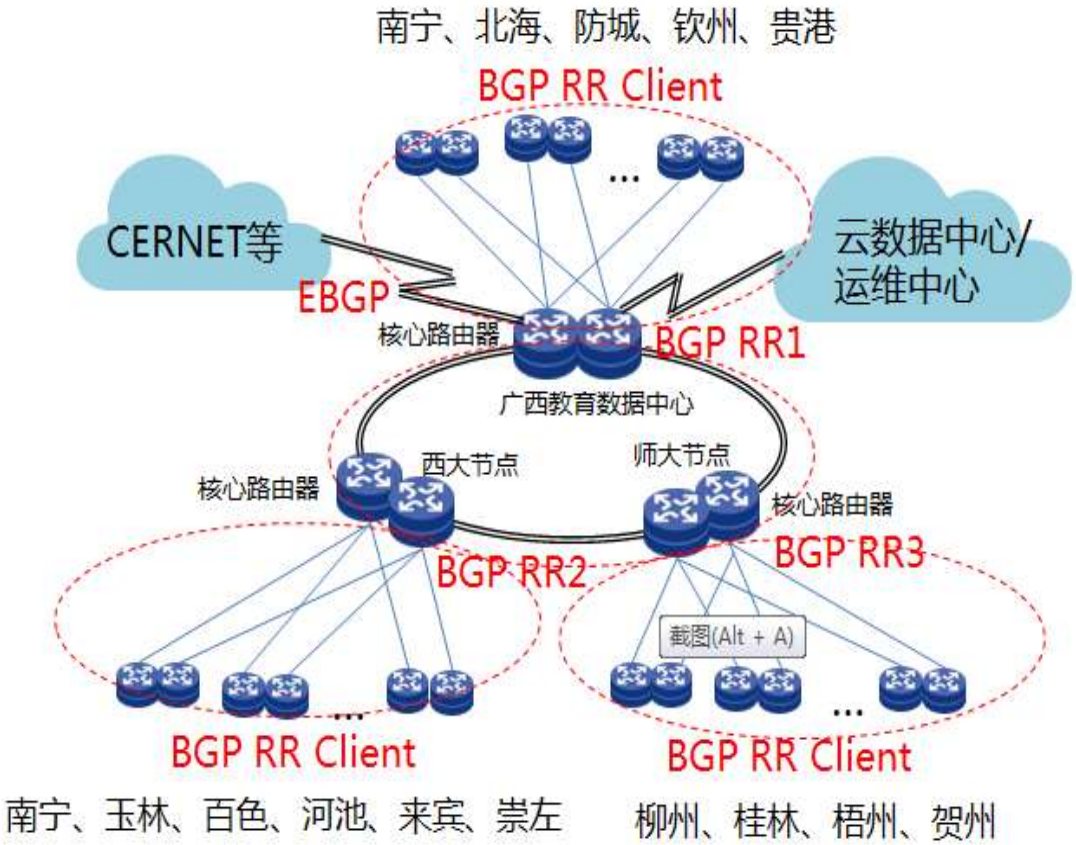
私网路由引入方式：

私网路由通过 PE 上配置私网侧的静态路由，并引入 MP-BGP 私网侧。

私网路由根据下联的加密方式有两种不同的方式：

方式一，加密方式为隧道方式，则只发布加密设备的隧道地址。需要在加密时将业务的 DSCP 值复制到外层隧道的 DSCP，用以识别不同业务。

方式二，加密方式为传输模式，只加密报文的负载，报文头不做加密。私网路由发布时，发布内网业务的明细地址。使用 VPN+地址区分不同业务。



BGP 邻居关系

2.5.5 路由策略设计

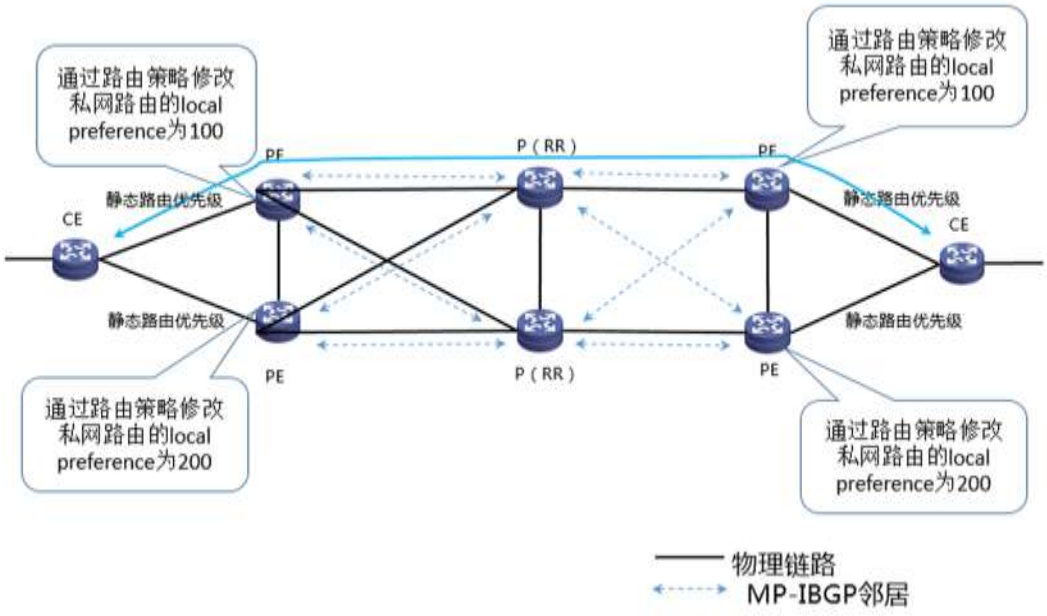
在骨干层 PE 为双节点时，直接接入骨干层 PE 的业务需要使用路由策略来区分主备 PE，以确保不同流量在 PE 上的负载分担。其他业务接入时都是单节点接入不存在此问题，无需配置策略。

MP-IBGP 路由策略

PE 侧引入私网路由通过策略修改 Local-preference 值，区分 PE 节点主备。不同私网业务使用不同策略确保业务在两台 PE 节点上负载分担。

全局路由以汇总方式进行通告，通过静态路由指向全局路由网段、以 Network 方式引入 IBGP，减少 IBGP 路由数量。根据用户接入需求，通过 BGP 丰富的路由属性、选路规则，进行路由过滤、路由策略制定。（途中以一端举例，两端策略对称。同一私网其他节点主备设备保持一致。）

接入侧通过静态路由优先级区分 PE 主备，需要与 BGP 策略一致。



策略说明

2.6 SRv6 路由设计

2.6.1 IGP 路由协议

骨干网内部采用 IGP 实现路由发布，常见的动态 IGP 协议有 OSPF 和 IS-IS（Intermediate System-to-Intermediate System，中间系统到中间系统），相比较 OSPF，ISIS 具有更好的开放性、扩展性和兼容性，同时 ISISv6 对 IPv6 的可扩展性更好，新技术标准进展更加成熟和全面，因此在骨干网部署 ISISv6 协议。

骨干网规划为 ISISv6 的 Level-2，有核心路由器和汇聚路由器都运行在 ISISv6 Level-2 进程内，对路由进行发布，从而学习到骨干网的拓扑信息和路由信息。

骨干网设备的 Loopback 接口/链路互联接口/SRv6 Locator 的 IPv6 地址都发布到 ISISv6 进程中，实现骨干网的路由互通。

2.6.2 MP-BGP 路由协议

骨干网采用 SRv6 技术进行 VPN 业务承载，作为一张 SRv6 VPN 专网，VPN 的路由需要通过 MP-IBGP 协议来进行通告学习。骨干网的 MP-IBGP 路由设计可以采用和 IBGP 路由相同的方式，在自治系统（AS）域内，需要在核心路由器 P 和汇聚路由器 PE 上部署 MP-IBGP 协议，同时为了保证 MP-IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。同时，在骨干网内部署 RR 反射器来解决这一问题。

2.6.3 RR 反射器设计：

RR 作为 MP-BGP 路由的反射器。核心 P 设备一般为高端设备，性能较强，所以直接由核心 P 设备兼任 RR。RR 设计包括如下几点：

2.6.3.1 在两个核心站点各选择一台 P 设备作为 RR 反射器，拟在广西教育数据中心和广西师范大学两个核心节点上进行部署；

2.6.3.2 所有的其他 PE/P 设备均与两台核心 P 设备建立 MP-BGP 邻居关系；

2.6.3.3 两台 RR 设备设置为同样的 Cluster ID 防止环路；

2.6.3.4 将所有其他的 PE/P 设备均指定为 RR client，并且仅与两台 RR 路由器建立 MP-BGP 连接；

2.6.3.5 使用 P/PE 设备的 Loopback 接口的 IPv6 地址建立 BGP 邻居。

2.6.4 SRv6 隧道设计

SRv6 隧道包含两种类型：SRv6 BE（SRv6 Best Effort）和 SRv6 TE（SRv6 Traffic Engineering），其中 SRv6 BE 是使用 IGP/BGP 选路算法计算得到的最优 IPv6 路径，该最优 IPv6 路径天然支持 ECMP。SRv6 TE 使用通过约束计算得到的满足一定 SLA 要求的路径，通常由控制器进行路径计算，然后下发到路由器。SRv6 BE 适合对于 SLA 要求不高或者对路径无要求的业务场景；SRv6 TE 适合对 SLA 要求较高的业务场景，以及不同业务之间有路径分离诉求的场景。

在骨干网中，不同业务的 SLA 承载诉求是同时存在的，并且有些业务在正常转发时对路径无要求，但是在网络拥塞或者有安全攻击时又需要指定路径，因此通常需要组合使用 SRv6 BE 和 SRv6 TE 路径，结合业务和场景来选择使用不同类型的路径。

2.7 QoS（Quality of Service，服务质量）设计

为保障教学工作顺利开展，骨干网需具备为关键教学业务提供专用带宽的能力，支持端到端针对关键教学业务提供网络切片，对关键教学业务进行带宽硬隔离，同时针对非关键教学业务还需具备 QoS 能力，为不同的业务提供端到端的差异化服务质量保证。

在路由器/交换机上对关键业务部署 IP QoS 策略，为不同业务定义差异化服务等级，并在 IP 报文头的 QoS 字段进行标记，保证网络拥塞时高优先级的重要业务得到优先处理，网络上所有路由器/交换机对具有相同 QoS 参数的业务采取相同的优先级调度策略。

骨干网针对不同的教学业务划分如下三个服务等级：

（1）关键业务：骨干网端到端进行网络切片，独享网络带宽，确保教学业务质量，如视频教学、视频教研等业务。

（2）次优业务：通过 QoS 策略优先保障，共享网络带宽，当网络发生拥塞时优先转发，如教学资源系统、教学管理系统等。

（3）普通业务：尽力转发，共享网络带宽，当网络发生拥塞时，调度优先级别低。如课件资料下载、互联网访问等。

2.8 传输线路配置

根据骨干网组网需求，核心环三个节点，每个节点之间 2 条专线，每条专线带宽不低于 10G，总计需 6 条专线。汇聚节点总计 13 个，其中南宁市 2 个节点、桂林市节点、贵港市节点与核心节点属于同一机房，采用直连光纤互联，其余 9 个城市节点每个节点至核心节点需要 2 条专线，每条专线带宽不少于 1G，共计需 18 条专线。

从保证传输网络安全性和可靠性方面进行考虑，核心节点之间以及核心节点与汇聚节点之间的链路承载在至少 2 家运营商的传输网络上，以保证传输网络有较高的冗余性，一旦出现其中 1 家运营商网络故障的时候，另 1 家运营商的传输网络仍然能保证骨干网的正常运行。

五、电子政务外网互联设计要求

为贯彻落实《国务院办公厅关于印发政务信息系统整合共享实施方案的通知》（国办发〔2017〕39 号）精神，按照自治区政府相关要求，广西教育厅 OA 办公、公文流转两个业务系统需要部署在政务云，同时实现自治区教育系统各高等院校、区直中等职业学校安全、便捷接入。教育网与电子政务外网之间，采用逻辑隔离和边界防护手段，实现双向数据交换。安全接入方案和设备应符合《国家电子政务外网信息安全标准体系框架》中的安全标准。

1.接入方案

1.1 高等院校、区直中等职业学校接入电子政务外网方案

高等院校、区直中等职业学校接入电子政务外网示意图

依照《广西电子政务外网市、县级节点技术规范》（2019 修订版）的要求，学校属于 B 类用户，各学校在访问 OA 以及公文流转业务时通过防火墙设置与其互联网出口流量的做强逻辑隔离。

在广西教育数据中心建立独立安全域，在该安全域部署两台 VPN 设备，VPN 设备支持 SM2

加密算法。各高等院校、区直中等职业学校通过 VPN 设备接入到广西教育数据中心。并通过防火墙、入侵防御、安全审计设备，对该区域进行重点安全防护。

广西教育数据中心通过专线连接到教育厅的电子政务外网出口，在经过访问控制、入侵防范和安全审计后访问部署在电子政务外网的 OA、公文流转系统。

2.安全防护方案要求

根据《接入政务外网的局域网安全技术规范》（GW0206-2014），电子政务外网边界为广西教育厅的本地局域网与本级政务外网城域网的接入边界，接入单位局域网应通过防火墙系统、入侵防御系统和安全审计系统等与政务外网进行逻辑隔离并对局域网进行安全防护。

具体要求包括：

2.1 访问控制

2.1.1 根据会话状态信息为数据流提供明确的允许/拒绝访问能力，控制粒度至少达到端口级。

2.1.2 应对用户设置有限的权限访问政务外网资源，并限制政务外网地址访问局域网。

2.1.3 对外提供服务节点时，应设置公用网络业务 DMZ 区，对该区单独实施安全策略，允许公用网络区访问内部业务区，禁止内部业务区服务器向外访问。

2.2 入侵防范

2.2.1 进行病毒过滤和入侵防御，并及时升级病毒和攻击特征库；

2.2.2 对病毒和入侵攻击行为进行实时告警及阻断。

2.3 安全审计

2.3.1 记录攻击源 IP、攻击类型、攻击目的 IP、攻击时间等关键信息。

2.3.2 记录公用网络访问行为、网络地址转换日志等信息。

2.3.3 审计信息保存 6 个月。

根据上述要求，构建“集权安全区”，将 VPN、RSA、统一身份认证、堡垒机等集权业务集中在该区域，并进行重点安全防护。

在集权安全区部署 2 台 SSL VPN：用于自治区范围内各高等院校、区直中等职业学校的接入。对于所有学校的接入，结合 SSL VPN 身份认证安全机制、终端安全控制机制、高强度加密机制、细粒度授权机制，保证应用仅可由指定用户、使用指定安全级别的终端、访问到指定应用的强控制。

在集权安全区部署 2 台下一代防火墙：下一代防火墙可针对用户的上网终端提供安全威胁过滤、木马恶意流量检测、DMZ 服务器保护、NAT、路由等安全防护功能。面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备。解决了传统安全设备在应用识别、访问控制、内容安全防护等方面的不足，同时开启所有功能后性能不会大幅下降。作为传统防火墙的升级替代产品，下一代防火墙不同于工作在 L2-L4 层的传统防火墙，可以对全网流量进行双向深入数据内容层面的全面透析。在安全策略制定方面，区别于传统防火墙五元组安全策略，下一代防火墙可对 L2-L7 层更多的元素（如，用户、应用类型、URL、数据内容等）制定双向的安全访问策略，使安全策略更精细、更有效，且满足业务的合规性；在安全防护能力方面，提升了传统的抗攻击的能力，不仅能防护网络层的攻击，针对来源更广泛、攻击更

容易、危害更大的应用层攻击也可以进行防护，实现 L2-L7 层的安全防护。

3.主要防护技术要求

3.1 以下一代防火墙为核心的边界防护设计

通过在物理边界部署下一代防火墙设备，提供主动的、实时的防护。方案在功能区边界构建以防火墙为核心的融合安全防御体系。

防护设计结构图

4.3.2 以 SSL VPN 为核心的安全接入

访问控制：采用 SSL VPN 对应用进行安全发布，避免需要将服务器直接挂在公网上造成的风险。

认证安全：在系统安全认证方面，采用登录 SSL VPN 身份验证、权限划分、登录应用身份验证的主线进行保障。SSL VPN 接入认证方式可采用用户名密码、USB KEY、短信认证、动态令牌、CA 认证、LDAP 认证、RADIUS 认证等两种或多种认证的组合。

服务器区隔离保护：将 SSL VPN 设备以单臂方式部署，通过配置使数据流经由 SSL VPN 后走向内网服务器区，对办公网与服务器区这两个不同安全级别的区域进行隔离。

六、IP 地址规划

1 IP 地址规划目标

1.1 建立高效的网络路由。

1.2 有效利用有限的 IP 地址资源。

1.3 支持网络技术的演变和发展。

2 IP 地址规划原则

2.1 简单性：地址的分配应该简单，避免在主干上采用复杂的掩码方式。

2.2 连续性：为同一个网络区域分配连续的网络地址，便于采用路由收敛及 CIDR(Classless Inter-Domain Routing，无类别域间路由)技术缩减路由表的表项，提高路由器的处理效率。

2.3 可扩充性：为一个网络区域分配的网络地址应该具有一定的容量，便于主机数量增加时仍然能够保持地址的连续性。

2.4 灵活性：地址分配不应该基于某个网络路由策略的优化方案，应该便于多数路由策

略在该地址分配方案上实现优化。

2.5 可管理性：地址的分配应该有层次，某个局部的变动不要影响上层、全局。

2.6 安全性：网络内应按工作内容划分成不同网段即城域网以便进行管理。

3.网络 IP 地址分类

3.1 设备管理/协议地址——Loopback 接口地址，SRv6 Locator 地址。

3.2 互联地址——即链路地址，通常配置在网络设备之间互联的接口上。

3.3 业务地址——即终端、服务器地址段。

4. IPv6 地址规划原则

在 IPv6 网络中，IPv6 地址规划遵循如下原则。

统一性原则：全网的所有 IP 地址统一规划，包括业务地址，平台地址，网络地址等。

唯一性原则：每个地址都能够做到全网唯一。

分离原则：业务地址和网络地址分开规划，方便在网络边缘进行路由控制和流量安全控制。

层次化和聚合原则：地址必须能够在不同的 IGP/BGP 之间被聚合发布，聚合会指数级减少网络中的路由数量，并且降低一个路由域中的路由震荡对其他路由区域的影响。

安全性原则：为达到 IPv6 地址可快速溯源，需要在 IPv6 地址中嵌入关键的溯源信息，包括地址属性，地址所属地域等信息。另外为方便地进行地址的过滤，需要梳理出于安全原因需要根据地址过滤流量的场景，将这些场景包括到 IPv6 地址规划中，例如前面分离原则中提到的业务地址和网络地址分离。

可演进性原则：地址规划时应在每个地址段内预留一定的地址空间用于业务未来发展，如果预留不足，则未来的地址扩充可能会导致地址无法满足前面的聚合性，安全性等原则。

可读性原则：由于 IPv6 地址通常以 16 进制（4bits）的形式书写，因此 IPv6 地址规划时以 4bits 为单位（也称为 ibble）进行划分，方便后续查看。

教育网使用私有地址，由自治区教育厅统一规划分配至各设区市级城域网、县级城域网、高等学校。城域网主管教育行政管理部门负责统一规划分配网内的学校和其它教育机构的 IP 地址。骨干网的路由 IP 使用中国教育和科研计算网（CRENET）IP 地址。

教育网全网支持 IPv6 部署和应用，支持 IPv6 和 IPv4 双栈协议。

5.网络安全保护等级标准

5.1 根据《关于广西教育行业网络安全等级保护工作实施意见》的要求，教育行业网络安全保护等级要求如下：

教育行政管理部门网络安全保护等级表

序号	分类	信息系统	安全保护等级		
			自治区级	地市	区县
A1	政务管理类	(01)办公与事务处理	第二级	第二级	第一级
A2		(02)公文与信息交换	第三级	第二级	第一级
A3		(03)人事管理	第二级	第二级	第一级
A4		(04)财务管理	第二级	第二级	第一级
A5		(05)资产管理	第二级	第二级	第一级
A6		(06)信访管理	第二级	第二级	第一级

序号	分类	信息系统	安全保护等级		
			自治区级	地市	区县
A7		(07)档案管理	第二级	第二级	第一级
A8		(08)党务管理	第二级	第二级	第一级
A9		(09)科研管理	第二级	第二级	第一级
A10		(10)教育统计管理	第二级	第二级	第一级
A11		(11)决策支持	第二级	第二级	第一级
A12		(12)应急指挥	第二级	第二级	第一级
A13		(13)舆情监测与管理	第二级	第二级	第一级
A14		(14)高等教育招生计划	第二级	第二级	第一级
A15		(15)普通高校招生网	第三级	第三级	第一级
A16		(16)教育考试考务管理与服务	第三级	第二级	第一级
A17		(17)评审、表彰管理	第二级	第二级	第一级
A18	学校管理类	(01)学校管理	第二级	第二级	第一级
A19		(02)学科、专业管理	第二级	第二级	第一级
A20		(03)教学改革管理	第二级	第二级	第一级
A21		(04)教学质量评估	第二级	第二级	第一级
A22		(05)校园安全与稳定管理	第二级	第二级	第一级
A23		(06)教育经费监管	第二级	第二级	第一级
A24	学生管理类	(01)学生学籍管理	第三级	第二级	第一级
A25		(02)招生录取管理	第三级	第三级	第一级
A26		(03)学生资助管理	第三级	第二级	第一级
A27		(04)学位授予管理	第三级	第二级	第一级
A28	教师管理类	(01)教师基本信息管理	第二级	第二级	第一级
A29		(02)教师资格认定管理	第二级	第二级	第一级
A30		(03)教师培训管理	第三级	第二级	第一级
A31		(04)教师教育管理	第二级	第二级	第一级
A32		(05)教师职称管理	第二级	第二级	第一级
A33	综合服务类	(01)门户网站	第三级	第二级	第一级
A34		(02)论坛、社区类网站	第二级	第二级	第一级
A35		(03)教育教学资源	第二级	第二级	第一级
A36		(04)毕业、就业信息管理	第二级	第二级	第一级
A37		(05)电子邮件	第二级	第二级	第一级
A38		(06)视频服务	第二级	第二级	第一级
A39		(07)安防监控	第二级	第二级	第一级
A40		(08)内网门户与身份	第二级	第二级	第一级
A41		(09)公共数据库	第二级	第二级	第一级
A42		(10)运维管理	第二级	第二级	第一级

网络安全区域设置安全策略参考表

目的源	边界接入区	核心网络区	前置服务区	安全接入区	安全云资源池	安全管理区	互联网接入区	应用服务器区	数据库服务区
边界接入区	—	授权	互通	授权	禁止	禁止	互通	禁止	禁止
核心网络区	互通	—	互通	授权	互通	互通	互通	互通	互通
前置服务区	禁止	禁止	—	互通	互通	禁止	禁止	互通	禁止
安全接入区	互通	互通	授权	—	授权	授权	授权	授权	授权
安全云资源池	互通	禁止	互通	授权	—	授权	禁止	禁止	互通
安全管理区	互通	互通	禁止	授权	互通	—	互通	互通	互通
互联网接入区	互通	互通	互通	授权	授权	互通	—	禁止	禁止
应用服务区	禁止	互通	互通	授权	互通	互通	禁止	—	授权
数据库服务区	互通	授权	禁止	授权	禁止	互通	禁止	禁止	—

访问控制策略应根据网络及业务变化和单位的安全基线进行合理配置和及时调整，及时删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化。

防火墙部署在各安全域边界，在互联网接入边界、安全管理区边界、核心业务区边界均需单独部署防火墙设备，设置严格的访问控制规则，并定期进行策略的检查和优化。

5.2 边界隔离与访问控制

通过部署防火墙或开通虚拟化防火墙服务来实现网络边界的安全访问控制，该组件集成访问控制、用户授权访问、虚拟系统、行为管理、应用层综合安全防护等功能，并支持与威胁感知、安全管理中心等智能联动，实现一体化的智能安全防护，核心功能包括：

（1）智慧发现。通过与其他安全系统的协同联动，借助外部的威胁情报、大数据分析等能力，对本地网络流量所产生的数据进行深入的检测和分析，从而及时发现传统防护手段无法检测到的威胁。

（2）智慧调查。系统对运行过程中所产生的多维数据进行自动关联，并利用可视化和递进式数据钻取的设计，给用户提供分析线索、发现异常、回溯事件等一系列分析面板，降低用户对风险、威胁、异常进行分析的难度。

（3）智慧处置。基于“智慧调查”的分析回溯结果，对受害主机或可确定的攻击源执行一键式的处置，并对处置后的结果进行持续监控，完成威胁管理的闭环操作。

通过主动网络扫描或渗透测试等方式验证网络隔离有效性。

防火墙部署在各安全域边界，在互联网接入边界、安全管理区边界、核心业务区边界均需单独部署防火墙设备，设置严格的访问控制规则，并定期进行策略的检查和优化。

七、运行维护

1.运维建设原则

为加强教育系统党组织对教育信息化工作的领导，落实网络安全主体责任，需明确主要负责人为运维工作的第一负责人，按照谁主管谁负责、谁应用谁负责、谁建设谁负责、谁运维谁负责的原则，确立分级运维制度，同时建立统筹协调的领导体制机制。完善信息化工作的规章制度，制订应急预案，开展应急演练，确保安全保障常态化、日常化。全面落实网络安全等级保护制度。加强网络安全技术防范，做到领导到位、机构到位、人员到位、责任到位、措施到位，实现有效、高效运维的目标。

2.总体运维方案

广西教育网由骨干网、城域网和校园网三部分构成。运维如下：

2.1 借助骨干网控制器可以实现对骨干网的智能运维管理

控制器支持通过界面和北向进行端到端的业务发放，实现业务开通一键式下发，具备以下能力：

2.2.1.资源池化。提前规划参数资源池，业务发放过程中，自动分配资源。屏蔽网络细节。资源池支持与网络设备同步，确保自动申请的资源不会与现网冲突。

2.2.2.灵活选路。支持按照全网带宽均衡，Cost 最优，时延最优进行路径选择，方便用户选取最优路径。当自动选路不满足用户诉求时，还支持用户在线设置必径/非必经结点和链路，调整路径。

2.2.3.E2E 跨域 SR。支持自动收集跨 AS 域的全网 L3 拓扑，自动完成跨域隧道的算路和建立。

2.2.4.VPN 业务可视。控制器支持对于 VPN 业务实现 360 度可视。

2.2.5.VPN 业务路径跨层可视。自动展示站点间业务与隧道的关联关系。隧道逐跳路径可视。

2.2.6.业务运维信息中心。支持用户查看业务告警，业务关联绑定的隧道，业务站点下路由协议的配置全部信息。

2.2.7.业务诊断中心。支持启动 RFC2544， Y.1564 业务诊断。

2.2.8.隧道路径智能调整。控制器支持对于隧道路径智能调整。

2.2.9.SLA 可保障。支持多因子约束算路。使隧道的业务路径可以按照带宽、时延、链路可用度、SRLG、主备分离、正反共路 SLA 保障算路。同时支持多种约束算路一起算路而不降低算法效率。

2.2.10.隧道可管可控。支持用户多维度规划自己的业务路径，保障业务流量可以按照用户期望的路径运行。

2.2.11.显示路径。支持用户指定必经/非必经业务路径，严格执行用户规划路径。

2.2.12.亲和属性。支持在三层拓扑上标示亲和属性，形成基于亲和属性的逻辑拓扑，指定亲和属性算路，可以保障业务路径只包含该亲和属性的链路。使用亲和属性算路，可以用于多业务之间的隔离。

2.2.13.隧道锁定。用户支持将规划好的隧道路径进行锁定。保障该隧道途径链路发生故障时，控制器重新算路快速恢复业务。当原有故障恢复时，还会将业务调整回原有锁定路径。这样就保证业务流量尽可能符合用户规划，同时又具备快速恢复高可靠。

2.2.14.质量感知。支持基于真实业务流的端到端和五元组粒度的网络丢包、时延检测，网络质量劣化时，能够针对劣化业务转发路径还原，并自动进行故障定位定界和告警。

2.3 计算资源和存储资源

本项目日常运维工作中，涉及到网络管理、安全管理、统一身份认证、上网日志留存、远程运维等各种业务软件，这些业务软件均需要计算资源和存储资源，为了保障本项目当前及未来 3 年的运维需求，本次设计在骨干网的 3 个核心节点和 10 个高校城市节点配置虚拟化一体机，为项目管理和运维业务提供相应计算资源和存储资源。

2.4 可视化运维能力

统一的可视化运维能力涉及到多个运营商、厂家等运维能力的整合，是一个长期建设完善的过程。因此，在建设初期，由运营商在各自运维系统上为教育行政管理部门开设账号，各级教育部门按照分权分域进行管理，可以查看所辖教育城域网内的网络拓扑、设备告警、线路告警以及流量监控等信息，实时查看网络运行状态，初步做到网络全程可见、可管、可控。随着教育网搭建成熟后，可以考虑引入第三方集成厂家，对各个运营商提供的运维数据进行集成展示，真正做到运维可视一张图，为运维提供直观化的管理手段。

3.网络安全运维要求

落实各级教育行政管理部门网络安全责任，分级管理分级负责。按统一的技术规范建设教育网网络安全管理系统，对敏感数据和网络信息进行安全管控。各级教育行政管理部门具备网络应用态势感知、快速反应和处置能力，配置有互联网出口的教育管理机构必须承担相应网络安全责任，按相关法规、标准和规范的要求建设实名制认证、应用管理等技术系统，并负责处置相关网络安全事件和事故。

4.运营商网络运维要求

4.1 属地化售后服务

为广西教育网提供线路服务的运营商，需建立专属售后维护机制，在各市县均设立有售后服务机构，提供相应的售后服务工作。

根据线路故障等级分为：骨干网故障、城域网故障，并遵循以下故障处理原则：

4.1.1 骨干网故障

如由运营商主动发现的骨干网故障，由运营商自治区级负责人向自治区教育厅负责人或授权人报备故障情况；如首先发现故障的是自治区教育厅，由自治区教育厅的负责人或授权人通知运营商自治区级专职客户经理，运营商客户经理协调相关部门进行故障处理。

故障处理过程中，运营商客户经理每 30 分钟主动反馈故障处理情况；故障处理完成后 30 分钟内，客户经理向教育厅负责人或授权人口头反馈故障原因和处理结果后，3 个工作日内按客户需要提交故障处理书面报告。

4.1.2 故障升级

当各市县城域网故障未在要求时限内修复时，上升为自治区级故障，由运营商市县级专职客户经理通知自治区区级专职客户经理，运营商自治区级专职客户经理第一时间向广西教育厅的负责人或授权人报备，同时协调相关部门进行故障处理。

4.2 业务恢复时限

业务故障指影响教育网线路运行，影响业务正常使用的故障，包括业务中断和一般故障。

业务中断故障是指教育网专线业务至少一个局向通信全阻的情况；一般故障是指未全阻情况下的其他故障，如业务性能劣化。

业务恢复时限指自各级教育管理机构提出故障投诉时或出现监控告警时起，至网络业务恢复正常所需要的时间，如采用 PTN/IPRAN 接入方式，业务恢复时限和及时率要求见下表（单位：小时）。

业务恢复时限和及时率表

故障类别	市区
骨干网	≤4
一般故障（含性能劣化）	≤24

注：业务恢复时间的统计可剔除不可抗力原因、各级教育管理机构自身网络原因及业务挂起的时长。

4.3 故障处理反馈

故障处理反馈指从各级教育管理机构提出故障申告时起，运营商按照相应的要求向各级教育管理机构反馈故障处理过程，要求见下表。

故障处理反馈表

故障处理反馈	处理要求
阶段反馈故障处理情况	按各级教育管理机构需要，每 30 分钟反馈
口头反馈故障原因和处理结果	故障处理完成后 30 分钟内向各级教育管理机构反馈

根据影响业务的程度，在故障处理结束后运营商按需向各级教育管理机构提交故障处理的书面报告；如需提供，需在故障处理结束后 3 个工作日内提供故障报告。

4.4 日常维护服务

日常维护服务是运营商为教育网提供的主动性维护服务，服务内容主要包括：网络运行监控服务、业务日常巡检、技术咨询与支撑、网络运行分析报告、客户端应急演练、售后服务联席会议、故障预警等内容。

4.4.1 网络运行监控

网络监控服务指运营商向各级教育行政管理部门提供 7x24 小时的设备层、电路层等网络监控，获取各类告警、故障信息，实时响应并及时恢复、解决。电路层监控，只向专线类业务提供。

4.4.2 业务巡检

业务巡检指运营商对业务运行情况开展主动性、预防性的检查，对涉及的设备告警、性能、运行状态进行检查分析。同时核对工程技术资料、电路资料、电路参数、维护路由、终端设备和内部组网等，保持客户资料的准确性和可用性，对客户端网络资源进行预警。

骨干网节点及城域网汇聚节点巡检周期为每半年一次。巡检后由运营商出具巡检报告，由各级教育行政管理部门签字确认。

4.4.3 技术咨询与支撑

技术咨询与支撑指在业务使用过程中由运营商专业技术专家向各级教育行政管理部门提供技术咨询和支撑，及时解决业务使用过程中遇到的疑难技术问题。

4.4.4 网络服务报告

网络服务报告是指根据各级教育管理机构需要，对网络在一段时间内的运行情况进行总结和分析。网络服务报告包括三类：网络运行分析报告、专项故障分析报告、业务分析与优化报告。

网络服务报告表

服务内容	金牌级服务
网络运行分析报告	按需提供，不高于每半年 1 次
专项故障分析报告	按需提供
业务分析与优化报告	按需提供

4.4.5 应急演练服务

应急演练是指假想客户端网络可能出现的问题，而进行的应急电路调度或者主备业务的倒换测试。这里的客户端网络是指运营商负责维护的设备和电路。网络应急演练周期规定为按各级教育管理机构需要，不高于每半年一次，如遇“两会”等重大活动或节假日重要通信保障，可根据需求增加测试次数。

4.4.6 售后服务联席会议

售后服务联席会议指运营商业务部门组织定期与各级教育管理机构共同对售后服务的质量进行检查和评估，对服务项目进行总结，形成备忘录/会议纪要。

4.4.7 故障预警

（1）运营商专线预警功能

故障发生后，系统会实时关联出运营商客户“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度，当前处理人，当前处理人联系电话”等信息，所有告警均通过短信、生成 ESOP 任务方式对客户经理、进行通知。

（2）故障累计预警

针对每月有累计故障考核的业务，结合运营商编码及专线名称，如 X 运营商的专线名称为 xx，可以设置月累计故障值为 2，当同一运营商的同一专线名称收到告警大于等于 2 次，则给该运营商客户的客户经理进行预警，通过发短信、生成任务单方式进行预警。

（3）预警报表统计查询功能

平台可按照“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度，当前处理人，故障解决时间，当前处理人联系电话”进行统计，查询字段为“运营商编号、运营商名称、运营商级别，预警业务、故障类型、故障开始时间、目前处理进度、故障解决时间”进行查询，定期分析运营商客户故障情况，并对故障情况进行分析，对故障发生超过设定门限专线进行预警重点保障，形成故障发生可监控、处理过程可管理、处理结果可分析优化的闭环管理机制。

4.5 应急维护保障

应急预案维护标准是要求能以最短的维护时限完成教育网故障网络的修复工作，同时要保证预案的可执行性、资源准确性、调度及时性。

5.运维权限规划

针对学校规模较大，如学生人数超过1000人以上的中小学等有较强个性化运维需求的学校，运营商可开放一些运维管理平台的账号，分配二级账号。

其他附件：

中小企业划型标准规定

工信部联企业〔2011〕300 号

一、根据《中华人民共和国中小企业促进法》和《国务院关于进一步促进中小企业发展的若干意见》（国发〔2009〕36 号），制定本规定。

二、中小企业划分为中型、小型、微型三种类型，具体标准根据企业从业人员、营业收入、资产总额等指标，结合行业特点制定。

三、本规定适用的行业包括：农、林、牧、渔业，工业（包括采矿业，制造业，电力、热力、燃气及水生产和供应业），建筑业，批发业，零售业，交通运输业（不含铁路运输业），仓储业，邮政业，住宿业，餐饮业，信息传输业（包括电信、互联网和相关服务），软件和信息技术服务业，房地产开发经营，物业管理，租赁和商务服务业，其他未列明行业（包括科学研究和技术服务业，水利、环境和公共设施管理业，居民服务、修理和其他服务业，社会工作，文化、体育和娱乐业等）。

四、各行业划型标准为：

（一）农、林、牧、渔业。营业收入 20000 万元以下的为中小微型企业。其中，营业收入 500 万元及以上的为中型企业，营业收入 50 万元及以上的为小型企业，营业收入 50 万元以下的为微型企业。

（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

（三）建筑业。营业收入 80000 万元以下或资产总额 80000 万元以下的为中小微型企业。其中，营业收入 6000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 300 万元及以上，且资产总额 300 万元及以上的为小型企业；营业收入 300 万元以下或资产总额 300 万元以下的为微型企业。

（四）批发业。从业人员 200 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 20 人及以上，且营业收入 5000 万元及以上的为中型企业；从业人员 5 人及以上，且营业收入 1000 万元及以上的为小型企业；从业人员 5 人以下或营业收入 1000 万元以下的为微型企业。

（五）零售业。从业人员 300 人以下或营业收入 20000 万元以下的为中小微型企业。其中，从业人员 50 人及以上，且营业收入 500 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（六）交通运输业。从业人员 1000 人以下或营业收入 30000 万元以下的为

中小微型企业。其中，从业人员 300 人及以上，且营业收入 3000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 200 万元及以上的为小型企业；从业人员 20 人以下或营业收入 200 万元以下的为微型企业。

（七）仓储业。从业人员 200 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（八）邮政业。从业人员 1000 人以下或营业收入 30000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 20 人以下或营业收入 100 万元以下的为微型企业。

（九）住宿业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十）餐饮业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十一）信息传输业。从业人员 2000 人以下或营业收入 100000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 100 万元及以上的为小型企业；从业人员 10 人以下或营业收入 100 万元以下的为微型企业。

（十二）软件和信息技术服务业。从业人员 300 人以下或营业收入 10000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 10 人及以上，且营业收入 50 万元及以上的为小型企业；从业人员 10 人以下或营业收入 50 万元以下的为微型企业。

（十三）房地产开发经营。营业收入 200000 万元以下或资产总额 10000 万元以下的为中小微型企业。其中，营业收入 1000 万元及以上，且资产总额 5000 万元及以上的为中型企业；营业收入 100 万元及以上，且资产总额 2000 万元及以上的为小型企业；营业收入 100 万元以下或资产总额 2000 万元以下的为微型企业。

（十四）物业管理。从业人员 1000 人以下或营业收入 5000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 1000 万元及以上的为中型企业；从业人员 100 人及以上，且营业收入 500 万元及以上的为小型企业；从业人员 100 人以下或营业收入 500 万元以下的为微型企业。

（十五）租赁和商务服务业。从业人员 300 人以下或资产总额 120000 万元以下的为中小微型企业。其中，从业人员 100 人及以上，且资产总额 8000 万元及以上的为中型企业；从业人员 10 人及以上，且资产总额 100 万元及以上的为小型企业；从业人员 10 人以下或资产总额 100 万元以下的为微型企业。

（十六）其他未列明行业。从业人员 300 人以下的为中小微型企业。其中，从业人员 100 人及以上的为中型企业；从业人员 10 人及以上的为小型企业；从业人员 10 人以下的为微型企业。

五、企业类型的划分以统计部门的统计数据为依据。

六、本规定适用于在中华人民共和国境内依法设立的各类所有制和各种组织形式的企业。个体工商户和本规定以外的行业，参照本规定进行划型。

七、本规定的中型企业标准上限即为大型企业标准的下限，国家统计部门据此制定大中小微型企业的统计分类。国务院有关部门据此进行相关数据分析，不得制定与本规定不一致的企业划型标准。

八、本规定由工业和信息化部、国家统计局会同有关部门根据《国民经济行业分类》修订情况和企业发展变化情况适时修订。

九、本规定由工业和信息化部、国家统计局会同有关部门负责解释。

十、本规定自发布之日起执行，原国家经贸委、原国家计委、财政部和国家统计局 2003 年颁布的《中小企业标准暂行规定》同时废止。