广西教育网建设项目
设计方案

（2023 年修订版）

广西壮族自治区教育厅

目　　录

第 1 章　项目概况

1.1 项目建设目标

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，由教育骨干网、教育城域网和各类学校校园网组成。广西教育网的各级各类教育机构和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。建设广西教育网标准规范体系，依据标准规范体系推进广西教育网建设，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。

1.2 项目建设内容

广西教育网的建设内容主要包括教育网标准规范、网络中心和传输网络，传输网络由教育骨干网、教育城域网和校园网三部分构成。

（一）教育网标准规范。

教育网标准化体系建设是广西教育系统自治区、市、县三级网

络实现互联互通、信息共享、业务协同、安全可靠运行的前提和基础，是广西教育网建设参考性指导标准。

教育网标准化体系建设主要包含如下建设内容:

1.标准体系构建及实施路径研究

围绕教育网建设工作需求系统梳理教育部、自治区教育厅和其他行业编制的相关标准、规范，紧密对接国家教育部的教育网标准体系，构建广西教育网建设的标准体系，根据自治区教育厅和各级院校的实际需求，结合目前已编、在编的相关标准、规范、指南、指引，制定教育网标准制定及申报的总体计划。

2.标准编制内容

广西教育网建设标准体系主要包含以下体系的编制。

（1）总体标准分体系

（2）管理标准分体系

（3）网络标准分体系

（4）安全标准分体系

3.标准技术咨询服务

引入标准技术咨询服务，指导编制教育网建设的总体标准、管理标准、网络标准和安全标准，组织行业专家就标准技术内容进行查询、收集、调研、论证，协助申报自治区行业标准。

（二）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。

（三）传输网络。

1.教育骨干网

教育骨干网在原有高校互联网络基础上实施升级改造；加大主干带宽，提升高等学校网络互联互通能力；扩展连接范围，支撑中等职业学校和中小学学校信息化应用的需要。教育骨干网在3个核心节点，12个高校城市节点租用运营商的传输网络线路进行组网。

核心节点设在广西教育数据中心（南宁）、广西大学（南宁）和广西师范大学（桂林）。核心节点租用2家不同运营商的IP网络线路组成2个环路，除了分担教育网流量承载和承担高校城市节点就近互联外，还承担本地的设区市本级教育城域网、县级教育城域网、高等学校、区直中等职业学校的网络互联。教育网在教育骨干网规划与自治区电子政务外网的统一互联接口。

12个高校城市节点租用2家不同运营商的传输网络线路就近接入核心节点，分别承担本地的设区市本级教育城域网、县级教育城域网、高等学校、区直中等职业学校的网络互联。

网络中心的互联网出口可供各级各类教育机构、学校、老师、家长、学生通过互联网拨入教育网VPN，使用教育网内网的资源。

2.教育城域网

每个教育城域网租用1家运营商网络线路，连接本地中小学学

校、幼儿园、中等职业学校的校园网络。

每个教育城域网统一建设2组网络出口。一是与教育骨干网互联的出口，通过租用运营商的IP网络线路与教育骨干网互联。二是互联网出口，通过租用运营商的互联网接入服务，且必须采用路由冗余设计。教育城域网内的中小学学校、幼儿园、中等职业学校通过教育城域网汇聚点外联，原则上不再保留互联网出口。

3.校园网

校园网用光纤或以太网电缆连接教室、计算机教室、办公室等的学校各功能区域信息终端，校园网出口用光纤上联教育城域网汇聚点。有条件的学校要在校园光纤网络基础上建设满足教学需要的无线网络（WiFi）。现有校园网络能够满足教学需要，且能与教育城域网匹配的，可以保留继续使用，逐步过渡到符合广西教育网建设技术规范的光纤网络。

（四）网络安全等级保护建设。

依据网络安全等级保护政策、标准、指南等文件要求以及用户业务安全需求，技术层面上，针对教育城域网，需要从通信网络防护、区域边界防护、计算环境防护、安全管理中心等各方面进行不同级别的安全防护设计。教育骨干网安全管理需符合国家等保2.0标准第三级的要求，教育城域网安全管理需符合国家等保2.0标准第二级的要求。广西教育网网络安全保护设计包括：安全技术体系

和管理要求。

围绕着“一个中心，三重防护”，在进行设计和建设时可以形成网络安全综合技术防护体系，突出技术思维和立体防范，并且注重全方位主动防御、动态防御、整体防控和精准防护。

（五）密码应用建设。

围绕《国家政务信息化项目建设管理办法》中关于政务信息系统在系统规划阶段的密码应用要求，综合考虑广西教育网物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用方案，使教育骨干网满足 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，各级市县教育城域网满足 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中二级指标要求，并为通过密码应用安全性评估奠定基础。

1.3 项目建设规模

广西教育网由自治区教育厅统筹规划建设，连接自治区城乡各级各类学校和教育机构，是支撑培养造就德智体美劳全面发展的社会主义建设者和接班人的教育行业专用网络，是教育信息化基础设施的重要组成部分。具体建设规模如下。

（一）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。

（二）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。

（三）用户规模。本项目服务范围将覆盖广西全区 3.46 万所大中小院校（含教学点）、1316.55 万名在读学生和 68.92 万名专任教师，广西教育网与互联网、电子政务外网、中国教育专网等外部系统实现互通，将使全区教育信息化、一体化水平再迈上一个新的台阶。

（四）带宽规模。本项目教育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，教育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。教育城域网与教育骨干网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。设区市城市、乡镇所在地的学校：教室下行带宽不少于 100M，上行带宽不少于 100M。计算机教室下行带宽不少于 200M，上行带宽不少于 200M。农村学校（教学点）：教室下行带宽不少于 100M，上行带宽不少于 30M 带宽。计算机教室下行带宽不少于 200M，上行带宽不少于 60M 带宽。

1.4 项目建设范围

广西教育网建设包含教育骨干网、教育城域网及校园网建设。自治区教育厅承担教育骨干网、可研和初步设计编制及评估、标准规范编制服务、竣工验收等费用，各市县统筹教育经费承担教育城域网及校园网费用支出，各市县承担网络安全等级保护测评、网络安全风险评估、商用密码应用安全评估等费用。

1.5 项目建设期

本项目建设周期为 3 年（2021-2023 年）。

第 2 章　总体建设思路

2.1 总体设计原则

广西教育网建设项目建设过程中，应坚持以下原则:

（一）共建共享。按照统一规划、统一技术规范、统一建设模式，由自治区教育厅统筹建设覆盖全区各级各类教育机构、各级各类学校的教育网络，实现全区教育网络有效的互联互通，支持教育资源高效快速流动，教学应用全区通畅可达。

（二）稳定可靠。充分考虑网络架构、链路和设备的适度冗余，保障网络具备高度稳定性和可靠性；充分考虑网络模块化设计和应用，可根据业务的需要进行顺利扩展或平滑升级；充分考虑已建网络或应用系统需求和特点，兼容存量信息化应用。

（三）满足应用。支持各种高带宽、低延时的教学应用场景，满足数字资源、同步互动教学教研、网络空间应用等各级各类教育管理和教学资源信息化应用，为教育大数据应用和智慧教育提供有效支撑。

（四）灵活扩展。组网设计必须具有良好的灵活性和可扩展性，能够满足系统业务不断深入发展的需要，方便扩展网络覆盖范围、扩大网络容量和提高网络的各层次节点的功能，具备支持多种通信媒体、多种物理接口的能力，提供技术升级、设备更新的灵活性，

满足发展需要，实现低成本扩展和升级的需求。

（五）适当超前。建设时充分考虑目前教育行业的业务要求，采用先进、成熟的技术、设计思想、网络结构，采用覆盖率高、标准化和技术成熟的软硬件产品，满足业务需求的同时也要兼顾相关的管理需求，使整个系统在相当一段时期内保持技术的先进性，以适应未来信息化发展的需要。

（六）安全可控。从物理、技术、管理等方面综合考虑，采用硬件备份、冗余等可靠性技术，提高整个网络系统的安全可靠性，同时设计和制定高效的网络运维和严密的网络安全方案，通过采集、积累、分析、展现深入挖掘各类网络运行数据，建设统一管理运维体系，形成包含网络运维、安全管控、应用支撑等多层次、全方位的网络管控能力，满足等保 2.0 的安全要求，能够保障教育信息数据的安全性。

（七）一地一案。针对已建成设区市本级教育城域网、县（市、区）本级教育城域网建设模式不同、组网结构多样、多家运营商承建的现状，将按自治区统一的技术规范进行扩容、升级和调整，结合各地实际，按一地一案的策略分别制定各市县教育城域网升级改造建设方案，实现各市县已有网络与教育网融合，构建全区统一教育行业专用网络。

2.2 总体架构

广西教育网由教育骨干网、教育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。广西教育网总体架构如下。

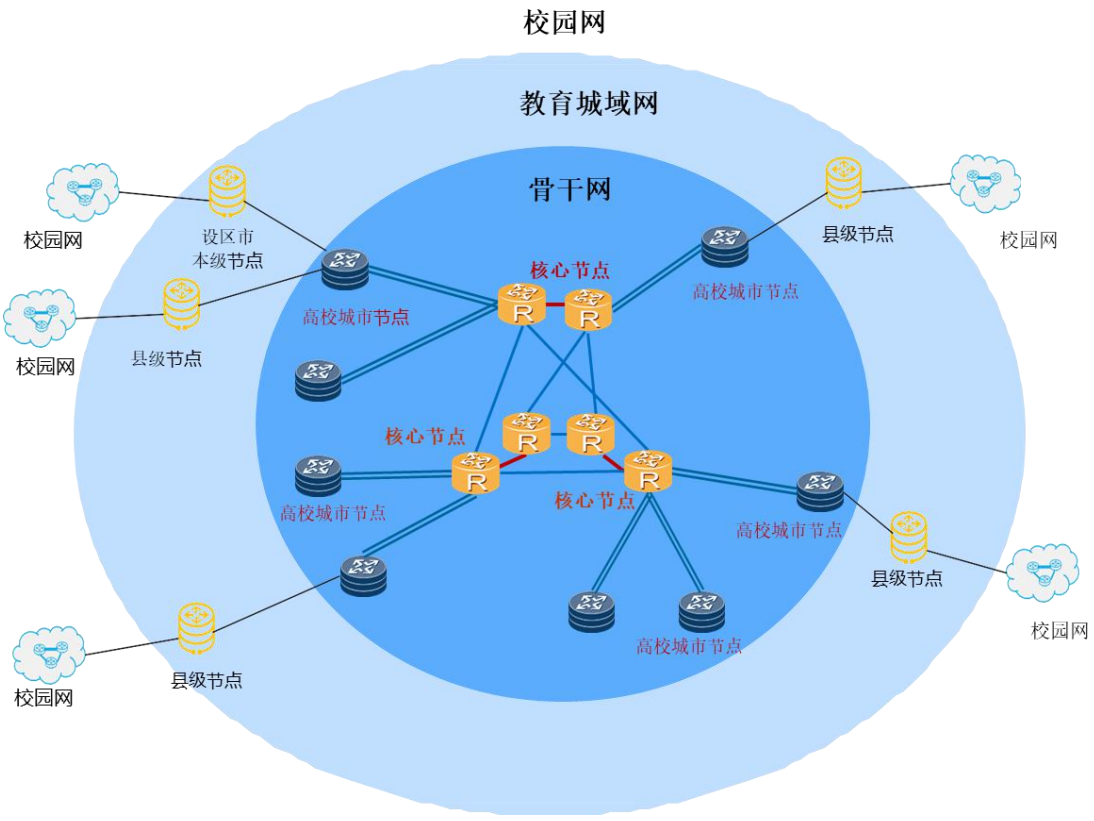

图 4-1 广西教育网总体架构图

通过建设教育骨干网核心节点，组建教育骨干网核心环路，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，建成教育骨干网。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、县级教育城域网。各设区市、县级教育城域网连接教育骨干网市级汇聚节点，

形成完整统一的教育基础网络。

（一）网络中心。在教育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、县级教育城域网、跨县域的教育城域网根据情况设立不同规模的网络中心。

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。

（二）教育骨干网。教育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。

教育骨干网及各端纵向接入城域网，实现与线路两端的互通。鉴于教育骨干网的重要性，教育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教育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。

（三）教育城域网。教育城域网是指在市县行政区域范围内，利用计算机网络、大数据、人工智能等技术，以光纤为传输介质，为连接本行政区域内各学校校园网和其它教育机构局域网的传输线路组成的网络，实现教育应用统一化，教育数据智能化分析。按行政区域管理层级和网络连接机构划分，可分为设区市本级教育城域网和县级教育城域网。

1.设区市本级教育城域网

设区市本级教育城域网是指由设区市教育行政部门主导，在设区市行政区域内建设的教育城域网，包括：设区市本级网络中心、设区市级骨干网、设区市属学校校园网、设区市属其他教育机构网络。

2.县级教育城域网

县级教育城域网是指由县（市、区）教育行政部门主导，在县级行政区域内建设的教育城域网，包括：县级网络中心、县级骨干网、县级所辖学校校园网、县级所辖其他教育机构网络等，鼓励设区市教育行政部门引领，组织所辖县级教育行政部门建设设区市行政区域内统一的教育城域网。鼓励地域相邻的县级教育行政部门组成联盟，共建共享跨县（市、区）域的教育城域网。

（四）校园网。校园网是教育城域网的延伸，指在学校区域内，利用计算机网络技术，通过以太网、光纤、WiFi6 等，将学校区域内信息终端连接起来的通信网络。单一校区的学校建成校园局域网，

有2个（含）及以上校区的教育集团根据实际需要建设本教育城域网内或者跨教育城域网的校园网络。

（五）安全系统。本项目网络安全建设的最终目标是使教育骨干网符合网络安全等级保护第三级要求，教育城域网符合网络安全等级保护第二级要求。

本项目统筹规划教育骨干网和广西教育数据中心的网络安全设计和建设，统一实施网络安全的管理和运维。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，教育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。

本项目的各级教育城域网是教育骨干网延伸到终端的线路。各级教育城域网独立设置网络汇聚点，以光纤专线方式直接与教育骨干网连接，与教育骨干网之间部署专属的网络安全设备系统，实现与教育骨干网的边界隔离，实行分级管理分级运维，与教育骨干网实现网络安全态势感知一体化管理。各级教育城域网内不部署应用系统和数据系统，根据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）有关网络和终端的条款，结合我区的实际，教育城域网的网络安全保护等级定级第二级，按网络安全等级保护第二级的要求进行设计、建设、管理和运维。

本项目根据等级保护的指导思想，以技术保障为基础、以管理运维为抓手、以监测预警为核心、以协同响应为目标规划网络安全

防御体系并落地为具体的安全建设方案。将安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全需求，转化为可以实现的技术防护能力、安全管理措施和安全运营手段，为教育网的安全运行保驾护航。

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。

第 3 章　项目建设方案

3.1 总体网络架构

广西教育网将各级各类学校（教学点）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，搭建网络基础。广西教育网总体架构如下图。

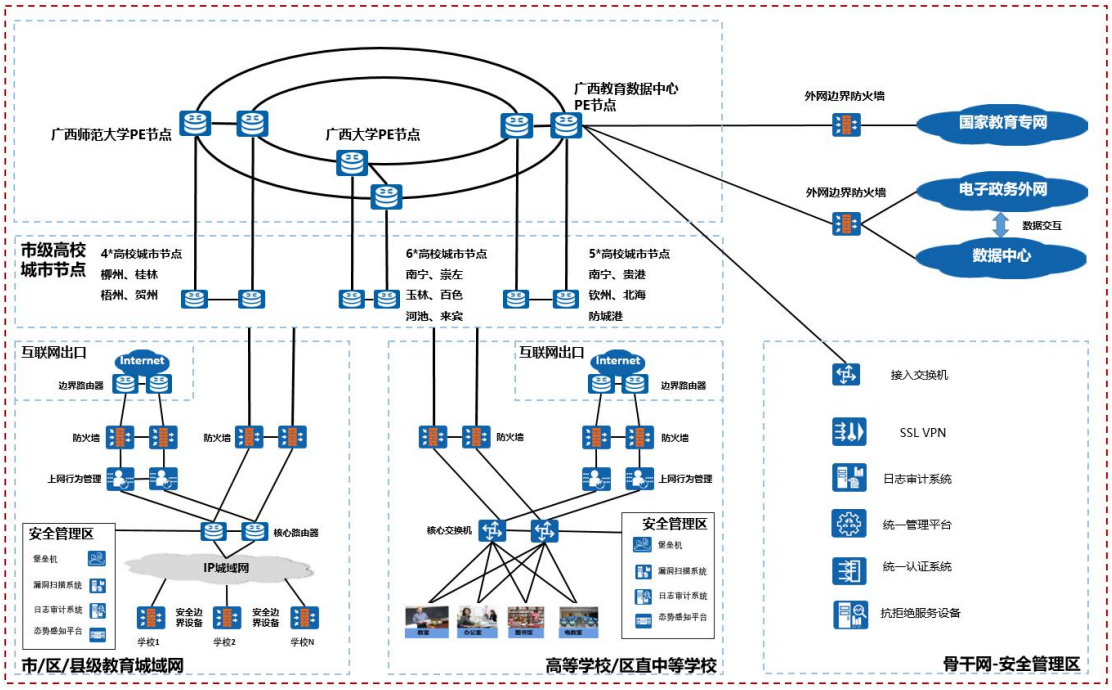

图 5-1 教育网拓扑图

通过建设教育骨干网核心节点，组建教育骨干网核心环路，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，建成教育骨干网。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，形成教育城域网。各教育城域网连接教育骨干网市级汇聚节点，形成完整统一的教育基础网络。

3.2 教育网建设标准规范编制

3.2.1 工作原则

根据标准的内涵、地位与作用，在构建标准体系和制定标准的过程中，应遵循的基本原则包括：科学性、系统性、完整性、兼容性、先进性和开放性。

（一）科学性。科学性是标准化最基本的原则，是信息系统安全、可靠、稳定运行的根本保障。标准体系中，分类要科学、合理，要能够准确地反映教育网建设的总体需求和具体需求，便于应用。

（二）系统性。指标准体系中各个标准之间内部联系和区别的体现。恰当地将系统涉及的各类标准安排在相应的分体系中，做到层次分明、合理，充分体现出标准之间互相衔接配套关系，避免交叉。

（三）完整性。指标准体系结构完整、内容全面。所需要的各种标准在标准体系中都应有的相应的位置，各标准之间互相协调、配套，同时，也要侧重应用。

（四）安全性。标准体系须考虑网络安全性，履行网络安全主体责任，满足《网络安全法》等法律法规的合规性要求。

（五）兼容性。应充分体现优先采用国家标准和行业标准，以保持与它们的一致性和兼容性。

（六）先进性。在编制标准体系时，既要考虑目前的需要和技术水平，也要对未来的发展有所预见，使之能够满足教育网建设业

务和技术发展的需要。

（七）开放性。标准体系要具有开放性，即可扩充性；要能够根据科学技术、标准和应用的发展，方便地进行扩充和完善。

3.2.2 体系构建及实施路径研究

（一）教育网标准体系研究。

围绕教育网建设工作需求系统梳理教育部、自治区教育厅和其他行业编制的相关标准、规范，紧密对接国家教育部的教育网标准体系，构建广西教育网建设的标准体系，明确教育网建设标准体系的层级和板块，以及每个版块下对应的具体标准，成为广西教育网建设各成员单位的共识框架。

（二）教育网标准体系实施路径研究。

包括更新完善标准清单和待制定标准清单。在教育网标准体系框架的指导下，根据自治区教育厅和各级院校的实际需求，结合目前已编、在编的相关标准、规范、指南、指引，制定教育网标准制定及申报的总体计划。更新完善标准清单和待制定标准清单，具体包括缺项技术标准的新编、已有技术标准的修编、多项已有技术标准的精简整合、规范文件向技术标准的提升转化等，明确每项标准建议申报的级别及发布形式,明确各业务处室负责制定的标准分工。

（三）统筹协调管理应用和技术支持。

统筹协调教育网技术类标准板块和管理类技术标准板块的工作。包括技术标准体系、管理标准体系和安全管理标准板块之间的

衔接协调、基础资料及相关文件汇总收集、项目工作例会材料准备、厅内工作会议材料准备、工作成果统筹等工作。

3.2.3 编制内容

（一）总体标准分体系。

1.术语标准

教育网建设术语，是教育网建设过程中所形成的基本概念的语言指称，该标准规范化的描述网络环境、信息资源、数据交换、安全保障、业务应用、应用支撑、项目建设与管理、运行维护等基本概念和专有术语。

该标准是针对教育网建设制定的术语，主要目的是让使用者在使用教育网建设相关标准时能够形成统一的理解。该标准适用于教育网成员单位、设计咨询单位、监理单位、集成商、网络集成商、安全集成商等单位，参与教育网建设相关人员（包括：业务人员、系统分析人员、系统设计人员、系统实施人员、监理人员、项目管理人员、系统维护人员等）。

该标准用于指导教育网建设所有子系统的设计、开发、建设实施和管理维护等阶段术语的使用。教育网建设项目实施办公室、设计咨询单位、监理单位、集成商、网络集成商、安全集成商在编制文档、报告或进行书面沟通时，应使用该标准中规定的术语和定义。

2.主题词表

该词表规范教育网建设主题词，主要内容有词表结构、选定词、

主题词款目格式、排序、主表、附表、索引等。

该词表按电子政务涵盖面、层次关系和使用范围，将主题词分为网络、管理、安全等方面。

该词表通过规范主题词的格式和主题词表，以实现检索语言在网络环境下的兼容与共享，指导主题词的选定和标引。主题词表的编制，是实现信息主题词检索服务的基础。

3.建设标准体系

是按照国家电子政务标准化建设的要求，遵循已有的国家和国际标准，结合教育行业的业务特点，重新进行规划、设计，逐步建立各类标准和规范。广西教育网建设的标准化和规范化，是各成员单位相关部门之间、教育系统与自治区相关厅局、地市区县乡镇教育及相关部门之间的各种系统兼容互通、资源共享的保障，为广西教育网建设奠定坚实基础。

标准需要描述广西教育网建设的总体架构、各标准的应用场景、广西教育网建设标准化建设的内容以及各标准之间的关系等内容。该标准的建设是在分布式网络环境下，实现数据、信息和系统的集成，实现互联互通并最大限度的进行互操作的一项重要的基础性工作。

4.建设标准化指南

该标准包括广西教育网建设各标准的内容归纳及维护管理两个方面。内容归纳主要是从标准的作用、应用范围、适用对象等方面

出发，介绍广西教育网建设各标准，为使用者提供指导性的意见。维护管理主要是从机构职责、标准制定、实施贯彻以及维护管理等方面进行规范，规范广西教育网建设各标准规范的管理流程。

该标准主要对使用者提供快速认识和了解广西教育网建设标准的工具。使广西教育网建设的建设单位和相关人员（包括：业务人员、系统设计人员、监理人员、项目管理人员、系统维护人员等）迅速熟悉广西教育网建设的相关标准，并指导广西教育网建设的建设、实施、维护等各个环节。

（二）管理标准分体系。

1.建设项目管理规范

该标准主要对广西教育网建设成员单位建设过程中有关项目的过程的目的、过程的活动、过程的输入输出及其工作产品等。该标准适用于与广西教育网建设有关的项目管理和沟通，是指导广西教育网建设所有参与单位进行项目管理的规范，既涉及业主单位的项目管理过程，也涉及广西教育网建设监理单位、承建单位和其他与广西教育网建设有关单位的项目管理以及它们和业主单位之间的业务联系和沟通。

该标准将项目管理过程分为工程管理实施过程、项目管理基本过程和项目管理支持过程。工程管理过程主要描述广西教育网建设各阶段，业主单位参与和协调的工程管理活动和相关要求；工程管理基本过程主要描述广西教育网建设项目管理的基本过程，覆盖从

项目启动到项目结束的整个项目生存周期的管理活动；工程管理支持过程描述在工程管理过程和项目管理基本过程中需要开展的活动和任务。

该标准的制定可提高广西教育网建设管理水平，促进项目管理的科学化和规范化，保证工程建设质量。

2.建设过程文档编制规范

该标准主要对各成员单位教育网建设过程和管理过程中应编制的主要文档及其编制内容、格式制定基本要求。它以模板范本的形式给出包括项目可行性研究报告、项目建设方案、运维服务方案、安全审计报告等在内的文档编写规则，使其做到及时、正确、简明和统一。同时该标准从文档的编制过程入手，对原材料的准备、计划、编制、评审等各环节进行相应的规范。

该标准适用于广西教育网建设项目建设的开发过程和管理过程，为项目的各类文档提供统一的编制规范，并对项目建设过程中的重要文档给予格式规定和说明。

3.建设运行维护规范

广西教育网建设运行维护规范是项目运行维护阶段的规范性文件。严格的制度是安全管理的需要，也是运维管理的核心，系统运维管理主要从技术管理和服务管理两个方面出发，对教育网的运行维护进行规范化管理。同时对执行情况进行质量考核，确保高质量的完成各项维护支持任务。

该标准指导广西教育网建设所有成员单位在运行维护阶段的管理工作，使各子系统运行维护和管理规范化、标准化、制度化，提高各子系统的运行维护水平。

（三）网络标准分体系。

1.教育骨干网建设规范

该标准依据广西教育网建设的基本需求及特点制定，以指导广西教育网骨干网的建设。

该标准主要是教育网建设单位建设过程的规范要求，内容包括但不限于:

（1）骨干网拓扑结构

（2）骨干网 IP 地址规划

（3）骨干网域名规划

（4）骨干网带宽规划

（5）骨干网路由策略

（6）骨干网与电子政务外网互联策略

（7）骨干网与教育科研网互联策略

（8）骨干网络安全

（9）骨干网网络设备选型技术要求

（10）骨干网机房要求

2.教育城域网建设规范

该标准依据广西教育网建设的基本需求及特点制定，以指导广

西教育网城域网的建设。

该标准主要是教育网建设单位建设过程的规范要求，内容包括但不限于:

（1）城域网拓扑结构

（2）城域网 IP 地址规划

（3）城域网域名规划

（4）城域网带宽规划

（5）城域网路由策略

（6）城域网与骨干网互联策略

（7）城域网与接入网互联策略

（8）城域网网络安全

（9）城域网网络设备选型技术要求

（10）城域网机房要求

3.广西教育网接入网建设规范

该标准依据广西教育网建设的基本需求及特点制定，以指导广西教育网接入的建设。

该标准主要是对成员单位、设区市级、县级局域网建设的规范要求。内容包括但不限于:

（1）教育网成员单位接入网的分层结构设计

（2）自治区级接入网总体技术要求

（3）设区市级接入网总体技术要求

（4）县级接入网总体技术要求

（5）乡镇级接入网总体技术要求

4.广西教育网网络管理规范

对广西教育网建设管理是一个长期的过程，需要制定一套相对完整的管理标准，用于网络的维护和管理的标准化。

该标准的主要内容包括以下部分:

（1）网络管理总体标准，描述网络管理总体实施规范。

（2）网络管理分体系标准，各种网络管理的标准分类和描述。

（四）安全标准分体系。

1.安全管理规范

该标准对信息安全管理进行指导，为后期安全管理提供指导和相应标准规范。主要包括管理目标、范围、适用人员、安全标准的总体结构描述，安全域基于安全标准的划分，建立安全的管理体制等方面内容。

2.安全技术框架指南

根据广西教育网定级标准，分析、研究广西教育网建设信息安全保障建设需求，结合国家以及广西电子政务标准化指南规范，制定广西教育网建设安全标准化体系框架，对重要的、关键性标准做出简单介绍。

该标准主要描述广西教育网建设安全标准体系框架，介绍信息安全标准采用列表，以及总体安全框架下的主要安全标准。

3.2.4 技术咨询服务

（一）指导编制教育网建设的总体标准、管理标准、网络标准和安全标准，确定编制大纲，理清标准编制界限，确定编制框架及思路。

（二）组织行业专家就标准技术内容进行查询、收集、调研、论证，避免标准内容交叉、重复、矛盾。

（三）协助申报自治区行业标准，并按照标准主管部门的相关要求，确定恰当的标准名称及规范的内容，协助准备行业标准立项所需的材料，并进行格式审查。

3.2.5 成果交付

提交包括但不限于以下项目成果:

（一）标准体系构建及实施路径研究。

1.《广西壮族自治区教育网标准体系构建和实施路径研究报告》的电子文档及纸质文件

2.更新完善标准清单

3.相关汇报材料。

（二）总体标准分体系。

1.《广西壮族自治区教育网建设总体标准规范》电子文档及纸质文件

2.编制过程说明、重点条款注释和意见落实情况等文件

（三）管理标准分体系。

1.《广西壮族自治区教育网建设项目管理规范》电子文档及纸质文件

2.《广西壮族自治区教育网建设过程文档编制规范》电子文档及纸质文件

3.《广西壮族自治区教育网建设运行维护规范》电子文档及纸质文件

4.编制过程说明，标准、指引、指南的重要条款注释，意见落实情况等文件

5.相关汇报材料

（四）网络标准分体系。

1.《广西壮族自治区教育网骨干网建设规范》电子文档及纸质文件

2.《广西壮族自治区教育网城域网建设规范》电子文档及纸质文件

3.《广西壮族自治区教育网接入网建设规范》电子文档及纸质文件

4.《广西壮族自治区教育网网络管理规范》电子文档及纸质文件

5.编制过程说明，标准、指引、指南的重要条款注释，意见落实情况等文件

6.相关汇报材料。

（五）安全标准分体系。

1.《广西壮族自治区教育网建设安全管理规范》电子文档及纸质文件

2.《广西壮族自治区教育网建设安全技术框架指南》电子文档及纸质文件

3.编制过程说明，标准、指引、指南的重要条款注释，意见落实情况等文件

4.相关汇报材料

（六）自治区行业标准申报成果。

将总体标准分体系、管理标准分体系、网络标准分体系、安全标准分体系、数据治理标准分体系所提及标准申报为自治区行业标准。

3.3 网络中心

在教育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，各设区市级、县级教育城域网、跨县域的教育城域网根据情况设立不同规模的网络中心。

网络中心主要用于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、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。机房运行环境依据《数据中心设计规范》（GB50174-2017）及《信息安全技术　信息系统密码应用基本要求》（GB/T 39786-2021）对物理和环境安全要求建设。设区市本级教育城域网和高等学校的网络中心应参照 B 级及以上标准建设；县级教育城域网的网络中心应参照 C 级及以上标准建设。

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。

网络中心的建设模式主要有三种：自建模式、托管模式、租用模式。

自建模式是指网络中心机房及全部设施、设备系统均由教育部门购置建设。

托管模式是指教育部门不建设网络中心机房，将自有的网络、服务器、存储等设备系统以托管的形式放置于第三方网络中心。

租用模式是指教育部门不建设网络中心机房,不购置任何网络、服务器、存储等设备系统，直接租用第三方网络中心机房及全部设施、设备系统，用于部署、管理运维、应用自己的教育教学系统。

建议各市县教育行政部门优先采用托管模式和租用模式建设教育城域网网络中心，可选择当地具备条件的运营商、高校城市节点、政府信息中心实施建设。

高等学校应该自建网络中心,鼓励在学校集中的园区组建联盟,共建共用网络中心。

3.4 教育骨干网

教育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、高等学校和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。

教育骨干网及各端纵向接入城域网，实现线路两端的互通。鉴于教育骨干网的重要性，教育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教育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。

3.4.1 设计原则

（一）可靠性。网络整体设计要求能可靠稳定承受业务信息的正常运行，在出现意外故障时尽可能保证业务可用，整体网络设计必须始终遵循可靠性第一的原则。

（二）安全性。具有多种有效手段，防范各种形式对网络的非法入侵和内部攻击，以保证网络的实体安全、网络安全、系统安全和信息安全，有效地保障正常的业务活动和防止内部信息数据不被非

法窃取、篡改或泄漏。

（三）先进性。方案设计要采用先进的概念、技术和方法，整个系统的生命周期应有比较长的时间，保证在系统建成以后比较长的一段时间内能满足教学业务不断发展的需要。

（四）扩展性。系统必须具有良好的可扩充性，在结构、性能容量等方面必须具有升级换代的冗余性，整体网络设备应当采用模块化的结构，符合网络的发展趋势并具有充分的扩展性。

（五）高性能。网络链路和设备具备足够高的数据转发能力，保证各种信息的高质量传输；交换系统具有较高的交换容量与多业务服务支撑的能力，保证网络服务的质量。

（六）可管理性。整体网络必须具有较强的易于管理和维护的特性。

（七）开放性和标准化。网络方案设计必须遵循国际标准化组织提出的开放系统互联的标准,设备和系统能对第三方进行标准兼容，整体网络具有良好的可扩展性、可移植性和互操作性。

3.4.2 建设模式

教育网传输网络的建设模式包括：租用运营商裸光纤、租用运营商信道、自行铺设光纤三种，从建设投入、建设效率以及后续维护专业性角度考虑，建议优先选择租用运营商信道模式实施建设。

3.4.3 架构设计

根据国家 IPv6 发展战略，本项目方案在原有高校互联网络基础上实施升级改造，以 IPv6 为网络基础协议。本项目方案全面支持 SRv6。在具备条件的环境下，近期内，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。未来通过 IPv6 技术实现教育骨干网多业务承载及运维，加大主干带宽，提升网络互联互通能力，并扩展连接范围，持续支撑中小学学校信息化应用的需要。为了保证全自治区教育信息化的可靠稳定、大带宽流量的需求，满足未来教育应用发展的支撑，保障网络具有良好扩容和可靠快速收敛。初步考虑有两个组网方案，两个方案对比分析如下:

方案 1：汇聚节点双上联至一个核心节点

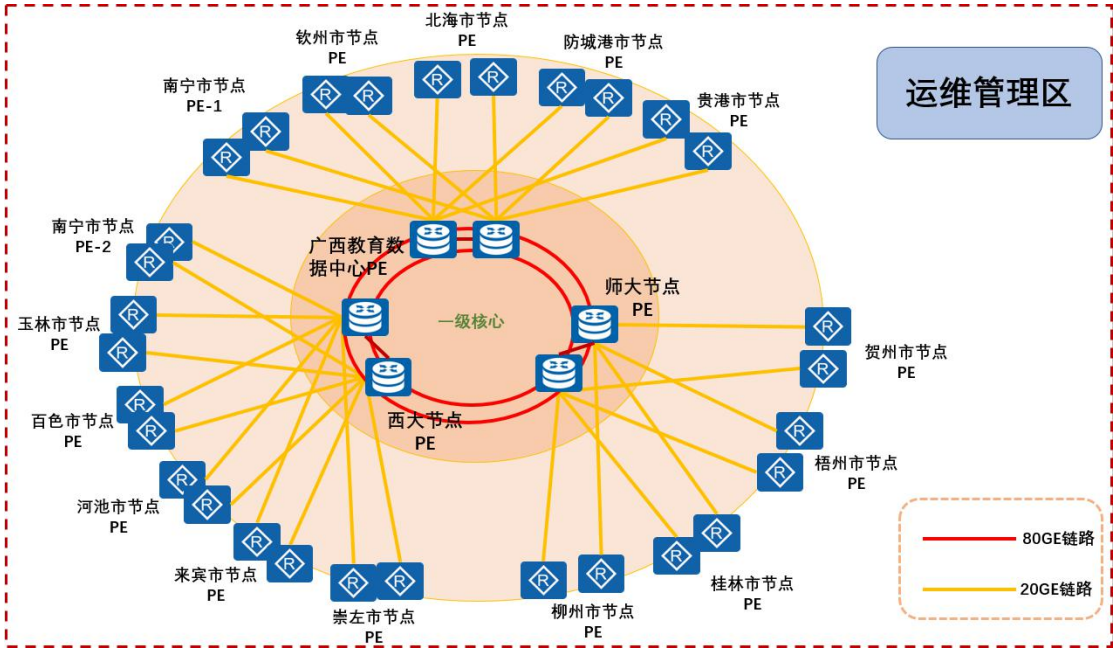

图 5-2 教育骨干网节点图方案 1

方案 2：汇聚节点双上联至两个核心节点

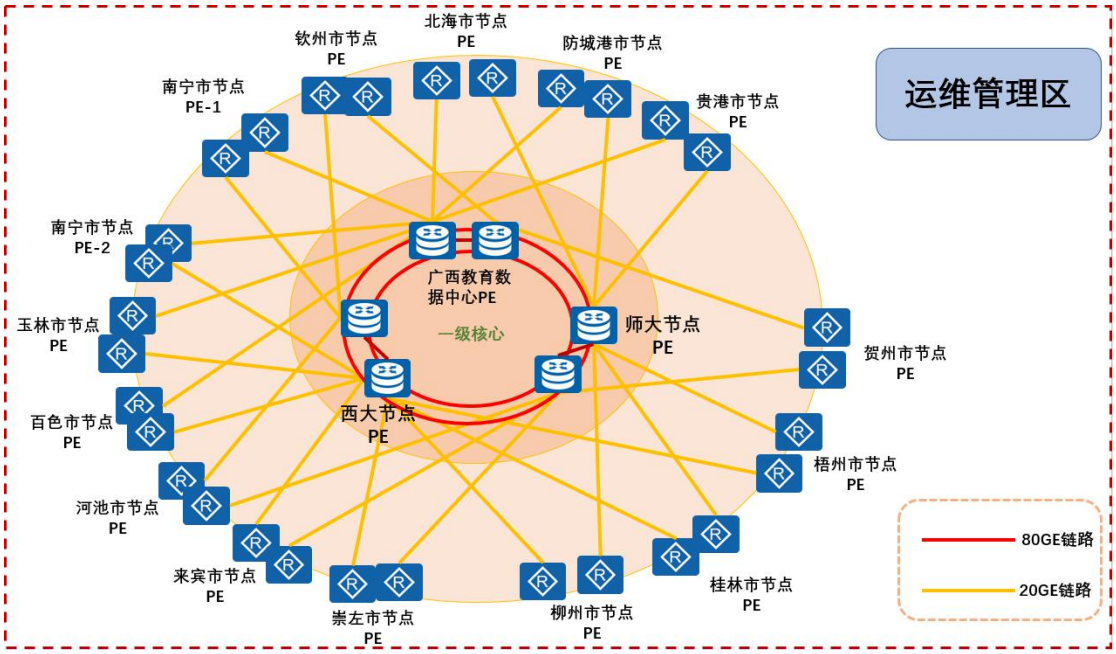

图 5-3 教育骨干网节点图方案 2

核心-汇聚层 组网方案	方案 1: 汇聚节点双上联至一个核心节点	方案 2: 汇聚节点双上联至两个核心节点
路由规划	上联同一节点，路由规划部署相对简单	上联双节点，路由规划部署较为复杂
安全性	同节点双设备配置已经有一定安全性保障，但是存在同节点双设备故障风险	避免同节点设备故障，安全性相对较高
传输链路成本	传输链路数量一致，但是方案 2 部分链路长度增加，供应商链路成本及网络时延会相应增加	
运维复杂度	运维复杂程度基本一致，方案 2 对各机房运维联动性相对要求高些	
应用场景	政企网络组网应用较多	通信运营商网络组网应用较多

考虑到方案 2 会增加教育网工程实施复杂度，而且方案 1 安全性基本已经可以满足教育网运行要求，建议本项目建设选择方案 1（汇聚节点双上联至一个核心节点），后续根据网络业务流量承载情况及链路带宽规模再评估进一步优化完善。

（一）核心环路。广西教育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，各新建两台核心路由器，通过租用 2 家运营商线路组成双环网，教育骨干网核心环总带宽不小于 80G（首次开通带宽不小于 20G）。

（二）市级节点部分。本项目在 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），各新建 2 台汇聚路由器，通过 2 家运营商就近接入核心节点，每个汇聚节点总带宽不小于 20G（首次开通带宽不小于 2G）。

鉴于北海市、防城港市的中小学整体规模较小，目前教育应用的整体流量需求较低，且其属地高等院校支撑高校城市节点建设、管理、运维的条件较弱，建议在钦州市（北部湾大学）设置汇聚节点，北海市和防城港市所辖的教育城域网全部接入钦州市（北部湾大学）汇聚节点。将来，北海市和防城港市的中小学整体规模上升后，再考虑单独设置汇聚节点。

3.4.4 汇聚节点规划

教育骨干网除了分担教育网流量承载和承担高校城市节点就近互联外，还承担本地的设区市级教育城域网、县级教育城域网、高等学校的网络互联。教育骨干网核心及汇聚节点选取，建议考虑以

下几个方面。

（一）教育骨干网节点选取依托现有网络情况，综合考虑机房情况、光缆路由、业务节点等多方面的因素，合理设置网络节点。

1.选择装机位置充裕、配套设施完备、光缆路由丰富等各方面条件较好的机房作为教育骨干网节点，适应未来长远发展;

2.教育骨干网节点可将业务有效疏通至其他相关节点;

3.教育骨干网与各设区市至少设置两条线路互联，市汇聚节点与城域传送网至少有两个节点互联，以保障网络的安全性。

（二）综合考虑现有传送网结构、业务需求（如种类、颗粒、流量流向等）、设备现状等多种因素，适当选择环网、口字型、星状、网状网结构。

（三）合理选择网络结构和资源配置，保证网络和业务的安全性，单处线路故障不应导致业务中断，单节点失效不应导致其它节点业务中断，单个设区市节点失效或电路中断不会导致其它设区市的业务中断。

依照以上因素考虑，初步建议各节点设置如下表:

表 5-1 教育骨干网节点表

核心节点		汇聚节点			
序号	汇聚节点	序号	设区市	设区市节点	备　注
1	广西教育数据中心（南宁）	1	南宁	广西教育数据中心	南宁市本级、兴宁区、江南区、青秀区、西乡塘区、良庆区、邕宁区、武鸣区

核心节点		汇聚节点			
序号	汇聚节点	序号	设区市	设区市节点	备　注
		2	钦州	北部湾大学	钦州、北海、防城港市本级，以及所辖的各县（市、区）
		3	贵港	广西工业职业技术学院	贵港市本级，以及所辖的各县（市、区）
2	广西大学（南宁）	4	南宁	广西大学	南宁市高新技术产业开发区、南宁市华侨投资区、南宁市经济技术开发区、横县、宾阳县、上林县、马山县、隆安县
		5	玉林	玉林师范学院	市本级，以及所辖的各县（市、区）
		6	百色	百色学院	市本级，以及所辖的各县（市、区）
		7	河池	河池学院	市本级，以及所辖的各县（市、区）
		8	来宾	广西科技师范学院	市本级，以及所辖的各县（市、区）
		9	崇左	广西民族师范学院	市本级，以及所辖的各县（市、区）
3	广西师范大学（桂林）	10	柳州	广西科技大学	市本级，以及所辖的各县（市、区）
		11	桂林	广西师范大学	市本级，以及所辖的各县（市、区）
		12	梧州	梧州学院	市本级，以及所辖的各县（市、区）
		13	贺州	贺州学院	市本级，以及所辖的各县）

在南宁设置两个汇聚节点，按照各设区市、县（市、区）学校规模以及区域，就近接入两个汇聚节点。

3.4.5 传输设计

（一）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。

（二）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 系统接入教育骨干网核心节点。

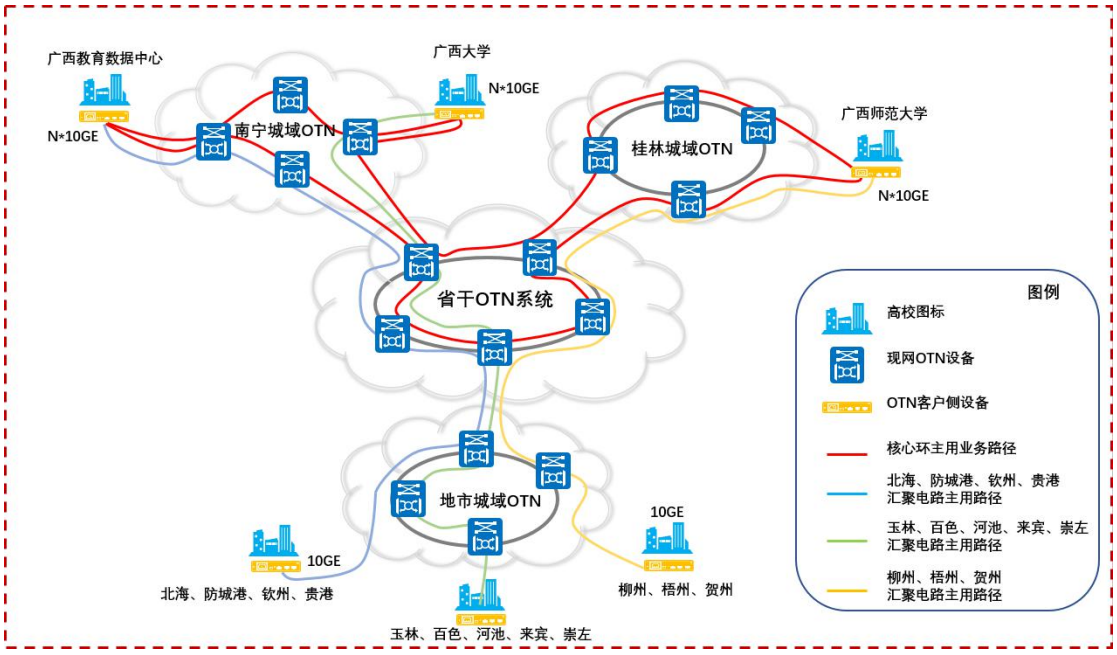

图 5-4 教育骨干网线路图

北海、防城港、钦州、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、桂林汇聚节点与骨干网核心节点共用机房，可通过光纤直连。

3.4.6 带宽要求

教育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，教育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。

3.4.7 VPN规划

（一）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。

（二）RD（Route Distinguisher，路由标示符）规划原则。

传统BGP无法正确处理地址空间重叠的VPN的路由。假设VPN1和VPN2都使用了10.110.10.0/24网段的地址，并各自发布了一条去往此网段的路由，BGP将只会选择其中一条路由，从而导致去往另一个VPN的路由丢失。PE路由器之间使用MP-BGP来发布VPN路由，并使用VPN-IPv4、VPN-IPv6地址族来解决上述问题。PE从CE接收到普通路由后，需要将这些私网VPN路由发布给对端PE。私网路由的独立性是通过为这些路由附加RD实现的。

在进行RD规划时，必须保证RD的全局唯一性。这样，即使VPN使用了同样的地址空间，PE路由器也可以向各个VPN发布不

同的路由。RD 的作用是添加了一个特定的前缀，使之成为全局唯一的 VPN 路由前缀。教育骨干网 RD 采用以下格式：16 位自治系统号：32 位用户自定义数字。

（三）RT（router target，路由目标）规划原则。

L3VPN 使用 BGP 扩展团体属性—Route Target 来控制 VPN 路由信息的发布。PE 路由器上的 VPN 实例有两类 RT 属性:

Export Target 属性: 在本地 PE 将从与自己直接相连的 Site 学到的 VPN 路由发布给其他 PE 之前，为这些路由设置 Export Target 属性;

Import Target 属性: PE 在接收到其他 PE 路由器发布的 VPN 路由时，检查其 Import Target 属性，只有当此属性与 PE 上 VPN 实例的 Export Target 属性匹配时，才把路由加入到相应的 VPN 路由表中。

也就是说，RT 属性定义了一条 VPN 路由可以为哪些 Site 所接收，PE 路由器可以接收哪些 Site 发送来的路由。RT 也必须全局进行规划。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。

（四）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。

3.4.8 路由设计

3.4.8.1 MPLS 路由设计

（一）路由规划原则。

承载网是一个大型并且相对复杂的网络系统,它覆盖多家单位，上联网络中心，承载多种网络业务，并需要具备可运营、可管理、高可用等特点。从路由设计的维度看，承载网需要重点考虑路由的收敛性、网络的可扩展性、网络的安全性和网络的可控性四个方面。基于以上这些因素，承载网路由设计原则如下。

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。

（二）路由总体设计。

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。

建议承载路由协议（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。

承载网路由总体模型如下：

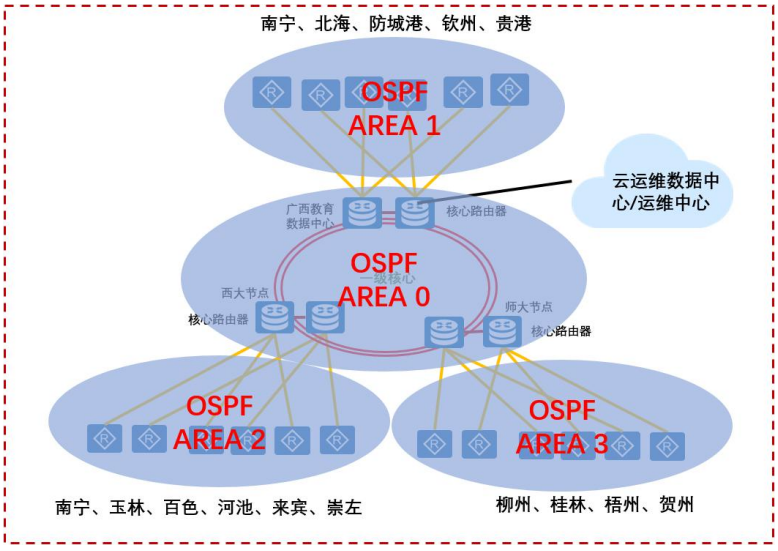

图 5-5 整网路由协议规划

（三）教育骨干网 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。指导流量在教育骨干网转发，并为 BGP 邻居关系建立提供路由可达条件。

在本项目承载网中,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。

（四）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）。

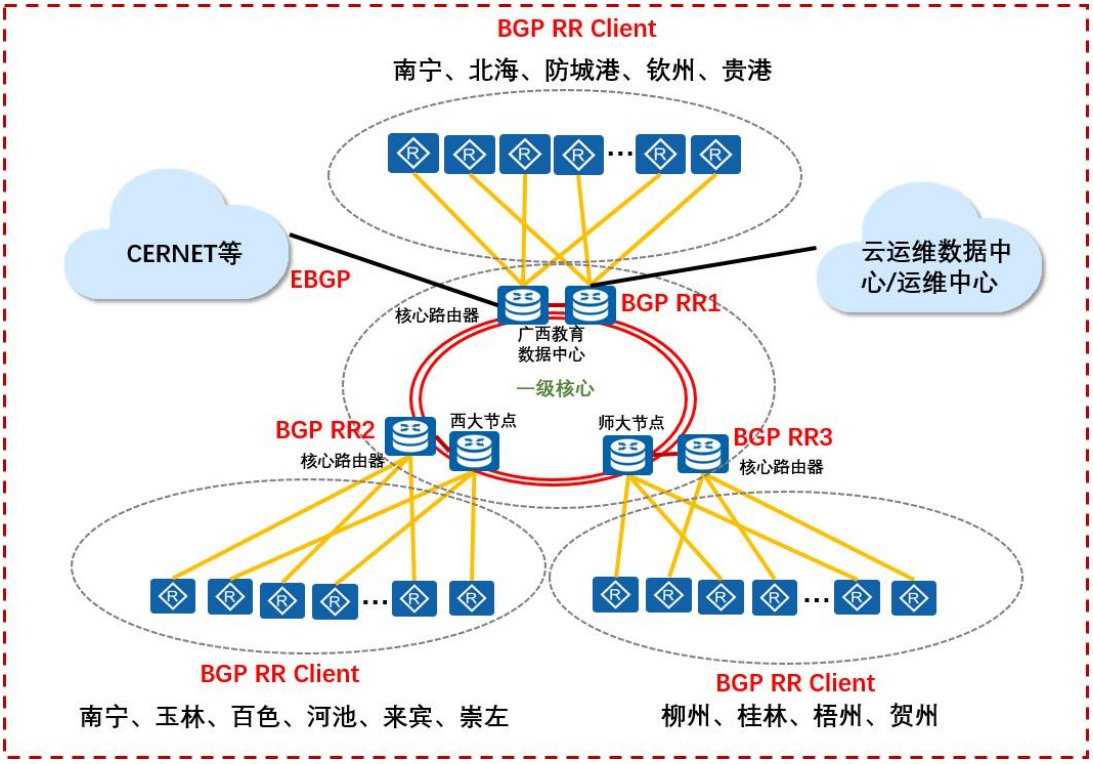

图 5-6 BGP 邻居关系

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。

（五）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。

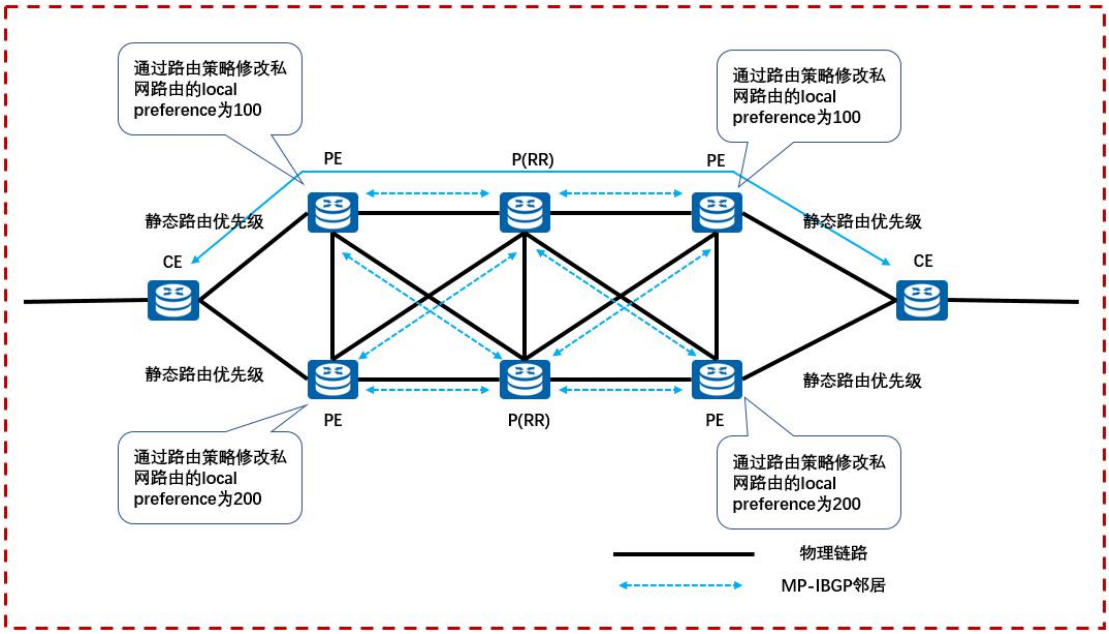

图 5-7 策略说明

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。

3.4.8.2 SRv6 路由设计

（一）IGP 路由协议。

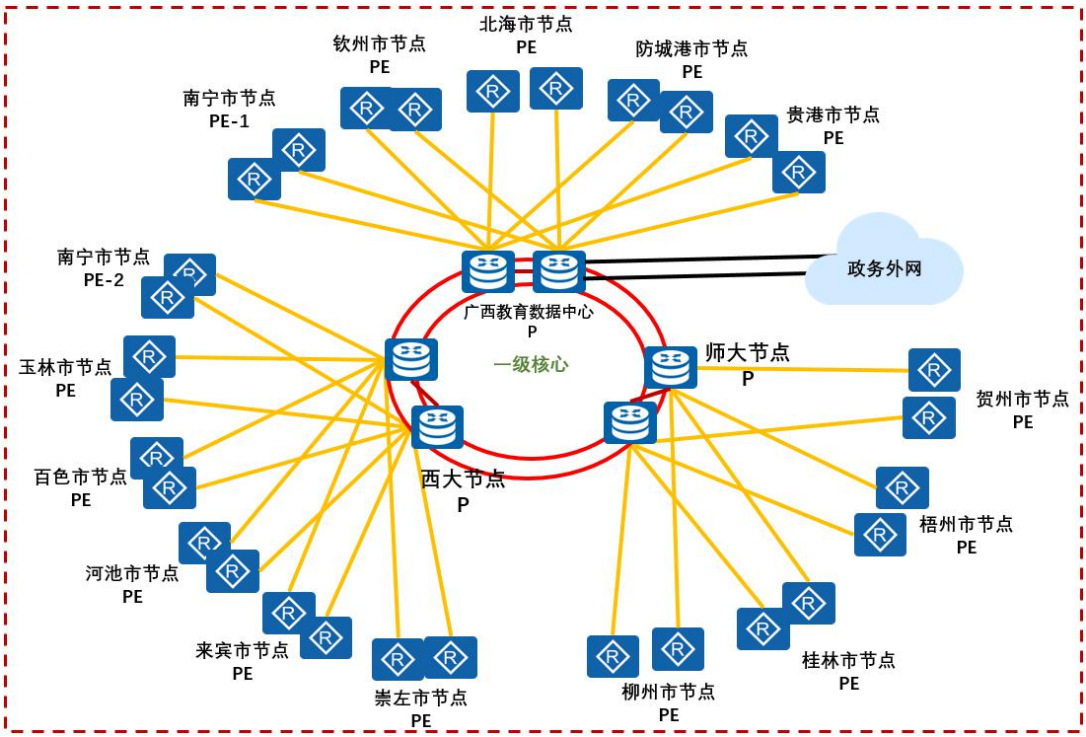

图 5-8 IGP 路由部署

教育骨干网内部采用 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，因此在教育骨干网部署 ISISv6 协议。教育骨干网规划为 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，从而学习到教育骨干网的拓扑信息和路由信息。

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

（二）MP-BGP 路由协议。

教育骨干网采用 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。教育骨干网的 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，建议在教育骨干网内部署 RR 反射器来解决这一问题。

（三）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：

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. 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；

3. 两台 RR 设备设置为同样的 Cluster ID 防止环路；

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；

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

（四）SRv6 隧道设计。

SRv6 隧道包含两种类型：SRv6 BE（SRv6 Best Effort）和 SRv6 TE Policy（Segment Routing IPv6 Traffic Engineering Policy），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 Policy 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 Policy 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。

●SRv6 BE 隧道：

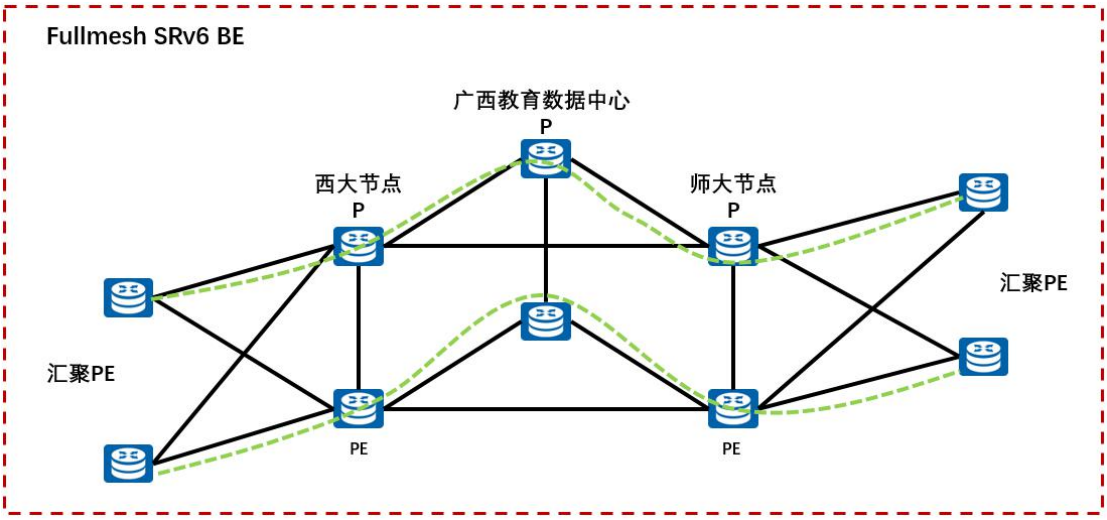

图 5-9 SRv6 BE 隧道

SRv6 BE 类似 LDP 隧道，是基于 IGP/BGP 最优路径计算出来的，当一台设备学习到另外一台设备的 Locator 路由（明细路由，聚合路由或者默认路由）后，则两台设备间的 SRv6 BE 就可以使用了。通过部署 Fullmesh 的 SRv6 BE 隧道打通教育骨干网设备之间的

数据通道。

●SRv6 TE Policy 隧道：

和 SRv6 BE 不同，SRv6 TE Policy 需要计算一条满足 SLA 要求的路径，路径计算需要实时收集带宽，时延等信息，通过具有全局视野的控制器来实现路径计算是一个比较好的选择。

控制器对 SRv6 TE Policy 的算路结果可以是严格路径（每一跳都指定链路），也可以是松散路径（只指定部分节点的链路）。在松散路径的场景下，对于未指定的节点，可以不用支持 SRv6，类似 SRv6 BE 的中间节点，这也是 SRv6 相对于 SR-MPLS 的一个较大的优势，不需要全网所有节点都支持 SRv6，只需要在容易拥塞或者时延不稳定的节点支持 SRv6。教育骨干网设备之间的 SRv6 TE Policy 隧道按需打通，提供业务 SLA 的保障。

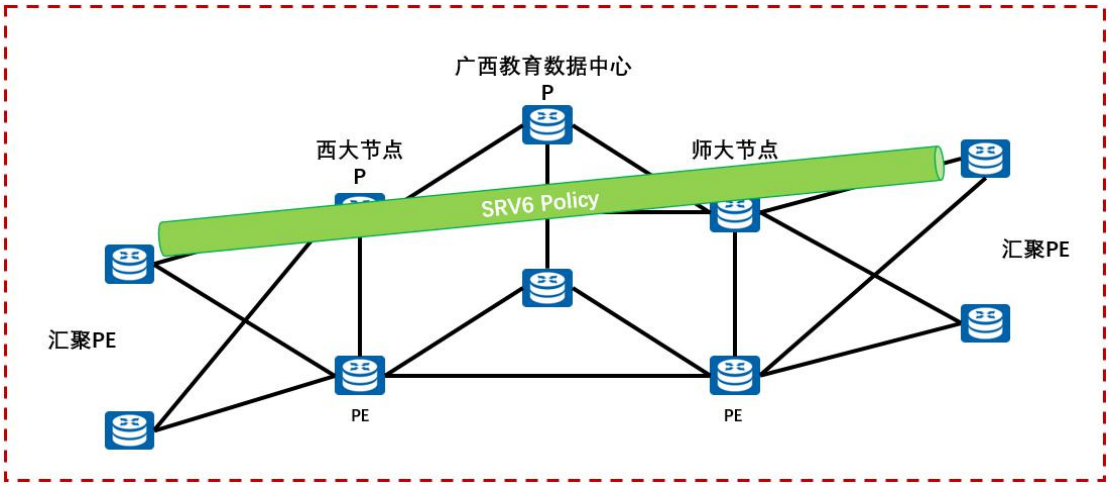

图 5-10 SRv6 TE Policy 隧道

在教育骨干网中，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 Policy 路径，结合业务和场景来选择使用不同类型的路径。

相对 MPLS 而言，SRv6 具备如下优势:

1. 简化网络协议

SRv6 通过扩展 IGP/BGP，去掉 LDP 和 RSVP-TE 等 MPLS 隧道技术,简化了控制面;在数据面直接使用 IPv6 地址作为转发标签，去除了 MPLS 标签；在控制面和数据面都实现了统一承载，极大地简化了网络协议，降低了运维的复杂度，让云、管、端可以基于同一个标准协议实现端到端可管可控，实现业务一线灵活入多云、业务敏捷开通。

2. Native IPv6 属性

SRv6 通过 IPv6 扩展报文头来实现，没有改变 IPv6 报文的封装结构，保持了对现有网络的兼容性；SRv6 依赖 IPv6 可达性可实现任意 IPv6 节点之间的互通，使得 SRv6 跨域部署更加简单；在报文转发过程中，普通中间节点仅支持 IPv6 转发即可，无需支持特殊的转发逻辑，使得 SRv6 可以打破运营商网络和数据中心网络之间的界限，进入数据中心网络，极大地增强了 SRv6 的扩展性和部署的灵活性。

3. 网络可编程能力

SRv6 的网络可编程能力体现在 SRH（Segment Routing Header）扩展头中，SRH 中有三层编程空间，SRv6 基于 SRH 的三层编程空间能够支持更多种类的封装,可以很好地满足新业务的多样化需求，

实现丰富的网络功能。

综上所述，教育骨干网采用 SRv6 技术进行路由设计。

（五）业务承载方案设计。

1.教学类业务方案设计

教学类的业务包括：课联网，云课堂，电子书包等。其中细分场景包含微课录制，电子白板，阅卷系统，名师课堂，名师网络课堂、专递课堂等。

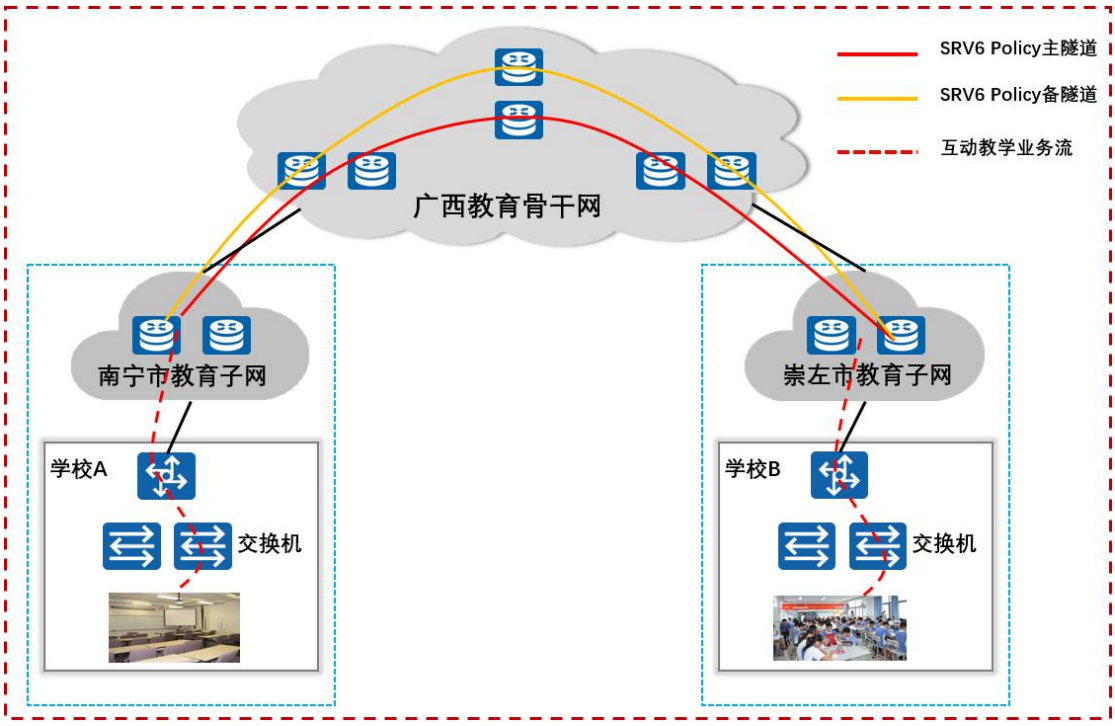

图 5-11 教学类业务示意图

对于部署在校内的应用，如电子备课、电子白板、课程录制等业务，业务流在校内即可完成交互。例如部署在校内的电子备课系统，老师通过电脑终端登录系统，访问位于校园机房的电子备课服务器，进行相关操作。

对于跨教育城域网的应用，如专递课堂，需要在主讲课堂和听课

课堂部署录播主机、摄像头、麦克风等录播设备，实现跨教育城域网的教学实时互动。跨教育城域网的互动教学业务流量需要穿越省级骨干网，针对互动教学的视频流量，省网采用 SRv6 TE Policy 技术部署专用通道，保证互动教学的稳定性和高优先级，为保证互动教学业务充分的可靠性，建议部署主备隧道，主隧道故障后可切换到备路径上保证教学业务的正常运行。

2.教研类业务方案设计

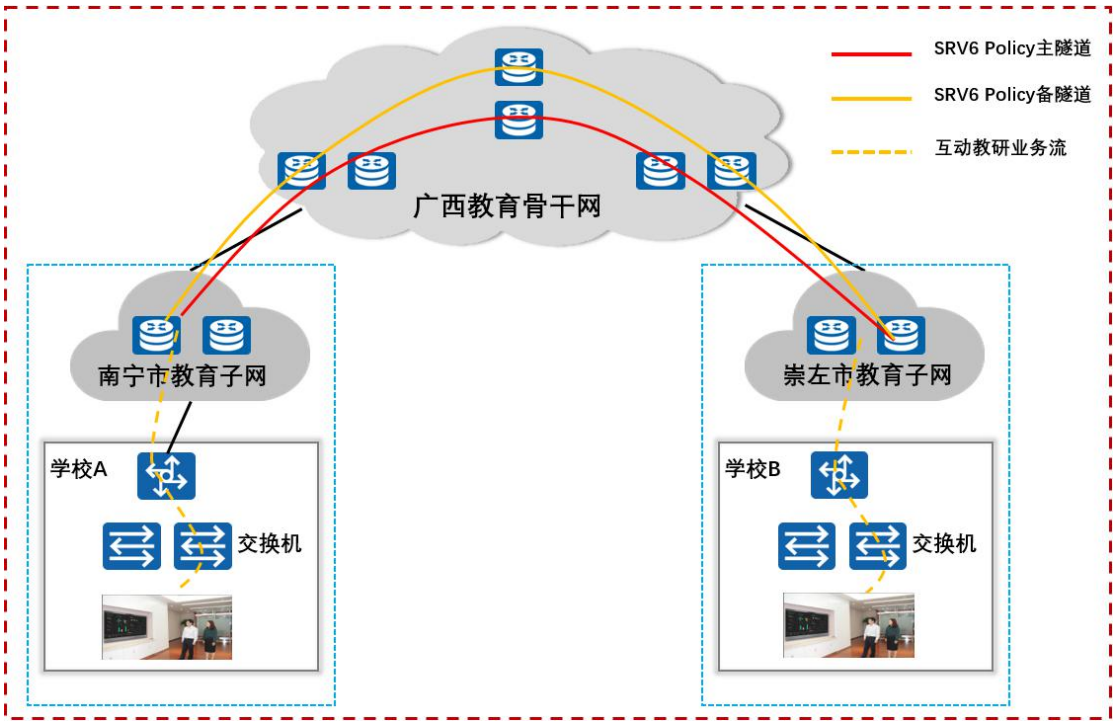

图 5-12 教研类业务示意图

教研类业务包括：教学云盘，办公 OA，语音电话，家校互动，互动教研，名师网络课堂等。办公类业务的应用场景主要在办公室，教师使用各类终端通过有线或者无线的方式接入校园网，访问办公所需的业务系统。例如，互动教研就是在学校内，采用会议大屏终端进行多个学校的教师进行互动交流研讨，采用的会议系统如钉钉、

腾讯、welink 等，互动教研的会议场景存在跨教育城域网的情况，此时，需要在省级教育骨干网提供稳定的网络环境，以保证正常、稳定的教研业务交流，在省网部署专用的 SRv6 TE Policy 视频会议通道，为充分考虑互动教研业务的运行质量，建议部署主备隧道，主隧道故障后可切换到备路径上保证教学业务的正常运行。

3.教务/办公类业务方案设计

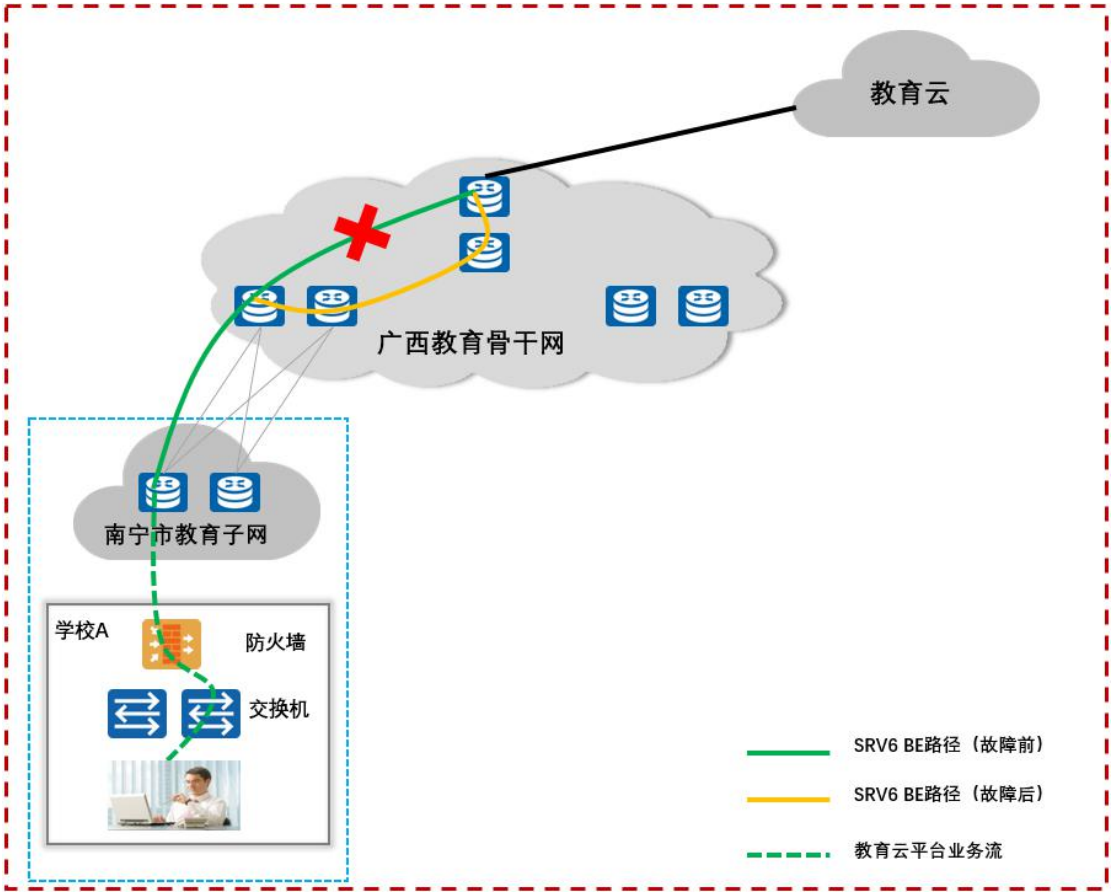

图 5-13 教务/办公类业务示意图

教务/办公类业务流：教务办公类业务多为学生、教室、学校的管理业务，其中以 OA 办公为主，教育云作为本次省网建设的内容之一，提供学校及教育机构对应的管理应用，如教育门户，教育测评，考勤管理，档案管理等。此类业务需要学校通过省网访问教育

云，优先级低于视频类业务，部署 SRv6 Be 隧道保障业务正常的访问可靠性，当隧道链路发生故障后 ，可以通过 TiLFA 机制快速切换。

4.高校互通业务方案设计

高校互访业务流：高校业务互访主要包括联合创新、学分互认等应用。近几年，我区正在推进高校学分互认政策的落地执行，通过高校之间的资源优势互补，实现优质高校教育资源的合理共享。各大高校通过省骨干网互联互通，部署 SRv6 Be 隧道保证学分互认等高校互访应用的稳定运行，当隧道链路发生故障后 ，可以通过 TiLFA 机制快速切换。

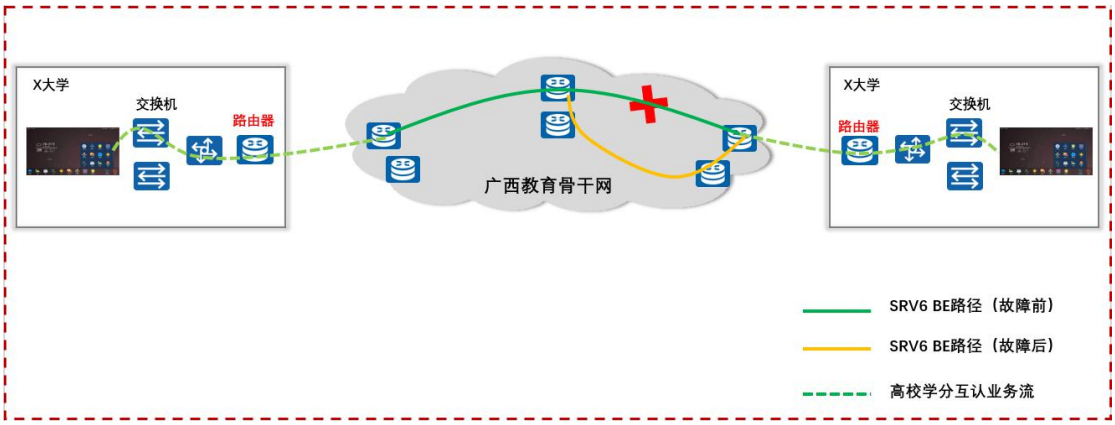

图 5-14 高校互通业务示意图

3.4.9 QoS 设计

随着网络承载的业务逐渐增加，网络流量激增，会导致网络拥塞，转发时延增加，严重时还会产生丢包，将导致实时类多媒体业务质量下降甚至不可用，因此为保障教学工作顺利开展，教育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（Quality of Service，服务质量）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。

教育骨干网针对不同的教学业务划分如下三个服务等级。

关键业务：教育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。

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。

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。

3.4.10 网络运维设计

网络运维管理上，为提高网络管理效率，采用 SDN 技术统一运维，为全面支持 SRv6，SDN 技术需支持 SRv6 Be、SRv6 Policy 等 SRv6 技术的自动部署。通过业务编排实现教育专网业务的端到端自动分钟级部署，能够满足一跳上云，业务快速开通部署的诉求。

VPN 是教育专网的最重要业务，对于 VPN 业务来说，如果采用传统的手工方法需要配置命令行，建立隧道，配置 VRF 实例等过

程，不仅对运维人员要求高而且容易因人为因素影响专网业务。基于 SDN 的 VPN 业务自动发放，应该满足以下要求:

（1）VPN 创建图形化、参数模板化。

通过层次化、可视化网络管理，提供完善的多层管理能力，实时获取网络承载关系，可视化操作，无须记忆命令行端到端可视化 VPN 及传输业务发放，利用业务模板创建业务，提升业务发放效率。

提供模板配置功能，在配置 VPN 的业务时，可以选择之前预定义的模板，快速设置业务参数，提高配置效率。

（2）提供隧道和 VPN 等业务导入功能。

可以从 excel 中配置业务参数，直接导入到管理系统中，进行业务参数检查后可以直接进行业务下发，

提供批量部署隧道的功能，选择网元和组网规则后，自动计算所有的隧道业务并统一下发配置，提高隧道部署效率。

（3）提供端到端的业务管理。

可以查看整个业务的业务状态，可以查看业务的路由信息，可以对路由进行调整。可以查看 VPN 业务的承载关系，了解资源使用情况。提供业务的复制功能，可以快速发放业务，提高业务的部署效率。

（4）VPN 隧道的可视化。

教育专网区分了不同的业务平面，并调整了网络的路径选择，使得不同级别的用户 VPN 需要通过不同的平面接入。通过隧道路径

的可视化，在 VPN 业务开通时，帮助管理维护人员确认流量是否按照规划的业务平面路径转发。

（5）网络管理可视化。

VPN 专线开通过程中，提供图形化界面管理和配置 CAR 参数、QOS 参数等速率参数。此外，教育专网还需要考虑能够可视化查看到当前各个用户单位 VPN 线路的状态,例如当前的端口速率,流量,SLA 信息等，提前预测网路状态。

3.4.11 传输线路配置

根据教育骨干网组网需求，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 100G，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 10G，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，核心环节点之间以及核心节点与汇聚节点之间的链路建议承载在至少 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教育骨干网的正常运行。

3.4.12 数据设备配置

（一）核心节点路由器。

按照教育骨干网组网需要，3 个核心节点各配置 2 台核心路由

器，总计需 6 台核心路由器;

（二）汇聚节点路由器。

13 个汇聚节点根据容量需求不同，需配置不同配置的汇聚路由器，总计需 26 台汇聚路由器。其中桂林、梧州、钦州、贵港、玉林、百色、河池节点所接入学校数超过 1000 个，教室数大于 5000 个，建议汇聚路由器配置更高的性能。

（三）同节点路由器厂家选择。

同节点路由器在实际部署时有可能出现同厂家或者异厂家两种情况，具体优缺点对比如下:

表 5-2 同节点路由器同/异厂家优缺点对比表

	优点	缺点
同厂家	便于实现设备主备、堆叠、集群等部署，后续升级不影响业务运行，便于管理维护，提高了节点整体冗余性、可用性、可维护性等。	若出现大的设备软件系统性故障，可能导致整个节点瘫痪。
异厂家	不同的业务承载在不同厂家的设备上，若其中一个厂家设备出现故障导致业务中断，不影响另一个厂家设备承载的业务。	设备难以进行主备、堆叠、集群等部署，管理维护复杂，由于是单点设备，存在设备故障、设备升级等导致承载业务中断的风险较高。

综合以上对比分析，考虑到同节点同厂家设备可以实现主备、堆叠、集群等部署，在可靠性、安全性等方面已有较大的冗余性，可维护性方面更具灵活性，未来设备升级更平滑，且出现系统性缺陷的概率较低，因此，建议采用同节点同厂家路由器进行部署。

（四）虚拟化数据处理和存储设备

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5年的运维需求,本次设计在教育骨干网的3个核心节点和10个高校城市节点配置虚拟化数据处理和存储设备，为项目管理和运维业务提供相应计算资源和存储资源。

（五）教育骨干网网络、管理及虚拟化设备需求汇总

表5-3 教育骨干网网络设备表

序号	货物名称	数量	单位	说明
1	核心路由器	6	台	广西教育数据中心、广西大学、广西师范大学各2台
2	汇聚路由器	26	台	南宁4台，柳州、桂林、梧州、钦州（含北海、防城）、贵港、玉林、百色、贺州、河池、来宾、崇左各2台
3	网络管理系统	1	套	
4	教育骨干网控制器	1	套	
5	虚拟化数据处理和存储设备	39	套	13个汇聚节点,每节点配置3套,每套包含服务器、超融合管理软件、计算虚拟化软件、存储虚拟化软件等

3.5 教育城域网

教育城域网是指在市县行政区域范围内，利用计算机网络、大数据、人工智能等技术，以光纤为传输介质，为连接本行政区域内各学校和其它教育机构的局域网的传输线路组成的网络，实现教育应用统一化，教育数据智能化分析。按行政区域管理层级和网络连接机构划分，可分为设区市本级教育城域网和县级教育城域网。

（一）设区市本级教育城域网。设区市本级教育城域网是指由设区市教育行政部门主导,在设区市行政区域内建设的教育城域网，包括：设区市本级网络中心、设区市本级骨干网、设区市所辖学校

校园网和其它教育机构网络。

（二）县级教育城域网。县级教育城域网是指由县教育行政部门主导，在县行政区域内建设的教育城域网，包括：县级网络中心、县级骨干网、县（市、区）所辖学校校园网和其它教育机构网络等。

鼓励设区市教育行政部门引领，组织所辖县级教育行政部门建设设区市行政区域内统一的教育城域网。鼓励地域相邻的县级教育行政部门组成联盟，共建共享跨县域的教育城域网。

3.5.1 设计原则

根据广西教育网整体规划，教育城域网建设方案基于星型层次化的结构设计，需遵循如下原则。

（一）层次清晰。将教育城域网划分为核心层、汇聚层、学校接入层。每层功能清晰，架构稳定，易于扩展和维护。

（二）冗余高效。关键设备采用双节点冗余设计，关键链路采用 Trunk 方式冗余备份或者负载分担；关键设备的电源、主控板等关键部件冗余备份，提高了整个网络的可靠性。

（三）体验优良。针对教学语音和视频业务，需要具备大带宽，低时延，优先保证这些实时性业务的体验。当业务出现故障时，能够秒级定界，迅速解决故障。

（四）安全可靠。教育城域网应具备有效的安全边界隔离，从终端安全、用户安全接入，用户授权访问控制再到网络中心应用层安全防护等，建立一套整网络安全体系。

（五）运维简便。网络应当具有良好的可管理性。为了便于维护，应尽可能选取集成度高、模块可通用的产品。

对于运维能力较弱的学校和教育机构，由所属教育城域网的中标服务商统一代维；对于运维能力较强的学校，可以进行分权分域管理运维，由学校管理本学校的设备和用户上网体验。

能够保证关键用户、关键业务的体验；智能识别典型网络问题，支持用户接入类问题协议回放，提升运维效率。

3.5.2 建设模式

教育城域网传输网络的建设模式包括：租用运营商信道、租用运营商裸光纤、自行铺设光纤三种。从建设成本、资源利用率、业务保障能力等多方面考虑，建议各级教育行政部门优先选择租用运营商信道的模式实施建设。

3.5.3 架构设计

教育城域网包含设区市级教育城域网及县级教育城域网，全区根据各级教育行政部门总计划分约 132 个教育城域网，每个教育城域网租用 1 家运营商网络线路，连接本地学校校园网和教育机构网络。教学点的网络互联是教育城域网建设的重要组成部分。

每个教育城域网统一建设两组网络出口。一是教育骨干网出口，租用运营商的 IP 网络线路与教育骨干网互联。二是互联网出口，租用运营商的互联网接入服务，且必须采用路由冗余设计。教育城域网内的学校和其它教育机构通过教育城域网汇聚点外联，原则上教

育城域网内的学校和教育机构不再保留互联网出口。

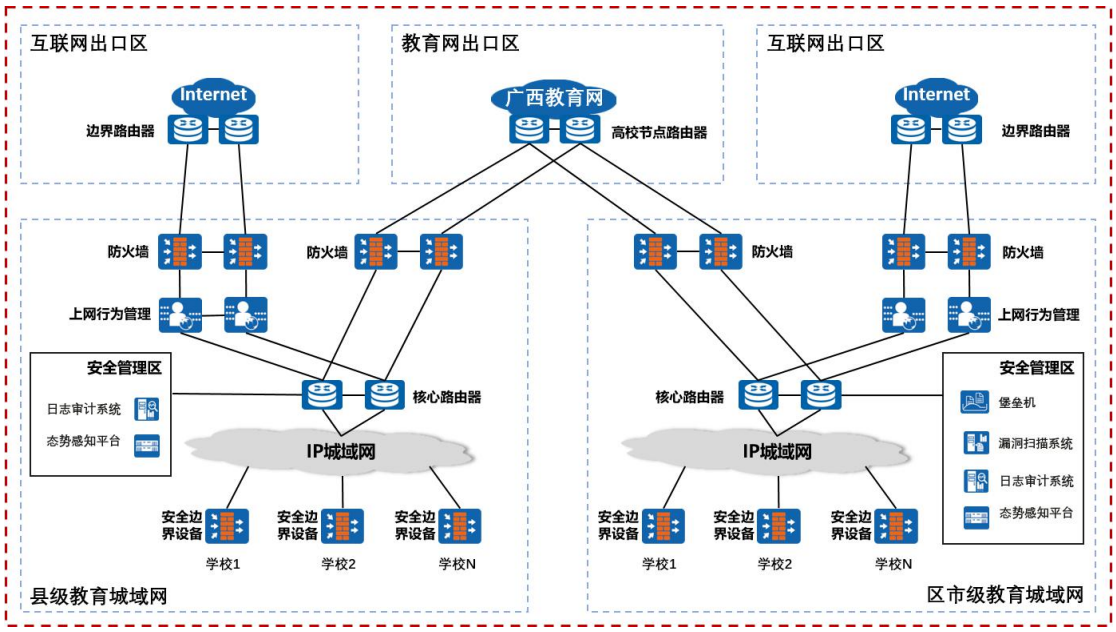

图 5-15 教育城域网组网架构

关于教育城域网与互联网互联接口应设置在各级教育城域网汇聚点，而不设置在设区市汇聚点，主要从以下几个方面考虑。

（一）出口流量规模。教育城域网出口所接入学校有限，流量相对较小，但如将业务汇聚到各设区市，出口流量将大大增加，对设备及网络资源的需求都将形成压力。如规模最大的玉林市需要连接 2988 所学校，25597 间教室，对安全管理设备容量、出口带宽需求极大。

（二）出口流量均衡。如业务在各市级出口汇聚，由于市级汇聚所带学校规模较大，业务高峰期与低谷期所需带宽有较大差距，如按照高峰需求建设，将导致建设投资加大，大部分时间设备及带宽资源处于闲置浪费。

（三）系统扩容升级。设区市级汇聚出口设备容量需要很大，

升级扩容难度也较大，如果由于部分教育城域网业务增加，需要扩容出口，设区市级出口的扩容难度较大，如果出口是建设在教育城域网，则只需要根据教育城域网业务的增加扩容相应教育城域网的出口设备。

（四）网络路由效率。从网络路由上看，县级出口较市级出口路由效率更高，通过县级出口直接访问互联网，可以减少教育城域网到教育骨干网线路的占用，避免由于需求过于集中，线路资源不足引起拥塞，影响业务体验。

（五）网络安全责任。将教育城域网与互联网互联接口设置在各级教育城域网汇聚点，按网络安全等级保护要求，各级教育城域网单独建设、管理和运维安全边界，以利于进行网络安全分级管理分级负责，落实各级党委党组网络安全责任。

3.5.4 教育城域网设置规划

广西教育网包含全区 14 个设区市、118 个县（市、区）行政区划，总计将建设 132 个教育城域网。

表 5-4 广西教育网行政区划信息表

市序号	地市	县序号	行政区划	学校数	班级数
1	南宁市	1	南宁市直属	49	3417
		2	横州市	354	3895
		3	宾阳县	266	3082
		4	上林县	166	1502
		5	马山县	148	1552
		6	隆安县	79	1210
		7	兴宁区	82	1544
		8	江南区	86	1718
		9	青秀区	108	2672

市序号	地市	县序号	行政区划	学校数	班级数
		10	西乡塘区	143	2959
		11	邕宁区	126	1272
		12	良庆区	119	1908
		13	武鸣区	159	1849
		14	南宁市经济技术开发区	40	1201
		15	南宁市高新技术产业开发区	25	993
		16	南宁市华侨投资区	9	329
2	柳州市	1	柳州市直属	15	1022
		2	城中区	20	814
		3	鱼峰区	39	988
		4	柳北区	54	1088
		5	柳南区	67	1556
		6	鹿寨县	65	1003
		7	融水苗族自治县	138	1465
		8	柳城县	94	913
		9	柳江区	86	1337
		10	融安县	44	722
		11	三江侗族自治县	172	1593
		12	柳州市柳东新区	17	397
		13	柳州市阳和工业新区	4	201
3	桂林市	1	桂林市直属	33	1399
		2	秀峰区	15	344
		3	叠彩区	15	389
		4	象山区	26	693
		5	七星区	33	729
		6	雁山区	16	203
		7	临桂区	124	1846
		8	阳朔县	88	933
		9	灵川县	92	1363
		10	全州县	255	2118
		11	兴安县	99	1008
		12	永福县	75	810
		13	灌阳县	138	933
		14	龙胜各族自治县	42	432
		15	资源县	95	572
		16	平乐县	145	1368
		17	荔浦市	94	1077
		18	恭城瑶族自治县	106	1054
4	梧州市	1	梧州市直属	21	766

市序号	地市	县序号	行政区划	学校数	班级数
		2	万秀区	48	562
		3	长洲区	46	752
		4	龙圩区	103	1208
		5	苍梧县	227	1543
		6	藤县	594	4481
		7	蒙山县	79	782
		8	岑溪市	405	4112
5	北海市	1	北海市直属	22	1004
		2	北海市涠洲岛旅游度假区	1	23
		3	海城区	33	1168
		4	银海区	50	816
		5	铁山港区	52	559
		6	合浦县	334	3941
6	防城港市	1	防城港市直属	9	475
		2	上思县	149	850
		3	东兴市	56	920
		4	港口区	30	629
		5	防城区	155	1581
7	钦州市	1	钦州市直属	13	1316
		2	灵山县	578	6456
		3	浦北县	380	3719
		4	钦南区	225	2426
		5	钦北区	309	3136
8	贵港市	1	贵港市直属	24	1702
		2	桂平市	658	7132
		3	平南县	456	5323
		4	港北区	153	2591
		5	港南区	204	2084
		6	覃塘区	168	2085
9	玉林市	1	玉林市直属	21	1045
		2	北流市	543	6799
		3	容县	337	3527
		4	陆川县	396	4172
		5	博白县	794	7401
		6	兴业县	241	2451
		7	玉州区	137	2645
		8	福绵区	142	1282
		9	玉林市玉东新区	28	640
10	百色市	1	百色市直属	9	418

市序号	地市	县序号	行政区划	学校数	班级数
		2	右江区	61	1424
		3	田阳区	38	913
		4	田东县	51	1231
		5	平果市	70	1724
		6	德保县	59	893
		7	靖西市	84	1677
		8	那坡县	56	628
		9	凌云县	55	808
		10	乐业县	30	562
		11	田林县	41	728
		12	隆林各族自治县	79	1489
		13	西林县	29	546
11	贺州市	1	贺州市直属	9	358
		2	八步区	219	2865
		3	平桂区	149	1638
		4	钟山县	183	1874
		5	昭平县	199	1687
		6	富川瑶族自治县	140	1285
12	河池市	1	河池市直属	3	191
		2	金城江区	65	1110
		3	宜州区	189	2216
		4	罗城仫佬族自治县	108	1195
		5	环江毛南族自治县	59	1016
		6	南丹县	105	1294
		7	天峨县	50	644
		8	东兰县	69	921
		9	巴马瑶族自治县	97	1126
		10	凤山县	68	821
		11	都安瑶族自治县	339	2927
		12	大化瑶族自治县	301	2015
13	来宾市	1	来宾市直属	13	572
		2	兴宾区	205	3109
		3	象州县	98	960
		4	武宣县	79	1294
		5	忻城县	98	1081
		6	金秀瑶族自治县	67	499
		7	合山市	14	287
14	崇左市	1	崇左市直属	10	604
		2	扶绥县	71	1321

市序号	地市	县序号	行政区划	学校数	班级数
		3	大新县	81	936
		4	天等县	95	1147
		5	宁明县	133	1168
		6	龙州县	43	653
		7	凭祥市	43	472
		8	江州区	47	858

3.5.5 带宽要求

依照未来业务应用规划，教育城域网与教育骨干网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。

教育城域网与互联网互联带宽设计要求：城镇学校班均出口带宽不小于10M，有条件的农村学校班均出口带宽不小于5M。教育城域网与互联网互联带宽按实际应用需要开通，在出现带宽占用率达到70%时进行扩容。

3.5.6 接入方式

各学校接入教育城域网方式有IPRAN、PTN、PON多种接入方式。

（一）IPRAN接入。

各学校通过接入就近运营商基站或者机房,通过IPRAN本地传输网，经运营商数据交换设备连接至教育城域网汇聚设备，连接至各级出口，访问网络资源。

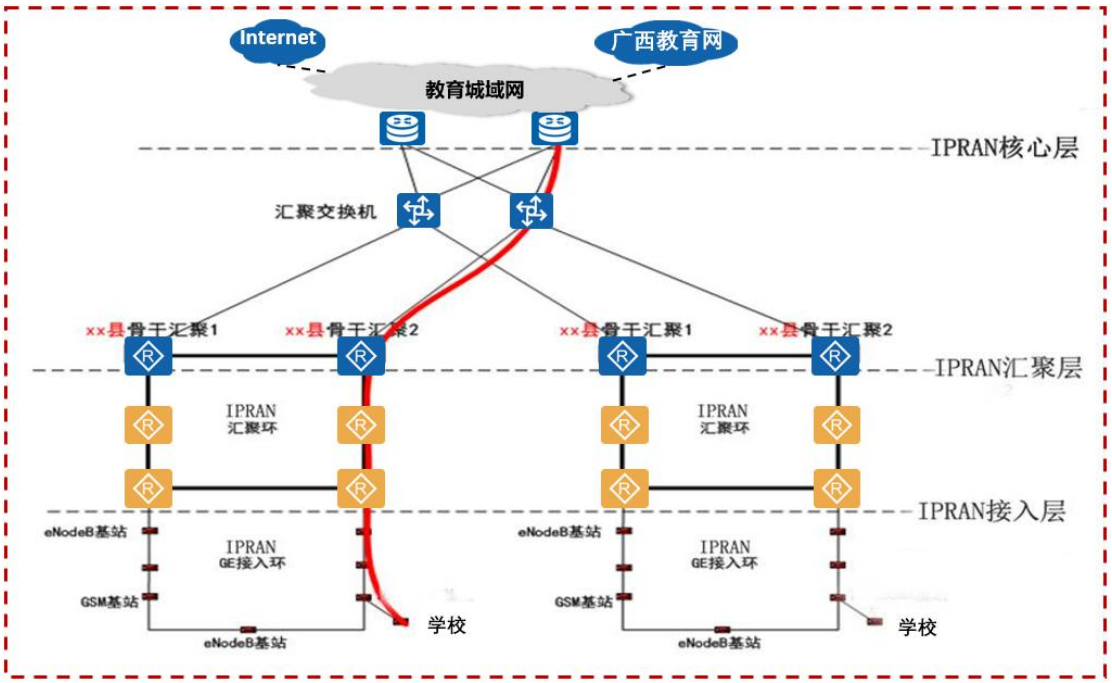

图 5-16 教育城域网 IPRAN 架构图

（二）PTN 接入。

各学校通过接入就近运营商基站或者机房，通过 PTN 本地传输网，经运营商数据交换设备连接至教育城域网汇聚设备，连接至各级出口，访问网络资源。

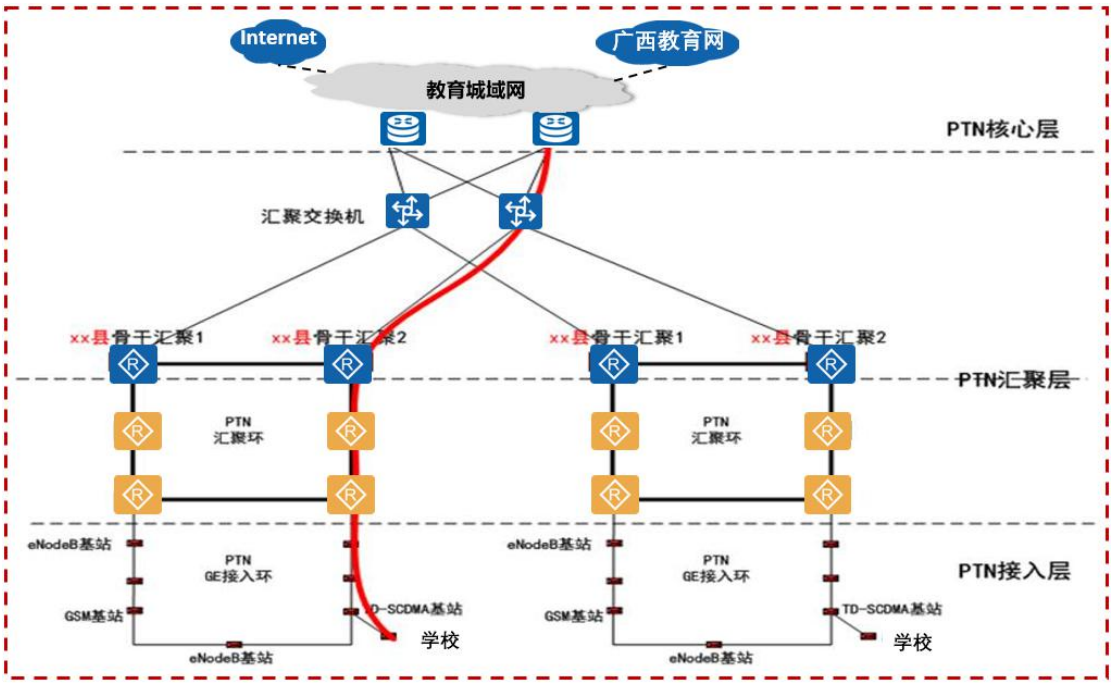

图 5-17 教育城域网 PTN 架构图

（三）PON 接入。

各学校通过 ONU 接入 OLT 设备，经 BRAS 或者 SR 设备链接教育城域网的汇聚设备，访问网络资源。

图 5-18-1 教育城域网 PON 架构图

（四）OTN 接入

各学校通过 OTN 接入运营商机房，通过 OTN 本地传输网连接到教育城域网汇聚设备，访问网络资源。

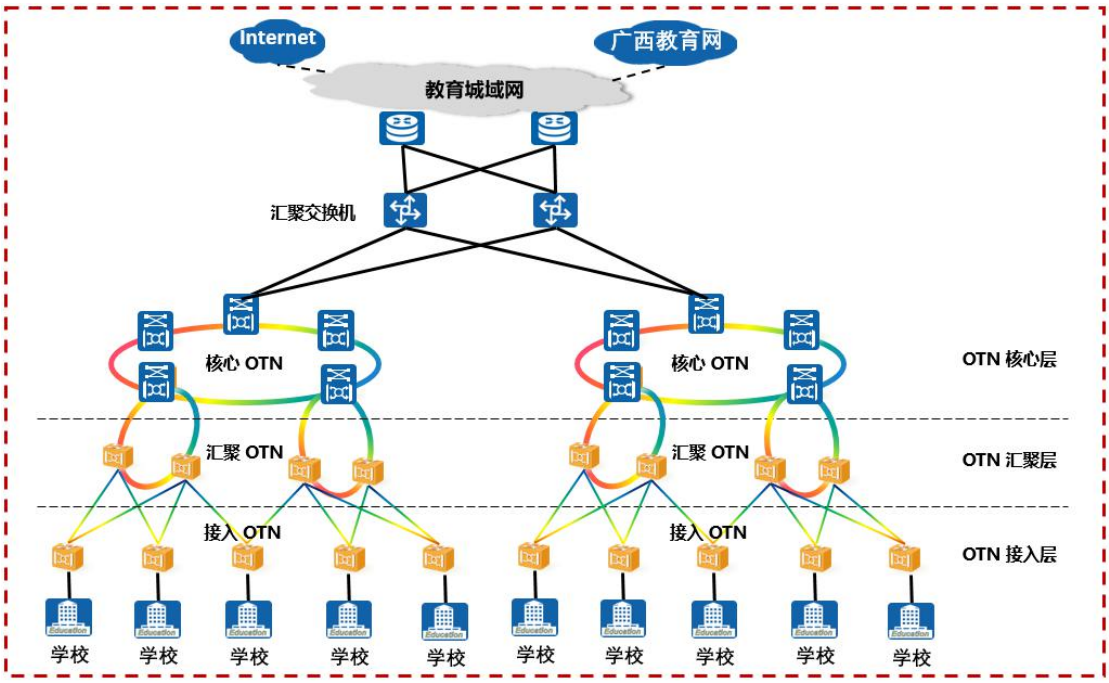

图 5-18-2 教育城域 OTN 网架构图

表 5-5 接入方式技术对比表

	OTN	IPRAN	PTN	PON
应用场景	OTN 是以波分复用技术为基础、在光层组织网络的骨干传送网。承载大带宽、低时延、有刚性管道需求的传统及新兴大颗粒重要业务	IPRAN 技术承载各类 IP 业务，并通过伪线仿真方式提供 TDM 业务，承载各行业多种需求的一般性中小颗粒专线业务	PTN 技术采用 MPLS-TP 协议，提供二层以太网业务、TDM 业务等，承载各行业多种需求的一般性中小颗粒专线业务	PON 通过 MPLS VPN 技术实现软件隔离专线组网，承载各行业多种需求的一般性中小颗粒专线业务
优点	1.多种客户信号封装和透明传输。2.大颗粒的带宽复用，交叉和配置。3.强大的开销和维护管理能力。4.增强了组网和保护能力。5.二层转发，链路保护功能完善，独享逻辑链路和带宽	支持二层和三层转发，三层转发、路由功能、IPv6 支持能力较强，与传统数通设备有良好的互通性，多业务融合承载能力强，支持带宽复用，带宽利用率高	支持二、三层（早期设备不支持）转发，链路保护能力及运维能力较强，设备转发时延低，网络规模较大，业务开通快，支持静态组网，规划及运维简单	支持二层（OLT 支持三层）转发，组网规划及运维相对简单，建设成本低，无源设备可靠性较高，支持带宽复用，带宽利用率高；故障定位快速，带宽分配灵活。

	OTN	IPRAN	PTN	PON
缺点	建设成本较高，在网络节点上、下光波长时大多采用 OADM 或 O/E/O 方式	组网规划相对较复杂，时延较高	少数早期接入层设备三层转发、路由功能等能力相对较弱	链路保护和业务 QoS 保障能力较弱，链路带宽稳定性相对不高，时延高

3.5.7 传输线路配置

各教育城域网按所属教育行政部门、接入学校和教育机构，总计需约 2 万条传输线路。各教育城域网传输线路需求如下表:

表 5-6 教育城域网传输线路需求表

市序号	设区市	县序号	教育城域网	线路数量需求（条）	合计
1	南宁市	1	南宁市直属	49	1959
		2	横州市	354	
		3	宾阳县	266	
		4	上林县	166	
		5	马山县	148	
		6	隆安县	79	
		7	兴宁区	82	
		8	江南区	86	
		9	青秀区	108	
		10	西乡塘区	143	
		11	邕宁区	126	
		12	良庆区	119	
		13	武鸣区	159	
		14	南宁市经济技术开发区	40	
		15	南宁市高新技术产业开发区	25	
		16	南宁市华侨投资区	9	
2	柳州市	1	柳州市直属	15	815
		2	城中区	20	
		3	鱼峰区	39	
		4	柳北区	54	
		5	柳南区	67	
		6	鹿寨县	65	
		7	融水苗族自治县	138	
		8	柳城县	94	
		9	柳江区	86	

市序号	设区市	县序号	教育城域网	线路数量需求（条）	合计
		10	融安县	44	
		11	三江侗族自治县	172	
		12	柳州市柳东新区	17	
		13	柳州市阳和工业新区	4	
3	桂林市	1	桂林市直属	33	1491
		2	秀峰区	15	
		3	叠彩区	15	
		4	象山区	26	
		5	七星区	33	
		6	雁山区	16	
		7	临桂区	124	
		8	阳朔县	88	
		9	灵川县	92	
		10	全州县	255	
		11	兴安县	99	
		12	永福县	75	
		13	灌阳县	138	
		14	龙胜各族自治县	42	
		15	资源县	95	
		16	平乐县	145	
		17	荔浦市	94	
		18	恭城瑶族自治县	106	
4	梧州市	1	梧州市直属	21	1523
		2	万秀区	48	
		3	长洲区	46	
		4	龙圩区	103	
		5	苍梧县	227	
		6	藤县	594	
		7	蒙山县	79	
		8	岑溪市	405	
5	北海市	1	北海市直属	23	492
		2	海城区	33	
		3	银海区	50	
		4	铁山港区	52	
		5	合浦县	334	
6	防城港市	1	防城港市直属	9	399
		2	上思县	149	
		3	东兴市	56	

市序号	设区市	县序号	教育城域网	线路数量需求（条）	合计
		4	港口区	30	
		5	防城区	155	
7	钦州市	1	钦州市直属	13	1505
		2	灵山县	578	
		3	浦北县	380	
		4	钦南区	225	
		5	钦北区	309	
8	贵港市	1	贵港市直属	24	1663
		2	桂平市	658	
		3	平南县	456	
		4	港北区	153	
		5	港南区	204	
		6	覃塘区	168	
9	玉林市	1	玉林市直属	21	2639
		2	北流市	543	
		3	容县	337	
		4	陆川县	396	
		5	博白县	794	
		6	兴业县	241	
		7	玉州区	137	
		8	福绵区	142	
		9	玉林市玉东新区	28	
10	百色市	1	百色市直属	9	662
		2	右江区	61	
		3	田阳县	38	
		4	田东县	51	
		5	平果市	70	
		6	德保县	59	
		7	靖西市	84	
		8	那坡县	56	
		9	凌云县	55	
		10	乐业县	30	
		11	田林县	41	
		12	隆林各族自治县	79	
		13	西林县	29	
11	贺州市	1	贺州市直属	9	899
		2	八步区	219	
		3	平桂区	149	

市序号	设区市	县序号	教育城域网	线路数量需求（条）	合计
		4	钟山县	183	
		5	昭平县	199	
		6	富川瑶族自治县	140	
12	河池市	1	河池市直属	3	1453
		2	金城江区	65	
		3	宜州区	189	
		4	罗城仫佬族自治县	108	
		5	环江毛南族自治县	59	
		6	南丹县	105	
		7	天峨县	50	
		8	东兰县	69	
		9	巴马瑶族自治县	97	
		10	凤山县	68	
		11	都安瑶族自治县	339	
		12	大化瑶族自治县	301	
13	来宾市	1	来宾市直属	13	574
		2	兴宾区	205	
		3	象州县	98	
		4	武宣县	79	
		5	忻城县	98	
		6	金秀瑶族自治县	67	
		7	合山市	14	
14	崇左市	1	崇左市直属	10	523
		2	扶绥县	71	
		3	大新县	81	
		4	天等县	95	
		5	宁明县	133	
		6	龙州县	43	
		7	凭祥市	43	
		8	江州区	47	

3.5.8 数据设备配置

教育城域网网络设备数量需求如下表。

表 5-7 教育城域网网络设备表

序号	货物名称	数量	单位	说明
1	汇聚路由器	264	台	每个教育城域网配置 2 台

序号	货物名称	数量	单位	说明
2	汇聚交换机	264	台	每个教育城域网配置 2 台

3.5.9 对于已建教育城域网建议

目前我区部分县（市、区）已自建教育城域网，但不符合本项目建设、管理运维、应用的技术规范，基于减少重复投资，减少重复建设，保障国有资产使用效益，以及项目建设平稳过渡的考虑，建议采用一地一案的方式，对这些教育城域网络进行认定和处置。在实施项目建设时，认定一批有技术条件、可在短时间内升级改造到符合本项目技术规范的教育城域网；对通过认定的教育城域网，可由教育城域网的供应服务商与教育城域网的教育行政部门友好协商达成一致，签订相关网络服务的补充协议，限时按本项目技术规范完成教育城域网升级改造，然后继续提供网络服务。

3.5.10 对于教育城域网互联网汇聚点建设的建议

鉴于我区设区市、县（市、区）教育行政部门、通信运营商的机构设置和人力资源配置的差异，为了提高教育城域网建设、管理和运维的效益，减少网络安全暴露面，提高网络安全等级保护保障能力，鼓励设区市和县（市、区）教育行政部门、县（市、区）教育行政部门之间加强联合，建设跨行政区域的城域网，鼓励通信运营商统筹协调内部网络资源，减少教育城域网与互联网物理外联汇聚点。

各教育城域网应建设统一的互联网出口汇聚点，若由通信运营

商统筹协调建设与互联网物理外联汇聚点的，应清晰地划分本级教育城域网互联网连接的逻辑边界，应落实互联网连接费用的划分，落实网络建设、管理、运维、网络安全的主体责任。

3.6 校园网

校园网是教育城域网的延伸，在校园网建立基础通信网络，为教育信息化服务在校园落地，提供网络基础。

校园网是指在学校区域内，利用计算机网络技术，通过以太网、光纤、WiFi6 等网络技术，将学校区域内信息终端连接起来的通信网络。单一校区的学校建成校园局域网，有 2 个（含）以上校区的学校还需要将各校区局域网连接起来。

本项目不包含无线网络（WiFi）建设内容，有条件的学校可以根据自身需要进行建设，建议自行建设的无线网络应满足本项目的相关技术要求，方便后续接入教育网。

3.6.1 设计原则

（一）便于管理。有线无线深度融合：有线无线用户统一认证和管理，提升用户使用体验。

1.简化管理

虚拟化技术减少设备数量，提升 IT 管理效率。

2.快速定位

智能网管快速故障定位，降低网络维护难度。

（二）业务隔离。采用 VLAN、VXLAN 等技术手段隔离。

（三）安全可靠。

1.安全防护

出口防火墙针对多出口实现智能选路，基于用户、应用、内容、时间、位置、威胁进行应用层的安全防护和管控。

2.入侵防御

入侵防御抵御漏洞攻击。

3.6.2 架构设计

校园网采用光纤或以太网电缆连接教室、计算机教室、办公室等学校各功能区域信息终端，校园网出口用光纤上联教育城域网汇聚点。有条件的学校要在校园网络基础上建设满足教学需要的无线网络（WiFi）。现有校园网络能够满足教学需要，且能与教育城域网匹配的，应该保留继续使用，逐步过渡到符合教育网建设技术规范的光纤网络。同时，根据各学校实际情况，运营商在搭建校园有线网络时需要预留无线网络接入的传输链路，满足学校未来的无线教学需求。

表 5-8 校园网规模分类表

类别	接入带宽	学校数量（个）
农村及以下学校	1G	15694
乡镇所在地学校	1-10G	2974
城市所在地学校	1-10G	940

根据学校班级数规模可将学校分为三大类,即农村及以下学校、

乡镇所在地学校和城市所在地学校。根据教育部要求，每个学校的接入带宽应不低于 1G，但是考虑农村、乡镇、城市学校的规模有一定的差异，建议根据实际需要开通带宽。

（一）农村及以下学校。

农村及以下学校因班级数量规模较小，可参照如下图方案一的网络架构进行配置校园网，利用接入交换机和汇聚交换机两层架构，通过安全边界设备接入教育城域网。农村及以下学校校园网还可以采用 PON 组网方式，参照 EPON/GPON 或 XG/XGS PON/10G-EPON 或更高带宽的 PON 网络技术标准，光纤直接进入各教室，并在各学校教室放置 ONU，通过无源光网络接入 OLT 设备，OLT 设备通过光缆直挂 MSE/BRAS 设备，实现学校班级同时访问互联网、教育网，并提供班级与班级、班级与学校之间的互访功能。

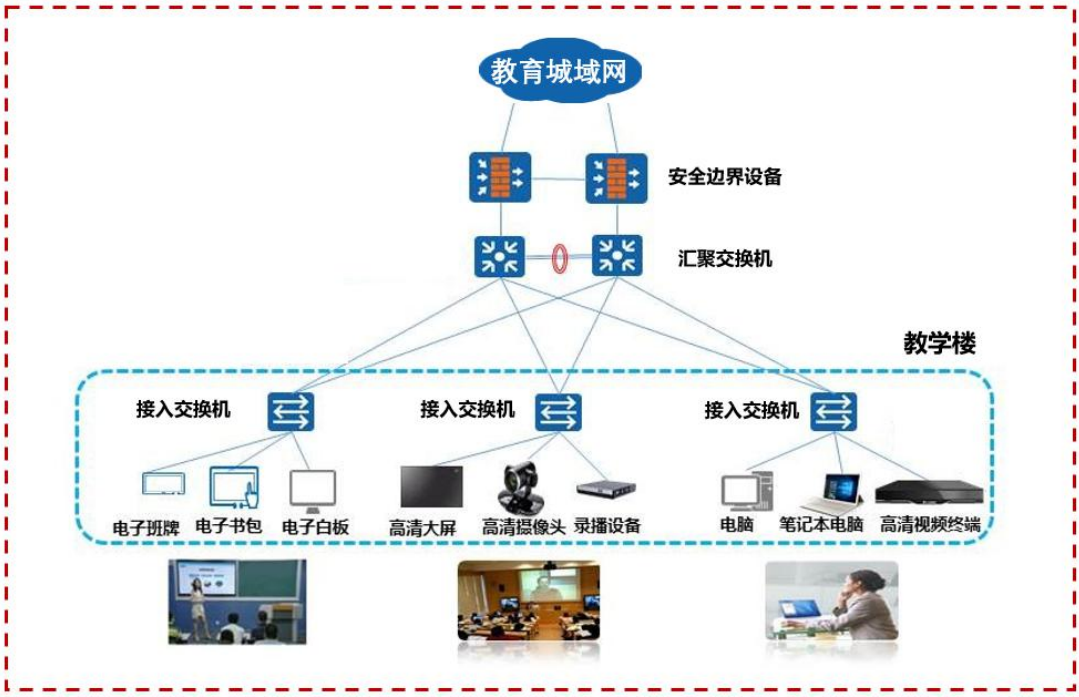

图 5-19 校园网网络架构方案一

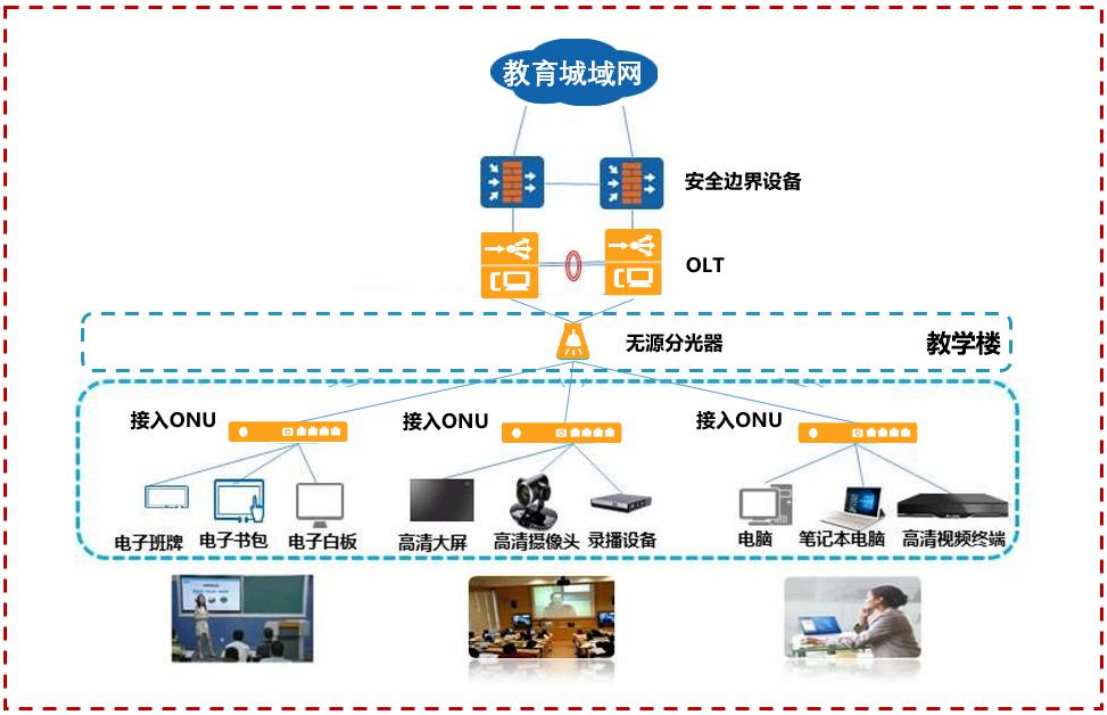

图 5-20 校园网网络架构方案二

（二）乡镇所在地学校。

对于班级数量在 13-36 个的乡镇所在地学校，考虑到班级较多，因此建议按照三层交换架构（参照图 5-21）或者采用 PON 组网的方式（参照图 5-21-1）部署网络接入教育城域网

对于班级数量在 12 个及以下的乡镇所在地学校，由于其需求与农村学校相似度较高，建议参考农村学校方式组网。

图 5-21 乡镇学校网络架构（班级规模 13-36 个）

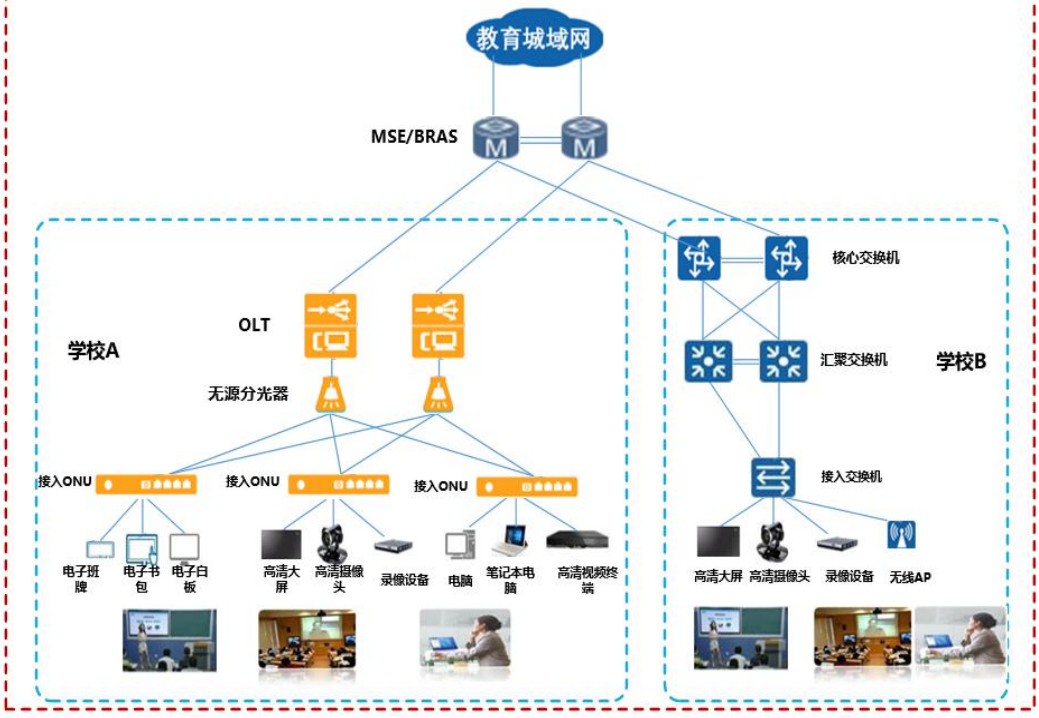

图 5-21-1 乡镇学校网络架构（班级规模 13-36 个）

（三）城市所在地学校。

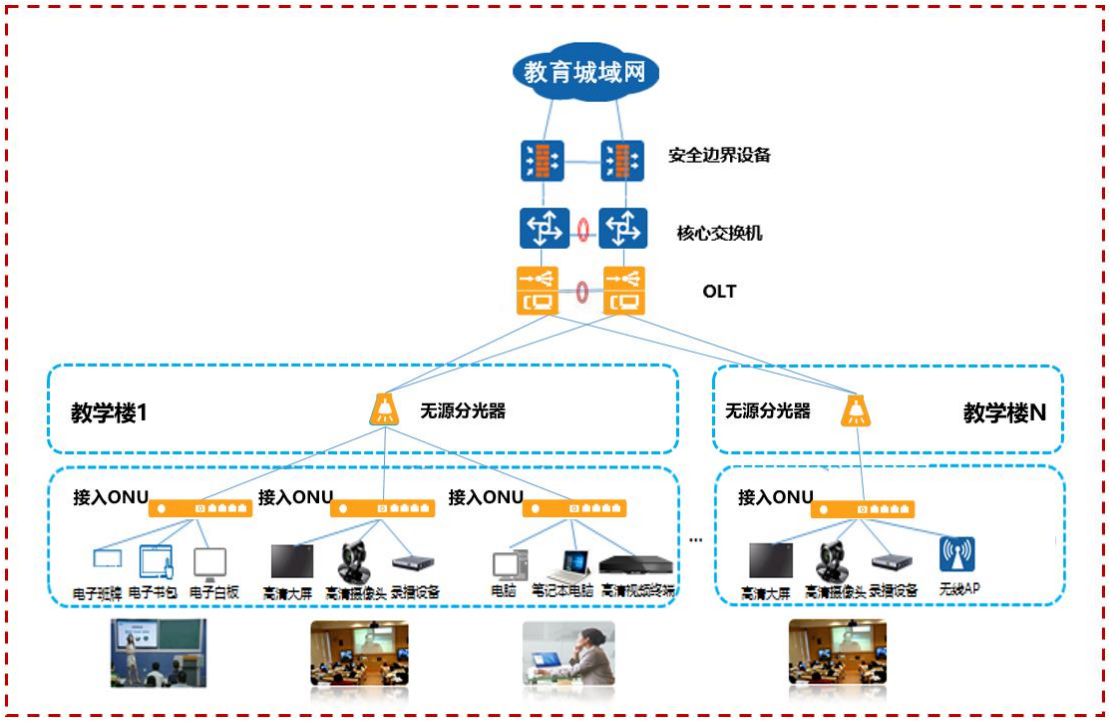

图 5-22 城区学校网络架构

城市所在地学校根据规模大小选择不同的建设模式：建议中小规模的学校参照乡镇学校采用三层交换架构（参照图 5-21）或者采用 PON 组网的方式（参照图 5-21-1）部署网络接入教育城域网；建议班级规模较大的学校校园网络采用“一张网”的融合网络建设模式，一张网涵盖有线、无线接入，整体统一管理，并根据业务进行隔离。可以采用三层组网架构或者 PON 组网的方式建设。

校园网有线网络建设根据不同场景及具体需求可以采用接入端双绞线方式的交换机组网、接入端光纤方式的 PON 全光网络组网，或两种方式进行融合进行建设。PON 全光网络建议采用 EPON/GPON 或 XG/XGS PON/10G-EPON 或更高带宽的 PON 网络技术标准; 校园有线网采用交换机和 PON 组网方式都能做到全网的统一管

理，同时，ONU、接入交换机、AP 均可以做到统一下发配置，减轻运维人员的运维负担。

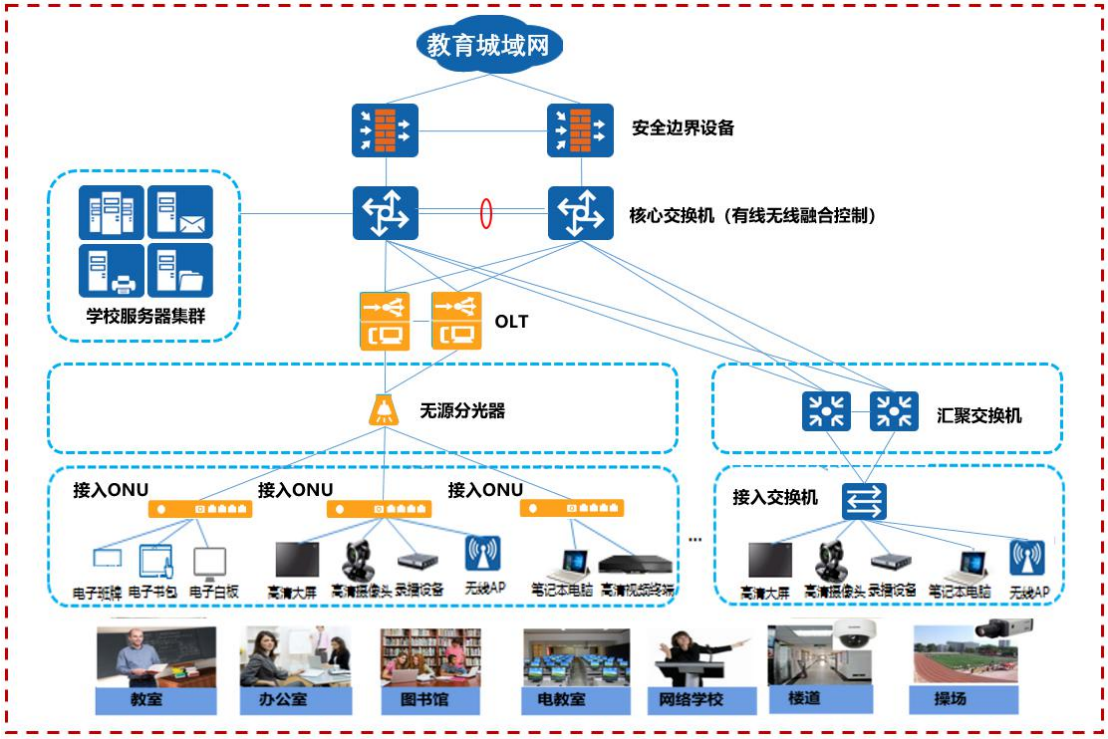

图 5-23 校园网网络拓扑图

（四）集团校区跨教育城域网建设方案。

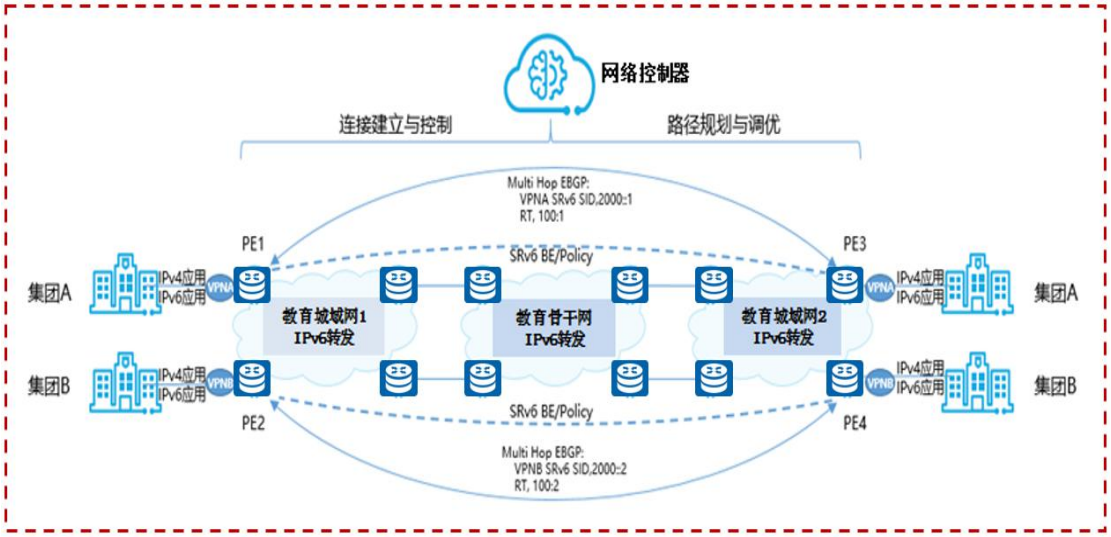

图 5-24 集团校区跨教育城域网互通方案拓扑图

如上图所示，教育集团 A、B 在教育城域网 1、2 内分别存在校

区，为实现教育集团内校区的快速连接，同时不同教育集团 A-B 间访问隔离，在教育集团 A 校区边界 PE1、PE3 之间建立 Multi Hop EBGP 邻居关系，并部署集团 A 的 EVPN VPNA，通过 EBGP 邻居关系分配 SRv6 SID 及路由 RT 100:1；教育集团 B 校区边界 PE2、PE4 之间建立 Multi Hop EBGP 邻居关系，并部署集团 B 的 EVPN VPNB，通过 EBGP 邻居关系分配 SRv6 SID 及路由 RT 100:2；网络控制器可控制整网校区之间连接建立与控制，教育城域网之间及教育骨干网支持 IPv6 转发即可，无需额外配置。在教育骨干网和教育城域网支持 SRv6 时，还可对校区间连接转发路径进行规划与调优。

教育集团 A、B 之间通过 EVPN 进行逻辑隔离，确保 A\B 之间业务安全；教育集团内校区同属于一个 EVPN，可实现互联互通。教育城域网间校区通过 SRv6 隧道一跳直达，避免了跨区域协调，实现了业务快速下发。

（五）无线校园建设方案。

图 5-25 校园无线网络

无线校园的建设是实现班班通的必经之路，在全国的很多省市地区都开始了全面建设。通过打造稳定、高效、敏捷、泛在的无线校园网，支撑课前、课中、课后三个阶段的教育资源共享与传输。通过构建“泛在的网络”来全面支撑“泛在的学习”，真正在达到“人人皆学、处处能学、时时可学”的泛在校园学习环境。

在校园内部打造泛在的高性能无线网络，支撑泛在学习。支撑学校的教学、管理以及相应的校园服务。

无线漫游。覆盖区域内无线漫游，用户终端从一个 AP 覆盖范围移动到另一个 AP 覆盖范围，无需重新登录和认证。

精细化控制。老师、学生、访客不同的角色拥护不同的权限，且教师和学生之间要隔离，限制教师和学生互访。

多用户调度。AP 能感知接入用户数量，灵活调整物理信道竞

争参数，降低碰撞几率，避免过多的用户接入同一 AP，保障服务质量和体验。

统一认证。新建 WLAN 网络必须考虑与原有有线网络之间的兼容，实现与有线网络使用同一个账号、密码进行认证，并获取相同的访问权限。

认证方式。认证系统需要支持 Portal、MAC、802.1x 等多种认证方式，以满足不同场景下，不同群体（老师，学生，访客）的接入认证需求。

AP 设备。室外 AP 设备的防尘、防水的防护等级达到 IP67 要求，同时 AP 具有 5kV 防雷器，减少工程施工和网络运维的困难。

AC 设备。AC 支持 1+1 热备份，解决 AC 单点故障问题。

网络链路。本地转发模式下，若遇到 CAPWAP 隧道中断、AC 故障、控制链路错误等问题时，AP 可进入半自治状态，继续对终端业务数据进行转发，业务不中断，保障用户体验。

网络监控。通过网管软件查看当前设备物理拓扑，直接显示设备间连接关系，监控设备及链路状态。通过 WLAN 业务拓扑监控无线设备告警、状态、网络设备逻辑结构，包括 AC、AP、终端用户、非法 AP 的逻辑连接关系及其详细信息，并在拓扑提供一定故障诊断处理能力。

故障恢复。通过网管远程批量重启 AP，恢复 AP 配置。通过网

管快速完成 AP 替换，替换后业务不变。

3.6.3 带宽要求

为保障校园应用的效果，教室应采用光纤接入校园网，考虑到部分地区学校已建设非全光网络，为避免重复投资建设，短期内建议利旧现有满足业务需求的非光纤接入方式，后续逐步升级改造成全光网。校园网主干设计带宽不小于 1G。

（一）设区市城市、乡镇所在地的学校。

教室下行带宽不少于 100M，上行带宽不少于 100M，配置不少于 4 个 100M 的 RJ45 端口。计算机教室下行带宽不少于 200M，上行带宽不少于 200M，配置不少于 8 个 100M 的 RJ45 端口（其中至少 2 个 1000M 自适应端口）。

（二）农村学校（教学点）。

教室下行带宽不少于 100M，上行带宽不少于 30M 带宽，配置不少于 4 个 100M 的 RJ45 端口。计算机教室下行带宽不少于 200M，上行带宽不少于 60M 带宽，配置不少于 8 个 100M 的 RJ45 端口（其中至少 2 个 1000M 自适应端口）。

3.7 电子政务外网互联方案

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。

3.7.1 高等院校、区直中等职业学校、教育城域网接入电子政务外网方案

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做强逻辑隔离。

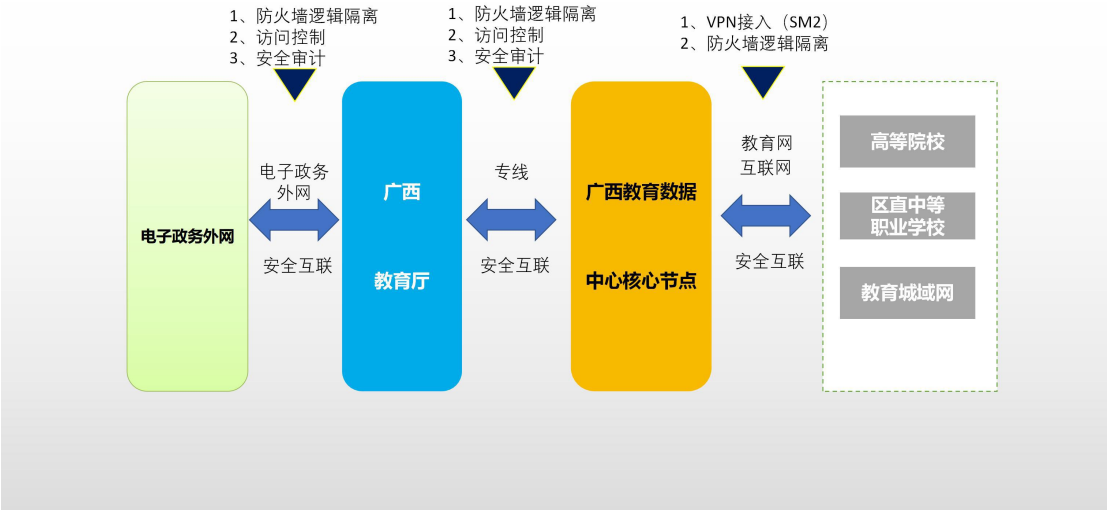

图 5-26 高等院校、区直中等职业学校接入电子政务外网示意图

在广西教育网广西教育数据中心核心节点建立独立安全域，配置防火墙、入侵防御、安全审计设备，对该区域进行重点安全防护。在该安全域部署 VPN 设备，选用的 VPN 设备支持 SM2 加密算法。

各高等院校、区直中等职业学校、市县教育城域网接入电子政

务外网有两种方式:

1.接入广西教育网骨干网，通过广西教育网连接广西教育网广西教育数据中心核心节点的 VPN 设备，接入电子政务外网。

2.通过互联网连接广西教育网广西教育数据中心核心节点的 VPN 设备，接入电子政务外网。

广西教育数据中心通过专线连接到自治区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、公文流转等应用系统。广西各级各类学校政务流量通过访问电子政务外网实现。

为满足广西教育网和广西电子政务外网日益增长的数据共享交换应用需求，下一步计划申请专线，由广西教育网广西教育数据中心核心节点直连广西电子政务外网。

3.7.2 各级教育行政部门接入方案

1.访问教育应用系统接入方案

目前，广西各级教育行政部门通过电子政务外网接入点就近接入电子政务外网，并通过电子政务外网互联网出口访问教育网的相关应用系统。待教育网建设完善后，各级教育行政部门改为通过电子政务外网的互联交换区直连教育网访问相关应用系统。

2.访问互联网方案

广西各级教育行政部门通过本级电子政务外网统一互联网出口访问互联网业务。

3.访问电子政务外网公共网络区方案

广西各级教育行政部门访问电子政务外网公共网络区业务通过电子政务外网广域网实现。

3.7.3 安全防护方案

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自治区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。

（一）访问控制。

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．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。

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。

（二）入侵防范。

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．对病毒和入侵攻击行为进行实时告警及阻断。

（三）安全审计。

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．记录公用网络访问行为、网络地址转换日志等信息。

3．审计信息保存 6 个月。

（四）集权安全区。

根据上述要求，本项目将构建“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，区域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。

1．高等院校、区直中等职业学校接入电子政务外网安全防护方案

现阶段各高等院校、区直中等职业学校通过互联网VPN拨号访问电子政务外网，访问路由如下图。

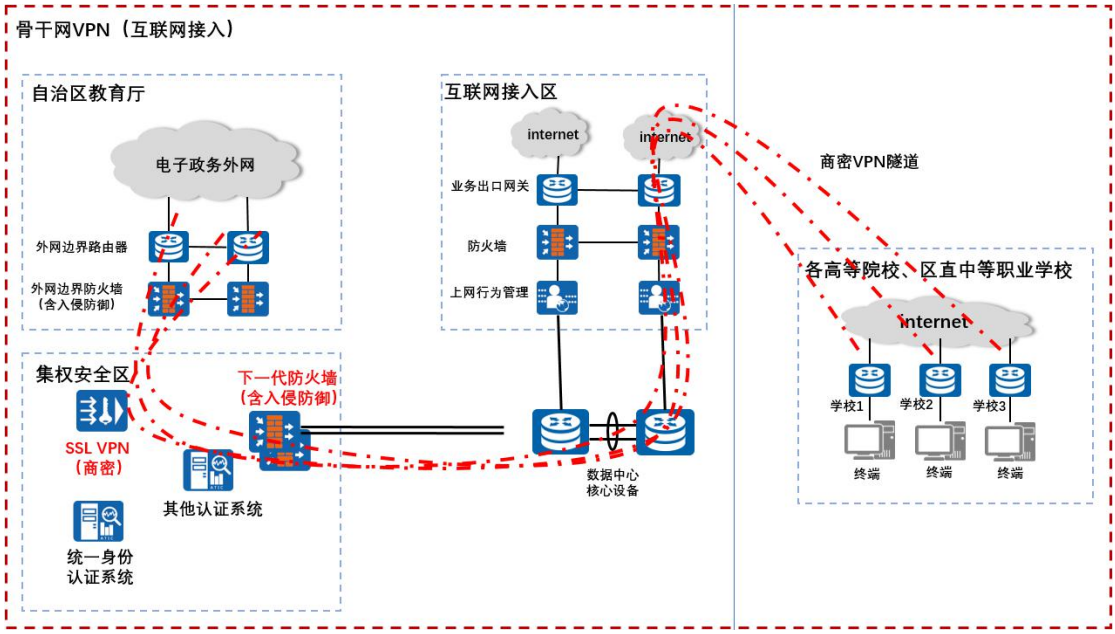

图5-27 高等院校、区直中等职业学校（互联网接入）访问电子政务外网路由图

待教育网建设完善后，各高等院校、区直中等职业学校改为通过教育网VPN拨号访问电子政务外网。

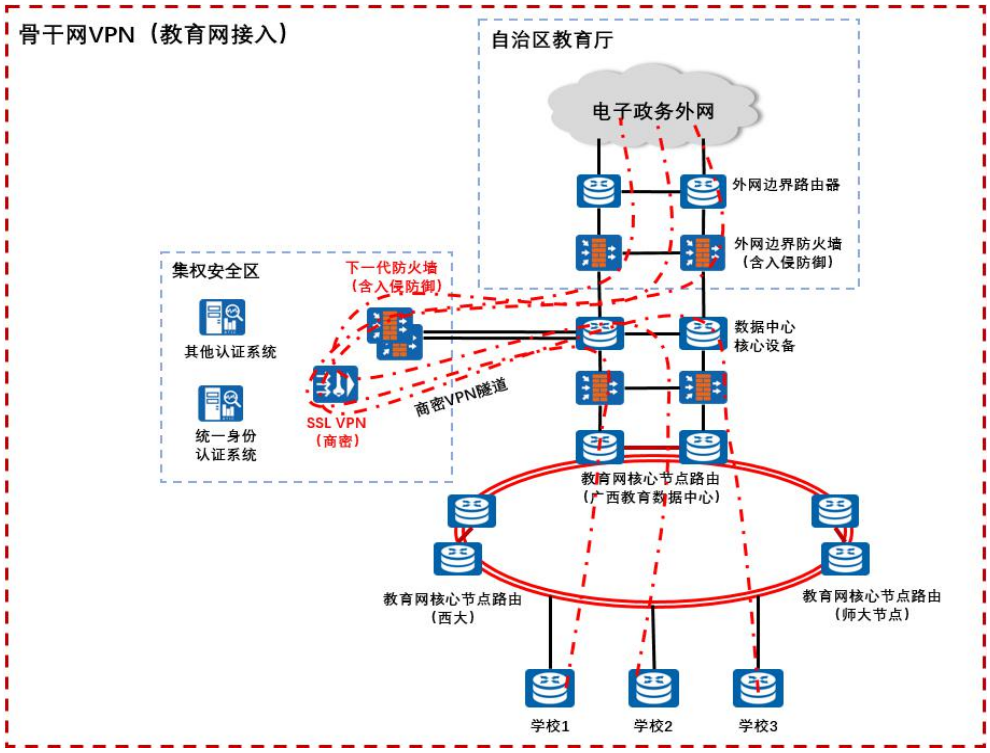

图 5-28 高等院校、区直中等职业学校（教育网接入）访问电子政务外网路由图

2．各级教育行政部门访问教育应用系统安全防护方案

目前，广西各级教育行政部门通过电子政务外网接入点就近接入电子政务外网，并通过电子政务外网互联网出口访问教育网的相关应用系统。

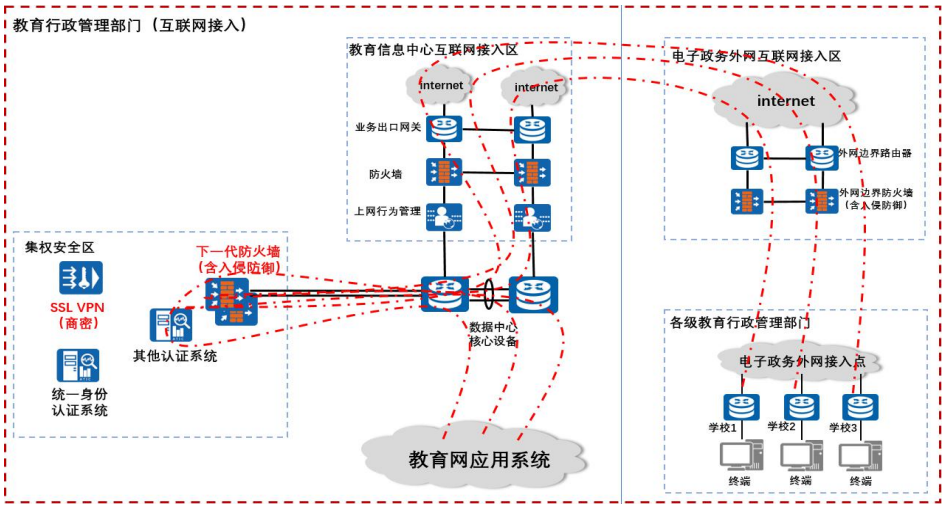

图 5-29 教育行政部门（互联网接入）访问教育应用系统路由图

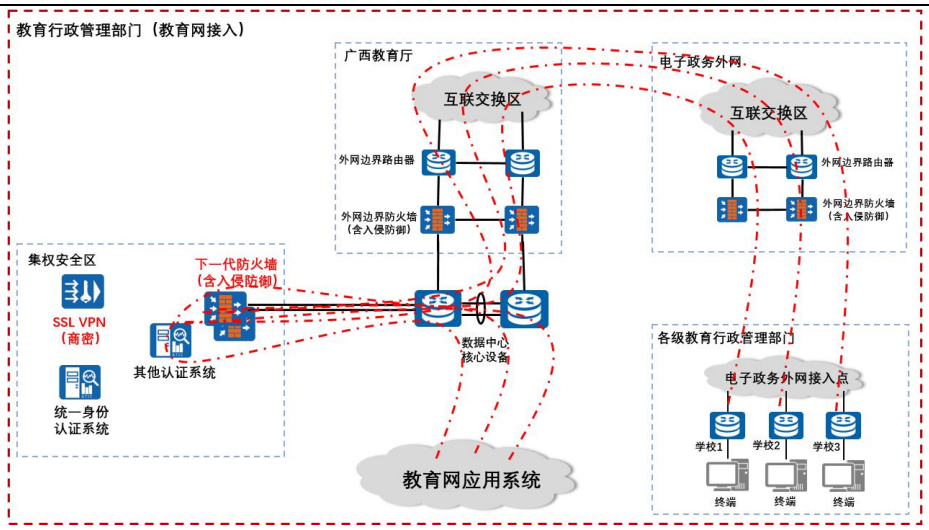

图 5-30 教育行政部门（教育网接入）访问教育应用系统路由图

待教育网建设完善后，各级教育行政部门改为通过电子政务外网的互联交换区直连教育网访问相关应用系统。

3.7.4 主要防护技术

（一）以下一代防火墙为核心的边界防护设计。

传统的安全建设往往通过大量不同品类的硬件设备堆叠进行边界防护体系的构建，这造成了各个安全功能的脱节和割裂，无法实现主动防御和智能联动。此次设计方案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。

融合不是单纯的功能叠加，而是依照业务开展过程中会遇到的各类风险，所提供的对应安全技术手段的融合，能够为业务提供全流程的保护，融合安全包括从事前的资产风险发现，策略有效性检测，到事中所应具备的各类安全防御手段，以及事后的持续检测和快速响应机制。

图 5-31 防护设计结构图

（二）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。用户在外需要进行内网接入时，可直接通过浏览器打开网页完成 SSL VPN 登录及安全隧道的建立，如同登录网银、邮箱一般符合日常的网络使用习惯，容易上手。而 SSL 协议是目前公认安全等级较高的网络安全议之一，现今网上银行基本都采用 SSL 协议进行数据传输保护，对于数据传输采用标准的 AES、RSA、RC4 等加密算法对传输数据进行加密，安全性有保障。

1．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，多重组合软硬结合确保接入身份的确定性。在用户接入 SSL VPN 后进行应用访问权限的划分对于享有访问权限的应用系统采用主从账号绑定 SSL VPN 登录账号和应用系统账号。用户只可采用指定的账号访问应用系统。由于登录 SSL VPN 的身份已通过多重认证的确认，而后又进行指定应用账号访问，即可保障登录应用系统的人员的身份。

2．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。由于 SSL VPN 设备对外只开放 443 端口，从而可屏蔽掉其他端口的攻击。SSL VPN 的数据流处理方式可隐藏内网服务器区结构，并对服务器访问的 IP、域名进行伪装。SSL VPN 在进行用户对服务器区发起的访问时，采用 SSL VPN 登录认证、细粒度应用访问授权、传输数据加密，从数据安全的角度提供隔离保护。

3.8 IP 地址规划

IP 地址规划关系到全网的通信质量，必须为全网的资源进行统一规划，所以需要尽可能的保证业务的连续性。教育网全网支持 IPv6 部署和应用，支持 IPv6 和 IPv4 双栈协议。教育网 IPv6 使用教科网（CRENET）IPv6 地址，由自治区教育厅统一规划分配至各教育城域网。各教育城域网网络管理部门负责统一规划分配网内的

IPv6 地址。教育网 IPv4 使用私有地址。自治区教育厅统一规划分配教育网骨干网的 IPv4 地址。各教育城域网内部 IPv4 地址由各教育城域网网络管理部门负责规划分配。各教育城域网的公网 IPv4 地址由自治区教育厅统一规划分配。各教育城域网网络管理部门负责在网络边界做 NAT 地址转换。

（一）IP 地址规划目标。

1．建立高效的网络路由。

2．有效利用有限的 IP 地址资源。

3．支持网络技术的演变和发展。

（二）IP 地址规划总体原则。

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．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。

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。

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。

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。

6．安全性：网络内应按工作内容划分成不同网段即教育城域网以便进行管理。

（三）网络 IP 地址分类。

1．设备管理/协议地址：即 Loopback 接口地址，SRv6 Locator 地址。

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．业务地址：即终端、服务器地址段。

（四）IPv4 地址规划原则。

IPv4 地址的分配，要与网络拓扑层次结构相适应，既要有效地利用地址空间，又要体现出网络的可扩展性、灵活性和层次性，同时能满足路由协议的要求，以便于网络中的路由聚类，减少路由器中路由表的长度，减少对路由器 CPU、内存的消耗，提高路由算法的效率，加快路由变化的收敛速度，同时还有考虑到网络地址的可管理性。IPv4 地址规划应遵循以下原则来分配:

1．唯一性：一个 IP 网络中不能有两个主机采用相同的 IP 地址;

2．可管理性：地址分配应简单且易于管理，以降低网络扩展

的复杂性，简化路由表;

3．连续性：连续地址在层次结构网络中易于进行路径叠合，缩减路由表，提高路由计算的效率；IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用率；采用 CIDR 技术，可减小路由器路由表的大小，加快路由器路由的收敛速度，也可以减小网络中广播的路由信息的大小。IP 地址分配尽量分配连续的 IP 地址空间；相同的业务和功能尽量分配连续的 IP 地址空间，有利于路由聚合以及安全控制;

4．可扩展性：地址分配在每一层次上都要留有一定余量，以便在网络扩展时能保证地址叠合所需的连续性；IP 地址分配处理要考虑到连续外，又要能做到具有可扩充性，并为将来的网络扩展预留一定的地址空间；充分利用无类别域间路由（CIDR）技术和变长子网掩码（VLSM）技术，合理高效地利用 IP 地址，同时，对所有各种主机、服务器和网络设备，必须分配足够的地址，划分独立的网段，以便能够实现严格的安全策略控制。

5．灵活性：地址分配应具有灵活性，以满足多种路由策略的优化，充分利用地址空间;

6．层次性：IP 地址的划分采用层次化的方法，和层次化的网络设计相应，在地址划分应采用层次化的分配思想。

（五）IPv6 地址规划原则。

在 IPv6 网络中，IPv6 地址规划建议遵循如下原则。

1．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。

2．唯一性原则：每个地址都能够做到全网唯一。IPv6 地址中，有三类单播地址可供选择：Global Unicast Address，Unique Local Address，Link-Local Address。Global Unicast Address 是全球唯一的地址，使用范围是最广；Unique Local Address 类似 IPv4 的 10.0.0.0/8，172.16.0.0/12 和 192.168.0.0/16 网段，是私网可用地址，但不能发布到 internet 上；Link-Local Address 是单链路范围内唯一的地址，只能在链路范围内使用，在运维方面非常不方便（例如不能从远端设备 ping 这个网段）。考虑到 IPv6 地址空间足够大，业务地址推荐使用 Global Unicast Address，不做 NAT 转换，网络互连地址也推荐使用 Global Unicast Address。

3．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。

4．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。

5．安全性原则：为了达到 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。另外为了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。

6．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。

7．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 地址规划时建议以 4bits 为单位（也称为 ibble）进行划分，方便后续查看。

3.8.1 IPv6 地址分配规划

广西教育网 IPv6 地址使用 Global Unicast Address，不做 NAT 转换，网络互连地址也使用 Global Unicast Address。广西教育网 IPv6 地址由广西教育网网络中心负责管理和规划。

各教育城域网申请接入骨干网时，向广西教育网网络中心提交城域网 IPv6 地址规划方案。广西教育网网络中心为各教育城域分配至少一个/41 的 IPv6 地址段。教育城域网管理部门根据分配到的 IPv6 地址进行教育城域网的 IPv6 地址规划，原则上应为教育城域网的每个接入单位规划至少一个/48 的 IPv6 地址段。其中各市县的 IPv6 地址规划表如下:

表 5-9　IPv6 地址分配规划信息表

序号	项目	地址段	说明
一	总段	2001:250:3436::/48 240C:CEAA::/32	
二	骨干网网络建设用地	2001:250:3436:F000::/52	

序号		项目		地址段	说明
		址段			
三		骨干网节点建设用地址段		2001:250:3436:E000::/52	
四		接入用户段		240C:CEAA:0000::/35 240C:CEAA:2000::/35 240C:CEAA:4000::/35 240C:CEAA:8000::/33	由广西教育网网络中心分配
五		广西教育数据中心	植物路	001:250:341E::/48（数据中心原 IPv6 地址）	
5.1	5.1.1	南宁	南宁市	240C:CEAA:8000::/41	
	5.1.2		横州市	240C:CEAA:8080::/41 240C:CEAA:8100::/41 240C:CEAA:8180::/41 240C:CEAA:8200::/41	
	5.1.3		宾阳县	240C:CEAA:8280::/41 240C:CEAA:8300::/41 240C:CEAA:8380::/41	
	5.1.4		上林县	240C:CEAA:8400::/41 240C:CEAA:8480::/41	
	5.1.5		马山县	240C:CEAA:8500::/41 240C:CEAA:8580::/41	
	5.1.6		隆安县	240C:CEAA:8600::/41 240C:CEAA:8680::/41	
	5.1.7		兴宁区	240C:CEAA:8700::/41	
	5.1.8		江南区	240C:CEAA:8780::/41	
	5.1.9		青秀区	240C:CEAA:8800::/41	
	5.1.10		西乡塘区	240C:CEAA:8880::/41 240C:CEAA:8900::/41	
	5.1.11		邕宁区	240C:CEAA:8980::/41 240C:CEAA:8A00::/41	
	5.1.12		良庆区	240C:CEAA:8A80::/41	
	5.1.13		武鸣区	240C:CEAA:8B00::/41 240C:CEAA:8B80::/41	
	5.1.14		经开区	240C:CEAA:8C00::/41	
	5.1.15		高新区	240C:CEAA:8C80::/41	
	5.1.16		华侨区	240C:CEAA:8D00::/41	
5.2	5.2.1	柳州	柳州市	240C:CEAA:8D80::/41	
	5.2.2		城中区	240C:CEAA:8E00::/41	
	5.2.3		鱼峰区	240C:CEAA:8E80::/41	
	5.2.4		柳北区	240C:CEAA:8F00::/41	

序号		项目		地址段	说明
	5.2.5		柳南区	240C:CEAA:8F80::/41	
	5.2.6		鹿寨县	240C:CEAA:9000::/41	
	5.2.7		融水县	240C:CEAA:9080::/41 240C:CEAA:9100::/41	
	5.2.8		柳城县	240C:CEAA:9180::/41 240C:CEAA:9200::/41	
	5.2.9		柳江区	240C:CEAA:9280::/41	
	5.2.10		融安县	240C:CEAA:9300::/41	
	5.2.11		三江县	240C:CEAA:9380::/41 240C:CEAA:9400::/41	
	5.2.12		柳东区	240C:CEAA:9480::/41	
	5.2.13		阳和区	240C:CEAA:9500::/41	
5.3	5.3.1	桂林	桂林市	240C:CEAA:9580::/41	
	5.3.2		秀峰区	240C:CEAA:9600::/41	
	5.3.3		叠彩区	240C:CEAA:9680::/41	
	5.3.4		象山区	240C:CEAA:9700::/41	
	5.3.5		七星区	240C:CEAA:9780::/41	
	5.3.6		雁山区	240C:CEAA:9800::/41	
	5.3.7		临桂区	240C:CEAA:9880::/41	
	5.3.8		阳朔县	240C:CEAA:9900::/41	
	5.3.9		灵川县	240C:CEAA:9980::/41	
	5.3.10		全州县	240C:CEAA:9A00::/41 240C:CEAA:9A80::/41 240C:CEAA:9B00::/41	
	5.3.11		兴安县	240C:CEAA:9B80::/41	
	5.3.12		永福县	240C:CEAA:9C00::/41	
	5.3.13		灌阳县	240C:CEAA:9C80::/41 240C:CEAA:9D00::/41	
	5.3.14		龙胜县	240C:CEAA:9D80::/41	
	5.3.15		资源县	240C:CEAA:9E00::/41	
	5.3.16		平乐县	240C:CEAA:9E80::/41 240C:CEAA:9F00::/41	
	5.3.17		荔浦市	240C:CEAA:9F80::/41 240C:CEAA:A000::/41	
	5.3.18		恭城县	240C:CEAA:A080::/41	
5.4	5.4.1	梧州	梧州市	240C:CEAA:A100::/41	
	5.4.2		万秀区	240C:CEAA:A180::/41	
	5.4.3		长洲区	240C:CEAA:A200::/41	
	5.4.4		龙圩区	240C:CEAA:A280::/41	
	5.4.5		苍梧县	240C:CEAA:A300::/41	

序号		项目		地址段	说明
				240C:CEAA:A380::/41 240C:CEAA:A400::/41	
	5.4.6		藤县	240C:CEAA:A480::/41 240C:CEAA:A500::/41 240C:CEAA:A580::/41 240C:CEAA:A600::/41 240C:CEAA:A680::/41 240C:CEAA:A700::/41	
	5.4.7		蒙山县	240C:CEAA:A780::/41	
	5.4.8		岑溪市	240C:CEAA:A800::/41 240C:CEAA:A880::/41 240C:CEAA:A900::/41 240C:CEAA:A980::/41	
5.5	5.5.1	北海	北海市	240C:CEAA:AA00::/41	
	5.5.2		海城区	240C:CEAA:AA80::/41	
	5.5.3		银海区	240C:CEAA:AB00::/41	
	5.5.4		铁山港区	240C:CEAA:AB80::/41	
	5.5.5		合浦县	240C:CEAA:AC00::/41 240C:CEAA:AC80::/41 240C:CEAA:AD00::/41	
5.6	5.6.1	防城港	防城港市	240C:CEAA:AD80::/41	
	5.6.2		上思县	240C:CEAA:AE00::/41 240C:CEAA:AE80::/41 240C:CEAA:AF00::/41	
	5.6.3		东兴市	240C:CEAA:AF80::/41	
	5.6.4		港口区	240C:CEAA:B000::/41	
	5.6.5		防城区	240C:CEAA:B080::/41 240C:CEAA:B100::/41	
5.7	5.7.1	钦州	钦州市	240C:CEAA:B180::/41	
	5.7.2		灵山县	240C:CEAA:B200::/41 240C:CEAA:B280::/41 240C:CEAA:B300::/41 240C:CEAA:B380::/41 240C:CEAA:B400::/41	
	5.7.3		浦北县	240C:CEAA:B480::/41 240C:CEAA:B500::/41 240C:CEAA:B680::/41 240C:CEAA:B700::/41	
	5.7.4		钦南区	240C:CEAA:B780::/41 240C:CEAA:B800::/41	

序号		项目		地址段	说明
	5.7.5		钦北区	240C:CEAA:B880::/41 240C:CEAA:B900::/41 240C:CEAA:B980::/41	
5.8	5.8.1	贵港	贵港市	240C:CEAA:BA00::/41	
	5.8.2		桂平市	240C:CEAA:BA80::/41 240C:CEAA:BB00::/41 240C:CEAA:BB80::/41 240C:CEAA:BC00::/41 240C:CEAA:BC80::/41 240C:CEAA:BD00::/41	
	5.8.3		平南市	240C:CEAA:BD80::/41 240C:CEAA:BE00::/41 240C:CEAA:BE80::/41 240C:CEAA:BF00::/41 240C:CEAA:BF80::/41	
	5.8.4		港北区	240C:CEAA:C000::/41 240C:CEAA:C080::/41	
	5.8.5		港南区	240C:CEAA:C100::/41 240C:CEAA:C180::/41	
	5.8.6		覃塘区	240C:CEAA:C200::/41 240C:CEAA:C280::/41	
5.9	5.9.1	玉林	玉林市	240C:CEAA:C300::/41	
	5.9.2		北流市	240C:CEAA:C380::/41 240C:CEAA:C400::/41 240C:CEAA:C480::/41 240C:CEAA:C500::/41 240C:CEAA:C580::/41	
	5.9.3		容县	240C:CEAA:C600::/41 240C:CEAA:C680::/41 240C:CEAA:C700::/41 240C:CEAA:C780::/41	
	5.9.4		陆川县	240C:CEAA:C800::/41 240C:CEAA:C880::/41 240C:CEAA:C900::/41 240C:CEAA:C980::/41	
	5.9.5		博白县	240C:CEAA:CA00::/41 240C:CEAA:CA80::/41 240C:CEAA:CB00::/41 240C:CEAA:CB80::/41 240C:CEAA:CD00::/41 240C:CEAA:CD80::/41	

序号		项目		地址段	说明
				240C:CEAA:CE00::/41 240C:CEAA:CE80::/41	
	5.9.6		兴业县	240C:CEAA:CF00::/41 240C:CEAA:CF80::/41 240C:CEAA:D000::/41	
	5.9.7		玉州区	240C:CEAA:D080::/41 240C:CEAA:D100::/41	
	5.9.8		福绵区	240C:CEAA:D180::/41 240C:CEAA:D200::/41	
	5.9.9		玉东区	240C:CEAA:D280::/41	
5.10	5.10.3	百色	百色市	240C:CEAA:D300::/41	
	5.10.4		右江区	240C:CEAA:D380::/41	
	5.10.5		田阳县	240C:CEAA:D400::/41	
	5.10.6		田东县	240C:CEAA:D480::/41	
	5.10.7		平果市	240C:CEAA:D500::/41	
	5.10.8		德保县	240C:CEAA:D580::/41	
	5.10.9		靖西市	240C:CEAA:D600::/41 240C:CEAA:D680::/41	
	5.10.10		那坡县	240C:CEAA:D700::/41	
	5.10.11		凌云县	240C:CEAA:D780::/41	
	5.10.12		乐业县	240C:CEAA:D900::/41	
	5.10.13		田林县	240C:CEAA:D980::/41	
	5.10.14		隆林县	240C:CEAA:DA00::/41 240C:CEAA:DA80::/41	
	5.10.15		西林县	240C:CEAA:DB00::/41	
5.11	5.11.1	贺州	贺州市	240C:CEAA:DB80::/41	
	5.11.2		八步区	240C:CEAA:DC00::/41 240C:CEAA:DC80::/41	
	5.11.3		平桂区	240C:CEAA:DD00::/41 240C:CEAA:DD80::/41	
	5.11.4		昭平县	240C:CEAA:DE00::/41 240C:CEAA:DE80::/41	
	5.11.5		钟山县	240C:CEAA:DF00::/41 240C:CEAA:DF80::/41	
	5.11.6		富川县	240C:CEAA:E000::/41 240C:CEAA:E080::/41	
5.12	5.12.1	河池	河池市	240C:CEAA:E100::/41	
	5.12.2		金城江区	240C:CEAA:E180::/41	
	5.12.3		宜州区	240C:CEAA:E200::/41 240C:CEAA:E280::/41	

序号		项目		地址段	说明
	5.12.4		罗城县	240C:CEAA:E300::/41 240C:CEAA:E380::/41	
	5.12.5		环江县	240C:CEAA:E400::/41	
	5.12.6		南丹县	240C:CEAA:E480::/41 240C:CEAA:E500::/41	
	5.12.7		天峨县	240C:CEAA:E580::/41	
	5.12.8		东兰县	240C:CEAA:E600::/41	
	5.12.9		巴马县	240C:CEAA:E680::/41 240C:CEAA:E700::/41	
	5.12.10		凤山县	240C:CEAA:E780::/41	
	5.12.11		都安县	240C:CEAA:E800::/41 240C:CEAA:E880::/41	
	5.12.12		大化县	240C:CEAA:E900::/41 240C:CEAA:E980::/41 240C:CEAA:EA00::/41 240C:CEAA:EA80::/41	
5.13	5.13.1	来宾	来宾市	240C:CEAA:EB00::/41	
	5.13.2		兴宾区	240C:CEAA:EB80::/41 240C:CEAA:EC00::/41 240C:CEAA:EC80::/41	
	5.13.3		象州县	240C:CEAA:ED00::/41	
	5.13.4		武宣县	240C:CEAA:ED80::/41	
	5.13.5		忻城县	240C:CEAA:EE00::/41	
	5.13.6		金秀县	240C:CEAA:EE80::/41	
	5.13.7		合山市	240C:CEAA:EF00::/41	
5.14	5.14.1	崇左	崇左市	240C:CEAA:EF80::/41	
	5.14.2		扶绥县	240C:CEAA:F000::/41	
	5.14.3		大新县	240C:CEAA:F080::/41	
	5.14.4		天等县	240C:CEAA:F100::/41 240C:CEAA:F180::/41	
	5.14.5		宁明县	240C:CEAA:F200::/41 240C:CEAA:F280::/41	
	5.14.6		龙州县	240C:CEAA:F300::/41	
	5.14.7		凭祥市	240C:CEAA:F380::/41	
	5.14.8		江州区	240C:CEAA:F400::/41	

各市县如有中等职业技术学校和幼儿园接入城域网的，可以与广西教育网网络中心联系，另外规划、申请专用于中等职业技术学校和幼儿园的 IPv6 地址。

3.8.2 IPv4 地址分配规划

广西教育网骨干网 IPv4 地址规划由广西教育网网络中心负责规划和管理。

广西教育网使用 100.64.0.0/10（RFC 6958）作为业务地址，业务地址由广西教育网网络中心统一规划和管理。教育城域网申请接入骨干网时，广西教育网网络中心为教育城域网分配业务地址。业务地址在广西教育网全局可路由，教育城域网和骨干网的网络通信通过业务地址进行。

各教育网城域网内的 IPv4 地址可使用私网 IPv4 地址，由各教育城域网管理部门负责规划和管理。在项目建设前，应根据本地实际切实做好 IPv4 地址规划，包括并不仅限于:

1.出口公网 IPv4 地址数量和地址规划。

2.教育城域网 IPv4 地址规划描述,包括设备管理地址、互联地址、业务地址（同步课堂、办公、 IP 广播等）等各类地址规划分配的规则。

3.每一类地址具体的 IPv4 地址段(如果不能细化到每一个学校，须根据规划分配的规则规划出具体的 IPv4 地址段）。

3.9 教育域名规划

根据《互联网信息服务管理办法》《中国互联网络域名管理办法》《中国教育和科研计算机网 EDU.CN 网络域名注册办法》的要求，按行政区域编制广西教育网的教育域名规划。

3.9.1 命名规则

各市、县（市、区）教育行政部门申请注册一级域名，所辖学校申请注册一级域名下的二级域名。教育行政部门申请注册的一级域名按“gx”+“设区市标识”+“县（市、区）标识”+“jy.edu.cn”规则编制。学校申请注册的二级域名，按“学校标识”+“.”+“上级教育行政部门一级域名”组成，学校标识由校名中文全称或简称的每个汉字拼音首字母组成，例如：南宁市青秀区桂雅路小学为“gylxx.gxnnqxjy.edu.cn”，南宁市第三中学为“nnsz.gxnnjy.edu.cn”（市直属学校）。

3.9.2 教育域名规划

表 5-11 广西各级教育行政区域教育域名信息表

序号	区域名称	教育域名	备注
1	南宁市教育局	gxnnjy.edu.cn	
2	南宁市横州市教育局	gxnnhzjy.edu.cn	
3	南宁市宾阳县教育局	gxnnbyjy.edu.cn	
4	南宁市上林县教育局	gxnnsljy.edu.cn	
5	南宁市马山县教育局	gxnnmsjy.edu.cn	
6	南宁市隆安县教育局	gxnnlajy.edu.cn	
7	南宁市兴宁区教育局	gxnnxnjy.edu.cn	
8	南宁市江南区教育局	gxnnjnjy.edu.cn	
9	南宁市青秀区教育局	gxnnqxjy.edu.cn	

序号	区域名称	教育域名	备注
10	南宁市西乡塘区教育局	gxnnxxtjy.edu.cn	
11	南宁市邕宁区教育局	gxnnynjy.edu.cn	
12	南宁市良庆区教育局	gxnnlqjy.edu.cn	
13	南宁市武鸣区教育局	gxnnwmjy.edu.cn	
14	南宁市经济开发区教育局	gxnnjkjy.edu.cn	
15	南宁市高新技术产业开发区教育局	gxnngxjy.edu.cn	
16	南宁市华侨投资区教育局	gxnnhqjy.edu.cn	
17	柳州市教育局	gxlzjy.edu.cn	
18	柳州市城中区教育局	gxlzczjy.edu.cn	
19	柳州市鱼峰区教育局	gxlzyfjy.edu.cn	
20	柳州市柳北区教育局	gxlzlbjy.edu.cn	
21	柳州市柳南区教育局	gxlzlnjy.edu.cn	
22	柳州市鹿寨县教育局	gxlzlzjy.edu.cn	
23	柳州市融水苗族自治县教育局	gxlzrsjy.edu.cn	
24	柳州市柳城县教育局	gxlzlcjy.edu.cn	
25	柳州市柳江区教育局	gxlzljjy.edu.cn	
26	柳州市融安县教育局	gxlzrajy.edu.cn	
27	柳州市三江侗族自治县教育局	gxlzsjjy.edu.cn	

序号	区域名称	教育域名	备注
28	柳州市柳东新区教育局	gxlzldjy.edu.cn	
29	柳州市阳和工业新区教育局	gxlzyhjy.edu.cn	
30	桂林市教育局	gxgljy.edu.cn	
31	桂林市秀峰区教育局	gxglxfjy.edu.cn	
32	桂林市叠彩区教育局	gxgldcjy.edu.cn	
33	桂林市象山区教育局	gxglxsjy.edu.cn	
34	桂林市七星区教育局	gxglqxjy.edu.cn	
35	桂林市雁山区教育局	gxglysqjy.edu.cn	
36	桂林市临桂区教育局	gxgllgjy.edu.cn	
37	桂林市阳朔县教育局	gxglysxjy.edu.cn	
38	桂林市灵川县教育局	gxgllcjy.edu.cn	
39	桂林市全州县教育局	gxglqzjy.edu.cn	
40	桂林市兴安县教育局	gxglxajy.edu.cn	
41	桂林市永福县教育局	gxglyfjy.edu.cn	
42	桂林市灌阳县教育局	gxglgyjy.edu.cn	
43	桂林市龙胜各族自治县教育局	gxgllsjy.edu.cn	
44	桂林市资源县教育局	gxglzyjy.edu.cn	
45	桂林市平乐县教育局	gxglpljy.edu.cn	
46	桂林市荔浦市教育局	gxgllpjy.edu.cn	

序号	区域名称	教育域名	备注
47	桂林市恭城瑶族自治县教育局	gxglgcjy.edu.cn	
48	梧州市教育局	gxwzjy.edu.cn	
49	梧州市万秀区教育局	gxwzwxjy.edu.cn	
50	梧州市长洲区教育局	gxwzczjy.edu.cn	
51	梧州市龙圩区教育局	gxwzlxjy.edu.cn	
52	梧州市苍梧县教育局	gxwzcwjy.edu.cn	
53	梧州市藤县教育局	gxwztxjy.edu.cn	
54	梧州市蒙山县教育局	gxwzmsjy.edu.cn	
55	梧州市岑溪市教育局	gxwzcxjy.edu.cn	
56	梧州市工业园区教育局	gxwzgyyjy.edu.cn	
57	北海市教育局	gxbhjy.edu.cn	
58	北海市海城区教育局	gxbhhcjy.edu.cn	
59	北海市银海区教育局	gxbhyhjy.edu.cn	
60	北海市铁山港区教育局	gxbhtsgjy.edu.cn	
61	北海市合浦县教育局	gxbhhpjy.edu.cn	
62	防城港市教育局	gxfcgjy.edu.cn	
63	防城港市上思县教育和科学技术局	gxfcgssjy.edu.cn	
64	防城港市东兴市教育和科学技术局	gxfcgdxjy.edu.cn	

序号	区域名称	教育域名	备注
65	防城港市港口区教育和科学技术局	gxfcggkjy.edu.cn	
66	防城港市防城区教育和科学技术局	gxfcgfcjy.edu.cn	
67	钦州市教育局	gxqzjy.edu.cn	
68	钦州市灵山县教育局	gxqzlsjy.edu.cn	
69	钦州市浦北县教育局	gxqzpbjy.edu.cn	
70	钦州市钦南区教育局	gxqzqnjy.edu.cn	
71	钦州市钦北区教育局	gxqzqbjy.edu.cn	
72	贵港市教育局	gxggjy.edu.cn	
73	贵港市桂平市教育局	gxgggpjy.edu.cn	
74	贵港市平南县教育局	gxggpnjy.edu.cn	
75	贵港市港北区教育局	gxgggbjy.edu.cn	
76	贵港市港南区教育局	gxgggnjy.edu.cn	
77	贵港市覃塘区教育局	gxggqtjy.edu.cn	
78	玉林市教育局	gxyljy.edu.cn	
79	玉林市北流市教育局	gxylbljy.edu.cn	
80	玉林市容县教育局	gxylrxjy.edu.cn	
81	玉林市陆川县教育局	gxyllcjy.edu.cn	
82	玉林市博白县教育局	gxylbbjy.edu.cn	

序号	区域名称	教育域名	备注
83	玉林市兴业县教育局	gxylxyjy.edu.cn	
84	玉林市玉州区教育局	gxylyzjy.edu.cn	
85	玉林市福绵区教育局	gxylfmjy.edu.cn	
86	玉林市玉东新区教育局	gxylydjy.edu.cn	
87	百色市教育局	gxbsjy.edu.cn	
88	百色市右江区教育局	gxbsyjjy.edu.cn	
89	百色市田阳区教育局	gxbstyjy.edu.cn	
90	百色市田东县教育局	gxbstdjy.edu.cn	
91	百色市平果县教育局	gxbspgjy.edu.cn	
92	百色市德保县教育局	gxbsdbjy.edu.cn	
93	百色市靖西市教育局	gxbsjxjy.edu.cn	
94	百色市那坡县教育局	gxbsnpjy.edu.cn	
95	百色市凌云县教育局	gxbslingyjy.edu.cn	
96	百色市乐业县教育局	gxbsleyjy.edu.cn	
97	百色市田林县教育局	gxbstljy.edu.cn	
98	百色市隆林各族自治县教育局	gxbslljy.edu.cn	
99	百色市西林县教育局	gxbsxljy.edu.cn	
100	贺州市教育局	gxhzjy.edu.cn	
101	贺州市八步区教育和	gxhzbbjy.edu.cn	

序号	区域名称	教育域名	备注
	科学技术局		
102	贺州市平桂区教育和科学技术局	gxhzpgjy.edu.cn	
103	贺州市昭平县教育和科学技术局	gxhzzpjy.edu.cn	
104	贺州市钟山县教育和科学技术局	gxhzzsjy.edu.cn	
105	贺州市富川瑶族自治县教育和科学技术局	gxhzfcjy.edu.cn	
106	河池市教育局	gxhcjy.edu.cn	
107	河池市金城江区教育局	gxhcjcjjy.edu.cn	
108	河池市宜州区教育局	gxhcyzjy.edu.cn	
109	河池市罗城仫佬族自治县教育局	gxhclcjy.edu.cn	
110	河池市环江毛南族自治县教育局	gxhchjjy.edu.cn	
111	河池市南丹县教育局	gxhcndjy.edu.cn	
112	河池市天峨县教育局	gxhctejy.edu.cn	
113	河池市东兰县教育局	gxhcdljy.edu.cn	
114	河池市巴马瑶族自治县教育局	gxhcbmjy.edu.cn	

序号	区域名称	教育域名	备注
115	河池市凤山县教育局	gxhcfsjy.edu.cn	
116	河池市都安瑶族自治县教育局	gxhcdajy.edu.cn	
117	河池市大化瑶族自治县教育局	gxhcdhjy.edu.cn	
118	来宾市教育局	gxlbjy.edu.cn	
119	来宾市兴宾区教育体育局	gxlbxbjy.edu.cn	
120	来宾市象州县教育体育局	gxlbxzjy.edu.cn	
121	来宾市武宣县教育体育局	gxlbwxjy.edu.cn	
122	来宾市忻城县教育体育局	gxlbxcjy.edu.cn	
123	来宾市金秀瑶族自治县 教育体育局	gxlbjxjy.edu.cn	
124	来宾市合山市教育体育局	gxlbhsjy.edu.cn	
125	崇左市教育局	gxczjy.edu.cn	
126	崇左市扶绥县教育局	gxczfsjy.edu.cn	
127	崇左市大新县教育局	gxczdxjy.edu.cn	
128	崇左市天等县教育局	gxcztdjy.edu.cn	
129	崇左市宁明县教育局	gxcznmjy.edu.cn	
130	崇左市龙州县教育局	gxczlzjy.edu.cn	
131	崇左市凭祥市教育局	gxczpxjy.edu.cn	
132	崇左市江州区教育局	gxczjzjy.edu.cn	

3.10 系统安全建设方案

3.10.1 总体目标

本项目系统安全建设的最终目标是使教育骨干网符合国家网络安全等级保护第三级要求，教育城域网符合国家网络安全等级保护第二级要求，**构建安全合规、责任清晰、风险可视、简单高效的网络安全体系**。

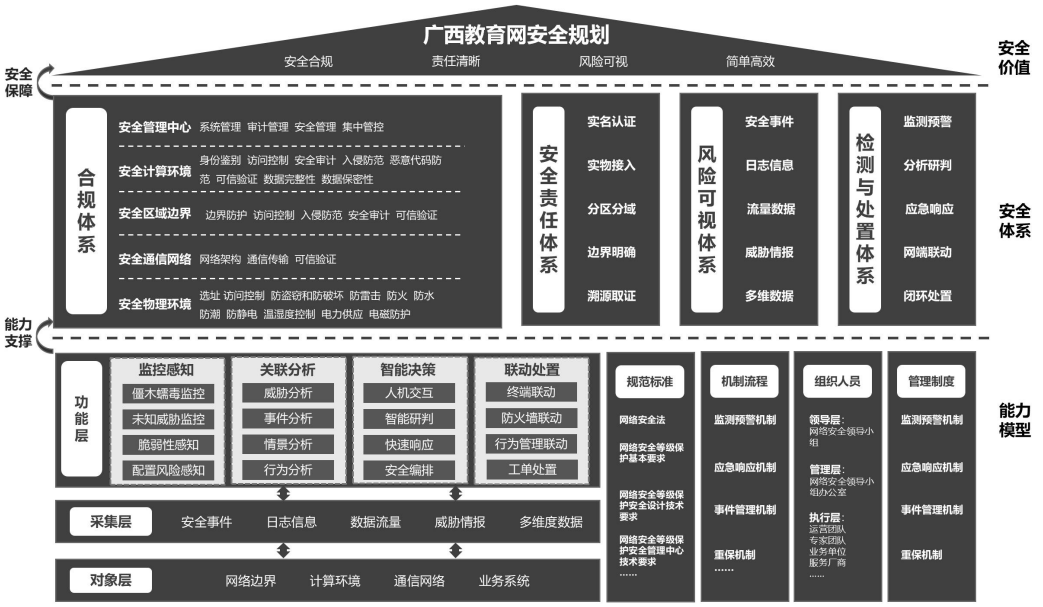

图 5-32 广西教育网安全规划

本项目根据等级保护指导思想，以技术保障为基础、以管理运营为抓手、以监测预警为核心、以协同响应为目标规划网络安全防御体系并落地为具体的安全建设方案。将物理和环境、网络和通信、设备和计算安全、应用和数据安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理等各个层面的安全需求，转化为可以实现的技术防护能力、安全管理措施和安全运营手

段，为教育网的安全运行保驾护航。

3.10.2 体系架构

3.10.2.1 设计原则

安全防御体系设计以安全合规要求为基础，以实际业务安全需求为主导，构建网络安全等级保护深度防御体系。在建设过程中，遵循统一规划、统一标准、统一管理、适度保护、重点保护、强化管理的原则。在网络系统的安全设计环节重点把握如下原则:

（一）统一性。教育网是一个有机的整体，为适应目前以及未来业务发展的需要，为业务系统提供可靠的安全保障，需要有一个统一、可靠的整体安全体系。

对整个网络安全防御体系实行统一规划，统一标准，并进行一体化安全建设、安全管理和安全运营；按照总体规划、部署和要求，做好各层面的统一建设和管理工作。

（二）完整性。网络系统是一个复杂的计算机系统，它本身在物理上、操作上和管理上不同层次不同位置上的种种漏洞构成了系统的安全脆弱性，尤其是多用户网络系统自身的复杂性、资源共享性使单纯的技术保护防不胜防。攻击者使用的是“最易渗透原则”，必然在系统中最薄弱的地方进行攻击。因此，充分、全面、完整地对系统的安全威胁和安全风险进行分析、评估和检测，是网络系统的安全设计的必要前提条件。安全机制和安全服务设计的首要目的

是防止最常用的攻击手段，重要目标是提高整个系统的“安全最低点”的安全性能。

（三）立体性。任何单一层次的安全措施都不是绝对安全的，都可能被攻破。必须建立系统性的安全防护措施，从多层次，多维度进行多重保护，各个层次的保护相互补充，形成统一协调的安全策略，避免防护短板，层层防护，即使某一层保护被攻破时，其它层保护仍可保护信息系统的安全。

（四）可用性。必须具备一定的冗余和前瞻性，能随着网络性能及安全需求的变化而变化，要在整个系统内尽可能引入更多的灵活自适应的因素，并具有良好的扩展性。要能够为将来业务扩展提供足够的安全扩展能力。

3.10.2.2 设计思路

本项目将根据网络安全等级保护相关要求，通过分析系统的实际安全需求，结合其业务信息的实际特性，并依据及参照相关政策标准，设计安全保障体系方案，综合提升系统的安全保障能力和防护水平，确保教育网的安全稳定运行。具体设计将遵循以下思路开展。

（一）将合规要求与业务风险分析相结合的设计思路。

安全风险分析是识别网络系统面临安全威胁和系统脆弱性的方法，通过风险分析方法可以全面掌握网络系统面临安全风险的全貌，

并根据安全风险等级确定信息安全建设的重点。

在完成基于资产风险分析的基础上，对网络系统现状进行实际调研，掌握网络系统防护现状与等级保护基线要求间的实际差距，结合安全风险评估的方法，对网络系统进行全面的资产、脆弱性、威胁和业务风险等方面系统化的评估分析，发现基于业务的安全风险问题。将差距分析结果与风险评估结果进行充分结合与提炼，综合形成能够符合等级保护建设要求并充分保障业务安全的建设需求。

（二）纵深防御的安全体系设计思路。

安全体系建设的思路是根据分区分域防护的原则，按照层次化的纵深防御的思想，建设网络系统安全等级保护深度防御体系。

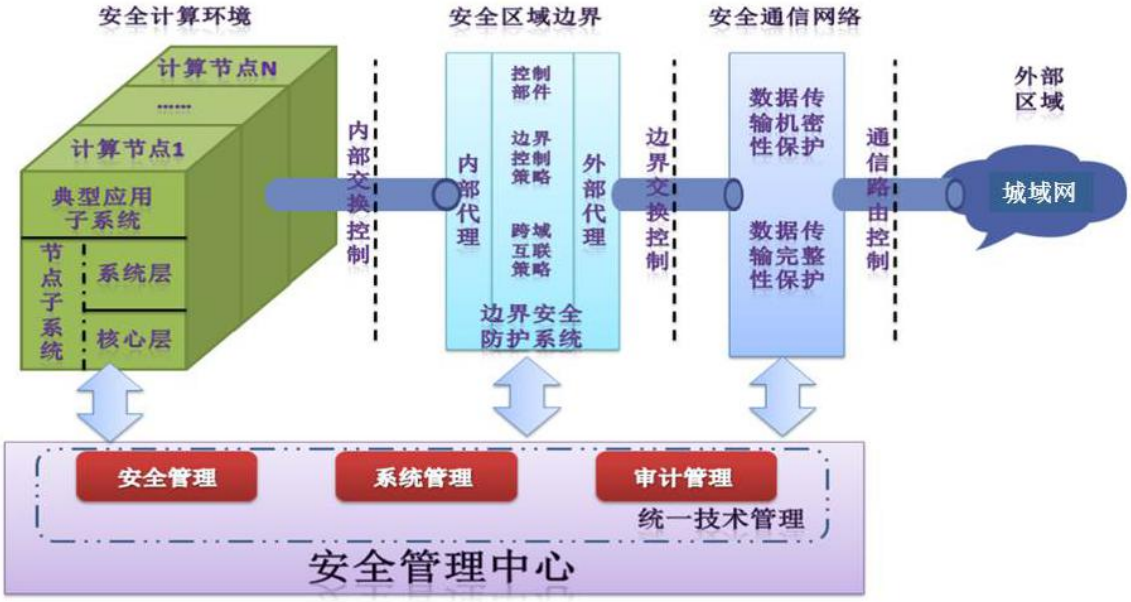

图 5-33 纵深防御安全体系图

按照通信网络系统业务处理过程将系统划分成安全计算环境、

安全区域边界和安全通信网络三部分，以计算节点为基础对这三部分实施保护，构成由安全管理中心支撑下的计算环境安全、区域边界安全、通信网络安全所组成的“一个中心，三重防护”结构。

（三）体系化安全保障框架设计思路。

一个完整的网络安全体系应该是安全技术、安全管理、安全运营的结合，三者缺一不可。为了实现对网络系统的多层保护，真正达到网络安全保障的目标，国内外安全保障理论也在不断的发展之中，根据网络系统的实际情况，参照国际安全控制框架的有关标准，形成符合教育网需要的安全保障体系框架。

在方案设计中“三个体系”（安全技术体系、安全管理体系和安全运营体系）各自相对独立，又相互依赖和互补，共同形成整体的安全保障体系框架。

3.10.2.3 总体安全策略

（一）安全技术体系总体策略。

1. 以《网络安全等级保护基本要求》中第三级（教育骨干网）和第二级（教育城域网）保护要求为控制要求，建设基础安全技术体系框架。

2. 安全技术体系建设覆盖物理环境、通信网络、区域边界、计算环境和安全管理中心五个方面。

3. 通过采用成熟可靠的安全技术及安全产品，结合专业技术人

员的安全技术经验和能力，系统化的搭建安全技术体系，确保技术体系的安全性与可用性的有机结合，达到适用性要求。

（二）安全管理体系总体策略。

1. 建立网络安全领导小组和工作组，形成等级保护基本要求的网络安全组织体系职责。

2. 建立网络安全管理制度和策略体系，形成符合等级保护基本要求的安全管理制度要求。

3. 建立符合系统生命周期的安全需求、安全设计、安全建设和安全运维的运行管理要求。

4. 系统安全建设过程应落实等级保护定级、备案、建设整改、测评等管理要求。

5. 系统安全运营过程应落实等级保护监督检查的管理要求。

（三）安全运营体系总体策略。

1. 通过互联网等领域所形成的新技术适当提升安全能力，强化风险应对（监测、预警、防护、处置、溯源等）能力。

2. 建立规范的信息化安全运营体系，以安全视角规范教育网安全运营的整个过程，形成安全业务标准与流程。

3. 建立网络安全运营中心，安全运营实行分级保障，加强安全运营的可持续性建设。

3.10.2.4 总体安全设计

（一）技术防护措施。

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 AV 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. 采用应用身份认证系统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. 采用态势感知与安全运营平台和抗 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. 采用多种安全设备如防火墙、上网行为审计、终端安全监测、态势感知以及及统一身份认证系统智能联动的机制，实现安全事件的快速处置与闭环，降低安全管理与安全运维的难度。

12. 采用统一身份认证系统进行教育网用户的身份认证，实现多因素身份认证。

（二）网络安全保护等级标准。

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建议如下:

表 5-12 教育行政部门网络安全保护等级建议表

序号	分类	信息系统	建议安全保护等级		
			自治区级	设区市	县（市、区）
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
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	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

序号	分类	信息系统	建议安全保护等级		
			自治区级	设区市	县（市、区）
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	第二级	第二级	第一级
A29		(02)教师资格认定管	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

3.10.3 技术体系

3.10.3.1 物理环境

物理安全是整个网络系统安全的前提，可能面临的物理安全风险有：地震、水灾、火灾、电源故障、电磁辐射、设备故障、人为物理破坏等，这些风险都可能造成系统的崩溃。因此，物理安全必须具备环境安全、设备物理安全和防电磁辐射等物理支撑环境，保护网络设备、设施、介质和信息免受自然灾害、环境事故以及人为物理操作失误或错误导致的破坏、丢失，防止各种以物理手段进行

的违法犯罪行为。

等级保护基本要求对系统的物理安全要求较为严格，主要涉及的方面包括环境安全（防火、防水、防雷击等）设备和介质的防盗窃防破坏等方面。具体包括：物理位置选择、物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应和电磁防护等十个控制点。

网络中心机房建设应严格按照国家对信息系统机房的建设标准，机房应在各方面满足等级保护的相关要求。

教育网所涉及的服务器、存储设备、网络设备、软件系统等软硬件均位于中国境内，符合网络安全等级保护对云计算安全的扩展要求。

3.10.3.2 通信网络

参照等级保护的要求对系统安全区域进行划分设计，实现内部办公、数据共享交换与外部接入区域之间的安全隔离，并对核心区域进行冗余建设，用以保障关键业务系统的可用性与连续性。

安全域是由安全保护对象中安全计算环境和安全区域边界综合组成，根据安全域的描述可以把保护对象进行进一步的划分，同时使整个网络逻辑结构清晰。

安全域可以根据其更细粒度的防护策略，进一步划分成安全子域，其关键是能够区分防护重点，形成重要资源重点保护的策略。

（一）业务保障原则。安全域方法的根本目标是能够更好的保障

网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率。

（二）适度安全原则。在安全域划分时会面临有些业务紧密相连，但是根据安全要求又要将其划分到不同安全域的矛盾，必须综合考虑业务隔离的难度和合并安全域的风险，从而给出合适的安全域划分。

（三）结构简化原则。安全域方法的直接目的和效果是要将整个网络变得更加简单，简单的网络结构便于设计防护体系。

（四）等级保护原则。安全域的划分要做到每个安全域的信息资产价值相近，具有相同或相近的安全等级安全环境安全策略等。

（五）立体协防原则。安全域的主要对象是网络，但是围绕安全域的防护需要考虑在各个层次上立体防守，包括在物理链路网络主机系统应用等层次；同时，在部署安全域防护体系的时候，要综合运用身份鉴别访问控制检测审计链路冗余内容检测等各种安全功能实现协防。

（六）生命周期原则。对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑不断地变化；另外，在安全域的建设和调整过程中要考虑工程化的管理。

3.10.3.3 区域边界

（一）边界访问控制。

1. 边界防护与访问控制

针对新的边界安全威胁,边界访问控制已经成为基本安全措施，必不可少，但为了更加有效的应对当前的网络威胁，防火墙设备应当更加智能化、联动化，以满足安全有效性和防御实时性的切实需求。

当前，下一代防火墙技术已经逐步成熟，通过相关功能实现及策略配置，可实现上述要求，防火墙主要功能及配置要求如下:

（1）访问控制

能够基于 IP、安全域、VLAN、时间、用户、地理区域、服务协议及应用等多种方式进行访问控制，一条安全策略可配置应用控制、入侵防护、URL 过滤、病毒检测、内容过滤、网络行为管理等高级访问控制功能。能对 HTTP、SMTP、POP3、IMAP、FTP、TELNET 协议进行细粒度的控制，过滤不受信任的网络行为。

（2）应用层访问控制

能实现文件过滤、URL 过滤、邮件过滤等、实现针对主要的应用协议如 HTTP、FTP、POP3、SMTP、IMAP 等的双向内容传输过滤，可预定义或自定义敏感信息库进行敏感信息定义。

（3）入侵防范

对于主要攻击能进行防护，包括：Flood（SYN Flood、ICMP Flood、UDP Flood、IP Flood）、恶意扫描（禁止 tracert、IP 地址扫描攻击、端口扫描）、欺骗防护（IP 欺骗、DHCP 监控辅助检查）、异常包攻击（Ping of Death、Teardrop、IP 选项、TCP 异常、Smurf、

Fraggle、Land、Winnuke、DNS 异常、IP 分片）、ICMP 管控（禁止 ICMP 分片、禁止路由重定向报文、禁止不可达报文、禁止超时报文、ICMP 报文大小限制）、应用层 Flood（DNS Flood、HTTP Flood）、SYN Cookie 等。

（4）负载均衡

作为主要的链路设施，能实现基于 IP、ISP、应用、用户、服务等的多链路负载均衡，DNS 流量的负载均衡，基于服务器地址的负载均衡。

（5）高可靠性

具备双机热备功能，在路由和透明模式下能支持“主-备”、“主-主”模式，能实现接口联动，链路探测。

（6）动态 QoS 功能

可配置带宽限制策略。策略类型包括共享型和独享型，用户优先级分为高、中、低，服务类型包括应用层的多种协议。在用户都满足保证带宽情况下，高优先级用户将抢占中、低优先级用户带宽，中优先级用户将抢占低优先级用户带宽。当网络中存在空闲带宽时，防火墙系统会根据当前网络带宽分配情况，自动将空闲带宽分配给重要业务，保证重要业务的正常访问。

（7）支持 IPv6

能够支持完整的双栈协议，支持 IPv6 下的多种功能，包括网络功能和安全功能，包括 IPv6 接口、IPv6 路由、IPv6 认证管理、IPv6

日志管理、IPv6 VPN、IPv6 安全功能及安全策略等。

（8）虚拟防火墙

具备虚拟系统功能，即将防火墙虚拟成多个相互隔离并独立运行的虚拟防火墙，每一个虚拟系统都可以为用户提供定制化的安全防护功能，并可配备独立的管理员账号。

（9）协同联动

能够与终端安全管理系统、云端的 URL 库、病毒库、应用识别库等资源进行联动，提升对已知威胁的识别效率，并能对在终端发现的威胁从网络层及时阻断。

（10）日志管理

对各类日志，如流量日志、威胁日志、URL 过滤日志、邮件过滤日志、行为日志等进行分析和日志外发，能基于 IP、用户、接口、地区、应用等过滤条件搜索自定义时间段内的历史日志。

各安全区域都应针对自身业务特点设定访问控制策略，下表表述了各安全区域之间的访问控制关系，在对各网络安全区域设置安全策略时，可以此为参考原则进行设置:

表 5-13 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

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
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、核心业务区边界均建议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。

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，该组件集成了访问控制、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，给用户提供了分析线索、发现异常、回溯事件等一系列分析面板，降低了用户对风险、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、核心业务区边界均建议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。

（二）边界入侵防范。

1. 边界入侵防御

（1）安全风险

随着国家信息化的发展，网络攻击活动也愈演愈烈，而网络攻击造成的破坏性因信息化程度的高度集中也越来越大。主要呈现如下趋势：网络应用越来越复杂，单纯的依靠端口识别应用以达到攻击检测的目的不再有效；网络带宽的快速增长给入侵防护系统的处理能力带来挑战，仅依靠防火墙这样的边界防护设备实现网络攻击

检测已经远远不能满足要求，具备大流量业务并发处理能力的专业设备尤其重要；除具备针对网络层/传输层的基础攻击防护外，针对应用层深度识别和防御能力越发重要。

因此，如何有效的对网络攻击行为、异常行为进行监测防御，是边界安全的重要一环。

（2）控制要求

根据等级保护的要求，针对“安全区域边界”和“安全计算环境”的防护要求包括:

应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为。

应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为。

检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。

应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

（3）控制措施

在网络区域的边界处，需要通过部署入侵防御设备对网络攻击行为进行检测与阻断，并及时产生报警和详尽的报告。

入侵防御设备需要具备以下功能:

①具备新一代检测分析技术

新一代检测引擎能结合异常检测与攻击特征数据库检测的技术，同时也包含了深层数据包检查能力，除了检查第四层数据包外，更能深入检查到第七层的数据包内容，以阻挡恶意攻击的穿透，同时不影响正常程序的工作。

②多层多类型攻击检测

可以检测多层多种类型攻击，如应用型攻击: 包括 Web cc、http get flood、DNS query flood 等攻击；流量性攻击：包括 SYN Flood、UDP Flood、ICMP Flood 、ARP Flood、Frag Flood、Stream Flood 等攻击; 蠕虫连接型攻击; 普通常见攻击: 包括 ipspoof、sroute、land、TCP 标志位攻击、fraggle 攻击、winnuke、queso、sf_scan、null_scan、xmas_scan、ping-of-death、smurf、arp-reverse-query、arp-spoofing 等。

③双向攻击检测

通过对进出网络的流量进行采集分析，可对由内向外发起的网络攻击行为和由外向内发起的网络攻击行为均进行检测和告警。

④日志告警和阻断

网络入侵防御系统除了需要能检测辨别出各种网络入侵攻击，保护网络及服务器主机的安全外，还需要提供完整的取证信息，提

供客户追查黑客攻击的来源，这些信息包括黑客攻击的目标主机、攻击的时间、攻击的手法种类、攻击的次数、黑客攻击的来源 IP 地址等，并提供包括 Email/SNMP trap/声音等方式的告警。对于在线部署模式，可以对攻击行为进行实时阻断。

⑤高可用性

对于在线部署模式的设备，当出现软件故障、硬件故障、电源故障时，系统 bypass 电口自动切换到直通状态以保障网络可用性，能够避免单点故障，不会影响业务。

（4）设备部署

入侵防御系统支持在线部署和旁路部署，针对广西自治区教育厅的网络环境及业务需求，通过在互联网接入边界部署入侵防御系统，实现对网络事件的检测，入侵防御系统采用串接方式部署在防火墙和核心交换机之间，能够有效检测和阻断入侵攻击。

2. 高级威胁攻击检测

（1）安全风险

近年来，具备国家和组织背景新型网络攻击日益增多，其中最为典型的为 APT 攻击，而 APT 攻击采用的攻击手法和技术都是未知漏洞、未知恶意代码等未知行为，在这种情况下，依靠已知特征、已知行为模式进行检测的 IDS、IPS 在无法预知攻击特征、攻击行为模式的情况下，理论上就已无法检测 APT 攻击。

APT 攻击的隐蔽性、持久性和复杂性远超普通的网络攻击行为，且针对的往往是政府、企业、金融等单位的关键应用系统，正式由于 APT 攻击的这些特点，其造成的破坏性往往也是巨大的，使单位、行业乃至国家安全面临严峻挑战，必须采用专门的技术措施对这类攻击进行检测、发现和分析，并能够追踪溯源。

（2）控制要求

面对新的安全威胁形势，新等级保护标准中除了对边界攻击检测能力提出要求外，还明确提出了对高级威胁攻击和未知攻击的检测、发现能力，应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析。

（3）控制措施

通过部署专业的 APT 检测设备，实现对新型网络攻击行为的发现、分析、追溯的能力，设备所需具备的功能包括:

①APT 攻击发现

由于 APT 攻击的复杂性和背景的特殊性，仅依赖于单一企业的数据经常无法有效的发现 APT 攻击，难以做到真正的追踪溯源，而从互联网数据进行发掘和分析，由于任何攻击线索都会有相关联的其他信息被互联网数据捕捉到，所以从互联网进行挖掘可极大提升未知威胁和 APT 攻击的检出效率，而且由于数据的覆盖面更大，可以做到攻击的更精准溯源。

②APT 攻击定位、溯源与阻断

用威胁情报的形式对各种攻击中常出现的特点和背景信息进行记录和传输，而威胁情报将通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化，可对未来扩展攻击特征并进行精准攻击定位和溯源提供支撑。

对 APT 攻击的定位、溯源和阻断离不开专业的安全分析团队，需要能够针对用户网内发现的 APT 攻击等行为进行深度挖掘和分析，减少损失。

③未知恶意代码检测

针对新型攻击和病毒，需要采用机器学习等人工智能算法，通过恶意代码智能检测技术，对海量程序样本进行自动化分析，解决大部分未知恶意程序的发现问题。

④未知漏洞攻击检测

可采用基于沙箱的未知漏洞攻击检测引擎对客户端应用中已知漏洞和未知漏洞的攻击利用进行检测。

（4）设备部署

APT 攻击检测设备旁路部署在核心交换机上，对用户网络中的流量进行全量检测和记录，所有网络行为都将以标准化的格式保存于数据平台，云端威胁情报和本地文件威胁鉴定器分析结果与本地分析平台进行对接，为用户提供基于情报和文件检测的威胁发现与

溯源的能力。

（5）云计算边界入侵防御

通过主机入侵防御组件对云内流量包进行检测过滤，主要功能包括:

●支持多种针对系统、应用漏洞的入侵防御规则，并定期更新规则库。

●对已知的漏洞进行虚拟修补，在虚拟机系统及应用不进行安全补丁升级的情况下，防御针对漏洞的攻击。

●系统自动侦测虚拟机系统的内容，动态的调整用于检测的入侵检测的规则库，提高检测的效率。

●自动更新功能，及时防御针对最新漏洞的攻击。

①东西向攻击防护

通过虚拟化安全的主机防火墙组件对云内主机间的流量进行流量识别、业务关系拓扑、网络访问控制、安全策略管理等安全防护能力。

●对虚机进行微隔离，不但能控制南北向流量，还可以控制云平台内部虚拟机之间的东西向流量。

●按照 IP 地址、端口、流量类型以及流量方向来配置防火墙规则。

②高级威胁感知系统

高级威胁感知系统基于自有的多维度海量互联网数据，进行自动化挖掘与云端关联分析，提前洞悉各种安全威胁，并向客户推送定制的专属威胁情报。同时结合部署在客户本地的软、硬件设备，系统能够对未知威胁的恶意行为实现早期的快速发现，并可对受害目标及攻击源头进行精准定位，最终达到对入侵途径及攻击者背景的研判与溯源。

③可视化分析告警

通过对异常流量的汇总采集分析，检测出外部-内部或内部-外部的异常攻击行为，并通过可视化展示或告警方式通知管理员。

●支持海量安全日志数据的分析及查询。

●安全威胁地图，描述安全威胁发生的地理位置。

●网络流量地图，对网络的新增连接、数据流量、地理位置的分析及数据挖掘。

●以虚拟机、操作系统、应用程序、攻击类型、恶意代码类型、地理位置、时间等多个维度。

●对文件、网络的海量安全数据进行关联性分析，并辅以多种图表形式，对同一数据进行描述，便于用户理解。

●支持安全事件的数据挖掘，便于管理人员及时准确的找到攻

击源，阻断安全威胁。

（三）边界完整性检测。

1. 网络安全准入

针对网络层的非授权连接行为管控可以通过网络安全准入系统（NAC）进行控制，网络安全准入系统需实现以下功能:

（1）安全管理与访问控制

利用网络安全准入系统的动态检测技术和安全策略管理，针对接入用户和终端进行网络访问控制功能。不符合安全策略的计算机终端进行隔离，并友好提示，提供向导式的安全修复指引。拦截可疑的计算机终端或设备、恶意尝试认证的用户，支持强制下线和账号锁定功能。对接入用户进行动态 VLAN 的分配管理，有效的对网络访问权限进行控制。

（2）终端安全合规检查

网络安全准入系统的安全检查策略会检测终端入网安全状态，能快速定位发现入网计算机终端的安全合规状态，并利用其本地防火墙隔离管控技术立即将这个设备与网络上的其它设备隔离起来，只能够访问修复区，同时依照策略进行引导修复。对于已授权合规终端，如发现运行阶段又不符合安全检查策略，可调用周期检查或定时检查引擎，对该终端的安全状态进行二次检查，期间如发现不合规进行再次隔离，禁止其访问企业核心资源，可提供安全检查结

果详情和全网安全状态统计等日志报表。

（3）访客注册申请

针对外来人员临时性的访问需求，能够进行访客入网管理，包括访客用户注册申请、访客认证、用户审批流程，经管理员审批或系统自动审批后才能认证入网，审批结果可邮件通知用户。

（4）第三方认证源联动

能够实现多种认证源认证方式,包括本地用户、AD 认证、LDAP 认证、Email 认证、Http 认证适应用户不同网络环境，满足用户实名制认证、集中统一管理的入网需求。

（5）认证绑定管理

支持多种条件绑定认证，即用户和终端、交换机、VLAN、交换机端口等进行绑定认证、提高入网安全强度。

（6）设备例外管理

用户网络中存在大量的哑终端设备，如：网络打印机、视频会议系统等设备，并分散在各地，能够提供设备的白名单管理，当添加到白名单的合法设备可以直接接入网络，反之非法设备不允许接入，此方式可适应于多种认证技术方式，如：Portal 和 802.1X 认证方式。

（7）强制隔离

用户正常的 802.1X 认证成功后,如果认证会话没有过期网络会

持续可用，系统专有的认证客户端可以实时接收认证服务器的控制指令，管理员可以在任何时候强制在线的用户和终端下线、注销当前登录的网络，确保非正常情况下可对终端入网进行控制和强制隔离处理。

网络安全准入系统（NAC）采用旁路部署，通过监听来发现和评估哪些终端入网是否符合遵从条件，判断哪些终端是否允许安全访问企业核心资源，不符合会被自动拦截要求认证或安装客户端才能进行访问，并可配置入网安全检查策略，不符合进行隔离和修复，达到合规入网的管理规范要求。

2. 违规外联检测

对于终端的非法外联可以通过终端安全管理系统或者采用专业的上网行为管理设备进行控制。终端安全管理系统可对终端的外联端口、外联能力进行检查和阻断，上网行为管理设备通过在网络出口处进行安全策略的配置，限制单位用户的外联访问行为，具体功能如下:

（1）上网行为管理系统

①URL 访问审计与过滤

采用 URL 分类数据库，通过管理员配置基于 URL 分类的控制策略（策略条件可包括用户、部门、时间段、访问类别、URL 关键字、网页内容关键字、下载文件类型等），进行 WEB 访问控制，发现非法访问可进行阻断、记录或报警。

②应用控制

通过应用特征与行为特征对应用进行识别。所谓应用特征，是指在成序列的数据包的应用层信息中，存在有规律的字节特征，它可以唯一地标识某种应用协议。行为特征，是指连续多个包或者多个并发的网络连接表现出来的某种行为模式具有一定规律性，通过这些行为模式可以识别特征值不明显的应用类型。通过精细化的控制策略设置，可以实现对单位应用访问的精细化管理。

③内容审计和过滤

对内容的审计可以有效控制信息的传播范围，控制敏感信息的泄露，避免可能引起的安全风险，内容审计和过滤包括邮件收发审计和过滤、论坛发帖审计和过滤、搜索引擎关键字审计和过滤、HTTP 文件传输审计和过滤、FTP 文件传输审计和过滤等。

④共享接入监控

共享接入是指使用 NAT 等技术将一个网络出口共享到多个主机，共享接入监控能够对接入网络的设备做观察、控制，能够检测到一个用户或 IP 所共享的终端数量，并可以对数量做策略控制，以达到掌控用户终端数量的目的，在监控到用户使用的终端数后，可以对此进行控制，屏蔽该用户的上网流量。

⑤日志审计

能够完整地记录内网用户网络访问的日志，包括上网时间、网络流量、Web 访问记录、接收与发送的邮件等等。为进一步的查询

统计与报表分析提供了完整的基础信息。

（2）终端安全管理系统

为了防止计算机终端用轻易通过拨号、私设代理、多网卡通讯等非法外联手段，造成内部机密外泄的情况发生，终端安全管理系统提供非法外联管控功能，可根据探测类型，使用对应的技术手段如域名解析，对传入的 ip 或是网址进行连接，如果连接成功则根据策略处理措施，进行对应的提示、断网或关机处理。

①外联设备控制（可以禁用终端上可能运行的外联设备——冗余有线网卡、移动数据网卡、MODEM 设备、ISDN 设备、ADSL 设备、WIFI 及 SSID 例外）

②外联能力探测（选择探测方式发现终端是否具有外联能力）

③外联控制措施（发现终端具有外联能力后的处理措施——提示、断网、关机）

上网行为管理系统可以串接和旁路镜像部署在单位的互联网出口处，在串接模式下，串接方式能实现对上网行为的控制，并完整审计所有上网数据。串接包括网桥和网关两种模式，采用网桥模式时，当单位拥有两个互联网出口，且单位内部不同教育城域网需要通过不同的互联网出口连接互联网时，上网行为管理系统可提供双入双出，双网桥的部署模式。通过一台设备即可同时管控两条链路内的用户互联网行为。

3. 边界恶意代码检测

下一代防火墙一般均具有专业的 AV 模块，能在网络重要节点处（如互联网入口）进行病毒的检测和清除，但考虑到部分单位已有的防火墙性能不高，也可以采用专业的防病毒网关，在网络边界处进行病毒的检测和阻断。

下一代防火墙通过启用一体化安全防护策略，将反病毒、漏洞防护、防间谍软件、恶意 URL 防护等功能集成到一条策略，并基于优越的架构设计保障高性能的安全能力。

通过在互联网边界启用下一代防火墙的漏洞防护、防间谍软件、反病毒、URL 过滤等功能，基于本地安全引擎，能高效拦截常见漏洞入侵、间谍软件、病毒、木马、钓鱼网站、恶意 URL 访问等网络威胁。

同时，防火墙通过云端协同可以极大提升特征库数量级，补充本地识别库，并提升防火墙对高级威胁的识别能力，提高防火墙拦截的精确度和高效性。

防火墙的特征库能够支持自动升级，定期进行病毒库的升级和系统的更新。

为实现对病毒的实时阻断，在互联网边界需串接防火墙，开启 AV 模块，或在防火墙后串接专业的防病毒网关，实现从网络层检测和阻断恶意代码。

4. 网络安全审计

网络安全审计系统通过镜像获取通过核心交换机上流量数据对

整个网络的流量进行审计分析，对用户的行为进行审计。包括以下内容:

●对用户的 HTTP、邮件、FTP、TELNET 等应用进行审计。

●对远程桌面、QQ 远程等远程访问行为进行审计。

●对用户的互联网访问行为进行审计。

●本地日志可以 FTP、USB 等方式导出，支持将日志发送至外置日志存储系统，确保日志记录满足合规要求。

网络安全事件的踪迹一般都分布在网络的边界设备、安全设备、访问控制设备的日志中，除对网络流量中用户的行为进行审计分析外，发现网络安全事件也是网络安全审计的重要目标，集中安全审计系统通过收集网络设备、安全设备、服务器、应用系统等的日志信息，结合网络流量日志进行关联分析，可以快速发现网络安全事件，并进行定位和报警。

云服务客户根据需求选择开通日志审计、云安全运维审计等审计系统，对云上用户访问行为、操作行为、安全运维审计等行为进行细粒度的日志审计、存储、分析等。

（1）综合日志审计

①提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计。

②保证无法单独终端审计进程，避免非授权和未预期地删除、修改或覆盖审计记录。

③审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等。

④应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

⑤日志审计功能应能提供给用户访问行为审计、审计信息查询、审计信息分析等模块，以及异常行为管理和配置与管理等供管理员使用的模块。

（2）访问行为审计

对系统访问行为数据进行收集、整理的基础上进行分析和审计。包括：用户标识与鉴别、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除文件、数据库中的记录）等。

（3）审计信息查询

查询范围应包括日期与时间、触发事件的主体与客体、事件的类型、事件中请求的来源、事件的结果等内容。

审计人员应能够通过内置的查询定义器方便地制作新的查询操作、搜索范围以及查询结果的表现形式，如列表、分组排列、柱状图、饼状图等。通用数据查询系统可以保存或按指定格式导出（如 Excel 或 XML）查询结果，支持对查询结果的分析加工。用户还可以在查询结果范围内进行再查询。

（4）异常行为管理

系统应提供异常行为注册、调整、删除和查询等功能，应具备对系统中的异常行为进行分类、注册、定义影响级别、配置报警方式（如短信、邮件和其它方式）的功能。

（5）系统配置与管理

配置与管理模块为后台管理员、审计人员和业务操作员提供对系统进行管理、配置的功能。主要应包括：配置查询条件、需要监控的资源以及报警方式等。对于查询条件，应能通过简单定义就可以实现复杂的查询条件组合查找需要的数据，还应可以自动跟踪查询与该数据相关联的明细数据；另外，系统应还可以通过配置实现对于重要应用系统和系统资源监控的添加和删除。

3.10.3.4 计算环境

（一）主机身份鉴别与访问控制。

针对主机的双因素身份鉴别一般可采用专业的终端安全登录产品，终端安全登录产品可结合现有的CA系统实现基于数字证书的双因素认证，终端安全登录产品所使用的密码设备应符合国家密码管理相关要求。

针对主机访问控制的要求，采用服务器加固系统，并进行以下安全配置:

1. 启用访问控制功能，依据安全策略控制用户对资源的访问;

2. 根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限;

3. 严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令;

4. 及时删除多余的、过期的帐户，避免共享帐户的存在;

5. 对重要信息资源设置敏感标记;

6. 依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

对重要的主机系统采用专业的主机安全加固系统对主机进行整体安全防护，设置强制安全访问控制策略，从而使操作系统达到 B1 级高安全级别。对数据库进行安全配置，对于存储大量敏感数据的数据库采用安全数据库或数据库防火墙进行保护。

（二）一体化终端安全防护。

综合分析单位面临的终端安全风险，需要一个综合的终端安全管理系统，以应对不同层面的安全需求，满足合规要求，而满足这些安全需求的同时，又不会割裂这些系统之间的关系，使得他们能在统一的安全环境里执行一致的安全策略，并互相协同，发挥最大的安全防护效率。

采用终端安全管理系统作为终端合规管控一体化解决方案。通过建设恶意代码防范体系、落实终端安全管理技术措施、启用统一终端运维、开启安全审计功能，来建设终端合规一体化体系，一体

化终端安全管理的建设内容如下:

1. 终端恶意代码防护

全网部署终端安全管理系统客户端代理，通过集中管理端实现对病毒查杀策略、病毒库的统一升级管理。通过采用云查杀引擎、未知病毒检测等新技术，解决传统防病毒软件本地特征库对新型病毒查杀效果不明显的问题。

2. 终端统一安全管控

在终端安全管理系统的控制中心制定策略，进行全网终端的流量监控、非法外联监控、应用程序黑白名单控制、外设管控、桌面安全加固等。

3. 终端软件管理

通过策略配置和日志报表功能，管理员可以掌握网内软件使用情况，及时发现异常，保证企业内部网软件的正常运行和软件安全性，支持单位软件的统一分组、定时分发，并可实现自动安装应用以及强制卸载应用，帮助管理员按照企业规定管理终端用户软件的安装。

4. 统一补丁升级和管理

网络中存在各种不同类型的操作系统及不同版本的操作系统都需要进行全面的补丁管理，终端安全管理系统控制中心对全网计算机进行漏洞扫描把计算机与漏洞进行多维关联，根据终端或漏洞进行分组管理，并且能够根据不同的计算机分组与操作系统类型将补

丁错峰下发，并能实现对补丁库的统一升级和管理。

5. 终端统一安全运维

终端安全管理系统统一运维功能,实现全网终端硬件资产管理，并且通过远程协助功能，当终端需要远程帮助的时候，运维人员向终端用户发送远程控制请求，等终端用户确认后，协助 IT 维护人员高效的完成终端运维工作。

6. 终端综合审计

终端安全管理系统通过综合审计功能，对终端用户的行为进行审计，审计内容包括软件使用日志、外设使用日志、开关机日志、系统帐号日志、文件操作日志、文件打印日志、邮件记录日志等;并提供报表功能，对终端安全日志、漏洞修复、病毒日志、木马查杀、插件清除、安全配置、文件及应用日志、终端事件告警等信息进行报表统计。

在网络内部部署终端安全管理系统控制中心和终端，终端通过控制中心连接到升级服务器进行升级、更新等。终端根据控制中心制定的安全策略，进行杀毒、修复漏洞、运维管控、移动存储管理等安全操作。

（三）主机脆弱性评估与检测。

漏洞扫描系统针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况并进行综合评估，在黑客

发现系统漏洞前提供给客户安全隐患评估报告,提前进行漏洞修复,提前预防黑客攻击事件的发生。

通过部署漏洞扫描系统，可以帮助用户快速建立针对自己网络的安全风险评估体系。

1. 发现内部资产

帮助用户快速发现内部资产，避免未知资产带来的安全风险,实现内部 IT 资产的标识和分类管理,方便安全扫描策略的部署和风险评估的进行。

2. 实现针对内部网络的脆弱性评估

通过漏洞知识库以及多样的漏洞扫描策略，针对网络设备、系统主机、应用程序等存在的漏洞和风险进行有效评估，并生产完善的评估报告，帮助用户建立起高效的安全漏洞管理解决方案。

3. 建立完善的漏洞管理和风险评估体系

通过定期的漏洞扫描和漏洞验证帮助用户形成规范的全网漏洞管理体系，并辅以风险报表以及解决方案建议，为用户提供了完整的从漏洞发现、验证、修复建议的流程。

4. 解决漏洞原因造成的安全问题

实时漏洞扫描，定期安全漏洞评估帮助用户及时修复当前系统中存在的漏洞，避免漏洞问题造成的安全威胁和带来的安全隐患。

漏洞扫描系统可旁路部署在待评估网络中的核心交换机上，网络可达待评估的主机、网络设备和系统软件。

（四）虚拟机安全防护。

针对虚拟主机可以采用虚拟化安全管理系统对虚拟主机进行统一的安全防护。

1. 虚拟化安全管理系统可以实现以下功能。

（1）恶意软件防护。无需在虚拟机内部安装杀毒软件，防止其受病毒、间谍软件、木马和其他恶意软件的侵害。能实现恶意代码特征库的自动更新。

（2）进程管控。支持白名单和黑名单方式，可针对不同的用户场景灵活配置管控规则，未被允许的进程将无法使用，彻底阻止勒索软件或其他恶意软件执行。

（3）防火墙。对虚机进行微隔离，不但能控制南北向流量，还可以控制云平台内部虚拟机之间的东西向流量。按照 IP 地址、端口、流量类型以及流量方向来配置防火墙规则。

（4）应用控制。对应用协议进行分类，针对分类配置阻断、放行策略，对于新增的应用，能自动应用分类的配置策略。自动更新应用解析的规则库，不断增加新应用的支持，及时识别更新后的网络应用。

（5）入侵防护。对已知的漏洞进行虚拟修补，在虚拟机系统及应用不进行安全补丁升级的情况下，防御针对漏洞的攻击。防护 SQL 注入,跨站脚本攻击及其他的利用 Web 应用程序漏洞的攻击，并能及时防御针对最新漏洞的攻击。

（6）DDoS 防护。对 TCP、UDP 和 ICMP Flood 攻击的防护，能针对每台虚拟机单独进行流量清洗。

2. 虚拟化安全管理系统由管理中心和安全组件两部分组成。

（1）管理中心。接收安全组件上传的安全事件和网络流量日志，通过多维度、细粒度的大数据分析，并以可视化的形式展现给用户，从而帮助用户对已知威胁进行溯源，并对未知威胁进行预警。

（2）安全组件。安装在网络中心每个计算节点、物理服务器上，接收管理中心配置的安全策略，对虚拟机或物理终端进行文件、网络和系统的安全防护，并将安全事件及行为日志上传到管理中心进行分析。

（五）应用身份鉴别与访问控制。

因此，需要实现对应用系统访问的双因素认证，采用身份认证服务系统可以实现对用户身份的统一管理和多种方式组合的强身份认证。

身份认证服务系统可以与安全接入网关（SSL VPN）共同构建应用身份解决方案，该解决方案主要实现以下功能:

1. 多因素身份认证

根据不同的应用场景，可以提供动态口令、数字证书、指纹、二维码等身份安全机制。

2. 口令传输安全加密

身份认证系统与终端间传输的认证信息进行加密处理，加密算

法采用 RSA、DES、3DES、AES 等多种加密算法组合。为了满足国家信息安全的需要，系统同时支持 SM 系列国密算法，大大降低了认证信息被劫持、被破译的风险。

3. 数据传输加密

在用户通过认证接入 SSL VPN 后，客户端和服务端通信，传输的数据都默认使用安全的 SSL 传输技术。确保用户账号密码、动态秘钥、应用数据传输的高安全性及稳定性。同时支持移动终端隧道控制策略，实现移动终端连接 VPN 以后，移动终端数据只能走 VPN，不能访问互联网，从而实现防止数据泄密。

同时，为了满足国密办信息安全的相关规定，加强密码算法的安全性。SSL VPN 完整支持国密算法，包括 SM1、SM2、SM3、SM4。

4. 访问控制

为不同职责人员匹配不同业务应用，精细化访问控制技术能够细粒度控制接入可以到用户级、资源级，甚至下到 URL 和文件级的权限，这样不同的用户拥有不同的访问权限。

5. 虚拟工作区

为防止工作区的数据遗落到个人数据区，SSL VPN 采用虚拟工作区进行数据分离。个人数据与企业数据进行隔离，落地数据加密，第三方应用或转发到其它设备当中无法打开查看。启用虚拟工作区之后，终端数据落地加密，数据采用 AES256 或者 SM4 加密算法，

防止终端数据被拷贝出去而造成数据泄密。

当 VPN 客户端被卸载、设备进行了 Root 或者设备超过一定时间不能连接上网关的情况下，移动终端数据可以远程擦除，防止数据泄密。

身份认证系统分为两部分组成：硬件平台与客户端 APP。硬件平台采用旁路部署在企业内网，与用户的业务系统/认证系统做到网络可达。

（六）WEB 应用安全防护。

可以采用 WEB 应用防火墙对 WEB 应用进行安全防护。WEB 防火墙可针对 WEB 应用实现以下防护功能。

1. 漏洞防护

Web 应用防火墙能够对 SQL 注入、跨站脚本、代码执行、目录遍历、脚本源代码泄露、CRLF 注入、COOKIE 篡改、URL 重定向等多种漏洞攻击进行有效防护。

2. 攻击防护

Web 应用防火墙能够对用户请求提供多重检查机制和智能分析，确保对高安全风险级别攻击事件的准确识别率。针对 Flood 攻击、SQL 注入、跨站脚本、目录遍历等主要攻击手段，WAF 系统提供了有效识别、阻断并告警。

3. 网页代码检查

Web 应用防火墙能够对用 ASP、ASPX、JSP、PHP、CGI 等语

言编写的页面，对用 SQL Server、MySQL、Oracle 等数据构建的网站进行检查，能够在客户网站被挂马之前发现网站的脆弱点，从而使客户可以未雨绸缪，避免挂马事件的发生。

4. 访问加速

Web 应用防火墙通过在现有的互联网中增加一层新的网络架构，将网站服务器内容缓存到系统内存中，使用户可以就近取得所需内容，降低服务器的压力，解决互联网拥挤的状况，提高用户访问服务器的响应速度。从而解决由于网络带宽小、用户访问量大、网点分布不均等原因所造成的用户访问网站响应速度慢的问题。

5. 挂马检测

多数攻击者在成功入侵并不采取直接的网站篡改，为了获取更多的经济利益往往采取比较隐蔽的方式，其最终目的是为了盗取用户的敏感信息，如各类账号密码，甚至使用户电脑沦为攻击者的“肉鸡”。一旦网站服务器成为传播病毒木马的“傀儡帮凶”，将会严重影响到网站的公众信誉度。

6. 网页防篡改

Web 应用防火墙内置有网页防篡改监控平台，可以对网页防篡改客户端进行实时监控。当网页防篡改客户端与 Web 应用防火墙的网络中断时，网页文件会被自动锁定，所有“写”的权限进行封锁，只有“读”的权限。当网络恢复中，所有相关权限会自动下发，网站正常恢复更新。

为云平台互联网业务服务部署云端网站安全防护系统对 Web 攻击进行拦截，防止数据库被拖库、网页被恶意篡改、网站被挂马、被挂链接、网站敏感信息泄露等网站安事件的发生。在前置服务区采用纯透明串行模式部署 Web 应用防火墙,交换机上串行接入 Web 应用防火墙，所有 Web 请求和恶意访问攻击均由 Web 应用防火墙来承担处理，清洗、过滤后 Web 应用防火墙向真实的服务器提交请求并将响应进行整形、压缩等处理后送交给请求客户端。这样可以很好的防范来自互联网的威胁，保护网站的安全、稳定、高性能运行。

（七）应用开发安全与审计。

在系统开发过程中,应当在设计阶段同步考虑安全功能的设计,并在系统编码阶段同步实现安全功能，按照等级保护的要求，应用系统应具备以下安全功能:

1. 身份鉴别

应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换。

应提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施。

应强制用户首次登录时修改初始口令。

用户身份鉴别信息丢失或失效时，应采用技术措施确保鉴别信息重置过程的安全。

应采用两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用动态口令、密码技术或生物技术来实现。

2. 访问控制

应提供访问控制功能，对登录的用户分配账号和权限。

应重命名或删除默认账户，修改默认账户的默认口令。

应及时删除或停用多余的、过期的账户，避免共享账户的存在。

应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则。

访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级。

应对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。

3. 安全审计

应提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

应对审计记录进行保护，定期备份，避免受到未预期的删除、

修改或覆盖等。

应确保审计记录的留存时间符合法律法规要求。

应对审计进程进行保护，防止未经授权的中断。

4. 入侵防范

应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。

5. 数据完整性

应采用校验码技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

6. 数据保密性

应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

7. 剩余信息保护

应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

8. 个人信息保护

应仅采集和保存业务必需的用户个人信息。

应禁止未授权访问和非法使用用户个人信息。

第三方软件开发商应具备相应的开发资质，在应用开发过程中采用安全开发过程管理，并采用代码安全检测工具在开发过程中进行代码安全检测与审计，并要求第三方开发厂商提供系统源代码。

（八）数据加密与保护。

等级保护制度中，对于数据安全的防护要求主要是从完整性和保密性进行规范的，并主要定义了数据在传输和存储环节的安全要求，包括:

应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

应采用密码技术保证重要数 据在传输过程中的保密性,包括但不限于鉴别数据 、重要业务数据和重要个人信息等。

应采用密码技术保证重要数据在存储过程中的保密性，包括但

不限于鉴别数据、重要业务数据和重要个人信息等。

数据的完整性和保密性保护措施可以在应用系统开发过程中同步采取基于密码技术的相关功能实现,但数据保护是个复杂的过程,由于数据的分散性和流动性，在终端、网络、数据库等各层面也需要采用相关的数据防护措施。

通过以下具体的技术保护手段，在数据和文档的生命周期过程中对其进行安全相关防护，确保内部数据在整个生命周期的过程中的安全。

1. 加强对于数据的分级分类管理

对关键敏感数据须设置标记，对于重要的数据应对其本身设置相应的认证机制。

2. 加强对于数据的授权管理

对文件系统的访问权限进行一定的限制；对网络共享文件夹进行必要的认证和授权。除非特别必要，可禁止在个人的计算机上设置网络文件夹共享。

3. 数据和文档加密

保护数据和文档的另一个重要方法是进行数据和文档加密。数据加密后，即使别人获得了相应的数据和文档，也无法获得其中的内容。

网络设备、操作系统、数据库系统和应用程序的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实

现传输保密性和存储保密性。

当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

4. 加强对数据和文档日志审计管理

使用审计策略对文件夹、数据和文档进行审计，审计结果记录在安全日志中，通过安全日志就可查看哪些组或用户对文件夹、文件进行了什么级别的操作，从而发现系统可能面临的非法访问，并通过采取相应的措施，将这种安全隐患减到最低。

5. 进行通信保密

用于特定业务通信的通信信道应符合相关的国家规定，密码算法和密钥的使用应符合国家密码管理规定。

对于存在大量敏感信息的系统，还可针对信息系统和数据在使用过程中面临的具体风险进行整体地分析，采用专业的数据防泄密系统对数据进行全生命周期防护。

（九）数据访问安全审计。

数据库审计系统能够对业务网络中的各种数据库进行全方位的安全审计，具体包括:

1. 数据访问审计。记录所有对保护数据的访问信息，包括文件操作、数据库执行 SQL 语句或存储过程等。系统审计所有用户对关键数据的访问行为，防止外部黑客入侵访问和内部人员非法获取敏感信息。

2. 数据变更审计。统计和查询所有被保护数据的变更记录，包括核心业务数据库表结构、关键数据文件的修改操作等等，防止外部和内部人员非法篡改重要的业务数据。

3. 用户操作审计。统计和查询所有用户的登录成功和失败尝试记录,记录所有用户的访问操作和用户配置信息及其权限变更情况，可用于事故和故障的追踪和诊断。

4. 违规访问行为审计。记录和发现用户违规访问。支持设定用户黑白名单，以及定义复杂的合规规则，支持告警。

数据库审计系统旁路部署在服务器区，对数据库访问行为进行审计。

（十）数据备份与恢复。

等级保护制度中，针对数据的备份和恢复要求，应用数据的备份和恢复应具有以下功能:

1. 应提供重要数据的本地数据备份与恢复功能。

2. 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

3. 应提供重要数据处理系统的热冗余，保证系统的高可用性。

数据库区作为内网系统中最为关键的区域，存储着重要的信息数据，分布着学籍系统数据库、教师管理数据库、综合教务系统数据库、学生就业信息系统数据库等，所有需要安装数据库的业务系统的操作数据会实时的存储于数据库中，故对数据区的保护为重中

之重。再者为了数据更加安全的角度考虑，可以将数据库中的数据定向到存储区域的磁盘阵列中，更加长久安全的保护了重要数据。

为了实现网络中心改造后虚拟化架构子系统的资源优化和高可用功能，通过搭建存储区域网络来满足虚拟机文件和的存储需求。存储区域利用 2 台光纤交换机和 2 套磁盘阵列系统来构建，磁盘阵列用来存储 DMZ 区域中所有虚拟机文件及服务器区虚拟机文件。

而分布式存储系统利用多台 PC 服务器中的存储空间聚合成一个能够给应用服务器以及数据库服务器提供统一访问接口和管理界面的存储池，应用及数据库可以通过该访问接口非常容易的管理存储池后端物理存储设备上所有的磁盘，充分发挥存储设备的性能和磁盘利用率。

3.10.3.5 管理中心

按照等保“一个中心三重防护”建设思路，一个中心是指“安全管理中心”。根据安全管理中心相关要求，划分“安全管理区”，并在该区域部署相关设备系统:

1．根据等保系统管理要求，在教育骨干网该区域部署运维安全管理系统。配置可以访问所有管控对象，包括教育城域网内设备，以及直属管理的校园网出口设备，通过逻辑上将管理人员与目标设备分离，建立“人->管理主账号->授权->目标从账号->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控

制策略，与各网络设备、安全设备，以及后续增加的服务器和数据库等进行连接，实现集中精细化运维操作管控与审计，并对高危操作进行授权审批。

2．根据等保集中管控要求，在教育骨干网该区域部署安全态势感知系统。教育网可以通过安全态势感知系统实现整个教育网的安全运营，借助安全可视和安全事件工单制实现各级党组党委责任分明，权责明确；通过安全运营机制不断发现教育网的安全问题，并且不断完善安全防御体系，保持教育网的健壮性；通过安全态势感知系统现有内置的驻留程序实现对终端设备的入网认证信息同步，保证教育网终端设备可视安全可控。同时，教育骨干网新增安全态势感系统需要和广西教育数据中心实现一体化管理运维，实现完整有效、更全面、更直观可视的展示。

3．根据等保集中管控要求，在教育骨干网该区域部署统一身份认证管理系统。统一身份认证管理系统强调以人为中心进行访问控制，提供统一身份管理、统一身份认证、统一门户/单点登录(SSO)、集中应用授权、审计与分析等功能，让认证更简易、身份更安全、应用访问更可控。同时，实现身份全生命周期管理，降低管理员账号开户、变更、销户等带来的运维复杂度，让管理更高效。未通过身份认证的用户、设备禁止接入教育网和互联网，仅能在接入的教育城域网内限时使用。本项目统一身份认证管理系统通过教育部省级部署的全国教育管理信息系统(全国中小学生学籍信息管理系统、

全国学前教育管理信息系统、全国中等职业学校学生管理信息系统、全国教师管理信息系统）获取身份数据，根据个人分配的账号密码比对用户身份实现鉴权登录。支持同步身份到安全态势感知平台进行统一展示，确保发现安全问题及攻击威胁时，能第一时间定位到终端位置及使用人，方便运维人员进行快速处理，实现安全问题的快速闭环。

4．根据安全管理的要求，在安全管理区（广西教育数据中心和高校城市节点机房）部署终端安全管理系统管理端，在本级教育城域网、下属教育城域网内终端上部署终端安全管理系统，实现教育城域网内主机终端病毒的查杀，使主机终端免受病毒、特洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散布到整个教育城域网的网络环境，具备完整的病毒扫描防护功能，对主流系统平台下进行完整病毒查杀；同时终端安全管理系统还具备进程管理、软件管理、补丁管理、外设管理等功能，能够实现主机终端入侵防范的能力，统一下发应用软件，统一实现漏洞修复，以及非法外联的管控。由自治区教育厅“广西教育信息化终端应用管理和安全态势感知管理信息系统”承担相关建设、管理和运维工作，教育网项目不涉及此项目建设。

5. 在各级教育城域网安全管理区部署安全日志审计系统。配置可以接收所有日志对象，包括本级教育城域网内设备、下属校园网和教育机构网络出口设备，实时采集不同厂商的安全设备、网络设

备产生的日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，出具丰富的报表报告，获悉教育城域网的整体安全运行状况，实现全生命周期的安全管理。

6. 在各级教育城域网安全管理区部署运维管理系统。配置可以访问所有管控对象，包括本级教育城域网内设备，以及直属管理的校园网出口设备，通过逻辑上将管理人员与目标设备分离，建立“人->管理主账号->授权->目标从账号->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控制策略 ，与各网络设备、安全设备，以及后续增加的服务器和数据库等进行连接，实现集中精细化运维操作管控与审计，并需要对高危操作进行授权审批。

7. 在各级教育城域网核心交换区部署检测探针。通过网络流量镜像在内部对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行初步的攻击识别、违规行为检测与内网异常行为识别，同时可以将检测数据与分析结果上传至广西教育数据中心核心节点进行汇总分析。

8. 在各级教育城域网安全管理区域部署安全态势感知系统，对检测探针的数据和各个安全设备日志进行收集，并通过可视化的形式为用户呈现内网业务资产及针对内网关键业务资产的攻击与潜在威胁，安全态势感知系统支持下发策略至防火墙等安全设备，对攻

击进行一键封锁，并形成安全问题工单，派发工单通知内部运维人员进行处置，通过该系统对现网所有安全系统进行统一安全管理。通过安全安全态势感知系统现有内置的驻留程序实现对终端设备的入网认证信息同步，保证教育网终端设备可视可控。

安全态势感知系统应配置开放接口，可以使用公开标准接口或公开标准协议，与广西教育数据中心核心节点的安全态势感知系统共享交换数据，在广西教育数据中心核心节点可以实现对广西教育网全网安全的可视化和感知管控。

9. 在各级教育城域网安全管理区部署漏洞扫描系统，配置可以访问所有检测对象，包括本级教育城域网内设备、下属校园网和教育机构的出口设备，评估各个网络区域的安全状况，包括现有的网络设备和安全设备，以及后续增加的 WEB 应用、服务器区域、数据库等。通过漏洞扫描系统，能够主动对网络中的资产进行细致深入的漏洞检测、分析，并能提供专业、有效的漏洞防护建议，帮助运维管理人员落实安全整改问题。

3.10.4 管理体系

3.10.4.1 管理制度

（一）安全策略和制度体系。

1. 建设思路

安全技术措施的有效实施需要安全管理制度的助力，同样，安

全管理制度的落实也常常需要技术措施的支撑，两者是相辅相成，相互关联的，等级保护对于安全制度体系的建设要求参照了 ISO 27001 的相关标准，即安全管理制度体系自上而下分为安全策略、管理制度和操作规程、记录表单，单位需要建设符合单位实际情况的管理制度体系，应覆盖物理、网络、主机系统、数据、应用、建设和运维等管理内容，并对管理人员或操作人员执行的日常管理操作建立操作规程。

2. 建设内容

单位信息安全管理制度体系应结合实际业务需要，建立符合本单位实际情况的安全制度体系，需包括信息安全方针、安全策略、安全管理制度、安全技术规范以及流程等，如下所示。

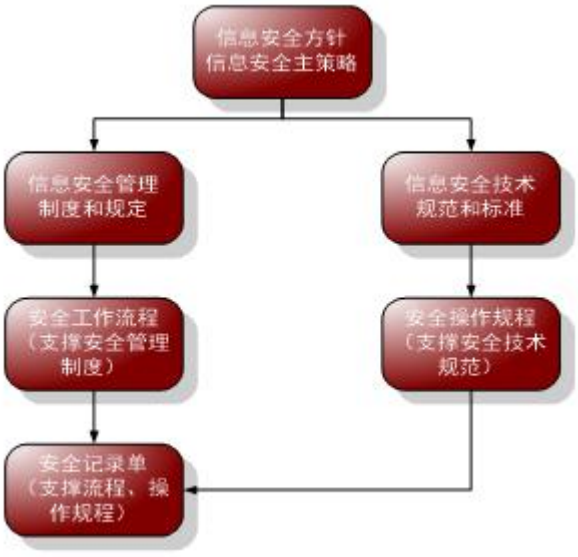

图 5-34 安全管理制度体系图

（1）安全方针和策略

包括：最高方针，纲领性的安全策略主文档，陈述本策略的目的、适用范围、信息安全的管理意图、支持目标以及指导原则，信息安全各个方面所应遵守的原则方法和指导性策略。

（2）安全管理制度

包括：各类管理规定、管理办法和暂行规定。从安全策略主文档中规定的安全各个方面所应遵守的原则方法和指导性策略引出的具体管理规定、管理办法和实施办法，是必须具有可操作性，而且必须得到有效推行和实施的。

（3）安全技术标准和规范

包括：各个安全等级区域网络设备、主机操作系统和主要应用程序的应遵守的安全配置和管理的技术标准和规范。技术标准和规范将作为各个网络设备、主机操作系统和应用程序的安装、配置、采购、项目评审、日常安全管理和维护时必须遵照的标准，不允许发生违背和冲突。

（4）安全流程和操作规程

为信息安全建立相关的流程，保证安全运营可以遵照标准流程制度执行，主要的内容包括。

①流程制定。建立健全流程管理制度，主要包括的流程有安全事件处置流程、安全风险评估流程、安全事件应急响应流程、安全

事件溯源取证流程、安全设备上线交割流程等。

②流程变更维护。定期的维护和修订相关的管理制度。

③流程发布。根据需要，定期发布变更后的全套流程到相关的组织范围内，并对发布的流程进行相关的培训。

（5）安全记录单

安全记录单是落实安全流程和操作规程的具体表单，根据不同等级信息系统的要求可以通过不同方式的安全记录单落实并在日常工作中具体执行。主要包括日常操作的记录、工作记录、流转记录以及审批记录等。

（二）制度文件管理。

1. 建设思路

制度文件需要正式发布并进行定期评审修订和版本控制。信息安全管理制度应该得到单位负责人的签发和认可，只有被正式发布并真正落实的管理制度才能促使单位安全管理能力的提升和安全技术措施的有效运行。

2. 建设流程

信息安全管理制度体系是不断改进和完善的过程，包括以下:

（1）制定和发布

安全制度系列文档制定后，必须有效发布和执行。发布和执行

过程中除了要得到管理层的大力支持和推动外,还必须要有合适的、可行的发布和推动手段，同时在发布和执行前对每个人员都要做与其相关部分的充分培训，保证每个人员都知道和了解与其相关部分的内容。

安全制度在制定和发布过程中，应当实施以下安全管理:

●安全管理制度应具有统一的格式，并进行版本控制。

●安全管理职能部门应组织相关人员对制定的安全管理制度进行论证和审定。

●安全管理制度应通过正式、有效的方式发布。

●安全管理制度应注明发布范围，并对收发文进行登记。

必须要注意到这是一个长期、艰苦的工作，需要付出艰苦的努力，而且由于牵扯到许多部门和绝大多数员工，可能需要改变工作方式和流程，所以推行起来的阻力会相当大；同时安全策略本身存在的缺陷，包括不切实可行，太过复杂和繁琐，部分规定有缺欠等，都会导致整体策略难以落实，需要不断改进。

（2）评审和修订

网络安全领导小组应组织相关人员对于信息安全制度体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视安全策略系列文档，具体检查内容包括:

●信息安全策略中的主要更新。

●信息安全标准中的主要更新。信息安全标准不需要全部更新，可以仅对因变更而受影响的部分进行更新；如果必要，可以使用年度审视／更新流程对信息安全标准做一次全面更新。

●安全管理组织机构和人员的安全职责的主要更新。

●操作流程的主要更新。

●各类管理规定、管理办法和暂行规定的主要更新。

●用户协议的主要更新等等。

3.10.4.2 管理机构

（一）网络安全组织机构及职责。

1.建设思路

网络安全管理机构是行使单位网络安全管理智能的重要机构，一般由网络安全管理领导机构和执行机构构成，网络安全领导机构需确保整个组织贯彻单位的网络安全方针、策略和制度等。等级保护制度中明确规定“单位应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权。”并设立网络安全管理的职能部门。

2.建设内容

单位应根据管理工作需要设立安全管理机构，但至少应包括网

络安全领导小组和网络安全管理职能部门，其工作职责分工如下:

（1）网络安全领导小组

网络安全领导小组是网络安全工作的最高领导决策机构，负责网络安全工作的宏观管理,其最高领导由单位主管领导担任或授权，职责如下:

贯彻执行国家关于网络安全工作的方针、政策，组织落实网络安全体系建设工作的目标、方针、政策。

审定网络安全相关策略、规范及管理规定。

监督、检查网络安全相关制度的落实与执行情况。

协调指挥网络安全重大突发事件的应急处理。

完成上级单位交办的有关工作。

（2）网络安全管理部门

网络安全管理部门负责落实网络安全领导小组各项决策，协调组织各项网络安全工作，具体职责如下:

负责网络安全日常工作的协调和处理。

负责网络安全总体规划设计与实施。

组织网络安全管理规定的编制。

督促网络安全重大突发事件应急预案的落实。

组织网络安全培训的相关工作。

完成网络安全领导小组交办的有关事项。

（二）岗位职责及授权审批。

1. 建设思路

网络安全管理应落实岗位安全责任，网络安全组织机构及职责明确了组织层面的管理职责,但管理职责的落实需要层层落实到人，等级保护中明确要求要“设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责”，并设立系统管理员、审计管理员和安全管理员，并明确岗位工作职责。

2. 建设内容

根据单位实际情况，设立相关的网络安全管理岗位，但至少应包括安全主管以及“三员”(系统管理员、审计管理员和安全管理员)，且“三员”工作职责需分工明确，互相监督，安全管理员需专职，不得兼任其他岗位工作。

三员的岗位职责建议如下:

（1）安全管理员

安全管理员不能兼任网络管理员、系统管理员，其职责是:

组织网络系统的安全风险评估工作,并定期进行系统漏洞扫描，形成安全现状评估报告。

定期编制网络安全状态报告，向网络安全领导小组报告网络安全整体情况。

负责核心网络安全设备的安全配置管理工作。

编制网络安全设备和系统的运行维护标准。

负责网络系统安全监督及网络安全管理系统、补丁分发系统和防病毒系统的日常运行维护工作

负责沟通、协调和组织处理网络安全事件，确保网络安全事件能够及时处置和响应。

（2）系统管理员

系统管理员不能兼任安全管理员，其职责是:

负责网络及网络安全设备的配置、部署、运行维护和日常管理工作。

负责编制网络及网络安全设备的安全配置标准。

能够及时发现、处理网络、网络安全设备的故障和相关安全事件，并能根据流程及时上报，减少网络安全事件的扩大和影响。

负责服务器的日常安全管理工作，确保服务器操作系统的漏洞最小化，保障服务器的安全稳定运行。;

负责编制服务器操作系统的安全配置标准。

能够及时发现、处理服务器和操作系统相关安全事件，并能根

据流程及时上报，减少网络安全事件的扩大和影响。

（3）安全审计员

安全审计员的职责是:

定期审计网络安全制度执行情况，收集和分析网络系统日志和审计记录，及时报告可能存在的问题。

对安全、网络、系统、应用、数据库管理员的操作行为进行监督，对安全职责落实情况进行检查。

单位可根据实际管理需要进行岗位职责的细化，如将系统管理和网络管理工作分别由不同的人负责，对重要的应用系统设置业务系统管理员，对机房、数据库、信息资产进行专门的管理，设置机房管理员、数据库管理员、网络资产管理员等，并明确岗位职责。

在明确岗位职责过程中，单位需梳理在网络安全管理过程中需要授权审批的事项，并根据各个部门和岗位的职责明确授权审批部门和批准人等，对于系统变更、重要操作、物理访问和系统接入等重要事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度，并定期审查，及时更新相关信息。

（三）内部沟通和外部合作。

1. 建设思路

网络安全管理工作不是孤立的，在单位业务工作中离不开安全

管理工作的保障，同样，网络安全管理工作也离不开单位业务部门的配合，要使网络安全管理工作顺利开展，需“加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题”，加强内部沟通。

同时，单位的网络安全工作也需要得到外部专家和技术力量的支持，包括监管部门、供应商、业界专家及其他安全组织等。

2. 建设内容

聘请专家和外部顾问成员，这些成员需要对网络安全或相关领域有丰富的知识和经验，如安全技术、电子政务、等级保护或质量管理等。专家和外部顾问负责对网络安全重要问题的决策提供咨询和建议。

同时加强与供应商、业界专家、专业的安全公司等安全组织的合作和沟通。建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。

（四）安全审核与检查。

1. 建设思路

网络安全管理工作是否有效，安全制度和规范是否得到落实需要单位网络安全管理部门定期进行检查，以便及时发现问题，持续改进和提升网络安全管理能力。按照等级保护的要求，单位网络安全检查可分为定期常规安全检查和定期全面安全检查，安全检查工

作需进行认真准备，保留记录。

2. 建设内容

单位可根据实际情况，进行安全检查工作安排。包括:

（1）定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。

（2）定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；由于单位人员及安全技术能力有限，全面安全检查可请专业的安全厂商协助完成。

（3）制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。单位也可参照上级单位或自行制定安全检查评价指标，以便量化考核安全工作的执行情况。

3.10.4.3 管理人员

（一）内部人员安全管理。

1. 建设思路

人是网络安全工作的主体，也是网络安全威胁的主要来源，调查发现，越来越多的网络安全事件是由内部人员的恶意或工作疏忽导致，因此，加强人员安全管理是网络安全管理工作的重中之重，

其中，尤其需要加强对内部人员的安全教育和审核。

2. 建设内容

针对内部人员的安全管理需从人员的录用、安全培训和教育、技能考核和调用、离岗审核等全过程进行安全管理，具体管理要求包括:

（1）录用前

指定或授权专门的部门或人员负责人员录用。

应对被录用人员的身份、安全背景、专业资格或资质等进行审查， 对其所具有的技术技能进行考核。

与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

（2）工作期间

对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训。

定期对不同岗位的人员进行技能考核。

（3）调离岗

及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、

徽章等以及机构提供的软硬件设备。

办理严格的调离手续，并承诺调离后的保密义务后方可离开。

（二）外部人员安全管理。

1. 建设思路

在日常业务工作中，单位越来越多地与外部单位人员进行业务合作和往来，外部人员包括指软件开发商，硬件供应商，系统集成商，设备维护商和服务提供商，以及实习生、临时工、调用人员等。这些人员由于工作需要需临时或短期访问单位内部网络，进出单位工作场所，非内部人员由于流动性强，背景情况不明，给单位网络系统的安全带来较大隐患，必须建立严格的物理和网络访问授权审批制度，并有效执行。

2. 建设内容

单位应制定外部人员物理访问和网络接入的管理制度，并记录相关内容，具体要求如下:

（1）在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案。

（2）在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案。

（3）外部人员离场后及时清除其所有的访问权限。

（4）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。

3.10.4.4 建设管理

（一）系统定级和备案。

1. 建设思路

根据新等级保护制度的要求，二级以上（含二级）信息系统在定级工作中需要组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定，新建信息系统在规划阶段就可根据信息系统将承载的业务的重要程度对信息系统进行定级，按照相应等级进行等级保护安全体系设计和建设，对二级以上（含二级）信息系统还需按照教育行政部门的要求进行备案。

2. 建设内容

为了进一步明确信息系统定级、备案的相关责任和流程，应明确系统定级、备案和系统测评流程，包括以下内容

（1）明确定级备案责任部门和责任人。

（2）跟教育部门沟通明确定级备案相关材料要求和格式。

（3）制定系统定级和备案工作的时间计划。

（4）定级评审相关单位和专家联系和确定。

（5）组织定级评审工作，并获得上级或相关部门的批准。

为确保系统等级保护定级备案工作的规范性和专业性，可选择专业的等级保护咨询服务完成相关工作。

（二）系统安全方案设计。

1. 建设思路

按照“三同步”的原则，网络安全需要与信息化建设同步规划、同步建设、同步使用，在系统建设规划阶段需明确安全建设的目标和建设需求并进行安全规划方案的设计，安全方案应经过评审，经过批准后才能实施。

2. 建设内容

安全方案设计需根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施。

安全方案应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件。

安全建设项目根据实际建设阶段需设计不同的安全方案，包括总体建设规划方案、详细设计方案、建设实施方案等，安全方案需组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。

（三）安全产品采购管理。

1. 建设思路

网络安全产品的采购和使用应符合国家的有关规定，对于密码产品的采购和使用需符合国家密码主管部门的要求，并预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

2. 建设内容

需严格按照设备采购管理流程和政府设备采购目录来采购相应的安全产品；并且在搭建的模拟系统中对这些安全设备和软件进行测试和试运行验证，以防止产生对系统产生不可预见的影响。

（四）外包软件开发管理。

1. 建设思路

对于外包软件开发由于开发过程可控，在系统上线后可能引发各种安全问题，且难以从源头解决，因此，在等级保护制度中，对于外包软件开发明确要求应在软件交付前检测其中可能存在的恶意代码，并要求开发单位提供软件设计文档和使用指南，对于三级系统的外包软件开发还要求开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。

2. 建设内容

针对外包软件开发建议可选择专业的安全公司作为第三方进行开发过程的安全管理,包括协助开发单位建立安全开发制度和流程,并在软件开发的关键节点进行代码检测，代码检测采用自动化工具+专家审核的检测方式，既提高检测准确性和效率，又能发现系统逻辑错误等问题。

（五）工程实施管理。

1. 建设思路

网络系统安全建设过程中，涉及产品安装部署、功能启用、策略配置、与应用系统集成等各方面工作，安全工程建设整个过程本身还需要安全可控，需要由专门的部门或人员负责工程实施过程的管理，并制定安全工程实施方案，控制工程实施过程。对于三级信息系统，等级保护还明确要求需通过第三方工程监理控制项目的实施过程。

2. 建设内容

本项目实施周期较长，在实施过程中将通过招投标方式确定第三方监控单位，并指定专门的项目安全工作负责人，制定项目管理制度和项目实施方案。

（六）测试及交付管理。

1. 建设思路

项目建设完成后在正式上线前应进行系统测试，应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告，按照等级保护的要求，应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

在系统交付时，应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对负责系统运行维护的技术人员进行相应的技能培训，提供建设过程文档和运行维护文档。

2. 建设内容

由于本系统的复杂性，在系统及各子系统交付时，要制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；对负责运行维护的技术人员进行相应的技能培训；确保提供建设过程中的文档和指导用户进行运行维护的文档。

系统安全性测试建议选择专业的安全公司进行系统上线前安全检测，并针对安全风险及时采取措施整改。

（七）系统等级测评。

1. 建设思路

在系统建设完成后，按照等级保护的要求必须选择国家认可的测评机构对信息系统进行等级测评，并在系统运行过程中定期进行测评，对于三级系统要求每年测评一次，二级系统要求每两年自行完成测评一次，对发现不符合相应等级保护标准要求的及时整改，

并在发生重大变更或级别发生变化时进行等级测评。

2. 建设内容

系统上线运行后，选择经过国家认可的等级保护测评机构进行测评，由于测评工作的专业性和复杂性，建议选择专业安全厂商协助单位进行测评工作,如在正式测评前协助单位进行自测和整改等。

（八）服务供应商选择。

1. 建设思路

来自供应链的安全威胁已经越来越引起人们的关注，加强对供应链的管理是新等级保护制度的变化之一，等级保护制度规定要确保服务供应商的选择符合国家的有关规定；与选定的服务供应商签订相关协议,明确整个服务供应链各方需履行的网络安全相关义务;并定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

2. 建设内容

确保选择有相应资质的安全服务商、安全集成商、系统集成商和软件开发商，并与其签订协议，明确相关安全义务和责任。

3.10.4.5 运维管理

按照等级保护要求，日常安全运维管理主要从环境管理、资产管理、介质管理、资产维护管理、漏洞和风险管理、网络和系统安

全管理、防病毒管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置管理、应急预案管理、外包运维管理几个方面进行考虑。

3.10.5 运营体系

只有安全技术体系和安全管理体系，并不能充分保障系统的安全性，这是因为：一方面，无论是技术控制措施还是管理制度，都需要人来落地操作，这类事情就是运营工作；如果出现不会操作、操作不好或违规操作的情况，而且安全管理者也没有能力对操作行为进行监控，那就必将导致技术体系无法真正发挥威力，也会导致管理体系难以落地；另一方面，技术体系的控制措施，主要通过软硬件系统来实现；然而，还有不少技术控制措施，需要通过人的专业服务来实现；专业安全服务是一类特殊的安全操作，也属于运营体系范畴。总之，安全运营体系的作用是支撑、连通技术体系和管理体系，使之真正发挥效能。

紧跟信息化发展趋势，充分利用安全产品、网络产品的数据收集、关联、分析等自动化分析能力，结合企业云端大数据资源及安全威胁情报信息，形成一套规范有序、高效运转、快速响应的安全运营体系，提升对未知威胁感知和防御能力，有效防御各种新型攻击，是新形势下网络安全保障工作的重要环节。

3.10.5.1 日常运营

日常安全运营是安全运营体系的基石，只有日常做好了安全运营工作，才能及时识别、研判、处置各类安全隐患和安全事件，将风险扼杀在萌芽状态；否则，在重大事件期间，就容易出现安全问题层出不穷、疲于应付的状态。

日常安全运营工作可分为风险管控、监控分析、安全运维三大类:

（一）风险管控。

风险管控是一个安全风险管理过程，包括：风险识别、风险分析、风险处置。要想做好风险分析，又需要从资产识别、威胁识别分析、脆弱性识别分析、已有安全措施确认来入手。

当前环境下，业务和人员上网的趋势势不可挡，所以，资产识别的核心工作是识别暴露在互联网的资产，特别是违规暴露、隐匿暴露的情况。本项安全控制措施，通过互联网资产发现服务来落地实现。

威胁识别分析，是识别、分析威胁源头、威胁入侵方式、威胁后果（安全事件），是发现、分析、确诊“真实发生”的安全问题；这有别于“脆弱性识别分析”只是发现信息系统自身的脆弱性，而这种脆弱性是否能够利用、是否已被利用则不得而知。从这个角度看，威胁识别分析是安全运营体系的刚需。因此，在安全运营体系设计

中，突出了威胁识别分析的控制措施。全流量订阅分析服务和 Web 失陷检测服务，就是这一控制措施的落地服务。

脆弱性识别分析，是识别、分析网元设备（网络设备、操作系统、中间件、数据库）和应用系统自身的安全弱点，包括漏洞和不安全配置；区别于威胁识别分析，尽管有脆弱性问题并不代表一定会受到入侵，但脆弱性问题的识别、分析和整改，仍是整个安全体系的重要一环，也是安全运营体系的关键控制措施。本控制措施，通过基础安全评估服务、渗透测试服务，进行黑盒的脆弱性检测；再辅以白盒的代码安全检测，实现了脆弱性分析实现方法的全覆盖。

已有安全措施的确认，也是通过基础安全评估服务，实现控制措施的落地。

（二）监控分析。

风险管控工作，离不开及时的监控分析，实际上监控分析和风险管控工作是联动的，监控分析发现的问题，导入风险管理流程。监控分析的关键是及时性。监控分析又可以分为几个维度：

1. 预警预测。预警预测在安全运营体系中的作用日渐突出，本质原因是漏洞本身难以避免，也是黑客入侵的核心方法之一；在目前这种基于移动互联网的、信息快速扩散的环境下，谁能及时获取安全情报、未雨绸缪及时整改，谁就掌握了先机，减轻甚至避免了严重损失。此项控制措施是通过“安全预警通告服务”来落地实现的。

2. 内网威胁监控。在目前勒索病毒、APT 攻击盛行的情况下，每个组织都不应对安全威胁掉以轻心，威胁监控是刚需性的控制措施，是确诊组织是否被入侵、如何被入侵、遭受了哪些损失的关键方法；此项控制措施是通过周期性的“流量订阅分析服务”来落地实现，服务监控到的结果，导入风险管控流程进行处理。

3. Web 监测。Web 是目前主要互联网应用模式，因为 B/S 架构的半开放性特点，网站安全的问题较为严重，需要设计控制措施及时发现网站的可用性、脆弱性等各类安全问题。本控制措施通过网站云监测服务来落地实现。

4. 安全态势监控。通过实时收集安全事件的分布情况、分类情况、损失情况等数据，研判分析安全体系的薄弱环节，以及安全态势的发展情况。本控制措施，通过态势感知与安全运营平台运营分析服务来落地实现。

（三）安全运维。

安全运维工作中，大部分是基础的运营服务，它们的服务对象主要是组织中的安全软硬件设备。通过安全运维服务，解决安全软硬件设备“不会用”、“用不好”的最后一公里问题，真正发挥安全防御体系的威力。此类服务，本方案中主要是驻场运维服务、安全巡检服务、态势感知与安全运营平台基础运营服务。

应急响应服务是一个高阶运营服务，和驻场运维、安全巡检、

态势感知与安全运营平台基础运营工作密切相关，它针对已经发生或可能发生的安全事件进行检测、分析、协调、处理，是安全对抗的重要一环。应急响应服务是最考验工程师和服务单位能力的安全服务之一,也是安全运营体系和整个等级保护安全体系的刚需环节，原因是：由于攻防的不对称性，面对 APT 类攻击，任何安全防御体系都有可能被击穿，这时候，应急响应服务就至关重要，它是整个等级保护安全体系的托底控制措施。

3.10.5.2 重大安全事件保障

一方面，重大事件期间，面临着更严峻的内、外部安全威胁，非常考验组织的安全运营能力，重大事件保障工作是组织安全运营能力的练兵场和试金石。

另一面，重大事件期间，网络安全工作的能见度大幅提升，安全运营工作如果能在此时发力，就能起到事半功倍的效果。

“重要时期安全保障服务”发展至今，已经是一个覆盖重保工作部署、现场安全值守、事件分析研判、应急处置等的多模块服务，可以根据需求进行灵活组合。

3.10.6 本项目的安全系统

本项目统筹规划教育骨干网和广西教育数据中心的网络安全设计和建设，统一实施网络安全的管理和运维。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，

教育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。

本项目的各级教育城域网是教育骨干网延伸到终端的线路。各级教育城域网独立设置网络汇聚点，以光纤专线方式直接与教育骨干网连接，与教育骨干网之间部署专属的网络安全设备系统，实现与教育骨干网的边界隔离，实行分级管理分级运维，与教育骨干网实现网络安全态势感知一体化管理。各级教育城域网内不部署应用系统和数据系统，根据《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）有关网络和终端的条款，结合我区的实际，教育城域网的网络安全保护等级定级第二级，按网络安全等级保护第二级的要求进行设计、建设、管理和运维。

本项目需要具备较为全面的安全防护能力,要对安全物理环境、安全通信网络、网络安全区域边界、安全管理中心和安全计算环境（应用安全除外）分别进行设计，最终目标是使教育骨干网符合网络安全等级保护第三级要求，教育城域网符合网络安全等级保护第二级要求。

3.10.6.1 教育骨干网

教育骨干网 3 个核心节点各自具有独立的安全域，教育骨干网主要承担教育城域网的接入，重点考虑网络链路的可用性，因此安全区域划分为网络接入区、安全防护区。

安全域划分示意图如下:

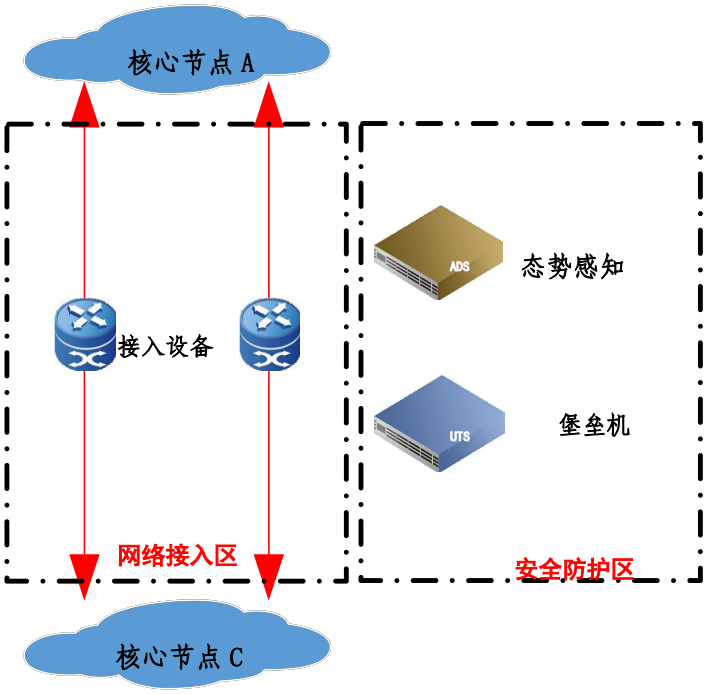

图 5-35 安全域划分示意图

网络接入区：由边界网络设备组成，承担双线路接入、负载均衡的功能。

安全防护区：由安全防护设备组成，承担入侵攻击阻断、威胁感知等功能。

广西教育数据中心核心节点是整个教育网最核心的部分，其安全建设将影响广西教育网全域的安全性，现阶段需要对自身的网络安全情况建立运营机制，以便后续教育城域网建设后对广西教育网进行整体监管。广西大学、广西师范大学两个核心节点，作用主要是帮助广西教育数据中心核心节点分担流量，因此只做网络建设，不做安全系统建设。

本次安全系统建设按照等保2.0框架当中“一个中心，三重防护”的思想进行设计，广西教育数据中心核心节点的安全防护示意图如下：

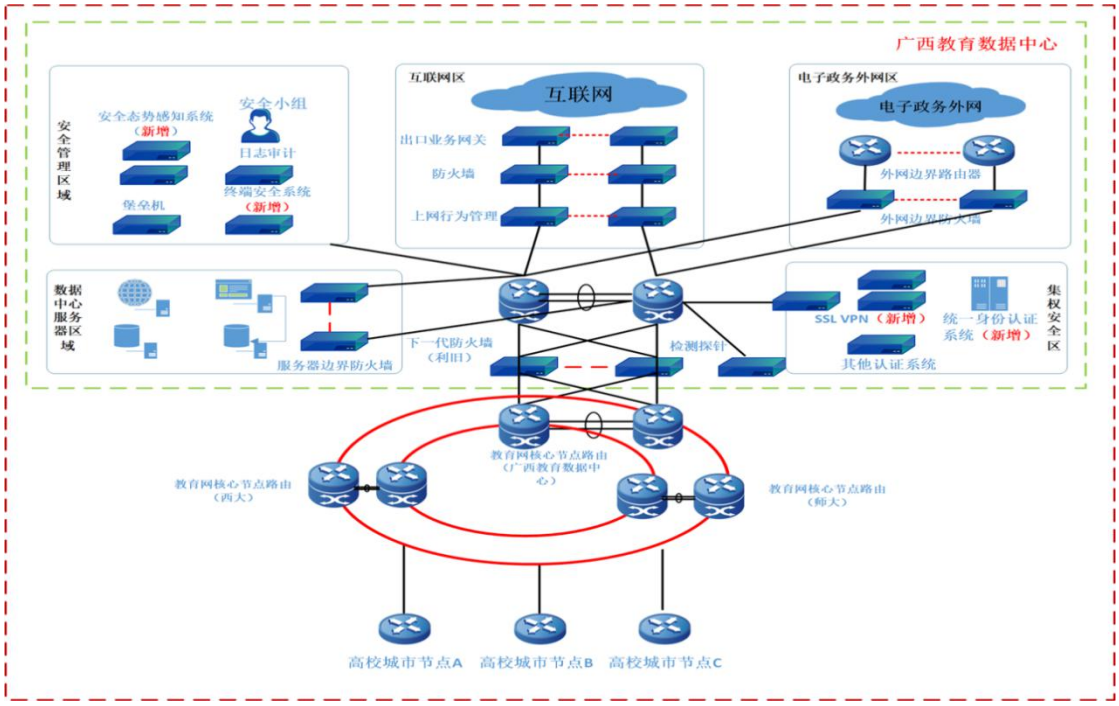

图 5-36 教育骨干网广西教育数据中心核心节点安全防护示意图

（一）安全物理环境。

1.技术要求

（1）物理位置选择

本项要求包括：

a）机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

（2）物理访问控制

机房出入口应配量电子门禁系统，控制、鉴别和记录进入的人员。

（3）防盗窃和防破坏

本项要求包括:

a）应将设备或主要部件进行固定,并设置明显的不易除去的标识。

b）应将通信线缆铺设在隐蔽安全处。

c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。

（4）防雷击

本项要求包括:

a）应将各类机柜、设施和设备等通过接地系统安全接地。

b）应采取措施防止感应雷,例如设置防雷保安器或过压保护装置等。

（5）防火

本项要求包括:

a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

b）机房及相关的工作房间和辅助房应采用具有耐灭等级的建筑材料。

c）应对机房划分区域进行管理，区域和区域之间设置幅离防火措施。

（6）防水和防潮

本项要求包括:

a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

c）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

（7）防静电

本项要求包括:

a）应采用防静电地板或地面并采用必要的接地防静电措施;

b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

（8）温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

（9）电力供应

本项要求包括:

a）应在机房供电线路上配置稳压器和过电压防护设备;

b）应提供短期的备用电力供应,至少满足设备在断电情况下的正常运行要求;

c）应设置冗余或并行的电力电缆线路为计算机系统供电。

（10）电磁防护

本项要求包括:

a）电源线和通信线缆应隔离铺设，避免互相干扰。

b）应对关键设备实施电磁屏蔽。

2.建设方案

本次项目建设教育骨干网的物理位置位于广西教育数据中心、教科网广西节点（广西大学、广西师范大学）、各高校城市节点的机房，其中数据中心物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、为适度控制、电力供应的相关内容均利旧现有机房设备。

（二）安全通信网络。

1.技术要求

通用安全通信网络设计技术要求本项要求包括:

（1）通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心集中管理，并对确认的违规行为进行报警。

（2）通信网络数据传输完整性保护

应采用由密码技术支持的完整性校验机制，以实现通网络数据传输完整性保护，并在发现完整性被破坏时进行恢复。

（3）通信网络数据传输保密性保护

应采用由密码技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

（4）可信连接验证

通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序及其关键执行环节的执行资源进行可信验证，并将验证结果形成审计记录，送至管理中心。

2.建设方案

（1）根据等保 2.0 网络架构相关要求，对接入服务设计了资源保证、优先处理等保障。包括：保证主要网络设备的业务处理能力具备冗余空间，通过 QoS 机制满足业务高峰期、优先级业务的需要；对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。教育骨干网分不同的教育城域网或

网段，并按照方便管理和控制的原则为各教育城域网、网段分配地址段。重要网段与其他网段之间采取可靠的技术隔离或边界防护措施。业务类网络设备（交换机、防火墙、路由器）成对部署，以虚拟化、堆叠、1+1 保护等方式工作。根据实际情况尽可能配置备份的路由或应急路由（最少 2 个）。在路由可达时，当由于某种原因主路由失效时候,可以使用备份路由或应急路由继续提供网络服务。

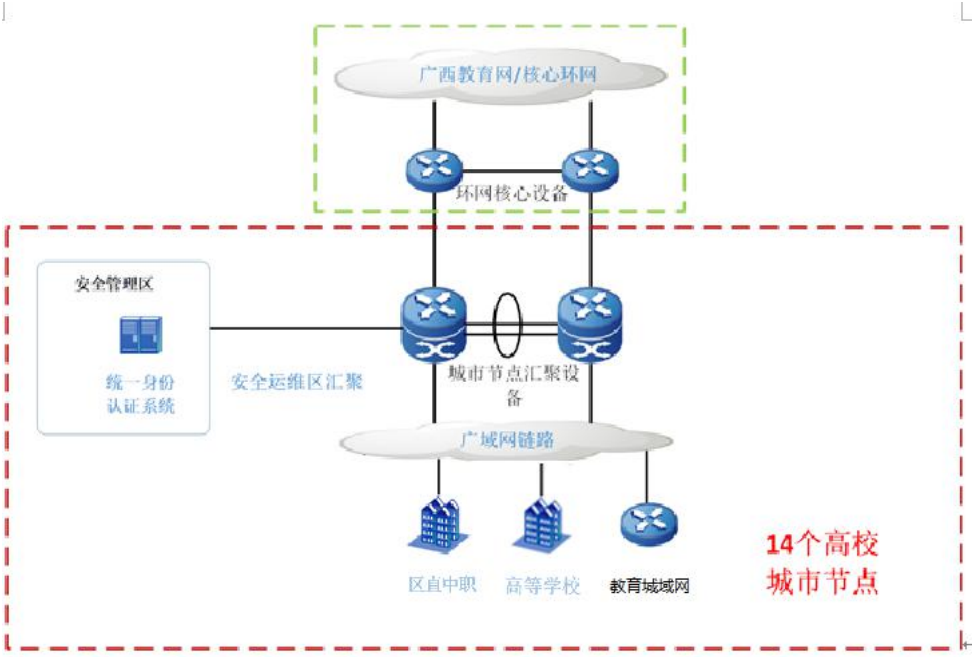

图 5-37 教育骨干网高校城市节点安全防护示意图

（2）根据等保通信传输相关要求，新增 SSL VPN 设备。用于自治区范围内各高等院校、区直中等职业学校与电子政务外网的接入，实现数据传输的加密。

（三）网络安全区域边界。

1.技术要求

通用安全区域边界设计技术要求本项要求包括:

（1）区域边界访问控制

应在安全区域边界设置自主和强制访问控制机制，应对源及目标计算节点的身份、地址、端口和应用协议等进行可信验证，对进出安全区域边界的数据信息进行控制，阻止非授权访问。

（2）区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协议、请求的服务等，确定是否允许该数据包进出该区域边界。

（3）区域边界安全审计

应在安全区域边界设置审计机制，由安全管理中心集中管理，并对确认的违规行为及时报警。

（4）区域边界完整性保护

应在区域边界设置探测器，例如外接探测软件，探测非法外联和入侵行为，并及时报告安全管理中心。

（5）可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、

区域边界安全管控程序等进行可信验证，并在区域边界设备运行过程中定期对程序内存空间、操作系统内核关键内存区域等执行资源进行可信验证，并在检测到其可信性受到破坏时采取措施恢复，并将验证结果形成审计记录，送至管理中心。

2.建设方案

根据等保建设分区分域的设计思路，将网络分为国家教育网接入区、电子政务外网区、安全管理区，以及集权安全区。根据边界防护、访问控制、入侵防范的要求，在教科网接入区、电子政务外网接入区利旧原有防火墙，在集权安全区新增 2 台下一代防火墙。

根据网络设备的安全审计要求，在路由器、交换机和防火墙等设备上启用日志审计功能，并利旧安全管理区的日志审计设备做网络、安全、服务器等设备日志的统一存储管理。

（四）安全管理中心。

1.技术要求

（1）系统管理

可通过系统管理员对系统的资源和运行进行配置、控制和可信及密码管理，包括用户身份、可信证书及密钥、可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操

作界面进行系统管理操作，并对这些操作进行审计。

在进行云计算平台安全设计时，安全管理应提供查询云租户数据及备份存储位置的方式；云计算平台的运维应在中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

在进行物联网系统安全设计时,应通过系统管理员对感知设备、感知网关等进行统一身份标识管理；应通过系统管理员对感知设备状态（电力供应情况、是否在线、位置等）进行统一监测和处理。

（2）安全管理

应通过安全管理员对系统中的主体、客体进行统一标记，对主体进行授权，配置可信验证策略，维护策略库和度量值库。

应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并进行审计。

在进行云计算平台安全设计时，云计算安全管理应具有对攻击行为回溯分析以及对网络安全事件进行预测和预警的能力；应具有对网络安全态势进行感知、预测和预判的能力。

在进行物联网系统安全设计时，应通过安全管理员对系统中所使用的密钥进行统一管理，包括密钥的生成、分发、更新、存储、备份、销毁等。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制系统设备的可用性和安全性进行实时监控，可以对监控指标设置

告警调值，触发告警并记录；应通过安全管理员在安全管理中心呈现设备间的访问关系，及时发现未定义的信息通讯行为以及识别重要业务操作指令级的异常。

（3）审计管理

应通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进行存储、管理和查询等。对审计记录应进行分析，并根据分析结果进行处理。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计：应通过运维审计系统对管理员的运维行为进行安全审计；应通过租户隔离机制，确保审计数据隔离的有效性。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制现场控制设备、网络安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的网络安全监控和报警、网络安全日志信息进行集中管理。根据安全审计策略对各类安全信息进行分类管理与查询，并生成统一的审计报告。系统对各类网络安

全报警和日志信息进行关联分析。

2.建设方案

按照等保“一个中心三重防护”建设思路，一个中心是指“安全管理中心”。根据安全管理中心相关要求，划分“安全管理区”。通过利旧技信中心现有负载均衡、态势感知、堡垒机、入侵防御、审计系统等设备，协助教育骨干网设备进行统一的安全防护。另外，在广西教育数据中心核心节点安全管理区域规划设计满足如下要求:

（1）根据等保系统管理要求，在该区域新增运维安全管理系统。配置可以访问所有管控对象，包括教育城域网内设备，以及直属管理的校园网出口设备,通过逻辑上将管理人员与目标设备分离，建立“人->管理主账号->授权->目标从账号->目标设备”的管理模式;在此模式下，通过基于唯一身份标识的集中账号与访问控制策略，与各网络设备、安全设备，以及后续增加的服务器和数据库等进行连接，实现集中精细化运维操作管控与审计，并对高危操作进行授权审批。

（2）根据等保集中管控要求，在该区域新增安全态势感知系统。教育网可以通过安全态势感知系统实现整个教育网的安全运营，借助安全可视和安全事件工单制实现各级党组党委责任分明，权责明确；通过安全运营机制不断发现教育网的安全问题，并且不断完善安全防御体系，保持教育网的健壮性；通过安全态势感知系统现

有内置的驻留程序实现对终端设备的入网认证信息同步，保证教育网终端设备可视安全可控。同时，教育骨干网新增安全态势感系统需要和广西教育数据中心实现一体化管理运维，实现完整有效、更全面、更直观可视的展示。

（3）根据等保集中管控要求,在该区域新增统一身份认证管理系统。统一身份认证管理系统强调以人为中心进行访问控制，提供统一身份管理、统一身份认证、统一门户/单点登录(SSO)、集中应用授权、审计与分析等功能，让认证更简易、身份更安全、应用访问更可控。同时，实现身份全生命周期管理，降低管理员账号开户、变更、销户等带来的运维复杂度，让管理更高效。未通过身份认证的用户、设备禁止接入教育网和互联网，仅能在接入的教育城域网内限时使用。本项目统一身份认证管理系统通过教育部省级部署的全国教育管理信息系统（全国中小学生学籍信息管理系统、全国学前教育管理信息系统、全国中等职业学校学生管理信息系统、全国教师管理信息系统）获取身份数据，根据个人分配的账号密码比对用户身份实现鉴权登录。支持同步身份到安全态势感知平台进行统一展示，确保发现安全问题及攻击威胁时，能第一时间定位到终端位置及使用人，方便运维人员进行快速处理，实现安全问题的快速闭环。

（4）根据安全管理的要求，在安全管理区（广西教育数据中心和高校城市节点机房）部署终端安全管理系统管理端，在本级教育

城域网、下属教育城域网内终端上部署终端安全管理系统，实现教育城域网内主机终端病毒的查杀，使主机终端免受病毒、特洛伊木马和其它恶意程序的侵袭，不让其有机会透过文件及数据的分享进而散布到整个教育城域网的网络环境，具备完整的病毒扫描防护功能，对主流系统平台下进行完整病毒查杀；同时终端安全管理系统还具备进程管理、软件管理、补丁管理、外设管理等功能，能够实现主机终端入侵防范的能力，统一下发应用软件，统一实现漏洞修复，以及非法外联的管控。由自治区教育厅“广西教育信息化终端应用管理和安全态势感知管理信息系统”承担相关建设、管理和运维工作，教育网项目不涉及此项目建设。

（五）安全计算环境。

1.技术要求

通用安全计算环境设计技术要求本项要求包括:

（1）用户身份鉴别

应支持用户标识和用户鉴别。在对每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受安全管理中心控制的口令、令牌、基于生物特征、数字证书以及其他具有相应安全强度的两种或两种以上的组合机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

（2）自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。自主访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级和（或）记录或字段级。自主访问操作包括对客体的创建、读、写、修改和删除等。

（3）标记和强制访问控制

在对安全管理员进行身份鉴别和权限控制的基础上，应由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制。强制访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。应确保安全计算环境内的所有主、客体具有一致的标记信息，并实施相同的强制访问控制规则。

（4）系统安全审计

应记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。应提供审计记录查询、分类、分析和存储保护；确保对特定安全事件进行报警；确保审计记录不被破坏或非授权访问。应为安全管理中心提供接口；对不能由系统独立处理的安全事件，提供由授权主体调用的接口。

（5）用户数据完整性保护

应采用密码等技术支持的完整性校验机制，检验存储和处理的用户数据的完整性，以发现其完整性是否被破坏，且在其受到破坏时能对重要数据进行恢复。

（6）用户数据保密性保护

应采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护

（7）客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

（8）可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在应用程序的关键执行环节对系统调用的主体、客体、操作可信验证，并对中断、关键内存区域等执行资源进行可信验证,并在检测到其可信性受到破坏时采取措施恢复，并将验证结果形成审计记录，送至管理中心。

（9）配置可信检查

应将系统的安全配置信息形成基准库，实时监控或定期检查配

置信息的修改行为，及时修复和基准库中内容不符的配置信息。

（10）入侵检测和恶意代码防范

应通过主动免疫可信计算检验机制及时识别入侵和病毒行为，并将其有效阻断。

2.建设方案

（1）根据等保 2.0 技术要求中身份鉴别的要求，在“安全管理区”新增统一身份认证管理系统、在“集权安全区”新增 SSL VPN 设备，上述两种设备与本章节教育骨干网安全设计中“安全通信网络建设”以及“安全管理中心建设”中提到的 SSL VPN 和统一身份认证系统是相同设备，为避免方案理解错误而造成重复建设特此说明。

（2）根据等保 2.0 技术要求中访问控制的要求，在“集权管理区”新增下一代防火墙，上述设备与本章节教育骨干网安全设计中“网络安全区域边界建设”中提到的下一代防火墙是相同设备，为避免方案理解错误而造成重复建设特此说明。

（3）根据等保 2.0 技术要求中安全审计的要求，利旧广西教育数据中心“安全管理区”中原有日志审计系统，并开启所有安全设备的日志记录功能。

3.10.6.2 教育城域网

为减少重复建设重复投资，避免浪费国有资产，本项目教育城域网安全系统建设在符合教育网的技术标准规范，满足教育网的主

要技术参数和性能指标要求的条件下，主要以利旧运营商现有设备系统方式实施。

在网络出口区域，针对互联网、教育网分别进行安全防护设计，包括结构安全、边界防护、访问控制、入侵防范、恶意代码防范等；在核心交换区域，针对本级教育城域网、下属校园网和教育机构网络的所有流量进行攻击检测、病毒木马检测、未知威胁检测等；在安全管理区域，针对本级教育城域网、下属校园网和教育机构网络实现安全审计、身份鉴别、授权管理、漏洞检测、终端安全管理、SSL VPN、动态密码服务系统等。教育城域网安全防护示意图如下:

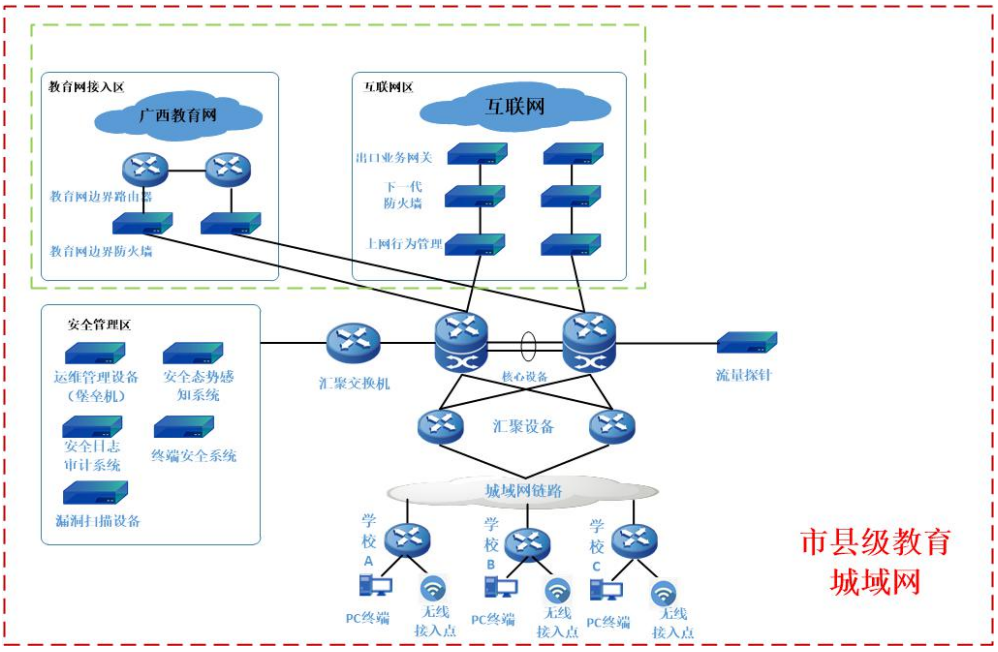

图 5-38 教育城域网安全防护示意图

（一）安全物理环境。

1.技术要求

（1）物理位置选择

本项要求包括:

a）机房场地应选择在具有防震、防风和防雨等能力的建筑内。

b）机房场地应避免设在建筑物的顶层或地下室,否则应加强防水和防潮措施。

（2）物理访问控制

机房出入口应安排专人值守或配置电子门禁系统，控制、鉴别和记录进入的人员。

（3）防盗窃和防破坏

本项要求包括:

a）应将设备或主要部件进行固定，设置明显的不易除去的标识。

b）应将通信线缆铺设在隐蔽安全处。

（4）防雷击

应将各类机柜、设施和设备等通过接地系统安全接地。

（5）防火

本项要求包括:

a）机房应设量火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

（6）防水和防潮

本项要求包括:

a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透。

b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透。

（7）防静电

应采用防静电地板或地面并采用必要的接地防静电措施。

（8）温湿度控制

应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。

（9）电力供应

本项要求包括:

a）应在机房供电线路上配置稳压器和过电压防护设备。

b）应提供短期的备用电力供应,至少满足设备在断电情况下的正常运行要求。

（10）电磁防护

电源线和通信线缆应隔离铺设，避免互相干扰。

2.建设方案

本次项目建设教育城域网的物理位置位于各市县教育行政部门租用运营商的机房，其中网络汇聚点的物理访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、为适度控制、电力供应的相关内容均利旧通信运营商现有机房设备。

（二）安全通信网络。

1.技术要求

根据《信息安全技术网络安全等级保护基本要求 2.0》标准，通用安全通信网络设计技术要求如下:

（1）通信网络安全审计

应在安全通信网络设置审计机制，由安全管理中心管理。

（2）通信网络数据传输完整性保护

可采用由密码等技术支持的完整性校验机制，以实现通信网络数据传输完整性保护。

（3）通信网络数据传输保密性保护

可采用由密码等技术支持的保密性保护机制，以实现通信网络数据传输保密性保护。

（4）可信连接验证

通信节点应采用具有网络可信连接保护功能的系统软件或可信根支撑的信息技术产品，在设备连接网络时，对源和目标平台身份、执行程序进行可信验证，并将验证结果形成审计记录。

2.建设方案

根据等保 2.0 网络架构相关要求，本次建设对接入服务设计了资源保证、优先处理等保障，包括：保证主要网络设备的业务处理能力具备冗余空间，通过 QoS 机制满足业务高峰期、优先级业务的需要；对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。各地区教育城域网分不同的教育城域网或网段,并按照方便管理和控制的原则为各教育城域网、网段分配地址段。重要网段与其他网段之间采取可靠的技术隔离或边界防护措施。业务类网络设备（交换机、防火墙、路由器）成对部署，以堆叠或 1+1 保护方式工作。根据实际情况尽可能配置备份的路由或应急路由（最少 2 个）。在路由可达时，当由于某种原因主路由失效时候,可以使用备份路由或应急路由继续提供网络服务。

（三）网络安全区域边界。

1.技术要求

根据《信息安全技术网络安全等级保护基本要求 2.0》标准，通用安全区域边界设计技术要求如下:

（1）区域边界包过滤

应根据区域边界安全控制策略，通过检查数据包的源地址、目的地址、传输层协义和请求的服务等，确定是否允许该数据包通过该区域边界

（2）区域边界安全审计

应在安全区域边异设置审计机制,并由安全管理中心统一管理。

（3）区域边界恶意代码防范

可在安全区域边界设置防恶意代码网关,由安全管理中心管理。

（4）区域边界完整性保护

应在区域边界设置探测器，探测非法外联等行为，并及时报告安全管理中心。

（5）可信验证

可基于可信根对区域边界计算节点的 BIOS、引导程序、操作系统内核、区域边界安全管控程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录。

2.建设方案

根据等保建设分区分域的设计思路,将网络分为教育网接入区、互联网区以及安全管理区。

根据等保 2.0 规范中边界防护、访问控制、入侵防范的要求，

在互联网接入区边界、教育网接入区边界分别部署下一代防火墙，以双机冗余方式运行，实行不同边界网络严格的访问控制，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量；启用网络防病毒功能，实现进出网络边界数据的木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀，以及 HTTP、FTP、POP3、SMTP 协议的病毒的检测查杀。需要能够和教育网终端安全管理系统实现数据对接，功能联动，能够根据终端安全状态对其进行教育网和互联网的准入控制。

在互联网出口双机部署上网行为管理系统，针对本级教育城域网、下属校园网和教育机构网络的终端的上网行为的管理、带宽的限制和内容的审计等，根据业务需要调整应用访问和带宽利用率，同时防止敏感数据泄密和非法访问行为。上网行为管理系统应配置开放接口，可以使用公开标准接口或公开标准协议，与广西教育数据中心核心节点的统一身份认证系统进行对接，实现对教育城域网内师生访问入网的准入认证，确保入网访问的身份安全。

（四）安全管理中心。

1.技术要求

根据《信息安全技术网络安全等级保护基本要求 2.0》标准，安全管理中心设计技术要求如下:

（1）系统管理

可通过系统管理员对系统的资源和运行进行配置、控制和可信管理，包括用户身份、可信证书、可信基准库、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复以及恶意代码防范等。

应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计。

在进行云计算平台安全设计时，安全管理应提供查询云租户数据及备份存储位置的方式。

在进行物联网系统安全设计时,应通过系统管理员对感知设备、感知层网关等进行统一身份标识管理。

（2）审计管理

可通过安全审计员对分布在系统各个组成部分的安全审计机制进行集中管理，包括根据安全审计策略对审计记录进行分类；提供按时间段开启和关闭相应类型的安全审计机制；对各类审计记录进

行存储、管理和查询等。

应对安全审计员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作。

在进行云计算平台安全设计时，云计算平台应对云服务器、云数据库、云存储等云服务的创建、删除等操作行为进行审计。

在进行工业控制系统安全设计时，应通过安全管理员对工业控制现场控制设备、网络安全设备、网络设备、服务器、操作站等设备中主体和客体进行登记，并对各设备的网络安全监控和报警、网络安全日志信息进行集中管理。根据安全审计策略对各类网络安全信息进行分类管理与查询，并生成统一的审计报告。

2.建设方案

按照等保“一个中心三重防护”建设思路，一个中心是指“安全管理中心”。根据安全管理中心相关要求，划分“安全管理区”，并在该区域部署相关设备系统。

（1）在安全管理区新增安全日志审计系统。配置可以接收所有日志对象，包括本级教育城域网内设备、下属校园网和教育机构网络出口设备，实时采集不同厂商的安全设备、网络设备产生的日志信息，并将这些信息汇集到审计中心，进行集中化存储、备份、查询、审计、告警、响应，出具丰富的报表报告，获悉教育城域网的整体安全运行状况，实现全生命周期的安全管理。

（2）在安全管理区部署运维管理系统。配置可以访问所有管控对象，包括本级教育城域网内设备、下属教育城域网内设备，以及直属管理的校园网出口设备，通过逻辑上将管理人员与目标设备分离，建立“人->管理主账号->授权->目标从账号->目标设备”的管理模式；在此模式下，通过基于唯一身份标识的集中账号与访问控制策略 ，与各网络设备、安全设备，以及后续增加的服务器和数据库等进行连接，实现集中精细化运维操作管控与审计，并需要对高危操作进行授权审批。

（3）在核心交换区部署检测探针。通过网络流量镜像在内部对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行初步的攻击识别、违规行为检测与内网异常行为识别，同时可以将检测数据与分析结果上传至广西教育数据中心核心节点进行汇总分析。

（4）在安全管理区域部署安全态势感知系统，对检测探针的数据和各个安全设备日志进行收集，并通过可视化的形式为用户呈现内网业务资产及针对内网关键业务资产的攻击与潜在威胁，安全态势感知系统支持下发策略至防火墙等安全设备，对攻击进行一键封锁，并形成安全问题工单，派发工单通知内部运维人员进行处置，通过该系统对现网所有安全系统进行统一安全管理。通过安全安全态势感知系统现有内置的驻留程序实现对终端设备的入网认证信息同步，保证教育网终端设备可视可控。

安全态势感知系统应配置开放接口，可以使用公开标准接口或公开标准协议，与广西教育数据中心核心节点的安全态势感知系统共享交换数据，在广西教育数据中心核心节点可以实现对广西教育网全网安全的可视化和感知管控。

（5）在安全管理区部署漏洞扫描系统,配置可以访问所有检测对象，包括本级教育城域网内设备、下属校园网和教育机构的出口设备，评估各个网络区域的安全状况，包括现有的网络设备和安全设备，以及后续增加的 WEB 应用、服务器区域、数据库等。通过漏洞扫描系统,能够主动对网络中的资产进行细致深入的漏洞检测、分析，并能提供专业、有效的漏洞防护建议，帮助运维管理人员落实安全整改问题。

（五）安全计算环境建设。

1.技术要求

安全计算环境设计技术要求本项要求包括:

（1）用户身份鉴别

应支持用户标识和用户鉴别。在每一个用户注册到系统时，采用用户名和用户标识符标识用户身份，并确保在系统整个生存周期用户标识的唯一性；在每次用户登录系统时，采用受控的口令或具有相应安全强度的其他机制进行用户身份鉴别，并使用密码技术对鉴别数据进行保密性和完整性保护。

（2）自主访问控制

应在安全策略控制范围内，使用户对其创建的客体具有相应的访问操作权限，并能将这些权限的部分或全部授予其他用户。访问控制主体的粒度为用户级，客体的粒度为文件或数据库表级。访问操作包括对客体的创建、读、写、修改和删除等。

（3）系统安全审计

应提供安全审计机制，记录系统的相关安全事件。审计记录包括安全事件的主体、客体、时间、类型和结果等内容。该机制应提供审计记录查询、分类和存储保护，并可由安全管理中心管理。

（4）用户数据完整性保护

可采用常规校验机制，检验存储的用户数据的完整性，以发现其完整性是否被破坏。

（5）用户数据保密性保护

可采用密码等技术支持的保密性保护机制，对在安全计算环境中存储和处理的用户数据进行保密性保护。

（6）客体安全重用

应采用具有安全客体复用功能的系统软件或具有相应功能的信息技术产品，对用户使用的客体资源，在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄露。

（7）恶意代码防范

应安装防恶意代码软件或配置具有相应安全功能的操作系统，并定期进行升级和更新，以防范和清除恶意代码。

（8）可信验证

可基于可信根对计算节点的 BIOS、引导程序、操作系统内核、应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录。

2.建设方案

根据等保 2.0 技术要求中安全审计的要求，在安全管理区新增安全日志审计系统，该设备和本章节“二、教育城域网安全设计”中“4、安全管理中心建设”描述的日志审计为同一台设备，为避免方案理解错误而造成重复建设特此说明。

3.10.6.3 校园网

为减少重复建设重复投资，避免浪费国有资产，本项目的校园网安全系统建设在符合教育网的技术标准规范，满足教育网的主要技术参数和性能指标要求的条件下，主要以利旧运营商现有设备系统方式实施。

校园网是学校的局域网络，用于汇聚学校内终端设备及教学设备，使用教育网内和互联网的教育资源。对于一些班级规模较大的学校，建议选配学校安全边界设备来区分不同的安全域。由于本项

目预算不包括无线网络的实施建设，因此安全域划分为边界接入区、终端用户区。

安全域划分示意图如下：

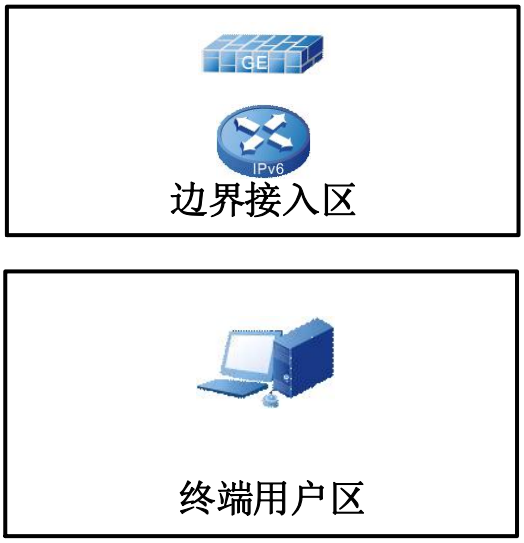

图 5-39 校园网安全域示意图

边界接入区：由边界安全设备及网络接入设备组成，承担网络接入、访问控制、安全防护的功能。

终端用户区：由各个终端 PC 组成，承担互联网访问、教学资源使用、教学服务使用的功能。

在校园网安全设计中，对高等院校、区直中等职业学校，主要考虑接入教育城域网边界安全，其他部分由学校自行建设；对中小学学校和其它教育机构，主要考虑校园网边界安全防护部分和终端安全部分，对于校园网内部的安全审计与管理，由学校自行根据情况自主建设。而根据设备部署方式和建设情况的不同，校园网边界安全防护主要分为以下两类：

（一）实体设备类。

该类适用于已经部署了边界安全防护设备，或班级规模较大的中小学，教育资源和教育服务需求较高，需要通过硬件设备进行防护的。该类学校接入设备原来已采购的，可以继续复用，需要将防护设备的管理权限提交至上级教育城域网的运维管理系统中实现统一管理，将防护设备的日志上传至上级教育城域网的安全日志审计系统和安全态势感知平台中进行分析。

安全防护示意图如下:

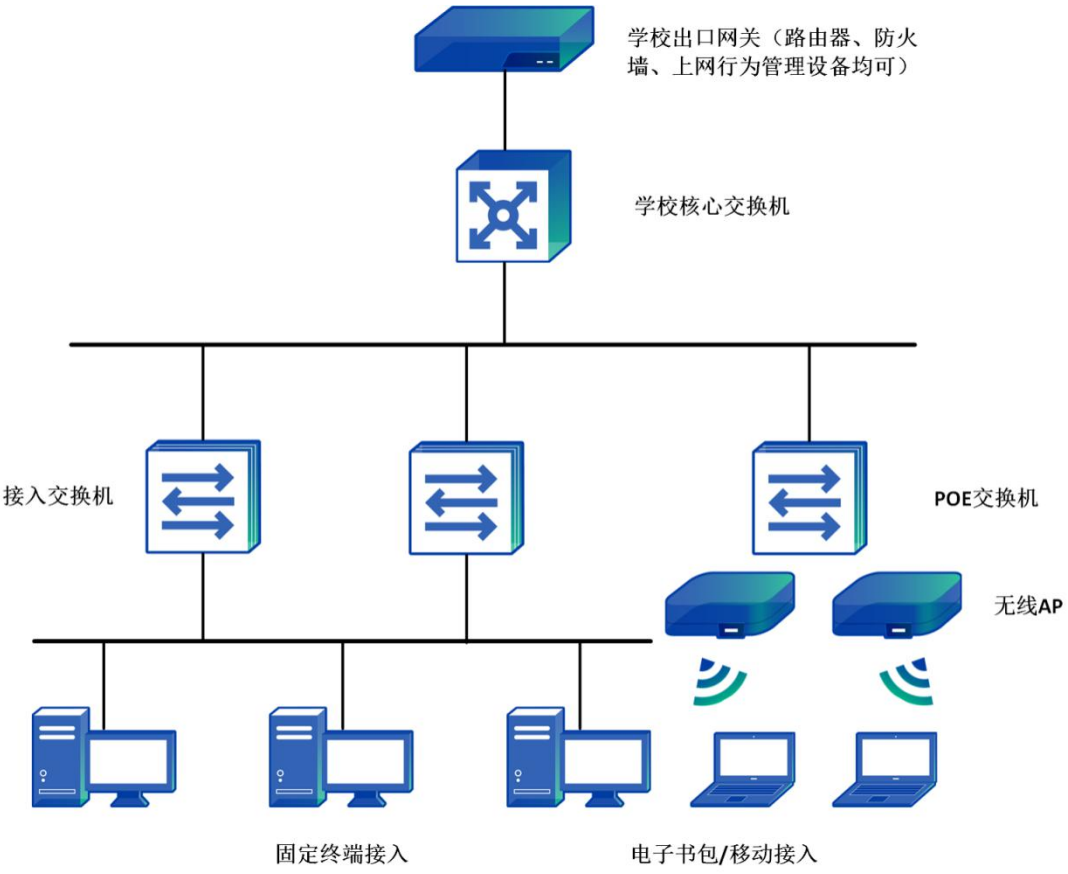

图 5-40 校园网实体设备安全防护示意图

在校园网边界部署硬件下一代防火墙，进行策略配置，实行访

问控制，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量；启用网络防病毒功能，实现进出网络边界数据的木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀，以及 HTTP、FTP、POP3、SMTP 协议的病毒的检测查杀；下一代防火墙要能接入运维管理系统实现统一管理，要能通过标准日志协议传输日志供安全日志审计系统进行汇总分析，要能提供 API 接口供安全态势感知平台进行统一管理、统一分析和统一配置，实现安全态势感知平台对有问题的终端及访问的一键封堵和隔离；下一代防火墙需要能够和教育网终端安全管理系统实现数据对接，功能联动，能够根据终端安全状态对其进行教育网和互联网的准入控制。

（二）虚拟化体设备类。

该类适用于不具备硬件部署环境、不具备人员基本维护能力的学校（如村完小），或班级规模较小的中小学，教育资源和教育服务需求较低，不需要进行针对性安全防护的。该类学校校园网出口不部署实体设备，建议在上级教育城域网中部署安全管理区，统一配置一套安全网关或者通过其他安全防护手段实现对每个校园网的安全监控和风险识别，统一汇总分析展示。安全防护示意图如下:

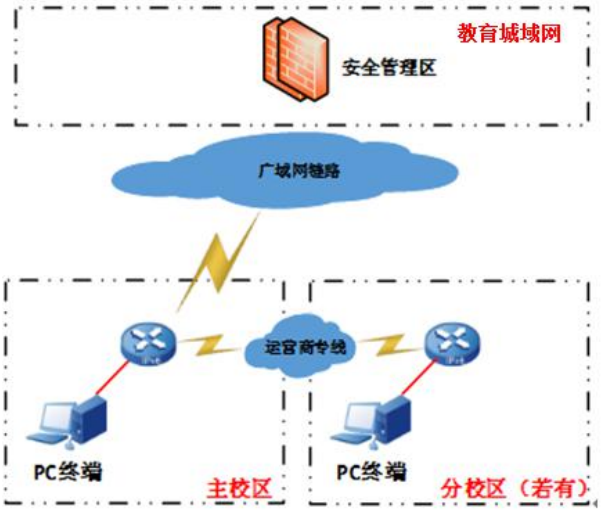

图 5-41 校园网虚拟化体设备安全防护示意图

在教育城域网内安全管理区为校园网统一配置一套安全网关或者通过其他安全防护手段实现不同学校的校园网进行统一监管，对存在的安全风险及时告警，并且可对发现安全隐患的学校流量采取控制措施，限制访问，防止各类非法攻击行为。启用入侵防御功能，实现 2~7 层数据的安全检测和阻断防护，提供对内部攻击、外部攻击和误操作的实时监控，实时、主动拦截黑客攻击、蠕虫、僵尸网络、后门木马、DOS 等恶意流量；启用网络防病毒功能，实现进出网络边界数据的木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀，以及 HTTP、FTP、POP3、SMTP 协议的病毒的检测查杀。

3.11 密码应用建设方案

密码是保障网络与信息全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。《密码法》的颁

布实施，从法律层面为开展商用密码应用提供了根本遵循，《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

图 5-42 广西教育网商用密码应用规划

为贯彻落实《密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》《关键信息基础设施安全保护条例》《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号）《广西壮族自治区人民政府办公厅关于印发广西政务信息化项目建设管理办法（试行）的通知》（桂政办发（2021）21 号），通过对广西教育网应用需求进行分析，依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等 4 个层面，以及密钥管理、安全管理等方面，设计了该系统密码应用的技术方案、安全管理方案和实施保障方案。

3.11.1 网络系统概述

3.11.1.1 网络拓扑

（一）教育骨干网。

教育骨干网的核心节点机房分别位于广西教育数据中心（南宁）、广西大学（南宁）和广西师范大学（桂林）。广西教育数据中心核心节点是整个教育网最核心的部分，其安全建设将影响广西教育网全域的安全性，现阶段需要对自身的网络安全情况建立运营机制，以便后续教育城域网建设后对广西教育网进行整体监管。广西大学、广西师范大学两个核心节点，作用主要是帮助广西教育数据中心核心节点分担流量，因此只做网络建设，不做安全系统建设。教育骨干网主要承担教育城域网的接入，重点考虑网络链路的可用性，因此安全区域划分为网络接入区、安全防护区。

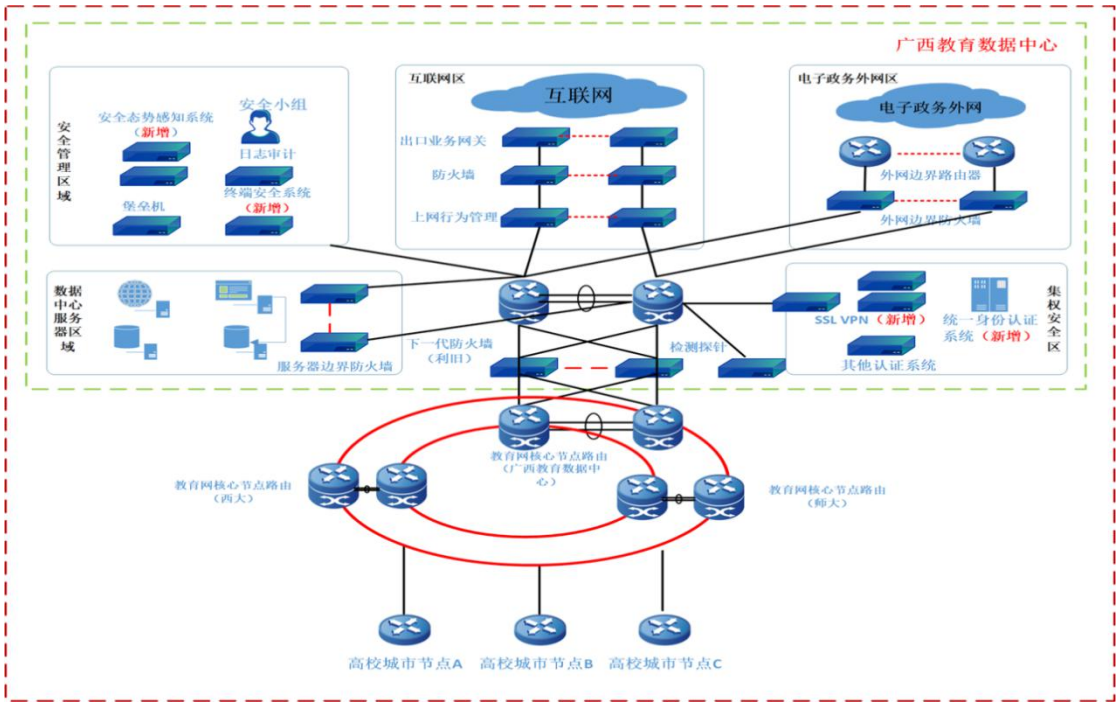

图 5-43 教育骨干网广西教育数据中心核心节点安全防护示意图

网络接入区：由边界网络设备组成，承担双线路接入、负载均衡的功能。

安全防护区：由安全防护设备组成，承担入侵攻击阻断、威胁感知等功能。

（二）教育城域网。

为减少重复建设重复投资，避免浪费国有资产，本项目各市县教育城域网安全系统建设在符合教育网的技术标准规范，满足教育网的主要技术参数和性能指标要求的条件下，主要以利旧运营商现有设备系统方式实施。

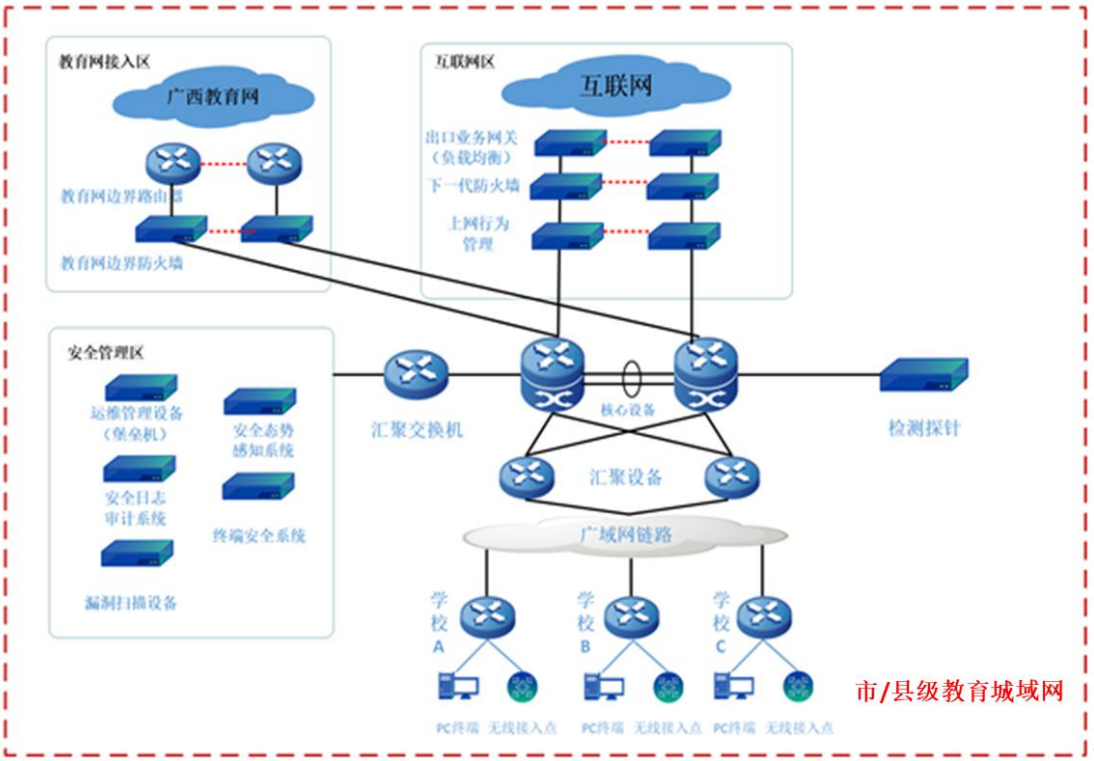

图 5-44 教育城域网安全防护示意图

在网络出口区域，针对互联网、教育网分别进行安全防护设计，包括结构安全、边界防护、访问控制、入侵防范、恶意代码防范等；

在核心交换区域，针对本级教育城域网、下属校园网和教育机构网络的所有流量进行攻击检测、病毒木马检测、未知威胁检测等；在安全管理区域，针对本级教育城域网、下属校园网和教育机构网络实现安全审计、身份鉴别、授权管理、漏洞检测、终端安全管理、SSL VPN、动态密码服务系统等。

3.11.1.2 承载的业务情况

教育骨干网，除了分担教育网流量承载和承担高校城市节点就近互联外，还承担各设区市本级教育城域网、县级教育城域网、高等学校、区直中等职业学校的网络互联。教育网在教育骨干网规划与自治区电子政务外网的统一互联接口。

教育城域网，承载本行政区域内各学校和其它教育机构的教育应用与教育网、互联网和电子政务外网的访问流量。

3.11.1.3 系统软硬件构成

本项目部署有路由器、防火墙、漏洞扫描、网络控制器、统一身份认证设备、SSL VPN、上网行为管理、日志审计、运维管理、流量探针、服务器、高速密码机等硬件设备，还包括安全态势感知系统、SDN 控制软件、安全运维软件、一体化管理软件、存储虚拟化软件、计算虚拟化软件、超融合管理软件、网络管理系统、统一认证系统，教育 RA 系统等。

3.11.1.4 管理制度

参考 5.10.4 章节安全管理体系，该安全管理体系汇编内容涉及安全管理制度、安全管理机构、安全人员管理、安全建设管理、安全运维管理等 5 个方面的安全管理要求。

3.11.2 密码应用需求分析

根据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），从物理和环境安全、设备和计算安全、应用和数据安全、安全管理等层面，对本系统进行风险分析，教育骨干网按照密评三级要求进行密码应用建设，各市县教育城域网按照密评二级要求进行密码应用建设。

3.11.2.1 物理和环境安全

（一）风险分析。

1.骨干网的广西教育数据中心、广西大学、广西师范大学三个核心节点机房和各高校城市节点机房属于自建机房，均采用指纹、ID 卡、密码对进入机房人员进行身份鉴别，虽然已使用密码技术对进入机房人员进行身份鉴别，但是因为使用 ID 卡作为身份识别的方式，且密码产品不完全达到《信息安全技术 密码模块安全要求》（GB/T37092-2018）安全二级的要求，依然存在非授权人员进入物理环境，对软硬件设备和数据进行直接破坏的风险。

2.骨干网的广西教育数据中心、广西大学、广西师范大学三个

核心节点机房和各高校城市节点机房的人员进出记录明文存储在门禁管理系统数据库中，视频监控数据明文存储在磁盘阵列中，未使用密码技术进行数据存储完整性保护，存在门禁进出记录和视频监控记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

3.城域网建设租用通信运营商线路组网，利旧各通信运营商机房，据调查，各市县通信运营商机房同样存在以上物理与环境安全风险。

（二）密码应用需求。

1.门禁身份认证。应部署符合《采用非接触卡的门禁系统密码应用技术指南》（GM/T 0036-2014）标准要求的密码技术对进出机房人员进行身份鉴别。

2.视频监控记录完整性保护。应部署符合密码相关国家、行业标准要求的密码设备或产品，解决进出门禁进出记录和视频记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

3.11.2.2 网络和通信安全

（一）风险分析。

骨干网核心节点之间的核心层设备之间、汇聚层设备之间以及核心层与汇聚层设备间通过租用通信运营商的裸光纤或光纤跳线（同个机房的核心层设备与汇聚层设备通信）进行数据传输。骨干网核心节点与各设区市高校城市节点之间，各教育城域网与各设区市高校城市节点之间通过租用通信运营商的光纤专线接入汇聚层设

备。

重要数据主要在骨干网核心节点和高校城市节点的机房间传输，传输通道能满足机密性和完整性保护，接入层的线路使用加密隧道实现数据传输，不存在非法设备从外部接入内部网络，通信数据在信息系统外部被非授权截取、非授权篡改风险。

（二）密码应用需求。

需建设单位协调提供线路租用服务的通信运营商提供证明材料进行判定，证明物理线路防护上有严格的安全保护措施，能够完全保证物理线路安全，不存在安全隐患，则该通道无需作为网络和通信安全层面的测评对象。

3.11.2.3 设备和计算机安全需求分析

（一）风险分析。

教育网运维管理利旧原广西教育数据中心的安全设备（系统）和教育 RA 系统，通过 SSL VPN、堡垒机和教育 RA 系统，对登录的用户进行身份鉴别，对远程运维管理通信过程中数据进行保护，因此不存在远程管理通道的安全问题。

（二）密码应用需求。

运维管理通道应使用国密算法。

3.11.2.4 应用和数据安全

（一）风险分析。

本项目是网络建设，无具体的应用和数据建设内容。

（二）密码应用需求。

无需求

3.11.2.5 安全管理

（一）风险分析。

广西教育网属于新建项目，需要根据相关的国家和行业标准制定密码应用方案，规划建设密码应用保障系统，系统上线前和运行后，开展密码应用安全性评估，需要依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）中的安全管理要求，制定密码相关管理制度，在本项目中落实密码相关国家政策要求，发挥密码在信息系统安全中的基础支撑作用。

（二）密码应用需求。

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），制定本系统密码应用建设方案，并委托密码测评机构对密码应用建设方案进行评估，方案评估通过后，建设密码应用保障系统，制定密码相关的管理制度，系统建设完成后，依据密码应用建设方案对系统进行密码应用性评估，评估通过后上线运行。

3.11.3 建设目标及设计原则

3.11.3.1 建设目标

根据密码应用建设方案建设密码应用保障系统，使骨干网满足

密评三级测评要求；使城域网满足密评二级测评要求。

3.11.3.2 设计原则

本次方案遵循的设计原则如下:

（一）统一性。统筹规划和统一设计系统结构。尤其是国产密码系统建设结构、数据模型结构、功能服务结构以及系统扩展规划等内容，均需从全局出发、从长远的角度考虑。

（二）先进性。国产密码系统构成必须采用具有国内先进水平，并符合国际发展趋势的技术、软件产品和设备。在设计过程中充分依照国际上的规范、标准，借鉴国内外目前成熟的主流网络和综合信息系统的体系结构，以保证系统具有较长的生命力和扩展能力。保证先进性的同时还要保证技术的稳定、安全性。

（三）高可靠/高安全性。国产密码系统设计中充分考虑系统的安全和可靠，要求采用的算法为自主可控的国产密码算法。

（四）标准化。国产密码系统各项技术遵循国际标准、国家标准、行业标准和相关规范。

（五）成熟性。国产密码系统要采用国际主流、成熟的体系架构来构建，实现跨平台的应用，不采用淘汰或落后的体系架构。

（六）适用性。国产密码产品结合广西教育网的实际情况，充分利用广西教育数据中心现有的软、硬件资源与广西教育网对接。同时对确实不适应总体规划要求的信息系统作适当调整。急用先行，在满足应用需求的前提下，尽量降低建设成本。

（七）可扩展性。国产密码系统设计要考虑到业务未来发展的需要，尽可能设计得简明，降低各功能模块耦合度，并充分考虑兼容性。系统能够支持对多种格式数据的存储。

3.11.3.3 设计依据

（一）中华人民共和国网络安全法

（二）中华人民共和国电子签名法

（三）关键信息基础设施安全保护条例

（四）信息安全技术信息系统密码应用基本要求（GB/T39786-2021）

（五）信息安全技术 信息系统密码应用基本要求（GB/T 39786-2021）

（六）电子文件密码应用指南》（GM/T0071-2019）

（七）党政机关电子公文系统建设规范》（GB/T33482-2016）

（八）采用非接触卡的门禁系统密码应用技术指南（GM/T0036-2014）

（九）IPSecVPN 网关产品规范（GM/T0023-2014）

（十）SSLVPN 技术规范（GM/T0024-2014）

（十一）SSLVPN 网关产品规范（GM/T0025-2014）

（十二）安全认证网关产品规范（GM/T0026-2014）

（十三）服务器密码机技术规范（GM/T0030-2014）

（十四）安全电子签章密码技术规范（GM/T0031-2014）

（十五）智能密码钥匙技术规范（GM/T0027-2014）

（十六）证书认证系统密码协议规范（GM/T0014-2012）

（十七）密码模块安全技术要求（GM/T0028-2014）

（十八）时间戳接口规范（GM/T0033-2014）

（十九）信息安全技术 签名验签服务器技术规范（GB/T 38629-2020）

（二十）信息安全技术 IPSecVPN 技术规范（GB/T36968-2018）

3.11.4 技术方案

在满足总体性、完备性、经济性原则的基础上，通过部署国密安全门禁系统、国密视频加密系统，利旧原广西教育数据中心的 SSL VPN、堡垒机和“教育数字证书认证系统集成建设项目”广西教育 RA 系统（含有高速密码机（渔翁 SJJ1115-B 3000）、身份认证网关（吉大正元 G3000-E）、签名验签服务器（吉大正元 V3000-S）、时间戳服务器（吉大正元 TSA3000-S）等密码产品），并正确部署配置，以满足本系统的密码应用需求。

广西教育数据中心现有 RA 设备一览表				
序号	设备名称	品牌型号	设备参数	数量
1	SSLVPN	深信服 VPN-1000 S2280	1. 提供多种身份认证方式，可以根据业务需求，采用 2 种以上的组合身份认证方式； 2. 提供 PC 端安全检查机制，检查终端的安全状态； 3. 提供基于 URL 授权的细粒度访问权限控制，让用户只能访问同一台	2 台

			Web 服务器上的有限页面，防止非法接入用户找到 SQL 注入漏洞页面； 4. 提供主从账号绑定功能，将 SSL VPN 与业务系统的帐号做绑定，防止内部用户主越权访问行为记录、展示及回溯： 5. 详细记录接入用户的访问行为，确保用户的访问过程可追溯加密算法有效性； 6. 根据不同业务的安全级别，提供 AES、3DES、RSA、RC4、MD5 及国密 SM1、SM2、SM3、SM4 等加密算法进行选择，保障数据的安全性提供更好的用户体验兼容性； 7. 具备操作系统和浏览器兼容性，兼容 Windows、MAC、移动终端等。	
2	堡垒机	绿盟 SAS NX3-H1100C-C	1. 机架式设备； 2. 交流供电，满配冗余电源； 3. 可管理设备数≥500 台； 4. 运维用户数无限制，图形并发≥100 个、字符并发≥400 个； 5. 支持用户多角色划分功能； 6. 支持定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能； 支持对运维操作会话的在线监控、实时阻断、日志回放、起止时间、来源用户、来源 IP、目标设备、协议/应用类型、命令记录、操作内容（如对文件的上传、下载、删除、修改等操作等）的详细行为日志； 7. 支持通过基于时间、IP/IP 段、用户/用户组、设备/设备组、设备账号、命令关键字、命令关键字正则表达式、危险级别、黑白名单等组合访问控制策略，授权用户可访问的目标设备。	2 台
3	网闸	天融信 TopRules 8000	1. 吞吐量：2Gbps； 2. 标准配置包含 web 访问模块、邮件访问模块、FTP 访问模块、数据库访问模块、视频监控模块、OPC 工业控制模块、自定义应用模块；	2 台

			3. 标配单电源，2U 机架式	
4	高速密码机	渔翁 SJJ1115-B3000	1. 采用硬件算法模块，严格按照国家服务器密码机相关规范设计。密钥使用经国家密码管理局批准的真随机数发生器产生，并以密文的方式存放在密码机内部，确保设备自身的数据安全； 2. 支持密钥长度 256 位的国密 SM2 椭圆曲线密码算法，支持国密 SM1、SM4 对称密码算法，支持国密 SM3 杂凑算法； 3. 支持 Windows、Linux、AIX、Solaris、FreeBSD 等主流操作系统； 4. 支持灵活多样的开发接口 支持国标接口，支持微软 CSP、PKCS#11、JCE 等国际标准开发接口，同时可根据用户需求定制接口； 5. 支持 B/S 模式管理，提供友好的管理界面。操作人员通过智能密码钥匙实现身份认证，操作终端与加密机之间建立 SSL 安全通道，保证设备管理操作的机密性、真实性和不可否认性。	2 台
5	身份认证网关	吉大正元 G3000-E	1. 机架式设备，2U； 2. 电源功耗：300W（单电源）； 3. 吞吐量：新建连接速度：1500 连接/秒；最大并发连接数：10000；最大并发用户数：1100；吞吐率：722 Mbps； 4. 提供基于数字证书的强身份鉴别、入门级访问控制、访问行为审计等功能；同时支持 RSA 和 SM2 算法。	2 台
6	签名验签服务器	吉大正元 V3000-S	1. 机架式设备，3U； 2. 电源功耗：550W（冗余电源）； 3. 吞吐量：256 位 SM2 数字签名：1000 次/秒；256 位 SM2 签名验证：700 次/秒；256 位 SM2 制作信封：700 次/秒；256 位 SM2 解密信封：800 次/秒；1024 位 RSA 数字签名：700 次/秒；1024 位 RSA 签名验证：3000 次/秒；1024 位 RSA 制作信封：2500 次/秒；1024 位 RSA 解密信封：800 次/	2 台

			秒； 4. 提供数字签名/签名验证、数字信封/解密信封、时间戳等功能；同时支持 RSA 和 SM2 算法。	
7	时间戳服务器	吉大正元 TSA3000-S	1. 机架式设备，2U； 2. 电源功耗：300W（单电源）； 3. 网络接口：2 个千兆电口； 4. 提供精确的、且不可抵赖的时间戳服务。同时支持遵循国际标准（RFC3161）和 RFC2630 两种时间戳协议的时间戳，采用标准的时间戳请求、时间戳应答以及时间戳编码格式，具有良好的兼容性能。	2 台

根据教育部和国家密码局联合组织的教育行业密码应用试点示范工程项目的工作要求，自治区教育厅已申报“广西数字教育密码应用体系建设”项目。据教育部通报，该项目将于今年实施建设。因此，本设计方案的密码应用建设应该与其衔接。

“广西数字教育密码应用体系建设”项目具体任务内容如下:

（一）教育数字认证子系统。

广西区教育厅已建成教育数字认证子系统（广西区 RA 中心），可实现 PC 端数字证书的发放与管理。现需对该系统进行升级，实现移动数字证书的签发和管理。各市级教育局和各学校根据需求建设 RA 或 LRA, 用于教育行政管理人员数字证书发放和管理。

教育数字认证子系统需新增移动制证模块、移动安全管理系统、移动端安全接口、移动终端密码等模块。

（二）教育密码综合服务子系统。

依托中央级教育密码基础服务平台和省级节点，建设教育密码

综合服务子系统，为本区域的教育信息系统提供统一的加密、统一的签验、统一的身份认证等密码服务及设备管理。

教育密码综合服务子系统主要包括密码统一服务、基础密码服务、密钥管理、密码设备管理、密码业务管理、密码业务监控、密码业务分析等模块。

（三）教育可信身份服务子系统。

依托教育基础数据和教育行业密码数字身份基础设施，建设教育可信身份服务子系统，为我区教育行政部门、大专院校等教育教学机构及学生和教师提供本地化的可信教育数字身份的申请激活、密钥管理、应用支撑等服务功能。

教育可信身份服务子系统主要包括可信教育数字身份的申请服务、领取与激活服务、生命周期管理、一体化密钥安全管理与应用服务等模块。

（四）教育电子证照服务子系统

依托中央级教育密码基础服务平台，教育密码服务节点建设教育电子证照服务系统，建设教育电子证照服务系统，实现本单位教育应用相关的“资质证书、证件、成绩单、奖状、通知”等教育电子证照的统一签发与管理，为教育行业信息化应用、跨行业以及社会化应用服务，提供教育电子证照的查询、验证、调用等安全可信服务。

教育电子证照服务子系统主要包括证照制作加工模块、证照网

页发布模块、证照离线保护模块、证照验证模块、证照模板设计模块等。

（五）教育电子签章服务子系统

依托中央级教育密码基础服务平台，教育密码服务节点建设教育电子签章服务子系统，为本区域应用系统、教育电子证照系统，提供统一的电子签章服务，有效解决电子成绩单、电子在读证明、电子荣誉证书等电子凭据的可信问题，便于学生留存、流转、应用。

教育电子签章服务子系统主要包括签章管理模块、印模管理模块、日志管理模块、安全控制模块等。

（六）教育电子证照档案可信服务系统。

依托中央级教育密码基础服务平台和省级节点，建设教育电子证照档案一体化服务子系统，对接教育电子证照服务子系统和教育电子签章服务子系统实现本单位教育应用相关的“资质证书、证件、成绩单、奖状、通知”等教育电子证照与档案的统一管理，为教育行业信息化应用、跨行业以及社会化应用服务。

教育电子证照档案可信服务系统主要包括教育电子证照共享模块、教育可信电子档案服务模块等。

（七）教育密码区块链服务系统。

依托中央级教育密码基础服务平台和省级节点，建设教育密码区块链服务基础平台，支持建立教育身份链、教育档案链、教育资产链等管理链与服务链。

（八）广西壮族自治区统一身份认证对接系统。

本系统将对接广西的统一身份认证系统，实现教育行业可信身份与密码体系与广西的认证与密码应用支撑体系的融合应用。

3.11.4.1 密码应用技术框架

本项目采用的密码产品主要包括:

（一）安全门禁系统和视频加密系统。符合《采用非接触卡的门禁系统密码应用指南》（GM/T0036-2014）的电子门禁系统对进出机房人员进行身份鉴别。

（二）服务器密码机。本地机房部署符合密码相关国家、行业标准要求的密码设备或产品，对门禁进出记录和视频监控数据进行机密性、完整性，同时提供安全、完善的密钥管理功能。

（三）SSL VPN 安全网关。采用密码技术建立一条安全的信息传输通道，保证通信过程中数据的完整性、机密性。产品符合《信息安全技术 密码模块安全要求》（GB/T 37092-2018），支持国产密码算法具有商用密码产品型号证书。

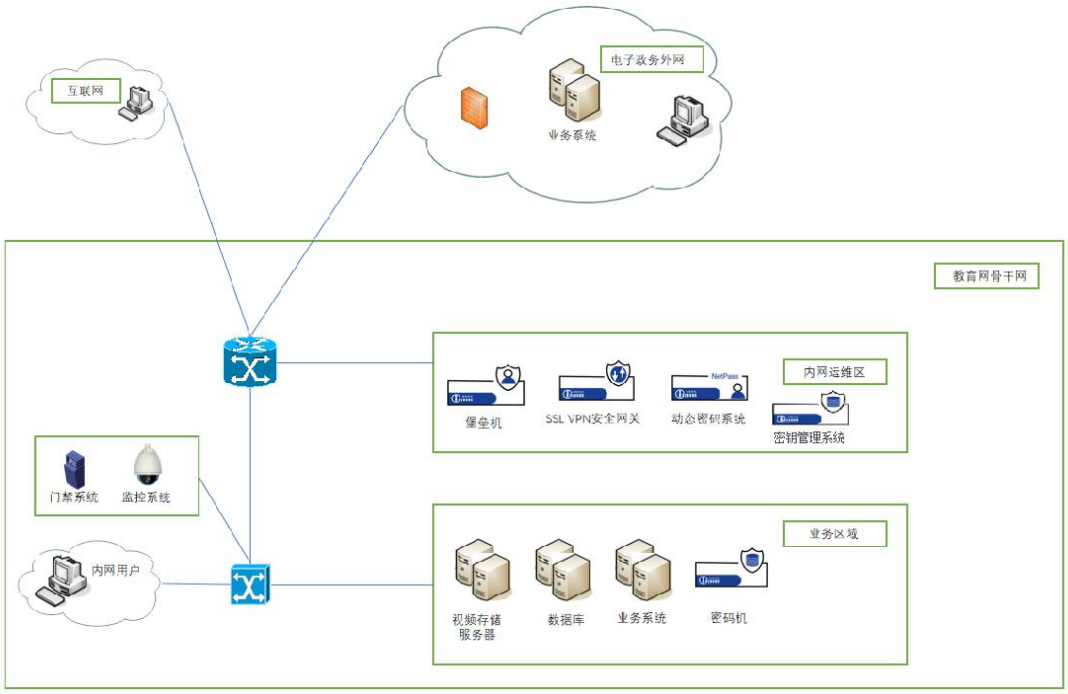

图 5-45 密码应用工作流程示意图

（四）动态密码系统。采用密码技术对登录运维设备进行的管理用户进行身份鉴别。

（五）USBKey。主要提供签名验签、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，身份鉴别 Key 中存放标识用户身份的数字证书,主要用于对用户身份真实性的鉴别。

（六）浏览器密码模块（二级）。主要提供签名验签、加密解密、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书。

（七）密钥管理系统。面向行业/企业内部信息系统和业务承载网络，提供统一的密钥生成、使用、分发、存储等应用服务和签名、加密、摘要等综合密码计算服务，对非对称密钥和对称密钥进行集中管理，以有效满足和适应网络、信息系统、物联网、移动应用等

多样化的密码需求。

3.11.4.2 物理和环境安全

（一）建设改造要点。

首先，对机房门禁系统实施改造，替换成符合《采用非接触卡的门禁系统密码应用指南》（GM/T0036-2014）的电门禁系统，使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行鉴别。

其次，撤除机房门禁系统中的 ID 卡电子门禁设备。

最后，在机房部署符合《服务器密码机技术规范》（GM/T0030-2014）的服务器密码机，使用 HMAC-SM3 技术对电子门禁系统进出记录和视频监控系统视频记录等数据进行完整性保护，其中 HMAC-SM3 密钥由服务器密码机生成，存储在服务器密码机中，不涉及密钥分发、导入与导出，密钥的备份和恢复、归档和销毁由密码设备管理员负责。

物理和环境全层面使用的密码算法、密码技术、密钥管理由符合《采用非接触卡的门禁系统密码应用指南》（GM/T0036-2014）、《服务器密码机技术规范》（GM/T0030-2014）、《密码模块安全技术要求》（GM/T0028-2014）的电子门禁系统和服务器密码机实现。

（二）责任划分。

骨干网的机房物理和环境安全建设改造按本方案实施。其中，

广西教育网网络中心的部分由自治区教育厅负责；广西大学和广西师范大学 2 个核心节点，以及 12 个高校城市节点的部分由所属学校负责，自治区教育厅按本方案提供建设改造专项经费补助。

城域网建设采用租用通信运营商线路组网，利旧各通信运营商机房，各通信运营商机房物理环境密码应用建设改造由所属通信运营商负责。

3.11.4.3 网络和通信安全

骨干网和城域网中所租用通信运营商的裸光纤和光纤专线由提供线路租用服务的通信运营商提供证明材料进行判定，证明物理线路防护上有严格的安全保护措施，能够完全保证物理线路安全，不存在安全隐患。

3.11.4.4 设备和计算安全

本次升级改造所使用的网络设备、安全设备和服务器，都使用基于 SM2、SM3 算法的 SSH 协议。

（一）安全设计。

设备与计算安全主要关注服务器的操作系统与核心数据库的安全。根据广西教育网、城域网应用密码应用需求，设备与计算安全设计内容如下:

通过动态密码服务器生成动态码，并通过短信网关发送给运维人员实现用户双因素登录认证，为运维管理人员提供可靠身份鉴别，

保障远程管理身份鉴别信息的机密性。通过 SSL VPN 建立的安全通道登录运维堡垒机。

设备日志记录完整性：通过调用服务器密码机对应用服务器、数据库服务器等设备日志进行完整性保护。

（二）密码应用工作流程。

通过网络和通信安全设计，建立运维的集中管理通道，保证数据的机密性和完整性，通过动态验证码对运维人员进行身份鉴别，包括服务器、网络设备等登录身份认证。

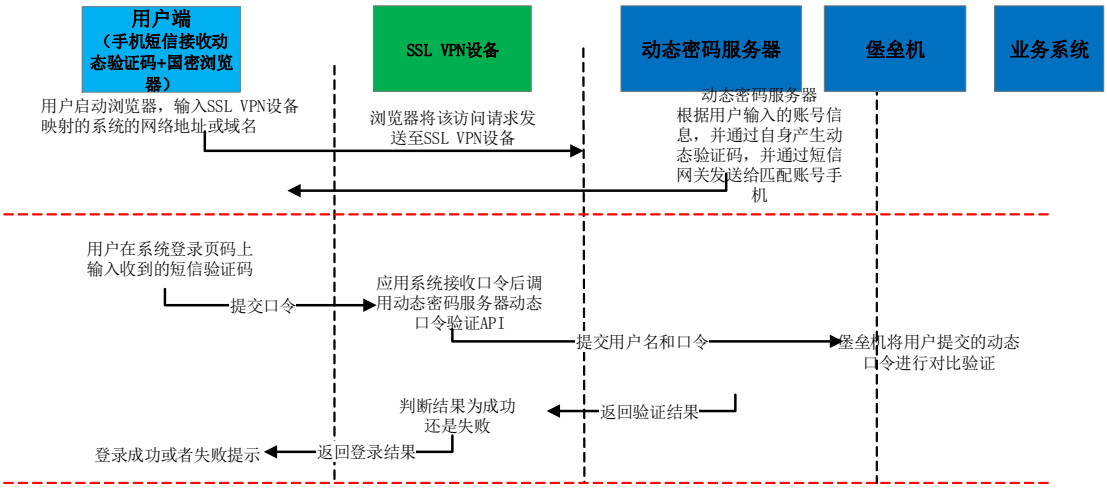

图 5-46 密码应用工作流程示意图

1.用户浏览器，输入 SSL VPN 设备应用系统的网络地址或域名。

2.浏览器将该访问请求发送至 SSL VPN 设备。

3.堡垒机根据用户输入的账号信息，并通过动态密码服务器产生动态验证码，并通过短信网关发送给匹配账号手机。

4.用户在系统登录页码上输入收到的短信验证码。

5.应用系统接收口令后调用动态密码服务器口令验证 API。

6.动态密码服务器将用户提交的动态口令进行对比验证。

7.验证通过则返回登录成功，否则则登录失败。

（三）责任划分

骨干网的机房物理和环境安全建设改造按本方案实施。其中，广西教育网网络中心的部分由自治区教育厅负责；广西大学和广西师范大学 2 个核心节点，以及 12 个高校城市节点的部分由所属学校负责。

城域网建设采用租用通信运营商线路组网，利旧各通信运营商机房，各通信运营商机房物理环境密码应用建设改造由所属通信运营商负责。

3.11.4.5 应用和数据安全

本项目不涉及具体的应用和数据安全，不适用。

3.11.4.6 密钥管理安全

部署独立的密钥管理系统，负责对称密钥、非对称密钥的安全产生和安全存储，以及各类密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和密钥管理服务。密钥管理系统主要包括密钥模板管理、预激活密钥管理、KEK 密钥管理、DEK 密钥管理、密钥司法取证、密钥归档以及应用主密钥管理等功能。

支持为外部业务应用提供密钥管理和密码计算服务接口，外部应用可通过该服务实现对应的密钥管理功能，包括对称密钥和非对称密钥的申请、更新、注销、恢复、失信、销毁、获取和查询等全

生命周期管理接口服务。以及提供数据加解密和数据数字签验服务等。同时系统还实现了请求协议转换、请求分发、密码资源调度和负载均衡等服务支撑。

3.11.4.7 密码应用部署

（一）教育骨干网。

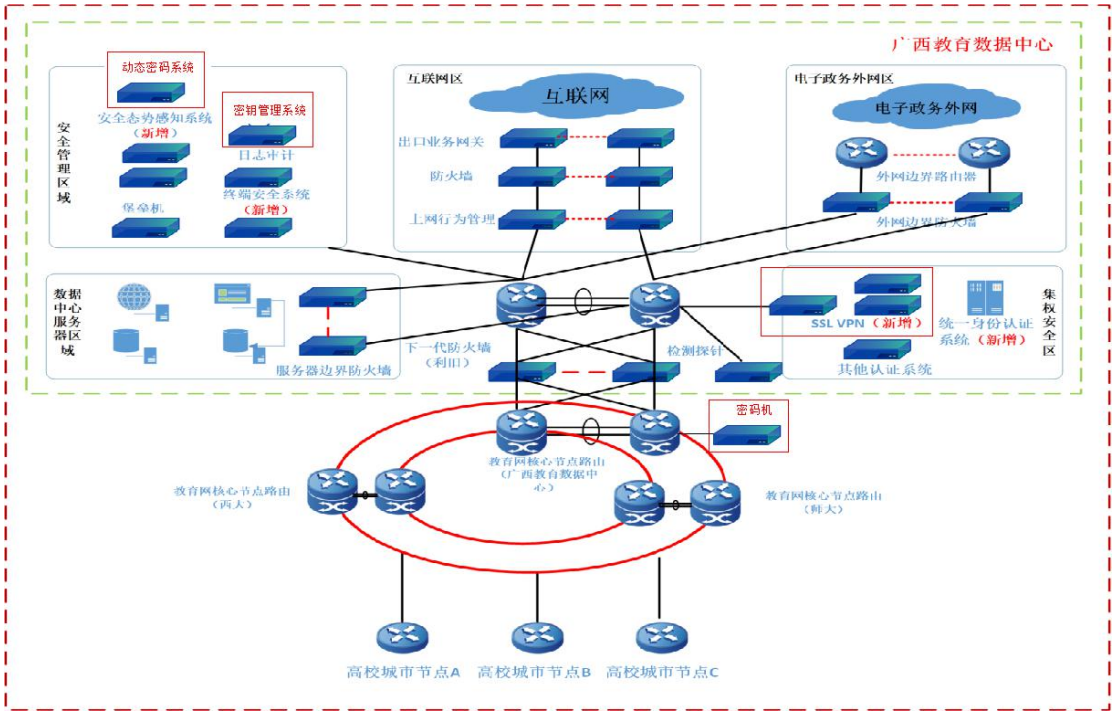

图 5-47 教育骨干网密码应用部署图

1.对机房门禁系统实施改造，替换成符合《采用非接触卡的门禁系统密码应用指南》（GM/T0036-2014）的电门禁系统，使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行鉴别。替换现有摄像头设备，替换成符合相关国家、行业密码标准要求的摄像头设备，解决门禁进出记录和视频记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

2.在安全管理区利旧教育 RA 系统实现动态密码系统功能，结合动态密码系统的双因子认证功能，通过 Ukey、动态令牌或手机短信等动态口令与静态密码相结合的方式，实现业务系统高强度的双因子动态身份认证。

3.在安全管理区利旧已有 SSL VPN。用于保障远程运维管理人员身份真实性，保证通信过程中数据的完整性、机密性。

4.在安全管理区复用升级改造后的教育 RA 系统实现密钥管理系统功能。用于对称密钥、非对称密钥的安全产生和安全存储，以及各类密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和密钥管理服务。密钥管理系统主要包括密钥模板管理、预激活密钥管理、KEK 密钥管理、DEK 密钥管理、密钥司法取证、密钥归档以及应用主密钥管理等功能。

5.在网络中心利旧密码机服务器。用与对骨干网视频监控数据、设备访问控制信息、应用及数据库服务器等设备日志进行完整性保护。

（二）教育城域网。

1.在安全管理区部署动态密码系统。结合动态密码系统，通过动态令牌或手机短信等动态口令与静态密码相结合的方式，实现业务系统高强度的双因子动态身份认证。

2.在安全管理区部署 SSL VPN。用于保障远程运维管理人员身份真实性，保证通信过程中数据的完整性、机密性。

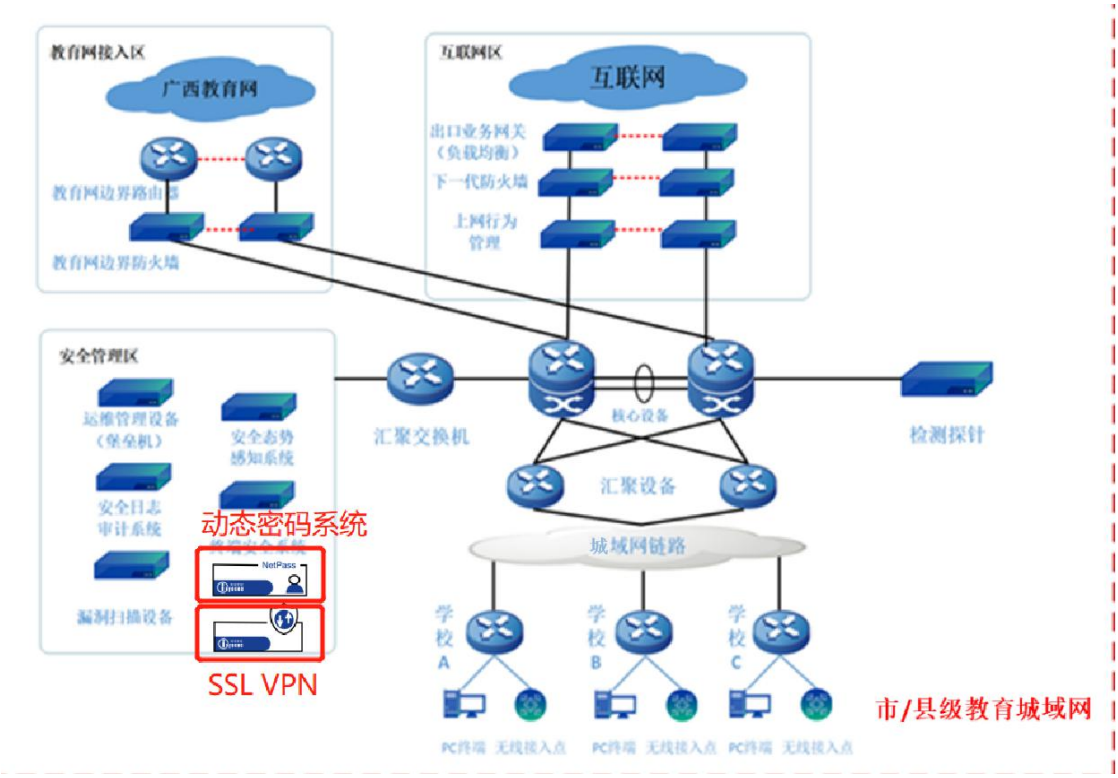

图 5-48 教育城域网密码应用部署图

3.11.4.8 密码软硬件产品清单

序号	产品名称	描述	数量	单位	备注
1	国密安全门禁系统	双开 4 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门禁控制器（双门）4 台、国密门禁人脸读卡器 4 台、国密 CPU 卡 50 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张	1	套	新增
2	国密视频加密系统	1、含国密网络摄像机 20 台、网络硬盘录像机 2 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	1	套	新增
3	服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	2	台	利旧现有设备
4	密钥管理系统	1、包括业务实现层、数据持久层和操作系统层。底层依托符合 GM/T0028 的三级及以上密码模块（密码机设备），实现密钥安全管理，支持对称密钥和非对称密钥的标准化全生命周期管理，以	1	套	复用升级后的教育

序号	产品名称	描述	数量	单位	备注
		及实现密码计算服务：包括为业务应用提供密钥级加解密、签名验签、摘要、MAC 等密码计算服务。 2、系统内部的服务框架层基于用户角色来实现权限管理机制和访问控制策略。系统内将权限管理点细分，并基于角色将相应的权限点与管理员公钥证书绑定，可以方便的实现安全访问控制策略。 3、系统基于 B/S 模式开发，在 Web 访问层中，使用符合国际/国密标准的 SSL 安全通信层协议，支持 X.509 证书标准，提供双向认证，保证交互数据的安全性和完整性。			RA 系统
5	国密安全门禁系统	双开 2 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门禁控制器（双门）1 台、国密门禁人脸读卡器 1 台、国密 CPU 卡 10 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张	14	套	新增
6	国密视频加密系统	1、含国密网络摄像机 4 台、网络硬盘录像机 1 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	14	套	新增
7	服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	14	台	新增
8	SSL VPN	基于国密 SSL 安全协议的 VPN 设备，集成了身份认证、访问控制和资源管理等功能；提供用户接入控制和数据传输的加/解密功能.标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存,4 个千兆电口、2 个千兆光口	132	台	新增
9	动态密码系统	系统具备动态密码种子生成、验证服务和服务管理三个子系统，产品提供多种终端形态支持，主要包括：时间型令牌，事件形令牌，多键令牌，手机软件、手机短信、二维矩阵等多种方式。标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存。最大支持 5000 用户，响应性能 500TPS	132	台	新增

3.11.4.9 安全与合规性分析

（一）教育骨干网。

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
物理和环境安全	身份鉴别	在系统所在机房部署符合要求的安全电子门禁系统，使用 SM4 算法进行密钥分散，实现门禁卡的“一卡一密”，并基于 SM4 算法对人员身份进行身份鉴别；使用 HMAC-SM3 技术对电子门禁系统进出记录进行完整性保护。	符合	无
	电子门禁记录数据完整性		符合	无
	视频监控记录数据存储完整性	使用服务器密码机，实现对视频监控数据进行完整性保护。	符合	无
	密码服务	本安全层面使用的密码设备均符合法律法规的相关要求，并依法接受检测认证，经过商用密码认证机构认证合格。	符合	无
	密码产品	采用的密码产品达到 GB/T 37092 二级的安全要求。	符合	无
网络和通信安全	身份鉴别	在本系统网络边界和数据灾备区域分别部署 SSL VPN，在系统安全管理区部署 SSL VPN。对通信双方进行身份鉴别，建立安全的数据传输通道，对访问控制信息进行完整性保护，对从外部网络连接内部网络的设备进行认证。	符合	无
	通信数据完整性		符合	无
	通信过程中重要数据的机密性		符合	无
	网络边界访问控制信息的完整性		符合	无
	安全接入认证		不适用	等保三级系统不适用
	密码服务	本安全层面使用的密码设备均符合法律法规的相关要求，并依法接受检测认证，经过商用密码认证机构认证合格。	符合	无
	密码产品	采用的密码产品达到 GB/T 37092 二级的安全要求。	符合	无
设备和计	身份鉴别	采用动态密码系统对登录运维系统的管理员进行身份鉴别，防止非授权人员	符合	无

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
算安全		登录。		
	远程管理通道安全	在本系统安全管理区域部署 SSL VPN，建立远程管理的安全通道，保护数据传输的机密性和完整性。	符合	无
	重要信息资源安全标记完整性	无	不适用	本系统不涉及重要信息资源的敏感标记
	系统资源访问控制信息完整性	在本系统业务服务区域部署服务器密码机，调用服务器密码机，对设备访问控制信息进行完整性保护。	符合	无
	日志记录完整性	在本系统业务服务区域部署服务器密码机，调用服务器密码机，对应用服务器、数据库服务器等设备日志的完整性保护。	符合	无
	重要可执行程序完整性、重要可执行程序来源真实性	在本系统业务服务区域部署服务器密码机，调用服务器密码机，实现重要可执行程序的完整性保护和来源真实性验证。	符合	无
	密码服务	本安全层面使用的密码设备均符合法律法规的相关要求，并依法接受检测认证，经过商用密码认证机构认证合格。	符合	无
	密码产品	采用的密码产品达到 GB/T 37092 二级的安全要求。	符合	无
应用和数据安全	身份鉴别	无	不适用	本项目是网络建设，无具体的应用和数据建设内容
	访问控制信息完整性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要数据传输机密性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	重要数据传输完整性		不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要数据存储机密性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要数据存储完整性		不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要信息资源安全标记完整性	无	不适用	本系统不涉及重要信息的敏感标记
	不可否认性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	密码服务	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	密码产品	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。

（二）教育城域网。

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
物理和环境安全	身份鉴别	无	不适用	不属于自建机房，应由责任单位建设和运维；
	电子门禁记录数据存储完整性			
网络	身份鉴别	部署 SSL VPN、动态密码系统。对通	符合	无

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
和通信安全	通信数据完整性	信双方进行身份鉴别，建立可靠安全的数据传输通道，保证通信数据的完整性、机密性。		
	通信过程中重要数据的机密性			
	网络边界访问控制信息的完整性		符合	无
设备和计算安全	身份鉴别	采用动态密码系统对登录运维系统的管理员进行身份鉴别，防止非授权人员登录。	符合	无
	系统资源访问控制信息完整性	系统中使用的密码机，能够实现了系统资源访问控制信息完整性。	符合	无
	日志记录完整性	系统中使用的密码机，能够实现了系统资源访问控制信息完整性。	符合	无
应用和数据安全	身份鉴别	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	访问控制信息完整性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要数据传输机密性	无	不适用	本项目是网络建设，无具体的应用和数据建设内容。
	重要数据传输完整性			
	重要数据存储机密	无	不适用	本项目是网络建设，无具体的应

指标要求	密码技术应用点	采取措施	标准符合性（符合/不适用）	说明（针对不适用项说明原因及替代性措施）
	性			用和数据建设内容。
	重要数据存储完整性			

3.11.5 安全管理方案

3.11.5.1 制度

根据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）中安全管理制度方面的要求，制定与本系统相适应的密码安全理制度和作规范，内容包括并不仅限于密码设计、建设、运维、人员、设备、密钥等6个方面，并在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

密码安全管理制度和操作规范发布后，每年7月起，在教育网运维涉及单位内部组织专家和密码应用相关人员对密码安全管理制度和操作规范在使用过程中的合理性和适应性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

3.11.5.2 人员

根据《信息安全技术信息系统密码应用基本要求》

（GB/T39786-2021）中安全管理人员方面的要求，对教育网运维涉及单位现有的人员管理制度进行补充完善。

（一）建立内部密码专题培训机制。每 6 个月组织一次密码应用专题培训。由教育网密码应用人员或聘请本系统外专家担任培训讲师，内容包括并不仅限于涉及密码相关法律法规和标准规范、商用密码应用、商用密码、应用安全性评估等方面。培训目标是使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行。

（二）做好密码应用系统操作培训。在本系统完成密码应用改造后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品。

（三）应配足相关工作人员。应结合自身实际情况，分别设立密钥管理员、安全审计员、密码操作员等岗位，明确各岗位职责，且每个岗位均由 2 人担任。

（四）应建立和完善密码应用管理制度。在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理人员、安全审计人员、密码操作人员与单位订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制

度承担相应的保密义务。

3.11.5.3 实施

完成本方案编制后，委托密码测评机构对本方案进行评估，评估通过后，将本系统密码应用改造方案报送自治区的密码管理局密码管理部门备案，并同步对本系统进行密码应用改造，选用通过检测认证合格的网络设备、安全设备、服务器和安全门禁系统等商用密码产品，合规、正确、有效的建设密码保障系统。

依据评估通过的密码应用方案改造完成后，委托密码测评机构对本系统进行密码测评，密码测评通过后上线运行。上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

3.11.5.4 应急

根据《信息安全技术信息系统密码应用基本要求》（GB/T39786-2021）中安全管理应急方面的要求，对本系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。针对密码安全方面的应急响应措施包括并不仅限于：当本系统发生密码相关安全事件时，在事发后 3 小时内向广西教育网网络中心进行报

告：事件处置完成后2个工作日内，向广西教育网网络中心汇报安全事件发生情况及处置情况。

3.12 运行维护建设方案

3.12.1 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。

3.12.2 总体运维方案

广西教育网由教育骨干网、教育城域网和校园网三部分构成。教育骨干网汇聚节点、教育城域网中心所在单位应指定运行技术负责人，负责日常运行事务，协同服务运营商实施网络运维。运维方案如下：

3.12.2.1 教育骨干网运维方案

自治区教育厅委托自治区教育技信中心建设教育骨干网管理运维系统，对教育骨干网各节点和各接入点实施监控，管理网络日常

流量承载，运营商负责教育骨干网网络线路的管理运维。

3.12.2.2 教育城域网运维方案

各教育城域网的主管教育管理行政部门负责监督、协助提供教育城域网组网服务的运营商做好教育城域网管理运维工作。运营商负责教育城域网管理运维具体工作,建设教育城域网管理运维系统,对教育城域网和网内各信息终端实施监控,管理网络日常流量承载,保障光纤线路连接。

3.12.2.3 校园网运维方案

对由运营商提供校园网组网服务的学校，运营商负责提供运维服务，并可委托校园网集成施工方负责校园网的运维的具体工作。

校园网业务故障指影响客户业务正常使用的故障，包括业务中断和一般故障。业务中断故障是业务至少出现一个局向全阻的情况，一般故障是指未全阻情况下的其他故障，如业务性能劣化。

对经相关教育行政部门审批同意保留使用的存量校园网，校园网内设备要具备远程配置与管理能力，校内设备加电可使用、免维护。

3.12.2.4 远程运维方案

远程运维服务是一种智能技术支持服务，以远程专家与智能工具相结合的方式，将技术知识体系和售后维护经验应用于用户网络问题处理中，帮助用户快速准确恢复网络，提高用户网络可用性。

广西教育骨干网在保障网络正常运行中的地位十分重要，管理运维技术要求高。正常状态下，系统安装调试交付使用后，除确有必要外，一般不作网络系统基础配置的变更。当出现特殊情况时，一般需要系统原厂商提供远程，甚至现场技术救援。因此，建议针对教育骨干网项目管理运维采购专业远程运维服务。

3.12.2.5 教育骨干网控制器

借助教育骨干网控制器可以实现对教育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:

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。

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。

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。

VPN 业务可视。控制器支持对于 VPN 业务实现 360 度可视。

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。

业务运维信息中心。支持用户察看业务告警，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。

业务诊断中心。支持启动 RFC2544， Y.1564 业务诊断。

隧道路径智能调整。控制器支持对于隧道路径智能调整。

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。

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。

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。

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。

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。

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。

3.12.2.6 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5年的运维需求,本次设计在教育骨干网的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。

3.12.2.7 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，建议由运营商在各自运维系统上为教育行政部门开设账号，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。

3.12.3 网络安全运维要求

落实各级教育行政部门网络安全责任，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。

3.12.4 运营商网络运维要求

3.12.4.1 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：教育骨干网故障、教育城域网故障，并遵循以下故障处理原则：

（一）教育骨干网故障。

如由运营商主动发现的教育骨干网故障，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。

（二）教育城域网故障。

如首先发现故障的是运营商，由运营商市县级专职客户经理第一时间联系各市县教育行政部门负责人或授权人，报备故障情况；如首先发现故障的是市县各教育行政部门，由市县各教育行政部门的负责人或授权人通知运营商市县级专职客户经理协调进行故障处理。

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，运营商客户经理向市县各教育管理机构负责人或授权人口头反馈故障原因和处理结果后，3 个工作日内按照客户需要提交故障处理书面报告。

（三）故障升级。

当各市县教育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。

3.12.4.2 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）。

表 5-14 业务恢复时限和及时率表

故障类别		设区市市区	县城、乡镇	农村	偏远校区
教育骨干网		≤4			
教育城域网		≤4	≤8	≤12	≤24
业务中断	校园网出口故障	≤4	≤8	≤12	≤24
	部分教室业务中断	≤4	≤8	≤24	≤48
一般故障（含性能劣化）		≤24	≤24	≤48	≤72

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。

3.12.4.3 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。

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。

表 5-15 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

3.12.4.4 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。

（一）网络运行监控。

网络监控服务指运营商向各级教育行政部门提供 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。

（二）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。

广西教育骨干网节点及教育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，由各级教育行政部门签字确

认。

（三）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。

（四）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。

表 5-16 网络服务报告表

服务内容	服务要求
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

（五）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。

（六）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。

（七）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。

3.12.4.5 应急维护保障

运营商需要充分、积极、有效地应对各种自然灾害、突发事件造成的通信设备瘫痪，做好在各种紧急情况下的重要客户网络应急通信保障和处理工作，保证教育网在出现重大通信故障时，合理、高效、迅速地恢复通信，缩短电路阻断历时，要求运营商将针对教育网特点制定相应网络安全的应急处理预案，提供多种应急处置方案。

应急预案维护标准是要求在预案的基础上，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。

3.12.4.6 运维权限规划

建议统一由运营商进行教育城域网,以及网络线路部分的维护,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。

3.13 软硬件配置

3.13.1 选型基本原则

（一）国产化原则。根据《鼓励软件产业和集成电路产业发展的若干政策》中规定，国家投资的重大工程和重点应用系统，应优先由国内企业承担，在同等性能价格比条件下应优先采用国产软硬件系统。

（二）开放性和扩展性原则。一方面，系统将与各部门的业务系统及数据库相连接，要采用开放性、标准化的设备、软件及信息资源；另一方面，系统对于未来可能增添的新的子系统、新的数据库、新的功能、新的用户都要留有接口和二次开发 API，并符合电子政务相关技术标准，系统可以随形势的发展而不断成长扩大。

（三）先进性和成熟性原则。信息技术尤其是软件技术发展迅速，新理念、新体系、新技术迭相推出，这造成了新的、先进的技术和成熟的技术之间的矛盾。而大规模、全局性的应用系统，其功能和性能要求具有综合性。因此，在产品选用方面要求先进性和成熟性的统一，以满足系统在很长的生命周期内有持续的可维护性和可扩展性。

（四）可靠性原则。在社会向信息时代迅速发展的同时也有潜在危机，即对信息技术的依赖程度越高，系统失效可能造成的危害和影响也就越大。因此，本系统的软硬件选择在尽可能有限的投资

条件下，从系统结构、网络结构、技术措施、设备选型以及厂商的技术服务和维修响应能力等方面综合考虑，确保系统整体运行的可靠性。

3.13.2 硬件选型原则

系统硬件平台是支撑应用系统运行的核心基础设施，主要包括高性能服务器、高容量存储设备和其他相关软硬件设备。其中，高性能服务器用于提供快速、可靠的计算，高容量存储设备用于容纳存储相关数据。硬件平台性能的好坏将直接影响到应用系统的运行效果。

由于应用系统的复杂性和特殊性，对于其硬件平台设计需要采用如下的原则。

（一）统一性。明确应用系统在规划期内的规模，对整个应用系统的模块、用户、流程进行分析，确定总体需求，从而定义出其硬件平台对应的架构和配置。

（二）高可用性。要求硬件平台具有单点失效保护，能够实现故障预警、报警，具有良好的故障应急处理能力。如在出现有限个数的服务器、磁盘、存储设备或交换机故障等情况下，系统可以继续运行，不影响业务处理。

（三）高扩展性。由于应用系统建设是一个长期持续的过程，日后随着城市规模扩大和业务量的增长，用户数可能会超出预期，

当硬件平台的处理能力不够时，要求可以在原有架构的基础上实现灵活扩展。硬件平台的扩展性主要分成两类：纵向扩展和横向扩展。纵向扩展是指通过增加硬件设备的 CPU、内存、通道和板卡等资源来提高原有设备的处理能力；横向扩展是指通过购买新的设备和原有设备并行工作，通过负载分担来实现处理能力扩展。

（四）高安全性。能够实现良好的信息安全能力，能够应用灵活的安全策略，如对不同用途的服务器进行安全分区以实现不同程度的隔离等。

（五）高可维护性。维护便捷简单，尽量减少宕机时间，特别是减少进行故障修复、系统扩展和变更时的宕机时间，能够提供友好、全面的监控工具。

（六）合适性价比。在满足需求并符合上述原则的前提下，良好的性价比是关键。各家硬件各有所长，关键是需要关注满足应用系统需求的技术，而不是一味追求先进技术，只要能解决主要问题，满足需求和原则，有合适的价格，就可以着重考虑。

3.13.3 软件选型原则

（一）系统软件。

1. 操作系统。服务器运行安全、稳定、可靠，硬件设备兼容性优异，支持多种软件集成，拥有高效完善网络功能和图形工作平台等。

2. 数据库软件。具有高可靠性，开放可扩展，编程接口符合国际通用标准，支持多个操作系统平台部署，拥有高效并发控制机制，提供查询优化策略，支持故障恢复，提供备份和还原，支持多媒体数据存储，提供全文检索功能，支持数据仓库，支持数据库集群等。

（二）平台软件。

1. 安全软件。技术安全可控，具有高度安全可靠性，开放可扩展，嵌入式安全管理，可信消息管控等。

2. 基础中间件。技术安全可控，提供 API 接口，并符合行业通用标准，开放可扩展。基于 J2SE 的 Java 语言，提供 HTTP/HTTPS 服务、Servlet/JSP 服务、SOAP/WS 服务、远程调用服务、SOA 服务总线、安全服务和日志服务，支持集群和负载均衡。

3. 交换处理中间件。技术安全可控，提供 API 接口，符合 SOA 标准，开放可扩展。提供数据存取、交换、访问、通讯、处理等功能，提供分布式服务。

4. 资源目录交换中间件。技术安全可控，提供 API 接口，并符合 LDAP 和 SOA 标准，开放可扩展。提供资源目录发现，资源目录状态监测，资源目录状态存储，资源目录索引，分布式资源目录检索等功能。

3.13.4 软硬件配置清单

本项目软硬件配置清单如下表。

表 5-17 软硬件配置清单表

序号	子系统名称	分类	产品名称	配置参数	单位	数量
1	教育骨干网	线路	线路租用	≥10G 点对点专线，租用期：3 年。	条	6
2			线路租用	≥1G 点对点专线，租用期：3 年。	条	18
3		密码应用建设	国密安全门禁系统	双开 4 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门禁控制器（双门）4 台、国密门禁人脸读卡器 4 台、国密 CPU 卡 50 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张	套	1
4			国密视频加密系统	1、含国密网络摄像机 20 台、网络硬盘录像机 2 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	套	1
5			服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	台	2
6			密钥管理系统	1、包括业务实现层、数据持久层和操作系统层。 底层依托符合 GM/T0028 的三级及以上密码模块（密码机设备），实现密钥安全管理，支持对称密钥和非对称密钥的标准化全生命周期管理，以及实现密码计算服务：包括为业务应用提供密钥级加解密、签名验签、摘要、MAC 等密码计算服务。 2、系统内部的服务框架层基于用户角色来实现权限管理机制和访问控制策略。系统内将权限管理点细分，并基于角色将相应的权限点与管理员公钥证书绑定，可以方便的实现安全访问控制策略。 3、系统基于 B/S 模式开发，在 Web 访问层中，使用符合国际/国密标准的 SSL 安全通信层协议，支持 X.509 证书标准，提供双向认证，保证交互数据的安全性和完整性。	套	1
7			国密安全	双开 2 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门	套	14

序号	子系统名称	分类	产品名称	配置参数	单位	数量
			门禁系统	禁控制器（双门）1 台、国密门禁人脸读卡器 1 台、国密 CPU 卡 10 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张		
8			国密视频加密系统	1、含国密网络摄像机 4 台、网络硬盘录像机 1 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	套	14
9			服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	台	14
10		网络数据交换和管理服务	核心路由器	基于国密 SSL 安全协议的 VPN 设备，集成了身份认证、访问控制和资源管理等功能；提供用户接入控制和数据传输的加/解密功能.标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存,4 个千兆电口、2 个千兆光口	台	6
11			汇聚路由器	1．双主控设计且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 2．独立交换网板总数≥2 并满配；整机支持业务载板插槽≥6 个（全尺寸业务卡槽位，非子卡槽位）。 3．配置万兆光口≥4 个，千兆光口≥10 个；配置万兆单模光模块≥4 个，千兆单模光模块≥10 个；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 4.支持网络资源、隧道路径、业务路径、及业务 SLA 的可视可管；支持广域网智能调优。 5．支持 SRv6，支持 SRv6 承载 VPN 业务。	台	26
12			网络管理系统	1．系统应支持大规模设备管理能力，可最多管理 20000 台网元；系统应支持多种设备的管理，包括并不仅限于交换机、路由器、防火墙、WLAN、服务器、存储、IP 话机、摄像头等；实配 50 个设备授权。 2．配置配套操作系统与数据库，以及配套的部署硬件设备。 3．提供告警、性能、有线无线资源、用户终端定位信息等报表管理能力。 4．网络质量监控：系统支持基于真实流的 IP 网络实时监测能力（非模拟报文监测或者探针式监测），监测结果可实时在拓扑上显示； 5．提供设备原厂不少于 50 台路由器、交换机等网络设备 5 年实时远程监控运维服务。	套	1

序号	子系统名称	分类	产品名称	配置参数	单位	数量
13			教育骨干网控制器	1．包含管理、控制和分析集成的统一云化架构，管理授权覆盖教育骨干网不少于 50 台路由器、交换机等网络设备。支持统一的 Portal 来访问所有的组件，包括设备管理，业务发放，网络优化，网络监控与仿真分析。 2．支持根据实时采集的网络状态和性能数据，按照链路带宽、质量、亲和属性等策略进行网络优化。 3．支持自动发现网络设备及链接关系，生成全网的网络拓扑、支持实时更新网络的拓扑变化；具备从业务到隧道再到链路，分层路径检视与可视化的能力。 4．支持提供业务性能和质量的统计报告及可视化呈现，包括并不仅限于丢包、时延、抖动。 5．配置与控制器匹配的处理设备和存储设备的支撑系统。	套	1
14		网络安全管理服务	统一身份认证设备	1．电源冗余设计且满配，≥4 个千兆电口，≥2 个千兆光口，且满配光模块。 2．支持并发用户数≥100000。 3．支持统一认证/统一门户/单点登录/多因子认证等功能；支持用户添加自定义属性管理；支持应用权限管理；支持行为日志审计。 4．支持密码自助找回、支持账号自助注册；支持用户信息自助修改。 5．与本项目投标所用到的安全态势感知、上网行为管理、下一代防火墙、SSL VPN 等需要用到身份信息的设备和系统实现数据对接和联动。	台	26
15			SSL VPN	1．电源冗余设计且满配，≥6 个千兆电口，≥4 个千兆光口，且满配光模块。 2．内存≥8G，硬盘 SSD ≥64G。 3．加密流量（Mbps）≥400，并发用户数≥6000，IPSec 加密流量（Mbps）≥200，设备整机吞吐量≥1.5Gbps，设备整机并发会话数≥160 万。 4．支持主从账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账号登陆。 5．提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力。	台	2

序号	子系统名称	分类	产品名称	配置参数	单位	数量
16			集权安全区防火墙	1．≥6 千兆电口，≥2 万兆光口，且满配光模块。 2.网络层吞吐量≥25G，应用层吞吐量≥3G，并发连接数≥2200000，新建连接数（CPS）≥200000。 3．支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 4．产品内置 IPS 检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 7000 种特征规则。 5．可以与安全态势感知系统和原有终端安全系统联动，实现对高危 IP、端口的封堵。	台	2
17			安全态势感知系统	1．电源冗余设计且满配，≥4 个千兆电口，≥2 个万兆光口，且满配光模块。 2．≥128G 内存，SSD 系统盘≥128G，SATA 存储≥40T，支持 RAID5/0。 3．具备对威胁的实时监测、预警与处置能力，提供 API 及其他数据接口，可接收各个教育城域网的资产信息、安全事件、脆弱性风险等信息，实现教育网网络中心和广西教育数据中心信息的融合展示以及一体化安全运维和管理。 4．支持与广西教育数据中心现有广西教育网络安全管理信息系统对接，上传安全日志和工单通报，工单通报内容包括事件描述、事件危害、所属单位、事件等级、处理时间、通报时间等信息。	台	1
18		虚拟化数据处理和存储服务	服务器	配置≥2 颗 20 核 CPU 模块，≥192GB 内存模块，≥2 块 600G SAS HDD 硬盘，≥12 块 8T SATA HDD 硬盘，≥3 块 960GB SSD HDD 硬盘，≥2 端口千兆电口网卡，≥2 端口万兆光口网卡含光模块，≥1 块 2G 缓存 RAID 卡含掉电保护模块，冗余电源。	套	39
19			超融合管理软件	配置 2 颗 CPU 管理授权；提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作；兼容主流虚拟化平台。		
20			计算虚拟化软件	配置 2 颗物理 CPU 授权许可；提供统一的虚拟机管理界面，在同一界面上提供虚拟机启动、暂停、恢复、休眠、重启、关闭、关闭电源、克隆、迁移、备份、模板导出、快照等功能；配置成虚拟化安全防护功能模块。		
21			存储虚拟化软件	配置 2 颗物理 CPU 授权许可；采用分布式的软件定义存储架构，在通用 x86 服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点。		

序号	子系统名称	分类	产品名称	配置参数	单位	数量
22			网络交换机	≥14 个万兆光口，≥8 个千兆电口，满配光模块，配套系统集成所需的线材。	台	26
23			一体化管理软件	配置 1 套管理软件；提供教育网网络中心统一管理≥45 套虚拟化一体机系统的许可；集成了云管理能力，对外提供一套集云资源、云服务、云运营、云运维为一体的管理平台。	套	1
24		配件	/	42U 标准机柜；系统集成所需的配件、配线等，所配的配件器材必须与组网连接线路和网络管理运维要求匹配。	批	1
25	教育城域网	线路	线路租用	≥1G 点对点专线，租用期：3 年。	条	19608
26		网络数据交换和管理服务	汇聚路由器	1．配置双主控且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 2．整机业务载板插槽≥6 个；配置万兆光口≥2 个，千兆光口≥10 个，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 3．支持广域网智能调优。 4．支持 SRv6，支持 SRv6 承载 VPN 业务。	台	264
27			汇聚交换机	1．电源冗余设计且满配。 2．支持千兆光口≥48 个，万兆光口≥6 个，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 3．支持 IPv4、Ipv6 协议。	台	264
28		网络安全服务	教育城域网出口防火墙	1．电源冗余设计且满配，≥4 个万兆光口插槽，≥2 个接口扩展插槽，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 2．网络层吞吐量≥20Gbps，应用层吞吐量≥8G，最大并发会话数≥200 万，每秒新建会话数≥12 万。在项目实施建设时，应根据本区域的学校及业务应用访问需求，充分论证，提前预判，匹配网络层和应用层吞吐量的主要技术参数指标要求。 3．可以与广西教育网安全态势感知系统和广西教育数据中心原终端安全管理信息系统联动，实现对高危 IP、端口的封堵。	台	264

序号	子系统名称	分类	产品名称	配置参数	单位	数量
29			互联网出口防火墙	1．电源冗余设计且满配，≥4 个万兆光口插槽，≥2 个接口扩展插槽，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 2．网络层吞吐量≥20Gbps，应用层吞吐量≥8G，最大并发会话数≥200 万，每秒新建会话数≥12 万。在项目实施建设时，应根据本区域的学校及业务应用访问需求，充分论证，提前预判，匹配网络层和应用层吞吐量的主要技术参数指标要求。 3．可以与广西教育网安全态势感知系统和广西教育数据中心原终端安全管理信息系统联动，实现对高危 IP、端口的封堵。	台	264
30			上网行为管理设备	1．电源冗余设计且满配，≥12 个千兆电口，≥12 个千兆 Combo 接口（光电复用），≥4 个万兆光口，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 2．含上网行为管理、流量管理、IPSec VPN 等功能。 3.支持与统一身份认证平台做身份认证信息对接，实现用户访问互联网的实名认证。	台	264
31			安全日志审计设备	4 个电口，存储容量 8TB，可接入 50 个日志源，可授权扩展，日志处理性能 2000EPS。	台	132
32			漏洞扫描设备	4 个电口，硬盘 1T，并发扫描数≥60 个 IP 地址，最大扫描速度 800 ip/h，支持授权 IP 数无限制。	台	132
33			运维管理设备	4 个电口，字符并发会话数≥180，图形并发会话数≥600，4T 存储空间，授权可管理设备数≥50 台。	台	132
34			安全态势感知系统	1．具备对威胁的实时监测、预警与处置能力； 2．提供 API 及其他数据接口，支持与广西教育网网络中心安全态势感知系统对接，可上传教育城域网的资产信息、安全事件、脆弱性风险等信息；支持与广西教育数据中心现有广西教育网络安全管理信息系统对接，上传安全日志和工单通报，工单通报内容包括事件描述、事件危害、所属单位、事件等级、处理时间、通报时间等信息。	台	132
35			安全流量探针	通过旁路部署方式对全流量信息进行采集。	台	132

序号	子系统名称	分类	产品名称	配置参数	单位	数量
36		密码应用安全服务	SSL VPN	基于国密 SSL 安全协议的 VPN 设备，集成了身份认证、访问控制和资源管理等功能；提供用户接入控制和数据传输的加/解密功能.标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存,4 个千兆电口、2 个千兆光口	台	132
37			动态密码系统	系统具备动态密码种子生成、验证服务和服务管理三个子系统，产品提供多种终端形态支持，主要包括：时间型令牌，事件形令牌，多键令牌，手机软件、手机短信、二维矩阵等多种方式。标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存。最大支持 5000 用户，响应性能 500TPS	套	132
38	校园网	网络数据交换服务	接入交换机	与组网连接线路匹配。（学校可以根据组网方式和需求考虑是否选配该服务）	台	24480
39		网络安全服务	安全边界设备	与组网连接线路匹配。（学校可以根据组网方式和需求考虑是否选配该服务）	台	24480
说明：以上软硬件配置及数量仅供参考，各地可根据实际情况适当调整。						

第 4 章　投资概算和资金来源

4.1 投资概算依据的有关说明

4.1.1 投资范围

本估算内容包含工程费、工程建设其他费、预备费等，具体内容详见估算表。

4.1.2 投资依据

1. 关于颁布《广西壮族自治区工程建设其他费用定额》的通知（桂建管〔2017〕87 号）

2. 国家信息产业部《电子建设工程概（预）算编制办法及计价依据》（信部规〔2015〕77 号）

3. 广西壮族自治区安装工程费用定额（2016 年）版

4. 广西壮族自治区物价局转发国家发展改革委关于降低部分建设项目收费标准规范收费行为等有关问题的的通知（桂价费〔2011〕55 号）

5. 工程建设其他费用参照“桂建标〔2018〕37 号”并结合本项目的实际情况进行计算。

6. 软、硬件购置费参考类似产品市场价格和厂商询价结果。

7. 教育骨干网建设资金来源为区本级教育厅自有资金，不计建设期贷款利息。

8. 参考兄弟省市教育网每生每年 20 元的标准完成了全省教育网建设

的成功案例，广西教育网建设需求与其有较大的相似性，考虑到广西教育网需要增加网络安全等级保护要求，因此，拟在20元的基础上上浮10%，即按每生每年不高于22元标准，预算广西教育城域网建设费用。按分级管理分级负责原则，教育城域网建设、管理和运维费用由各市、县（市、区）教育行政部门统筹教育经费，以及各市县财政共同承担，校园网建设纳入教育城域网建设内容。

9. 建设单位管理费参照《广西壮族自治区工程建设其他费用定额》(桂建标〔2018〕37号），由各市县财政统筹，不包含在本项目投资内。

10.可行性研究报告编制费、可行性研究报告评估费、初步设计评估费参照《广西壮族自治区工程建设其他费用定额》（桂建标〔2018〕37号）并结合市场实际进行估算，由自治区教育厅承担。

11.标准规范编制服务参照同类项目案例，结合市场实际进行估算，由自治区教育厅承担。

12.工程勘察费、工程设计费、招标服务费参照《广西壮族自治区工程建设其他费用定额》（桂建标〔2018〕37号），包含在网络服务租用费内，由项目中标供应服务商承担。

13.工程监理费参照《广西壮族自治区工程建设其他费用定额》（桂建标〔2018〕37号），考虑到教育城域网数量较多且租用时限较长，建议按照标准费用的2倍计取，包含在网络服务租用费内，由项目中标供应服务商承担，工程监理公司由各级教育网主管部门选择。

14.根据“一地一案”原则，教育城域网履约验收由各教育城域网主管部

门委托第三方验收单位完成，包含在网络服务租用费内，由项目中标供应服务商承担。

15.教育骨干网履约验收和教育网竣工验收由教育厅委托第三方验收单位完成，包含在网络服务租用费内，由自治区教育厅承担。

16.培训费参照桂财行〔2014〕26号文相关规定进行计取，包含在网络服务租用费内，由项目中标供应服务商承担。

17.信息安全等级保护测评费参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82号），并结合市场实际进行估算。骨干网的信息安全等级保护测评费由自治区教育厅承担,各城域网的信息安全等级保护测评费由项目中标供应服务商承担。

18.商用密码应用安全性评估费参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82号）的信息安全等级保护测评费用标准，并结合市场实际进行估算。骨干网的商用密码应用安全性评估费由自治区教育厅承担，各城域网的商用密码应用安全性评估费由项目中标供应服务商承担。

19.信息安全风险评估费按照教育骨干网每次评估工作量为4人月,教育城域网每次评估工作量为1人月，安全顾问每人月2万元进行估算。骨干网的信息安全风险评估费由自治区教育厅承担，各城域网的信息安全风险评估费由项目中标供应服务商承担。

20.安全生产费计费基础是建筑安装工程费,建筑安装工程费取工程费的50%，包含在网络服务租用费内，由项目中标供应服务商承担。

21. 工程竣工财务决算编制服务参照送审工程造价计费，参照《广西建设工程造价咨询服务行业收费参考标准》（桂价协字〔2019〕15 号），实行差额累进计费方式。包含在网络服务租用费内，由项目中标供应服务商承担。

22. 工程审计服务参照《广西壮族自治区物价局关于会计师事务所服务收费有关问题的通知》（桂价费〔2012〕74 号）的取费标准，含在网络服务租用费内，由项目中标供应服务商承担。

23. 教育网骨干网运维费参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82 号），并结合市场实际进行估算，由自治区教育厅承担。

24. 不计预备费。

4.2 项目总投资概算

本项目的总投资概算为 5.9458 亿元。

表 9-1 项目投资估算总表

序号	工程或费用名称	估算造价（万元）			投资占比	备注
		网络服务租用费	其他费用	合计		
一	**工程费**	**54704.05**		**54704.05**	**92.004%**	详见网络服务租用费表
1	教育骨干网	1762.45		1762.45	2.964%	由自治区教育厅承担
2	教育城域网（含校园网）	52941.60		52941.60	89.040%	各市县（市、区）教育行政部门统筹教育经费，以及各市县财政共同承担
二	**工程建设其他费**		**4754.00**	**4754.00**	**7.996%**	
1	建设单位管理费		0.00	0.00	0.000%	由自治区教育厅、各市县承担
2	可行性研究报告编制费		28.00	28.00	0.047%	由自治区教育厅承担
3	可行性研究报告评估费		2.00	2.00	0.003%	由自治区教育厅承担
4	初步设计评估费		2.00	2.00	0.003%	由自治区教育厅承担
5	标准规范编制服务		43.00	43.00	0.072%	由自治区教育厅承担
6	工程勘察费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
7	工程设计费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
8	工程监理费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
9	招标服务费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
10	信息安全等保测评费		1821.00	1821.00	3.063%	由自治区教育厅、各市县承担
11	商用密码应用安全性评估费		1821.00	1821.00	3.063%	由自治区教育厅、各市县承担
12	信息安全风险评估费		272.00	272.00	0.457%	由自治区教育厅、各市县承担
13	竣工验收费		405.00	405.00	0.681%	由自治区教育厅承担
14	骨干网运维费用		360.00	360.00	0.605%	由自治区教育厅承担
15	履约验收费		0.00	0.00	0.000%	含履约验收和竣工验收，包含在网络服务租用费内，由中标单位支付
16	培训费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付

序号	工程或费用名称	估算造价（万元）			投资占比	备注
17	安全生产费		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
18	工程竣工财务决算编制服务		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
19	工程审计服务		0.00	0.00	0.000%	包含在网络服务租用费内，由中标单位支付
三	**项目预备费**		**0.00**	**0.00**	**0.000%**	不计预备费
四	**项目总投资**			**59458.05**	**100.000%**	一+二+三

表 9-2 网络服务租用费内的工程其他费用估算表

序号	费用名称	计算公式	金额（万元）	投资占比	估算依据
1	工程勘察费	工程费*1.5%	820.56	1.380%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)，包含在网络服务租用费内，由中标单位支付
2	工程设计费	1764.09+(2154.06-1764.09)/(100000-80000)*(工程费-80000)	1270.86	2.137%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)，包含在网络服务租用费内，由中标单位支付
3	工程监理费	(1004.64+(1205.6-1004.64)/(100000-80000)*(工程费-80000))*2	1500.93	2.524%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)，考虑到教育城域网数量较多且租用时限较长，因此按照标准费用的 2 倍计取，包含在网络服务租用费内，由中标单位支付
4	招标服务费	按照 1 个教育骨干网和 132 个教育城域网分标。（100*0.63%+(500-100)*0.441%+(1000-500)*0.3465%+(教育骨干网工程费-1000)*0.2205%）+（100*0.63%+(500-100)*0.441%+(教育城域网工程费/132-500)*0.3465%）*132	276.57	0.465%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)，包含在网络服务租用费内，由中标单位支付
5	履约验收费	按照 1 个教育骨干网和 132 个教育城域网分标，总计 135 个节点。履约验收费每节点 3.5 万元	472.50	0.795%	根据“一地一案”原则，履约验收由教育厅制定验收标准并统一委托第三方验收单位完成，包含在网络服务租用费内，由中标单位支付

序号	费用名称	计算公式	金额（万元）	投资占比	估算依据
6	培训费	1、集中培训：400 元/人天 2、讲课费用：高级职称 1000 元/天 3、集中培训 500 人天，高级职称讲授 10 天	21.00	0.035%	参照桂财行〔2014〕26 号文相关规定进行计取，包含在网络服务租用费内，由中标单位支付
7	安全生产费	建筑安装工程费*1.5%	410.28	0.690%	安全生产费计费基础是建筑安装工程费，建筑安装工程费取工程费的 50%，包含在网络服务租用费内，由中标单位支付
8	工程竣工财务决算编制服务	1000*0.54%+（5000-1000）*0.42%+（20000-5000）*0.35%+（50000-20000）*0.29%+（工程费-50000）*0.25%	173.46	0.292%	参照送审工程造价计费，根据《广西建设工程造价咨询服务行业收费参考标准》（桂价协字〔2019〕15 号），实行差额累进计费方式。包含在网络服务租用费内，由中标单位支付
9	工程审计服务	按工程费的 1.5‰	82.06	0.138%	参照《广西壮族自治区物价局关于会计师事务所服务收费有关问题的通知》（桂价费〔2012〕74 号）的取费标准，含在网络服务租用费内，由中标单位支付
合计			5028.22	8.457%	

表 9-3 教育厅及各市县承担的工程其他费用估算表

序号	费用名称	计算公式	金额（万元）	投资占比	估算依据
1	建设单位管理费	540+(工程费-50000)*0.8%	577.63	0.000%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)，由自治区教育厅、各市县承担，不包含在本项目投资内
2	可行性研究报告编制费	/	28.00	0.047%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)并结合市场实际进行估算，由自治区教育厅承担
3	可行性研究报告评估费	/	2.00	0.003%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)并结合市场实际进行估算，由自治区教育厅承担
4	初步设计评估费	/	2.00	0.003%	参照《广西壮族自治区工程建设其他费用定额》(桂建标[2018]37 号)并结合市场实际进行估算，由自治区教育厅承担
5	标准规范编制服务	/	43.00	0.072%	参照同类项目案例，结合市场实际进行估算，由自治区教育厅承担
6	信息安全等保测评费	教育骨干网按照等保三级，8.6 万元/个，1 年评定 1 次；教育城域网按照等保二级，6.8 万元/个，2 年评定 1 次	1821.00	3.063%	参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82 号），并结合市场实际进行估算，教育网骨干网的费用由自治区教育厅承担，各教育网城域网的费用由各市县财政统筹支付
7	商用密码应用安全性评估费	教育骨干网按照等保三级，8.6 万元/个，1 年评定 1 次；教育城域网按照等保二级，6.8 万	1821.00	3.063%	参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》

序号	费用名称	计算公式	金额（万元）	投资占比	估算依据
		元/个，2 年评定 1 次			（桂财办〔2020〕82 号）的信息安全等保测评费标准，并结合市场实际进行估算，教育网骨干网的费用由自治区教育厅承担，各教育网城域网的费用由各市县财政统筹支付
8	信息安全风险评估费	根据风险评估国标及网络安全主管单位具体要求，完成对所有业务系统、承载网络、横向接入机构链路、纵向接入机构链路的全面风险评估，包括业务战略分析、资产赋值、威胁评估、脆弱性评估和风险分析，骨干网每次评估工作量为 4 人月，教育城域网每次评估工作量为 1 人月，按安全顾问每人月 2 万元计算	272.00	0.457%	参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82 号），并结合市场实际进行估算，教育网骨干网的费用由自治区教育厅承担，各教育网城域网的费用由各市县财政统筹支付
9	竣工验收费	按照 1 个教育骨干网和 132 个教育城域网分标，总计 135 个节点。竣工验收费每节点 3 万元	405.00	0.681%	根据“一地一案”原则，竣工验收由教育骨干网和教育城域网建设单位根据教育厅制定的统一验收标准完成，包含在网络服务租用费内，由自治区教育厅承担
10	骨干网运维费	3 个核心节点对应 12 个高校汇聚节点接入，西大和师大两个节点各分配 3 名运维人员，教育数据中心节点相对承载更多业务，分配 4 名运维人员（3 名网络运维+1 名安全运维人员），项目实施地按广西壮族自治区标准较高的南宁市计算，参考 2019 中国软件行业基准数据库（CSBMK-201906），根据软件运 维成本度量以及广西壮族自治区范围内软件行业发展水平，根据不同的运维难度及内容，运维预算支出标准在 8.39 万元/人年至 12.59 万元/	360.00	0.605%	参照《广西壮族自治区财政厅关于印发广西信息化建设项目预算支出标准（试行）》（桂财办〔2020〕82 号），并结合市场实际进行估算，由自治区教育厅承担。

序号	费用名称	计算公式	金额（万元）	投资占比	估算依据
		人年之间。一般项目按照 1 人/系统的标准配备运维 人员，大型项目按照实际运维内容进行工作量计算。按 12 万元/人年计算，运维费用=10*12 万元/人年*3 年=360 万元。			
合计			4971.63	7.390%	

表 9-4 网络服务租用费表

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
1	教育骨干网	线路	线路租用	≥10G 点对点专线，租用期：3 年。	条	6	136.39	818.34	
2			线路租用	≥1G 点对点专线，租用期：3 年。	条	18	31.56	568.08	
3		密码应用建设	国密安全门禁系统	双开 4 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门禁控制器（双门）4 台、国密门禁人脸读卡器 4 台、国密 CPU 卡 50 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张	套	1	9.63	9.63	广西数据中心机房，解决物理和环境安全层面的高风险项
4			国密视频加密系统	1、含国密网络摄像机 20 台、网络硬盘录像机 2 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	套	1	16.4	16.4	广西数据中心机房，解决物理和环境安全层面的高风险项
5			服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	台	2	0	0	对门禁、视频监控、运维设备数据、日记等进行完整性保护，用于教育数据中心节点，利旧教育数据中心现有密码机

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
6			密钥管理系统	1、包括业务实现层、数据持久层和操作系统层。 底层依托符合 GM/T0028 的三级及以上密码模块（密码机设备），实现密钥安全管理，支持对称密钥和非对称密钥的标准化全生命周期管理，以及实现密码计算服务：包括为业务应用提供密钥级加解密、签名验签、摘要、MAC 等密码计算服务。 2、系统内部的服务框架层基于用户角色来实现权限管理机制和访问控制策略。系统内将权限管理点细分，并基于角色将相应的权限点与管理员公钥证书绑定，可以方便的实现安全访问控制策略。 3、系统基于 B/S 模式开发，在 Web 访问层中，使用符合国际/国密标准的SSL 安全通信层协议，支持 X.509 证书标准，提供双向认证，保证交互数据的安全性和完整性。	套	1	0	0	用于广西教育骨干网对称密钥、非对称密钥的安全产生和安全存储，以及各类密钥的产生、更新、注销、失信、销毁、恢复和查询等全生命周期管理功能和密钥管理服务，复用改造后的教育 RA 系统实现。
7			国密安全门禁系统	双开 2 门；含门禁管理系统软件 1 套、密钥管理系统软件 1 套、门禁日志审计系统 1 套、门禁控制器（双门）1 台、国密门禁人脸读卡器 1 台、国密 CPU 卡 10 张、门禁发卡器 1 台、门禁密钥注入器 1 台、PCI-E 密码卡 1 张	套	14	7.35	102.90	广西教育骨干网西大、师大节点和 12 个汇聚节点各一套
8			国密视频加密系统	1、含国密网络摄像机 4 台、网络硬盘录像机 1 台； 2、视频播放客户端软件 1 套，含密码卡 1 张，完成视频数据显示端完整性保护	套	14	7.85	109.9	广西教育骨干网西大、师大节点和 12 个汇聚节点各一套

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
9			服务器密码机	放 RA 密钥，支持国密算法。支持 SM2、SM3、SM4 算法，具有密钥管理、密码运算、身份认证管理等功能。SM4 加/解密速率≧300Mbps；SM2 密钥对生成速率为 6000 对/秒，加/解密速率为 4.73Mbps/4.60Mbp	台	14	9.8	137.2	对门禁、视频监控、运维设备数据、日记等进行完整性保护，广西教育骨干网西大、师大节点和 12 个汇聚节点各一套
10		网络数据交换和管理服务	核心路由器	基于国密 SSL 安全协议的 VPN 设备，集成了身份认证、访问控制和资源管理等功能；提供用户接入控制和数据传输的加/解密功能.标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存,4 个千兆电口、2 个千兆光口	台	6	0	0	由中标供应商提供。3 个核心节点，每节点配置 2 台
11			汇聚路由器	1．双主控设计且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 2．独立交换网板总数≥2 并满配；整机支持业务载板插槽≥6 个（全尺寸业务卡槽位，非子卡槽位）。 3．配置万兆光口≥4 个，千兆光口≥10 个；配置万兆单模光模块≥4 个，千兆单模光模块≥10 个；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 4.支持网络资源、隧道路径、业务路径、及业务 SLA 的可视可管；支持广域网智能调优。 5．支持 SRv6，支持 SRv6 承载 VPN 业务。	台	26	0	0	由中标供应商提供。13 个汇聚节点，每节点配置 2 台

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
12			网络管理系统	1.系统应支持大规模设备管理能力，可最多管理 20000 台网元；系统应支持多种设备的管理，包括并不仅限于交换机、路由器、防火墙、WLAN、服务器、存储、IP 话机、摄像头等；实配 50 个设备授权。 2．配置配套操作系统与数据库，以及配套的部署硬件设备。 3．提供告警、性能、有线无线资源、用户终端定位信息等报表管理能力。 4．网络质量监控：系统支持基于真实流的 IP 网络实时监测能力（非模拟报文监测或者探针式监测），监测结果可实时在拓扑上显示； 5．提供设备原厂不少于 50 台路由器、交换机等网络设备 5 年实时远程监控运维服务。	套	1	0	0	由中标供应商提供。
13			教育骨干网控制器	1．包含管理、控制和分析集成的统一云化架构，管理授权覆盖教育骨干网不少于 50 台路由器、交换机等网络设备。支持统一的 Portal 来访问所有的组件，包括设备管理，业务发放，网络优化，网络监控与仿真分析。 2．支持根据实时采集的网络状态和性能数据，按照链路带宽、质量、亲和属性等策略进行网络优化。 3．支持自动发现网络设备及链接关系，生成全网的网络拓扑、支持实时更新网络的拓扑变化；具备从业务到隧道再到链路，分层路径检视与可视化的能力。 4．支持提供业务性能和质量的统计报告及可视化呈现，包括并不仅限于丢包、时延、抖动。	套	1	0	0	由中标供应商提供。

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
				5．配置与控制器匹配的处理设备和存储设备的支撑系统。					
14		网络安全管理服务	统一身份认证设备	1．电源冗余设计且满配，≥4 个千兆电口，≥2 个千兆光口，且满配光模块。 2．支持并发用户数≥100000。 3．支持统一认证/统一门户/单点登录/多因子认证等功能；支持用户添加自定义属性管理；支持应用权限管理；支持行为日志审计。 4．支持密码自助找回、支持账号自助注册；支持用户信息自助修改。 5．与本项目投标所用到的安全态势感知、上网行为管理、下一代防火墙、SSL VPN 等需要用到身份信息的设备和系统实现数据对接和联动。	台	26	0	0	由中标供应商提供。13 个汇聚节点，每节点配置 2 台
15			SSL VPN	1．电源冗余设计且满配，≥6 个千兆电口，≥4 个千兆光口，且满配光模块。 2．内存≥8G，硬盘 SSD ≥64G。 3．加密流量（Mbps）≥400，并发用户数≥6000，IPSec 加密流量（Mbps）≥200，设备整机吞吐量≥1.5Gbps，设备整机并发会话数≥160 万。 4．支持主从账号绑定，实现 SSL VPN 账号与应用系统账号的唯一绑定，VPN 资源中的系统只能以指定账	台	2	0	0	由中标供应商提供。

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
				号登陆。 5．提供环境检测、自动修复工具，支持对 Windows 的环境兼容性一键检测能力，以及对检测结果进行一键修复的能力。					
16			集权安全区防火墙	1．≥6 千兆电口，≥2 万兆光口，且满配光模块。 2．网络层吞吐量≥25G，应用层吞吐量≥3G，并发连接数≥2200000，新建连接数（CPS）≥200000。 3．支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。 4．产品内置 IPS 检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过 7000 种特征规则。 5．可以与安全态势感知系统和原有终端安全系统联动，实现对高危 IP、端口的封堵。	台	2	0	0	由中标供应商提供。
17			安全态势感知系统	1．电源冗余设计且满配，≥4 个千兆电口，≥2 个万兆光口，且满配光模块。 2．≥128G 内存，SSD 系统盘≥128G，SATA 存储≥40T，支持 RAID5/0。 3．具备对威胁的实时监测、预警与处置能力，提供 API 及其他数据接口，可接收各个教育城域网的资产信息、安全事件、脆弱性风险等信息，实现教育网网络中心和广西教育数据中心信息的融合展示以及一体化	台	1	0	0	由中标供应商提供。

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
				安全运维和管理。 4．支持与广西教育数据中心现有广西教育网络安全管理信息系统对接，上传安全日志和工单通报，工单通报内容包括事件描述、事件危害、所属单位、事件等级、处理时间、通报时间等信息。					
18		虚拟化数据处理和存储服务	服务器	配置≥2 颗 20 核 CPU 模块，≥192GB 内存模块，≥2 块 600G SAS HDD 硬盘，≥12 块 8T SATA HDD 硬盘，≥3 块 960GB SSD HDD 硬盘，≥2 端口千兆电口网卡，≥2 端口万兆光口网卡含光模块，≥1 块 2G 缓存 RAID 卡含掉电保护模块，冗余电源。	套	39	0	0	由中标供应商提供。13 个汇聚节点，每节点配置 3 套
19			超融合管理软件	配置 2 颗 CPU 管理授权；提供用户自助服务界面，用户能够通过自助服务门户完成云资源申请、使用、修改、销毁等操作；兼容主流虚拟化平台。					
20			计算虚拟化软件	配置 2 颗物理 CPU 授权许可；提供统一的虚拟机管理界面，在同一界面上提供虚拟机启动、暂停、恢复、休眠、重启、关闭、关闭电源、克隆、迁移、备份、模板导出、快照等功能；配置成虚拟化安全防护功能模块。					
21			存储虚拟化软件	配置 2 颗物理 CPU 授权许可；采用分布式的软件定义存储架构，在通用 x86 服务器部署，把所有服务器硬盘组织成一个虚拟存储资源池，提供分布式存储服务，无需独立的元数据及控制器节点。					
22			网络交换机	≥14 个万兆光口，≥8 个千兆电口，满配光模块，配套系统集成所需的线材。	台	26	0	0	由中标供应商提供。

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
23			一体化管理软件	配置 1 套管理软件；提供教育网网络中心统一管理≥45 套虚拟化一体机系统的许可；集成了云管理能力，对外提供一套集云资源、云服务、云运营、云运维为一体的管理平台。	套	1	0	0	由中标供应商提供。
24		配件	/	42U 标准机柜；系统集成所需的配件、配线等，所配的配件器材必须与组网连接线路和网络管理运维要求匹配。	批	1	0	0	由中标供应商提供。
25	小计 1							1762.45	
26	教育城域网	线路	线路租用	≥1G 点对点专线，租用期：3 年。	条	19608	2.7	52941.6	农村学校 14736 所，乡镇及城区学校 4872 所。
27		网络数据交换和管理服务	汇聚路由器	1．配置双主控且满配，电源冗余设计且满配，要求所有业务板卡及电源、风扇均可热插拔。 2．整机业务载板插槽≥6 个；配置万兆光口≥2 个，千兆光口≥10 个，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 3．支持广域网智能调优。 4．支持 SRv6，支持 SRv6 承载 VPN 业务。	台	264	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 2 台
28			汇聚交换机	1．电源冗余设计且满配。 2．支持千兆光口≥48 个，万兆光口≥6 个，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 3．支持 IPv4、Ipv6 协议。	台	264	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 2 台

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
29		网络安全服务	教育城域网出口防火墙	1．电源冗余设计且满配，≥4 个万兆光口插槽，≥2 个接口扩展插槽，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 2．网络层吞吐量≥20Gbps，应用层吞吐量≥8G，最大并发会话数≥200 万，每秒新建会话数≥12 万。在项目实施建设时，应根据本区域的学校及业务应用访问需求，充分论证，提前预判，匹配网络层和应用层吞吐量的主要技术参数指标要求。 3．可以与广西教育网安全态势感知系统和广西教育数据中心原终端安全管理信息系统联动，实现对高危 IP、端口的封堵。	台	264	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 2 台
30			互联网出口防火墙	1．电源冗余设计且满配，≥4 个万兆光口插槽，≥2 个接口扩展插槽，并满配相应光模块；所配光口和光模块必须与组网连接线路和网络管理运维要求匹配。 2．网络层吞吐量≥20Gbps，应用层吞吐量≥8G，最大并发会话数≥200 万，每秒新建会话数≥12 万。在项目实施建设时，应根据本区域的学校及业务应用访问需求，充分论证，提前预判，匹配网络层和应用层吞吐量的主要技术参数指标要求。 3．可以与广西教育网安全态势感知系统和广西教育数据中心原终端安全管理信息系统联动，实现对高危 IP、端口的封堵。	台	264	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 2 台
31			上网行为管理设备	1．电源冗余设计且满配，≥12 个千兆电口，≥12 个千兆 Combo 接口（光电复用），≥4 个万兆光口，并满配相应光模块；所配光口和光模块必须与组网连接线路	台	264	0	0	由中标供应商提供。132 个教育城域网，每个教育城

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
				和网络管理运维要求匹配。 2．含上网行为管理、流量管理、IPSec VPN 等功能。 3.支持与统一身份认证平台做身份认证信息对接，实现用户访问互联网的实名认证。					域网配置 2 台
32			安全日志审计设备	4 个电口，存储容量 8TB，可接入 50 个日志源，可授权扩展，日志处理性能 2000EPS。	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
33			漏洞扫描设备	4 个电口，硬盘 1T，并发扫描数≥60 个 IP 地址，最大扫描速度 800 ip/h，支持授权 IP 数无限制。	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
34			运维管理设备	4 个电口，字符并发会话数≥180，图形并发会话数≥600，4T 存储空间，授权可管理设备数≥50 台。	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
35			安全态势感知系统	1．具备对威胁的实时监测、预警与处置能力； 2．提供 API 及其他数据接口，支持与广西教育网网络中心安全态势感知系统对接，可上传教育城域网的资产信息、安全事件、脆弱性风险等信息；支持与广西教育数据中心现有广西教育网络安全管理信息系统对接，上传安全日志和工单通报，工单通报内容包括事件描述、事件危害、所属单位、事件等级、处理时间、通报时间等信息。	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
36			安全流量探针	通过旁路部署方式对全流量信息进行采集。	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
37		密码应用安全服务	SSL VPN	基于国密 SSL 安全协议的 VPN 设备，集成了身份认证、访问控制和资源管理等功能；提供用户接入控制和数据传输的加/解密功能.标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存,4 个千兆电口、2 个千兆光口	台	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
38			动态密码系统	系统具备动态密码种子生成、验证服务和服务管理三个子系统，产品提供多种终端形态支持，主要包括：时间型令牌，事件形令牌，多键令牌，手机软件、手机短信、二维矩阵等多种方式。标准 1U 设备，双电源 400W-600W，2 核 4 线程 CPU X1，1T 硬盘，8G 内存。最大支持 5000 用户，响应性能 500TPS	套	132	0	0	由中标供应商提供。132 个教育城域网，每个教育城域网配置 1 台
39	小计 2							52941.6	
40	校园网	网络数据交换服务	接入交换机	与组网连接线路匹配（学校可以根据组网方式和需求考虑是否选配该服务）。	台	24480	0	0	由中标供应商根据需要提供，此处取最大数。农村学校 14736 所，每所配置 1 台；乡镇及城区学校 4872 所，每所配置 2 台

序号	子系统名称	分类	产品名称	配置参数	单位	数量	单价（万元）	总价（万元）	备注
41		网络安全服务	安全边界设备	与组网连接线路匹配（学校可以根据组网方式和需求考虑是否选配该服务）。	台	24480	0	0	由中标供应商根据需要提供，此处取最大数。农村学校 14736 所，每所配置 1 台；乡镇及城区学校 4872 所，每所配置 2 台
42	小计 3							0	
43	总计							54704.05	

4.3 资金筹措与落实情况

本项目总投资估算约 5.9458 亿元，项目资金由自治区教育厅、各市县统筹教育经费，以及各市县财政共同承担，预计分 3 年完成拨付。自治区教育厅承担教育骨干网的建设、管理、运维等费用，承担骨干网的密码应用建设和测评、网络安全等级保护风评和测评等费用，以及教育网建设项目的可研和初步设计编制及评估、标准规范编制服务等费用。各市县统筹教育经费承担教育城域网建设、管理、运维等费用，各市县承担教育城域网网络安全等级保护风评和测评等费用。

本项目采用向通信运营商招标采购网络服务的方式进行建设。教育骨干网全部款项支付后由项目中标供应服务商向自治区教育厅移交教育骨干网的软硬件系统设备信息资产（不含传输线路）。