附件

海南省教育城域网接入规范及服务体系

海南省教育厅 发布

**目 录**

**[1](#_Toc204001550)****[总则](#_Toc204001550)** [1](#_Toc204001550)

**[2范围](#_Toc204001551)** [1](#_Toc204001551)

**[3规范性引用文件](#_Toc204001552)** [1](#_Toc204001552)

**[4术语和定义](#_Toc204001553)** [2](#_Toc204001553)

**[4.1](#_Toc204001554)****[海南省教育城域网](#_Toc204001554)** [2](#_Toc204001554)

**[4.2](#_Toc204001555)****[市县教育城域网](#_Toc204001555)** [3](#_Toc204001555)

**[5建设架构](#_Toc204001556)** [3](#_Toc204001556)

**[5.1](#_Toc204001557)****[网络层次结构](#_Toc204001557)** [3](#_Toc204001557)

**[5.2](#_Toc204001558)****[教育城域网结构](#_Toc204001558)** [4](#_Toc204001558)

**[6市县教育城域网接入标准](#_Toc204001559)** [7](#_Toc204001559)

**[6.1](#_Toc204001560)****[链路接入标准](#_Toc204001560)** [7](#_Toc204001560)

**[6.2](#_Toc204001561)****[IP地址和域名规划](#_Toc204001561)** [8](#_Toc204001561)

**[6.3](#_Toc204001562)****[路由规划与协议](#_Toc204001562)** [9](#_Toc204001562)

**[6.4](#_Toc204001563)****[服务质量（QoS）保障](#_Toc204001563)** [9](#_Toc204001563)

[6.4.1 服务质量（QOS）指标要求 9](#_Toc204001564)

[6.4.2 服务质量（QOS）流量分级控制 10](#_Toc204001565)

**[6.5](#_Toc204001566)****[市县认证、安全平台](#_Toc204001566)** [11](#_Toc204001566)

[6.5.1 市县认证接入要求 11](#_Toc204001567)

[6.5.2 市县认证接入策略授权 11](#_Toc204001568)

[6.5.3 IPv6认证设计 12](#_Toc204001569)

[6.5.4 IPv6 DNS设计 12](#_Toc204001570)

[6.5.5 安全策略 13](#_Toc204001571)

**[7市县安全、认证平台与省级平台对接标准](#_Toc204001572)** [15](#_Toc204001572)

[7.1 认证平台对接标准 15](#_Toc204001573)

[7.2 安全平台对接标准 16](#_Toc204001574)

[7.3 平台升级标准 16](#_Toc204001575)

**[8运维支撑人员组织架构](#_Toc204001576)** [17](#_Toc204001576)

[8.1运维管理小组 17](#_Toc204001577)

[8.2技术运维团队 17](#_Toc204001578)

[8.3服务运维团队 18](#_Toc204001579)

[8.4应急响应小组 19](#_Toc204001580)

1. **总则**

为深入贯彻落实《教育部等六部门关于推进教育信息基础设施建设构建高质量教育支撑体系的指导意见》《海南省国家中小学智慧教育平台全域应用试点方案》文件精神，推动高标准、高效率建成泛在互联、绿色安全的海南省教育城域网，支持国家中小学智慧教育平台全域全员全流程应用，全面整合优质教育资源，实现全方位多场景智能助力，着力建设海南全域智慧教育试验区，助力海南自由贸易港建设，特制定本建设指南。

1. **范围**

本规范对海南省教育城域网的建设提出相关规定，包括链路接入标准、IP地址规划、路由规划与协议、服务质量保障（QOS）、市县安全与省级平台对接标准、省认证平台对接市县NAS设备标准等方面的内容。

本规范适用于指导海南省级行政范围内，省级、市县级教育城域网的建设及使用。

1. **规范性引用文件**
2. 《海南省推进国家中小学智慧教育平台深化应用行动计划》（琼委教〔2024〕4号）；
3. 《海南省教育城域网建设指南》（2024年）；
4. 《IP网络技术要求-网络总体》（YD/T 1170-2015）；
5. 《宽带IP城域网工程设计规范》（YD/T 5117-2016）；
6. 《IP网络安全技术要求-安全框架》（YD/T 1163-2001）；
7. 《互联网业务服务质量技术要求》（YD/T 1641-2019）；
8. 《互联网业务服务质量测试方法》（YD/T 1642-2020）；
9. 《中华人民共和国计算机信息系统安全保护条例》（国务院第147号令） ；
10. 《安全防范工程技术规范》（GB 50348-2018）；
11. 《随机性检测规范》（GM/T 0005-2021）；
12. 《SSL VPN 技术规范》（GM/T 0024-2023）；
13. 《SSL VPN网关产品规范》（GM/T 0025-2023）；
14. 《商用密码管理条例》（2023年修订版）；
15. 《智能密码钥匙技术规范》（GM/T 0027-2021）；
16. 《密码模块安全技术要求》（GM/T 0028-2021）；
17. 《密码产品随机数检测要求》（GM/T 0062-2018）；
18. 《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》（GM/T 0034-2021）；
19. 《信息系统密码应用基本要求》（GM/T 0054-2018）；
20. 《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）；
21. 《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）；
22. 《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）；
23. 《信息安全技术网络安全等级保护测评要求》（GB/T28448-2019）；
24. 《信息技术安全技术信息技术安全性评估准则》（GB/T 18336-2015）；
25. 《信息安全技术数据库管理系统安全技术要求》（GB/T 20273-2020）；
26. 《数据中心设计规范》（GB 50174-2017）；
27. 《IPv6网络设备安全技术要求》（YD/T 2400-2022）；
28. 《信息安全技术 政务云安全要求》（GB/T 39477-2020）；
29. 《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）；
30. 《教育管理信息系统安全规范》（JY/T 1002-2023）。
31. **术语和定义**
	1. **海南省教育城域网**

海南省教育城域网是由海南省教育厅统一规划、部署和管理的教育行业专用网络，旨在连接全省各类学校和各级教育机构，为全体师生和教育工作者提供“高速、便捷、绿色、安全”的网络服务。海南省教育城域网是海南省教育信息化的核心基础设施，支持国家中小学智慧教育平台的全域应用试点工作，推动优质教育资源的互联互通和共建共享。海南省教育城域网由省级核心节点、市县教育城域网和校园网组成。省级核心节点向上连接中国教育和科研计算机网，向下连接市县教育城域网汇聚节点，同时高速连接省政务外网、省直属教育机构、省直属中学、高校和公众互联网。

* 1. **市县教育城域网**

市县教育城域网在教育城域网中起到承上启下的作用，向上连接城域网省级核心节点，横向连接公众互联网，向下连接市县教育机构和学校，确保学校信息终端快速安全访问教育城域网业务及资源。

1. **建设架构**
	1. **网络层次结构**

海南省教育城域网由海南省教育城域网核心节点、市县教育城域网汇聚节点和校园网节点三级架构组成。海南省教育城域网核心节点向上连接中国教育和科研计算机网，向下连接海南省教育城域网汇聚节点，同时高速连接海南省政务外网、海南省直属教育机构、海南省直属中学、海南省高校和公众互联网。

市县教育城域网汇聚节点在海南省教育城域网中起到承上启下的作用，向上连接海南省教育城域网核心节点，

横向连接公众互联网，向下连接市县教育机构和市县学校，确保市县学校信息终端快速安全访问教育城域网业务及资源。

校园网是指在学校范围内，以光纤、Wi-Fi等新一代信息技术为基础连接多媒体教室、计算机教室、实验室、功能教室、办公室等各功能区域信息终端的基础承载网络，用以支撑各类终端接入和信息服务。

图1  海南省教育城域网体系架构

* 1. **教育城域网结构**

**5.2.1总体要求**

教育城域网遵循层次化设计的原则，采用三层架构，具体内容如下：

**5.2.1.1 海南省教育城域网核心节点**

海南省教育城域网核心节点承担数据高效流转与交换的重任，确保教育信息在各级网络间的无缝衔接与快速响应。海南省教育城域网核心节点网络结构如图2所示，具体内容如下：

1. 核心层设备用于高速的数据转发，要求采用冗余核心设备组网，核心层线路带宽、速率、可靠性应满足教育城域网核心高速数据交换的需求；
2. 市县教育城域网经各运营商统一汇聚后上联至海南省教育城域网核心节点。



图2  海南省教育城域网核心节点网络结构图

**5.2.1.2 市县教育城域网汇聚节点**

市县教育城域网汇聚节点由市县教育城域网汇聚网络与辖区学校校园网及其他教育机构网络等连接构成。市县教育城域网汇聚节点向上连接海南省教育城域网核心节点，横向连接公众互联网，向下连接辖区学校校园网。市县教育城域网汇聚节点网络结构如图3所示，具体内容如下：

1. 市县教育城域网的汇聚节点由网关设备、出口防火墙、入侵检测设备、上网行为管理设备、态势感知平台、日志审计管理平台等组成；
2. 市县教育城域网汇聚节点汇聚设备用于市县教育城域网的接入，要求采用冗余汇聚设备组网，有效分担市县学校业务流量对汇聚设备的压力。
3. 如果单个市县教育城域网只有一家运营商提供服务，则由中标运营商建设汇聚节点所有设备，中标运营商将市县内所有教育城域网流量、安全溯源等数据汇聚后，将安全告警事件推送至省教育城域网省级平台，省级平台只对接中标运营商安全平台。
4. 如果单个市县教育城域网存在多家运营商共同提供服务，则每家运营商须各自建设提供服务范围的教育城域网汇聚节点内所有设备，承担自身网络、认证、安全及其他相关业务服务责任，并确定其中一家安全平台为本市县安全主平台，其他运营商安全平台接入主平台，向主平台推送安全告警日志、认证日志等市县教育局要求的信息，实现本市县教育城域网安全态势、服务质量等数据的汇聚和展示，并推送至省级平台。



图3 市县教育城域网汇聚节点网络结构图



图4 单市县存在多家运营商提供服务的市县教育城域网汇聚节点网络结构图

1. **市县教育城域网接入标准**
	1. **链路接入标准**

**6.1.1 各市县城域网与核心节点之间的链路带宽要求**

目前教育资源基本有教学资源、教育管理、交流沟通、教务教学、视频音频五大类应用。为满足各学校接入需求，各市县教育城域网上联海南省教育城域网核心节点的链路带宽应不低于10Gbps，可采用10G/40G/100G 以太网接口链路，实现与海南省教育城域网核心节点的无缝对接，横向采用多出口策略连接互联网，有效实现负载分担；校园网络采用光纤进班方式接入各类信息终端，确保每个终端接入的并行带宽不低于100Mbps。

**6.1.2 冗余与备份要求**

市县城域网必须具备冗余链路和备份策略。各市县城域网应至少采用双链路接入核心节点，主链路正常工作时，备份链路处于热备状态，实时监测主链路运行状况。一旦主链路发生故障，备份链路可在毫秒级内迅速切换，无缝承接数据传输任务，确保教育数据传输不出现任何中断。在路由层面实施动态备份，通过部署智能路由协议，如 OSPF 或 BGP 的优化策略，保障网络的高可用性，为教育教学活动的顺利开展保驾护航。

* 1. **IP地址和域名规划**

根据《教育部办公厅关于贯彻落实<推进互联网协议第六版 （IPv6）规模部署行动计划>的通知》（教技厅〔2018〕3 号）要 求，教育城域网建设过程，IP 地址采用 IPv4/IPv6 双栈覆盖方式，由省级统一负责地址分配。各级各类教育机构统一使用 edu.cn 域名，由省级统一负责域名申请及分配管理。IP地址分配方案。

1. IP地址规划原则

海南省教育厅各分配32个B类IPV4地址段给运营商，各运营商自行按需规划所中标市县的管理、业务等IP地址，各运营商网络汇聚后接入海南省教育城域网核心节点。

| **电信** | **移动** | **联通** |
| --- | --- | --- |
| **10.96.0.0/11** | **10.128.0.0/11** | **10.160 .0.0/11** |

海南省教育城域网IPv6使用各运营商IPv6地址。海南省教育城域网包含多个业务网络，各业务网络由相应管理部门统一规划分配自主的IPv6/IPv4地址，并明确各级的网络边界。各业务网络由海南省教育城域网核心节点制定统一的安全访问策略。

1.合理性：

根据各市县的实际用户数和设备数量，合理分配IP地址，避免地址浪费。

定期评估各市县的IP地址使用情况，及时调整。

2.可扩展性：

在地址规划时，预留一定的地址空间（如20%）以应对未来的扩展需求。

考虑到新学校、新设备的接入，确保有足够的地址资源。

3.易管理性：

采用清晰的地址分配策略，如按部门、学校或地理位置进行划分。

使用统一的命名规则和文档记录，以便于管理和维护。

4.安全性：

在地址规划中，确保网络的安全性，合理配置防火墙和访问控制列表（ACL）。

定期进行安全审计，确保网络不受攻击。

5.兼容性：

确保所采用的IP地址规划与现有的网络设备、系统兼容，避免因地址冲突导致的网络故障。

在进行网络设备升级或更换时，提前规划IP地址的迁移策略。

1. 域名规划原则

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，全省统一使用 hainan.edu.cn 作为一级域名，各使用单位 向省教育厅申请二级域名。

* 1. **路由规划与协议**

海南省教育城域网的路由规划与协议由各家运营商负责。

* 1. **服务质量（QoS）保障**

### 服务质量（QOS）指标要求

市县教育城域网服务质量要求运营商成立市县教育城域网运维小组，负责市县区域网络的日常运维及应急处置。市县教育城域网汇聚节点实时分析网络流量情况，每季度生成QoS监测报告，内容如下：

1.丢包率：

定义：在传输过程中丢失的数据包占总发送数据包的百分比（%）

评估内容：数据传输的可靠性或完整性。丢包通常由网络拥塞、线路错误、设备故障等原因引起。

标准参考：≤0.1%

2.错误率

定义：传输过程中发生比特错误的比率。

评估内容： 网络或服务持续稳定运行、无差错传输以及从故障中恢复的能力。

标准参考：≤0.1%

3.时延：

定义：数据包从源端发送到目的端所经历的事件（通常以毫秒ms为单位）。

评估内容：数据传输的速度或响应时间。

标准参考：≤40ms（往返时延） ≤20ms（单向）

4.可用性：

定义：网络或服务在指定时间段内可供正常使用的百分比。

评估内容： 网络或服务持续稳定运行、无差错传输以及从故障中恢复的能力。

标准参考：> 99.999%

5.线路带宽上下行流量曲线

出具历史时间6个月报告，按月、日、小时、分钟维度。

### 服务质量（QOS）流量分级控制

网络应用的优先级根据应用所使用的IP网段、源（目的）地址、TCP端口号、UDP端口号进行划分，优先级依次递增。

教育城域网数据流量分级具体如下表所示：

|  |  |  |
| --- | --- | --- |
| 应用类别 | 具体内容 | 优先级 |
| 一般数据流 | FTP等一般应用 | 1 |
| 普通业务数据流 | MAIL、HTTP等业务 | 2 |
| 重要应用数据流 | 智慧课堂业务 | 3 |
| 关键应用数据流 | 中小学智慧教育平台业务系统 | 4 |

* 1. **市县认证、安全平台**

### 市县认证接入要求

市县教育城域网NAS设备（按照运营商每个市县冗余2台）与省核心节点RADIUS对接，实现用户身份信息的同步。提升网络访问的安全性与合规性，确保网络安全与数据保护，为教育环境的健康发展保驾护航，终端接入实现网络接入的实名认证、授权；要求支持有线接入管控及无线接入管控；市县教育城域网NAS设备需支持多种PPPoE、Web+Portal接入认证方式。

省级核心节点统一认证平台支持各市县及教育主管机构申请使用用户话单信息等数据，数据使用方应根据数据安全保护法等相关要求，保证数据安全合理使用，避免数据泄露造成不良影响。市县及教育主管机构提出数据调用申请后与省级核心节点统一认证平台协商确认对接接口及数据字段等信息。

### 市县认证接入策略授权

用户接入教育城域网后，将进行实名制认证。根据接入用户的身份及所属用户组，系统将进行精细化的访问控制、上网行为管理及流量保障，实现教育网实名制用户的访问与管理。

对实名制用户进行业务访问控制，基于用户身份（如校领导、教师、学生）及所属用户组，实施细粒度的业务系统访问权限控制。设置安全策略，基于应用类型进行访问控制，严格防止非授权访问。

对实名制用户进行上网行为控制，根据不同用户类型（如学生、教师）实施差异化的上网行为管控策略，对学生等特定群体，实施URL分类过滤和访问控制，有效引导健康上网行为。

根据应用流量类型进行多层次的流量管理，优先保障关键教学应用（如在线课堂、教育云平台、视频会议）和办公业务所需的带宽，对非关键或大量占用带宽的应用流量（如P2P下载、大文件传输、在线视频娱乐）进行识别和带宽限制，确保网络资源合理分配。

通过在教育城域网中实施实名制访问控制与管理体系，使教育网管理人员能够根据校领导、教师、学生的不同身份，制定具有针对性的安全策略和上网行为策略。通过识别和区分关键应用与非关键应用，确保教学和办公核心业务的网络体验，优化整体带宽利用效率。

### IPv6认证设计

IPv6认证设计支持双栈和单栈两种认证方式。

双栈认证：双栈终端发起IPv6访问时，若未认证，其IPv6 HTTP请求将被重定向至预设的IPv4地址（默认1.1.1.1，可配置），终端通过IPv4完成WEB认证。认证通过后，同时放通IPv6与IPv4流量，确保用户上网体验。该方式在现有IPv4认证基础上增加IPv6转IPv4重定向流程，适用于双栈终端，仍对接IPv4 PORTAL服务器。

单栈认证：纯IPv6终端发起访问时，IPv6网关或AC设备检测到未认证终端IPv6 HTTP请求后，直接生成IPv6格式的重定向响应报文。终端通过IPv6与PORTAL服务器交互完成认证，认证信息由IPv6 RADIUS服务器鉴权。通过后，IPv6网关放行该终端的IPv6公网访问权限。

以上两种方式可根据实际需求选择部署。

### IPv6 DNS设计

遵循运营商提供的 IPv6 地址分配方案，结合教育城域网的层级结构，采用层次化的地址分配方式。

一、权威 DNS 服务器

对于教育城域网内的自有域名，依托权威机构DNS服务器能力进行解析，权威机构具备多节点DNS负载均衡和就近响应能力，可提升域名解析的可靠性、安全性和响应速度。​

二、递归 DNS 服务器

运营商的递归 DNS 服务器负责处理整个城域网内的递归查询请求。​

三、DNS 解析策略设计

本地优先解析：当教育城域网内的用户发起 DNS 查询请求时，运营商递归 DNS 服务器首先检查本地缓存，如果缓存中有对应的解析结果，则直接返回给用户，减少网络查询延迟。若本地缓存未命中，则向教育城域网内的运营商权威 DNS 服务器发起查询请求，优先获取城域网内部的域名解析结果。​

智能选路解析：对于需要访问外部网络资源的域名查询，递归 DNS 服务器根据运营商提供的网络拓扑信息和链路状态，选择最优的出口链路进行查询。例如，通过 BGP协议获取运营商网络的路由信息，根据链路的带宽、延迟、丢包率等指标，动态选择最佳的出口链路，将查询请求转发到运营商的递归 DNS 服务器或互联网上的根 DNS 服务器，实现智能选路，提高查询效率。​

负载分担解析：对于一些热门的域名或应用，递归 DNS 服务器通过轮询、加权轮询等负载分担算法，将解析请求分配到多个对应的权威 DNS 服务器副本上，避免单个服务器负载过高，保证解析服务的稳定性和可靠性。

### 安全策略

市县教育城域网的建设应符合《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）文件的要求，需达到网络安全等级保护二级标准。市县教育城域网出口部署出口防火墙、入侵检测设备、上网行为管理设备、态势感知平台、日志审计管理平台等安全防护设备及平台，作为互联网出口和市县教育城域网边界安全的设备，要实现对市县教育城域网和互联网流量的安全审计、安全告警、安全事件溯源。同时，安全日志保存期限不少于6个月，以满足安全审计和合规性要求。

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，通过安全策略可配置应用控制、入侵防护、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、HTTPS、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。同时能实现文件过滤、邮件过滤，实现针对主要的应用协议如 HTTP、HTTPS、FTP、POP3、SMTP、IMAP 等双向内容传输过滤，可预定义或自定义敏感信息库进行敏感信息定义。

1. 入侵防范

在市县教育城域网边界进行病毒过滤和入侵防御，并及时升级病毒和攻击特征库；对恶意代码（如病毒）和入侵攻击行为进行实时告警及阻断。对于主要常见攻击进行防护，包括：Flood（SYNFlood、ICMPFlood、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监测辅助检查）异常包攻击应用层Flood、SYN Cookie 等。

1. 未知威胁检测

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同时设备支持将安全事件、安全告警等相关事件信息上报到省级安全运营平台进行展示。

1. 上网行为审计

对教育网络的上网行为进行监控和管理，具备网络应用识别规则库。能够屏蔽游戏、色情、购物等和学习无关的网络访问业务。能够支持针对HTTP和HTTPS域名进行过滤，防止HTTP、HTTPS域名过滤逃逸情况，且能够适配针对IPv6扩展头、流标签、DSCP、VLAN等场景进行访问权限管控。

1. 全量日志采集与分析

借助网络全协议识别与还原技术，结合网络行为知识库，实现对城域网内安全防护网关、审计网关等关键节点的全流量采集。确保网络流量与事件的全面记录，为网络安全行为与事件检测、深度分析、快速发现及有效追溯提供坚实的数据基础。

1. 网络信息推送与共享

建立信息推送机制，实时将关键网络设备的运行日志及相关安全情报传输至海南省教育城域网核心节点的安全平台，实现安全信息的即时共享与协同处理，进一步提升整体安全防护水平。

1. 网络边界安全与管理

市县教育城域网出口处部署防火墙系统，实施访问控制与边界隔离策略。根据业务需求动态调整安全控制策略，定期进行策略优化与维护，确保网络边界的安全稳固。

1. **市县安全、认证平台与省级平台对接标准**

## 认证平台对接标准

认证接口：使用RADIUS标准协议对接，主要配置有RADIUS认证配置，具体配置如下：

（1） 配置AAA功能：

aaa new-model

aaa accounting network default start-stop group radius

aaa authentication webauth default group radius

aaa accounting update

aaa accounting update periodic 15

radius-server host 172.169.3.2 key HNSjyt@Ruijie

snmp-server community HNSjyt@Ruijie rw

（2） 配置同Radius通信源端口：

ip radius source-interface vlan 100

## 安全平台对接标准

海南省教育城域网省级核心节点建设安全事件日志中间库服务器，运营商分别将安全相关日志推送至中间库服务器，省平台从对接服务器读数据，进行事件展示。

运营商安全平台推送安全事件日志字段至少应包含以下必要字段：

1. 发生时间
2. 风险主机
3. 事件 ID
4. 举证信息
5. 原始请求详情
6. 威胁名称
7. 威胁IOC域名
8. 终端资产位置

## 平台升级标准

各平台采用语义化版本号管理机制，版本号格式为“主版本号.次版本号.修订版本号”。主版本号的变更表示平台进行了不兼容的重大功能升级或架构调整；次版本号的变更表示增加了新的功能且保持向后兼容；修订版本号的变更表示对现有功能的修复和优化。平台应在每次升级时，明确记录版本变更日志，详细说明每个版本的改进内容和新增功能。

各平台须具备自动检测升级的功能，每隔24小时自动连接到官方升级服务器，检查是否有可用的新版本。若检测到新版本，平台应在用户登录时以明显的提示信息告知用户，包括新版本的版本号、主要升级内容及推荐升级原因。对于涉及安全漏洞修复或重要功能改进的升级，平台可通过短信、邮件等方式向平台管理员发送升级通知，确保管理员及时知晓。

平台从官方升级服务器下载升级包。升级包下载完成后，进入预升级检查阶段，检查当前系统环境是否满足新版本的运行要求，如硬件资源是否充足、依赖的软件组件是否兼容。若预升级检查通过，平台开始执行升级操作，按照预定的升级脚本逐步更新平台的程序文件和数据库结构。升级完成后，自动进行功能测试和数据校验，确保平台升级后能够正常运行。若升级过程中出现任何错误，平台应能够自动回滚到升级前的状态，并向用户提供详细的错误报告。

1. **运维支撑人员组织架构**

海南省教育城域网的运维支撑对于保障教育网络的稳定、高效运行至关重要，其服务人员组织架构如下图所示：



图5  运维支撑人员组织架构图

## 8.1运维管理小组

1. 组长：由教育主管部门相关领导担任。全面负责运维工作的统筹规划，制定运维战略方向，协调与教育部门、学校以及其他相关机构的沟通与合作，保障运维工作与教育业务需求紧密结合。
2. 副组长：协助组长开展工作，分管具体的运维板块，如技术运维、服务运维。监督各运维团队的日常工作，及时发现并解决运维过程中的问题，确保运维工作按计划推进。

## 8.2技术运维团队

1. 网络工程师：负责教育城域网网络基础设施的维护和监控，包括网络设备（交换机、路由器等）的配置管理、故障排查与修复，保障网络通讯的稳定。实时监测网络流量，进行网络性能分析，根据业务需求进行网络优化，如调整网络拓扑、配置QoS策略等，确保网络满足教育教学对带宽、延迟等方面的要求。例如，当市县教育城域网枢纽节点链路负载达到70%且持续2小时，负责及时提升30%带宽，保障网络服务质量。
2. 系统管理员：维护服务器和存储设备，确保各类服务器（如认证服务器、应用服务器等）、存储系统正常运作。负责服务器系统的安装、升级、补丁管理，以及数据备份与恢复策略的制定和执行。定期对服务器和存储设备进行巡检，预防硬件故障，及时处理系统故障，保障教育城域网各类应用系统的稳定运行。
3. 数据库管理员：专门管理和维护教育城域网中的数据库，包括数据的存储、组织、检索和安全。负责数据库的设计、优化，确保数据的完整性和一致性。制定并执行数据库备份、恢复计划，应对可能的数据丢失或损坏情况。监控数据库性能，及时处理数据库相关的问题，保障教育数据的安全和高效访问。
4. 安全工程师：承担信息安全管理的重要职责，监控潜在的安全威胁。根据公安部《互联网安全保护技术措施规定》《公安机关互联网安全监督检查规定》的要求，实施用户统一认证和安全审计，确保网络安全合规。部署和维护网络安全设备（如防火墙、入侵检测系统等），定期进行安全漏洞扫描和修复，制定并执行安全应急响应预案，保障教育城域网免受网络攻击和数据泄露的威胁。

## 8.3服务运维团队

（1）服务台专员：作为与用户沟通的第一窗口，负责接听用户的咨询、投诉和故障申报电话，记录用户问题并及时转派给相关技术人员处理。跟踪问题处理进度，及时向用户反馈处理结果，确保用户问题得到妥善解决。定期对用户反馈进行统计分析，为运维工作的改进提供依据。

（2）现场维护工程师：在接到服务台转派的现场维护任务后，及时前往学校等用户现场进行故障排查和修复。负责用户端设备（如校园网络接入设备、终端计算机等）的安装、调试和维护，保障用户能够正常接入教育城域网并使用相关服务。对现场无法立即解决的问题，及时向上级汇报并协调技术专家支持。

（3）培训讲师：针对教育城域网的新功能、新技术以及常见问题的处理方法，为学校教师、管理人员和学生开展培训工作。提高用户对教育城域网的使用能力和故障初步排查能力，减少因用户操作不当导致的故障和咨询。根据用户需求和反馈，不断优化培训内容和方式。

## 8.4应急响应小组

（1）组长：通常由运维管理小组中的副组长兼任或指定经验丰富的技术骨干担任。负责应急响应工作的总体指挥和协调，制定应急响应策略和流程。在发生重大网络故障、安全事件等紧急情况时，迅速组织小组成员开展应急处置工作，确保将损失和影响降到最低。

（2）技术专家：由网络、系统、数据库、安全等各领域的资深工程师组成。在应急事件发生时，为应急响应提供技术支持和解决方案。分析故障或安全事件的原因，制定针对性的修复和防范措施，指导现场技术人员进行应急处理操作 。

（3）协调联络人员：负责与教育部门、学校、运营商其他部门以及外部相关机构（如网络安全监管部门、设备供应商等）的沟通联络。及时传达应急事件的相关信息，协调各方资源支持应急响应工作，确保应急处理过程中的信息畅通和协同合作。