附件 1-1
ICS 03.180
CCS Y 52

团　体　标　准

T/JYBZ XXX—202X

中小学数字校园网络设计指南

Guide for design of digital campus network in primary and secondary schools

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

202X-XX-XX 发布　　202X-XX-XX 实施

中国教育装备行业协会　发 布

目　录

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由北京师范大学提出。

本文件由中国教育装备行业协会归口。

本文件起草单位：北京师范大学、华为技术有限公司、新华三技术有限公司、江苏师范大学、紫光摩度教育科技有限公司、北京金山顶尖科技股份有限公司、深圳市宝安区教育局信息中心、北京师范大学附属实验中学、北京大学附属小学、自贡市教育科学研究所、青海省三江源民族中学。（拟）

本文件主要起草人：XXXXXXXXXXXX。

本文件为首次发布。

引　言

国家高度重视中小学校网络基础建设，通过构建高速、安全、绿色的教育网络，保障优质教育资源链路畅通，支撑个性化教与学，服务于教育数字化转型与教育强国建设目标。

在以新一代信息技术为核心驱动力的数字校园建设中，网络环境是支撑教学、管理、服务全流程的核心基础设施，其稳定性、覆盖范围与技术适配性，将直接决定着数字校园的整体建设质量与服务效能。为支撑教育强国建设、升级教育数字化基础设施、引导学校支持网络基础设施建设，特制定《中小学数字校园网络设计指南》团体标准。本指南旨在为中小学构建高带宽、低时延、全覆盖、智安全的网络支撑环境，为教育数字化转型提供坚实的“数字底座”。

本文件针对中小学数字校园网络，系统、具体地提出了数字校园中的常见网络架构与设计思路，为数字校园网络的架构设计与技术选择提供实施指南，对推动中小学数字校园的规范化建设具有积极意义。

中小学数字校园网络设计指南

1 范围

本文件给出了中小学数字校园网络（以下简称校园网络）设计的概述，提出了以太网络、无源光局域网、出口网络在校园网络中设计思路，以及校园网络信息安全管理体系的设计参考。

本文件适用于中小学新建或改扩建数字校园网络设计，幼儿园、特殊教育、中等职业学校等类型学校可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 36342 智慧校园总体框架

GB/T 36447 多媒体教学环境设计要求

GB/T 45940 网络安全技术 网络安全运维实施指南

GB 50174 数据中心设计规范

GB 50311 综合布线系统工程设计规范

YD/T 2000.1 平面光波导集成光路器件 第1部分：基于平面光波导(PLC)的光功率分路器

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字校园 digit campus

在传统校园基础上构建一个数字空间，实现从环境信息（包括教室、实验室等）、资源信息（如图书、讲义、课件等）到应用信息（包括教学、管理、服务、办公等）等全部数字化，从而为资源和服务共享提供有效支撑。

[来源：GB/T 36342—2018，3.1]

4 缩略语

下列缩略语适用于本文件。

AC：无线控制器（Access Controller）

AP：接入点（Access Point）

DHCP：动态主机配置协议（Dynamic Host Configuration Protocol）
GPON：吉比特无源光网络（Gigabit-capable Passive Optical Network）
IPv4：互联网通信协议第 4 版（Internet Protocol version 4）
IPv6：互联网协议第 6 版（Internet Protocol Version 6）
ODN：光分配网（Optical Distribution Network）
OLT：光线路终端（Optical Line Terminal）
ONU：光网络单元（Optical Network Unit）
PoE：以太网供电（Power over Ethernet）
POL：无源光局域网（passive optical LAN）
PON：无源光网络（Passive Optical Network）
SFP：小封装可插拔（Small Form Factor Pluggable）
SSID ：服务集标识（Service Set Identifier）
VLAN：虚拟局域网（Virtual Local Area Network）
XGS-PON：10Gbit/s 对称无源光网络（10-Gigabit-capable Symmetric Passive Optical Network）

5 概述

5.1 校园网络设计原则

为深入实施国家教育数字化战略，健全教育数字化保障体系，引导学校支持网络基础设施建设是推进教育数字化的重要工作。网络设计工作是网络顺利、合理建设的重要内容，是保障教育数字化工作有效实施的前提条件之一。

校园网络设计遵循“统一规划、适当前瞻、专网专用、集中管理、安全可控”的原则：

1）统一规划：

校园网络设计时统一规划网络架构、选型、VLAN 配置、IP 地址、无线网络等网络相关配置，后续网络建设结合原有网络基础进行建设，避免重复基础设施建设与分散管理；

2）适当前瞻：

充分考虑未来 5～10 年的业务发展和技术演进，规划具备前瞻性，保证系统的平滑扩展和可持续升级，保护既有投资，避免重复建设和技术断层。所有网络设备应支持 IPv4/IPv6 双栈协议以推进 IPv6 规模部署及应用。逐步实现校园无线网覆盖；

3）专网专用：

不同的业务系统建设时注意物理与逻辑隔离，充分利用 VLAN、带宽控制等技术手段将不同业务网络分离。对于校园网络中需要严格物理隔离的专网业务（如考试网络），单独建设物理网络。针对安全需求较高但无需物理隔离的专网业务（如教学管理专网、设备管理专网），可以使用同一套物理网络，利用 VLAN 实现逻辑隔离；

4）集中管理：

校园网络建立统一管控机制，将各类业务子系统整合至统一管理平台，形成标准化的管理入口与操作流程，实现校园网络的集中化、高效化管理；

5）安全可控：

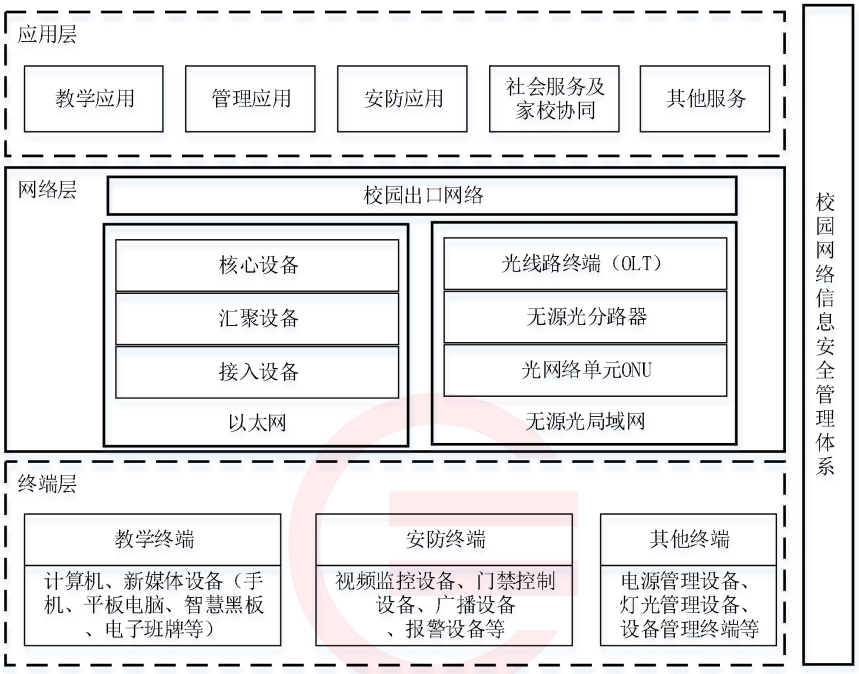
校园网络设计以信息安全为核心保障，构建技术防护和制度规范的双维度安全体系，构建纵深防御体系。技术层面上部署必要的安全防护设施，制度层面上建立覆盖数据全生命周期的安全管理制度，保障校园数据安全、系统稳定。

5.2 技术分类

校园网络按照采用的接入与传输技术，分为以太网和无源光局域网（POL）两种。

5.3 设计框架

校园网络总体框架如图 1 所示。



注1：应用层、终端层是本文件服务对象，本文件只描述服务内容。

注 2：网络层是本文件标准化对象，学校可选择以太网或无源光局域网两种技术之一进行设计。

图 1　校园网络总体框架

6　物理网络设计

6.1　以太网

6.1.1　架构

校园以太网架构分为核心层、汇聚层和接入层三层，各层以满足不同性能要求的交换机组成：

1）核心层：校园网络交互的核心节点，用于连接校园各个区域和网络。核心层提供多个 10Gbit/s 及以上速率的网络接口，带宽设计宜适当超前。核心层一般采用框式交换机，或采用两台盒式交换机，通过虚拟冗余技术以实现高可靠性组网。在核心层部署无线控制器（AC），用于无线接入网络的统一管理；

2）汇聚层：介于核心层和接入层之间，用于扩展端口、收敛带宽及流量转发，提供多个 10 Gbit/s 及以上速率的网络接口；

3）接入层：提供校园有线、无线、物联等终端接入。接入层设备具备高速二层转发能力，支持 VLAN 隔离，支持环路检测和自动阻断，能抑制广播和组播泛洪对网络的影响。接入层设备具有 PoE 供电能力，符合 802.3af、802.3at、802.3bt 标准要求，能为无线 AP 或摄像头等设备集中供电。采用 PoE 供电

时，双绞线线径应满足功率传输产生的温升要求，宜采用 23AWG 及以上线缆。

校园以太网架构图如图 2 所示。

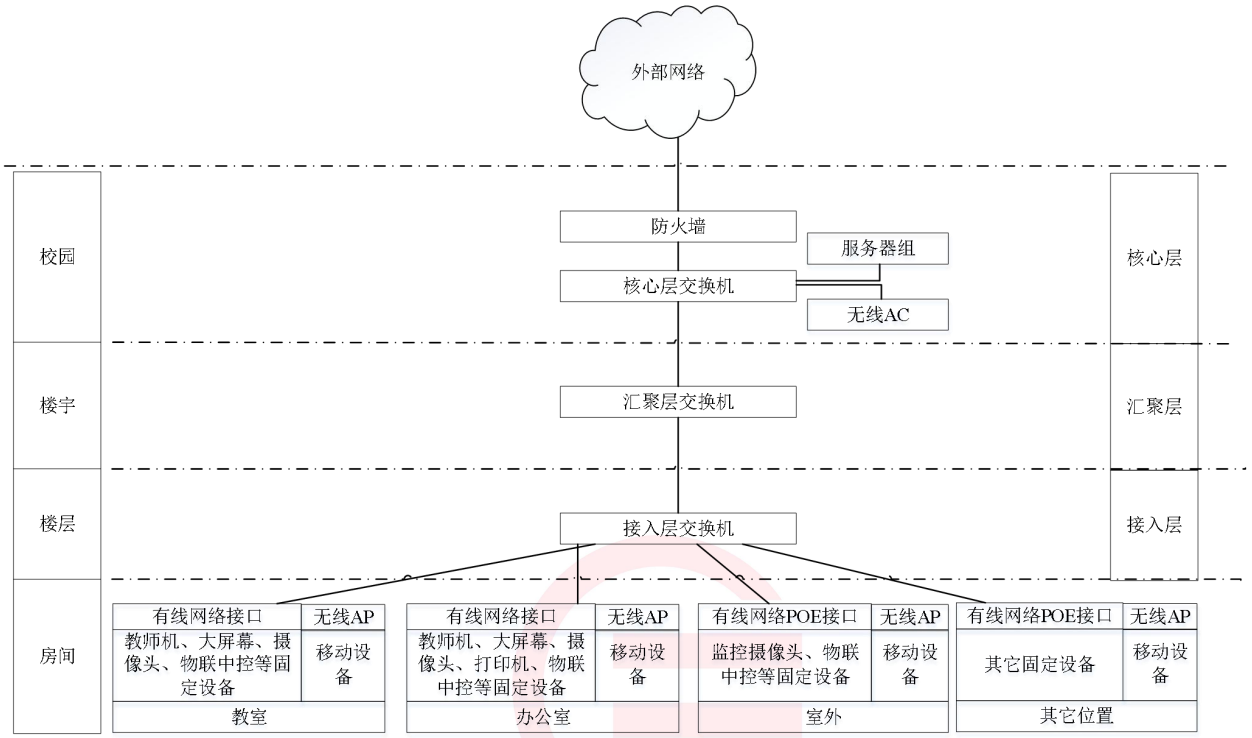


图 2　校园以太网架构

6.1.2　设备安装与布线

网络的核心层设备安装在学校网络机房中，汇聚层设备安装在网络机房或楼宇设备间，如未设置网络机房，核心层与汇聚层设备可安装在楼宇或楼层设备间。接入层设备安装在楼层设备间、楼道或房间内。在有线接入层设备安装在楼道或房间内时，采用信息箱嵌墙安装、壁挂明装、小型机柜安装或工作台下明装方式。

综合布线设计参考 GB 50311、GB/T 36447、GB 50174 进行光缆及双绞线布线设计，并按以下要求进行设计：

1）在核心机房、楼宇机房、楼层设备间之间采用光纤做为主要布线材料，在楼层到房间内采用光纤或双绞线进行布线材料。规模小的网络可采用双绞线进行布线；

2）对于接入层需要集中供电的设备，宜选用合适的光电混合缆实现同时供电和光链路部署；

3）在房间内使用 6 类及以上对绞电缆，以保障传输性能和 PoE 供电可靠；

4）布线设计适当前瞻，楼宇间和垂直子系统的主干光缆预留不小于 50%的冗余。

6.2　无源光局域网

6.2.1　架构

无源光局域网架构分为核心层与接入层两层：

1）核心层包括交换机与光线路终端 OLT，分别按以下要求设计：

a）交换机用于连接各个区域网络并与出口网络连接，按照 6.1.1 核心层要求设计；

b）OLT 是无源光网络与上层网络连接的设备，是无源光局域网的核心设备，通过无源分光器

及光纤线路与 ONU 连接。2000 人及以上学校采用可扩展的多功能插卡式 OLT 设备，2000 人以下学校采用盒式 OLT 设备。

c）插卡式 OLT 设备支持 GPON 板卡、XGS-PON 板卡混插，宜支持下一代万兆 PON 板卡混插；网络侧端口支持 10GE/100GE 以太网光口，用户侧端口支持 GPON、XGS-PON，可支持下一代万兆 PON 接口；主控板、电源板、风扇模块支持冗余保护；支持不中断业务升级软件；

2）接入层主要由光网络单元 ONU 组成。ONU 的网络侧端口支持 GPON 或 XGS-PON 接口，支持下一代万兆 PON 接口，并根据冗余保护模式配置 ONU；用户侧端口支持千兆/2.5 千兆/10 千兆以太网、传统电话业务等各种端口，以太网端口支持 PoE 供电功能，内置 Wi-Fi 功能。

校园无源光局域网架构如图 3 所示：

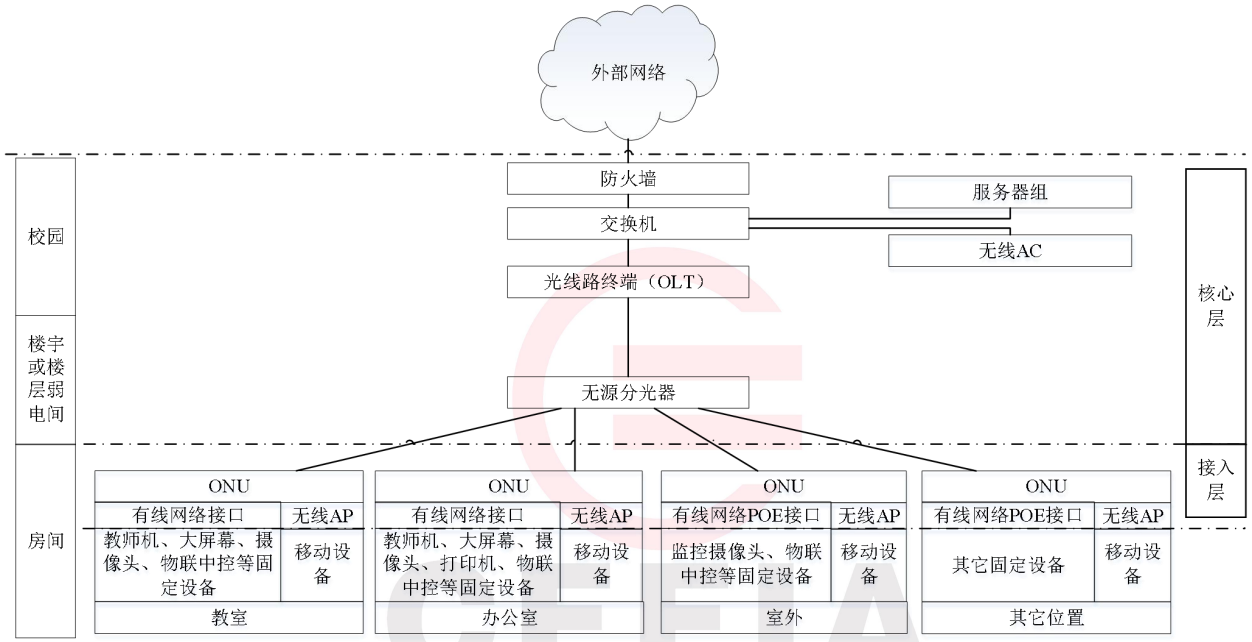


图 3 校园无源光局域网架构

6.2.2 设备安装与布线

交换机、OLT 安装于网络机房，如未设置网络机房，可安装于校园的设备间。无源分光器安装在楼宇的设备间。ONU 安装于房间内，可采用 SFP ONU 方式安装于终端设备内；室内安装宜采用信息配线箱内嵌墙安装、墙面明装，可采用桌面放置；面板式 ONU 宜采用嵌墙 86 盒或者桌面标准 86 盒安装。

无源光局域网布线参考 GB 50311、GB/T 36447、GB 50174 进行光缆布线设计，并按下列要求：

1）主干层光缆采用 G.652 类单模光纤，根据光缆规格预留不小于 10%的余量；

2）网络机房、楼宇之间安装主干光缆互通；

3）楼层配线设备可以经过主干光缆直接连至网络机房；

4）用户光缆可采用 G.652 光纤或模场直径与 G.652 光纤相匹配的 G.657 类光纤；

5）ONU 安装在信息箱位置；

6）每 ONU 的用户光缆根据用户分布情况配置，至少配置一条 2 芯及以上光缆；

7）无源分光器安装在用户光缆区域。当楼层信息点数量较多时光分路器宜安装于建筑物楼层设备间。当整栋建筑物信息点较少时光分路器宜安装于楼宇电信间，也可安装于楼层设备间；

8）无源分光器根据业务带宽需求和光功率预算选择合适的分路比；

9）插片式、盒式和机架式光分路器指标符合 YD/T 2000.1 的规定。

6.3 无线网络

校园网络逐步推进无线网络覆盖，无线网络按以下要求设计：

1）网络按业务设置无线 SSID，不同业务划分不同 VLAN，实现逻辑隔离；

2）用户接入无线网络分为认证接入和免认证接入，不同接入方式的业务应逻辑隔离；

3）用户认证方式包括 MAC 认证、802.1x 认证、Portal 认证、MAC+Portal 无感知认证，宜采用 MAC+Portal 无感知认证方式；

4）支持 IEEEE 802.11ax（Wi-Fi 6）及以上标准，宜支持 Wi-Fi 7（802.11be）及以上标准；

5）无源光局域网中在核心层接入无线控制器（AC），光网络单元（ONU）网络侧接入无线 AP。

根据不同场景的用户数量和部署要求，校园无线网络按照表 1 进行设计。

表 1　无线网部署设计表

典型场景	用户数量	部署要求	部署方案
小型办公室	1～2 人	环境简单，终端数量少，稳定安全	单台面板式 AP 或放装式 AP
普通教室	50 人以内	环境简单，无线设备少，可能存在视频等业务，带宽要求高	单台放装式 AP
普通办公室	10 人以内	环境宽敞，终端数量适中，注意金属柜等影响信号	
普通会议室	10～30 人	环境封闭，对带宽、稳定性要求较高	
专用教室/走廊	50 人以内	设备众多、人员密集、信息种类多、带宽要求高	高密 AP，根据空间大小及终端数量部署单台或多台，单 AP 并发不低于 40～60 终端
图书馆	50～200 人		
开放办公区/大型会议室/汇报厅等	50 人以上		
操场	50 人以上	开阔场景覆盖为主，应考虑 AP 防护及多 AP 协同覆盖，单个室外 AP 推荐覆盖半径 50～80 米	多个室外 AP 协同

6.4 分场景部署

校园无源光局域网分场景部署设计按照附录 A 进行设计。

7 逻辑网络设计

7.1 虚拟局域网 VLAN

VLAN 按以下要求设计：

1）业务 VLAN 设计：可按地理位置、人员组织结构、终端类型进行业务规划，例如教学 VLAN、办公 VLAN 等，通过 VLAN 实现逻辑隔离不同的业务网络。每个业务子网至少分配一个 VLAN，也可以分配多个 VLAN；

2）管理 VLAN 设计：有线网络设备和无线 AP 的管理网宜有固定的管理 VLAN，确保管理和业务互不干扰；

3）提供一定数量的预留 VLAN，便于后续业务扩容和 VLAN 管理；

4）VLAN 的规划与 IP 地址规划保持对应关系，便于管理和故障定位。

7.2 IP 地址

IP 地址按以下要求设计：

1）不同 VLAN 规划不同的 IP 地址段，满足 VLAN 内每个终端有唯一的 IP 地址。为满足业务终端的增长预期，宜为每个 VLAN 预留不少于 50%的 IP 地址空间；

2）使用静态 IP 地址和动态 IP 地址结合的方式。固定安装设备均使用静态 IP，移动设备或临时连接设备使用动态 IP。静态 IP 地址对应的终端的 IP 地址、MAC 地址、所处位置形成表格进行统一管理。动态 IP 地址，由 DHCP 服务器统一进行分配和管理；

3）同一个校园内不同网络区域的 IP 地址段不重复；

4）为所有 VLAN 同时规划 IPv4 和 IPv6 地址段，支持 IPv6 终端的接入。

7.3 DHCP 服务

DHCP 服务按以下要求设计：

1）校园网络中部署 DHCP 服务器，通过核心层接入网络，为终端提供动态 IP 地址的分配和管理。在网关设备上启用 DHCP 中继功能；

注：网关（gateway），一种用于连接具有不同网络体系结构的两个计算机网络的功能单元。

2）对于规模较小的网络（低于 12 间教室），可直接在核心交换机上开启 DHCP 服务来提供动态 IP 地址分配；

3）DHCP 服务支持将动态分配的 IP 地址绑定已分配 MAC 地址；

4）宜部署备份 DHCP 服务器。

8 校园出口网络设计

校园出口网络是校园网络与外部网络关联的接口，为校园网络提供获取外部网络资源的通道，并为学校信息公开提供接口。校园出口网络也是校园网络与外部网络隔离的关口，为校园网络信息提供保护。

校园出口网络设备应包括外网接入设备以及安全与网络隔离设备。外网接入设备外连不同网络服务商或上级教育网络，一般使用光纤上联外部网络，采用双机负载分担部署，提高可靠性。出口网络应部署防火墙、上网行为管理等边界防护设备，实现内外网逻辑隔离与流量清洗。出口设备应具备 IPv4/IPv6 双栈流量转发与安全管控能力。

校园网络出口带宽是影响数字校园资源获取、智能教学以及信息公开的重要因素，学校根据班级规模参考表 2 选择校园网络出口带宽。

表 2 校园网络出口带宽选择

班级数量	校园网络出口带宽	最大带机量参考值
12 间及以下	500～1000Mbit/s	1000
12～72 间	1～10Gbit/s	1000～3000
72 间以上	1～10Gbit/s	3000～10000

9 校园网络信息安全管理体系

建立校园网络信息安全管理体系，保障校园网络安全应做到以下内容：

1）校园网络宜符合 GB/T 22239 网络安全等级保护第二级及以上要求，关键业务系统（如考试系统、数据中心）应达到第三级；

2）信息系统（网站）不低于教育部《教育行业信息系统安全等级保护定级工作指南（试行）》文件规定的安全保护等级；

3）网络安全技术防护体系按照 GB/T 36342 要求做好括物理安全、网络安全、主机安全、应用安全和数据安全等工作。在校园网络出口区域部署相应的防火墙设备，并部署相关策略，包括结构安全、访问安全、安全审计、入侵防范、恶意代码防护等。针对互联网对校园网内业务系统访问，执行严格的访问控制策略，可依据源、目标地址、协议、端口，以限制互联网不同级别的终端，按照权限访问不同服务器的不同应用，并有效禁止非法的访问。宜部署统一的身份认证与网络准入系统，对接入终端进行安全合规检查；

4）做好对采集的用户身份信息的加密存储及脱敏处理；

5）参考 GB/T 45940 建立网络安全运维业务相关制度和流程。制定网络安全应急预案，明确应急处置流程和权限，提高网络安全应急处置能力；

6）根据实际需要配备网络安全设备和网络安全系统，规划日志服务器存储容量使网络设备日志保存时间不少于六个月；

7）网络认证系统应具备实名认证功能，支持基于用户身份的终端接入控制与溯源管理；

8）配置细粒度的访问控制策略（ACL），确保用户权限遵循“最小够用”原则，防止用户越权使用网络；

9）具备不健康信息过滤与网络监控功能，阻断淫秽色情等违法或不健康信息在校园网络上传播；

10）终端安全管理系统应支持对全网终端的补丁分发、病毒库统一升级及安全基线核查。

附 录 A
（规范性）
校园网络分场景部署设计表

A.1 校园网络分场景部署设计见表 A.1。

场景	主要终端设备	有线网络设计					无线网络设计	
		以太网接入层位置	无源光局域网 ONU 位置	下行出口带宽要求	下行出口数量要求	下行出口 PoE 要求	是否需要无线网络	终端数量设计
普通教室	教学大屏、教师计算机、若干摄像头等设备	室内	光纤到房间，ONU 在室内	不低于 1000Mbit/s	室内所有设备数量加上 20%～50%冗余	要	要	少量（少于 20），满足无线投屏和少量移动设备接入
办公室	教师用电脑、移动终端、大屏幕、共享打印机等	室内	光纤到房间，ONU 在室内	不低于 1000Mbit/s	室内所有设备数量加上 20%～50%冗余	要	要	大量（大于 20），按工位数 1.5 倍规划，满足所有教师移动设备接入
计算机教室	大量学生电脑、教学大屏、教师计算机、若干摄像头等设备	室内	光纤到房间，ONU 在室内	不低于 1000Mbit/s	室内所有设备数量加上 20%～50%冗余	要	要	少量（少于 10），满足无线投屏和少量移动设备接入
专用教室	智能化、数字化专用教学设备，大量小型数字化设备	室内	光纤到房间，ONU 在室内	不低于 1000Mbit/s	室内所有固定设备数量加上 50%以上冗余	要	要	大量（大于 20），满足实验设备无线接入
图书馆	感知系统、通信网络系统、数据库与服务器等。	室内	光纤到房间，ONU 在室内	不低于 1000Mbit/s	室内所有设备数量加上 50%以上冗余	要	要	大量（大于 20），按图书馆移动阅读设备数量加上 50%以上冗余
设备管理	各种设备的控制、监控模块或设备	楼层设备间或楼道		不低于 100Mbit/s	室内所有设备数量加上 50%以上冗余	否	否	无
安防网	监控系统及消防控制系统	楼层设备间或楼道		不低于 1000Mbit/s	室内所有设备数量加上 50%以上冗余	要	否	无

A.1 校园网络分场景部署设计表