ICS 35.240.99
CCS L 67

T/CAET

中 国 教 育 技 术 协 会 团 体 标 准

T/CAET 006—2025

校园网网络设备安全技术要求

Security technology requirements for campus network devices

2025－08－10 发布　　2025－10－10 实施

中国教育技术协会　　发 布

目　　次

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。

本文件由中国教育技术协会提出并归口。

本文件起草单位：浙江大学、教育部教育管理信息中心、厦门大学、北京大学、哈尔滨工业大学、东南大学、南开大学、北京师范大学、河海大学、西湖大学、长江大学、四川水利职业技术学院、成都农业科技职业学院、上海电子信息职业技术学院、川南幼儿师范高等专科学校、中国人民大学附属中学、惠州市第八中学、东莞市松山湖北区学校、东莞市松山湖第三小学、乌鲁木齐市教育信息服务中心、华为技术有限公司、新华三技术有限公司、锐捷网络股份有限公司、迈普通信技术股份有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、苏州盛科通信股份有限公司、创耀（苏州）通信科技股份有限公司、深圳市联软科技股份有限公司。

本文件主要起草人：袁书宏、单康康、云霞、曾德华、杨伟平、孙强、廖运华、李燕、郑海山、赖清楠、赵旭、胡轶宁、林初建、田小萍、管军、石刘洋、余华平、刘明锦、杨山金、邵瑛、赵新国、赵海涛、赖昱全、姚湘斌、欧劲、阿布都瓦依提·热合卖提多拉、秦神祖、胡俊理、陈佩珊、万晓兰、陈育锋、谯良刚、王洪军、郑嘉俊、王俊杰、郑宇、李晓峰。

校园网网络设备安全技术要求

1 范围

本文件规定了校园网网络设备的自身安全要求、安全功能要求以及安全保障要求。

本文件适用于各类院校的校园网网络设备的检测和选型，以及校园网规划、设计和建设，也适用于指导网络设备的生产和开发。

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 25069—2022 信息安全技术 术语

GB/T 32905—2016 信息安全技术 SM3密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4分组密码算法

GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

绿色上网 green internet

通过技术手段确保学生和教师在校园中安全上网的行为或活动。

3.2

防挖矿 anti-cryptomining

通过技术手段防止以隐藏或不易察觉的方式，未经用户许可使用该用户设备挖掘加密货币的行为。

3.3

防勒索 anti-ransomware

通过技术手段防止勒索软件对用户设备上的文件进行加密、篡改或删除，迫使用户支付赎金的行为。

3.4

口令字典 password dictionary

用于存储潜在密码组合的预设列表。

4 缩略语

下列缩略语适用于本文件。

AC：接入控制器（Access Controller）

ACL：访问控制列表（Access Control List）

AES-CBC:高级加密标准-密码块链接模式(Advanced Encryption Standard-Cipher Block Chaining)

AP：接入点（Access Point）

BRAS：宽带远程接入服务器（Broadband Remote Access Server）

CERNET：中国教育和科研计算机网（China Education and Research Network）

C&C：命令与控制（Command and Control）

CPU：中央处理器（Central Processing Unit）

DES：数据加密标准（Data Encryption Standard）

DGA：域名生成算法（Domain Generation Algorithm）

DMZ：隔离区（Demilitarized Zone）
DNS：域名系统（Domain Name System）
FPGA：现场可编程门阵列（Field-Programmable Gate Array）
FTP：文件传输协议（File Transfer Protocol）
HTTPS：安全套接字层超文本传输协议(Hyper Text Transfer Protocol over Secure Socket Layer)
ID：标识符（Identifiers）
IP：互联网协议（Internet Protocol）
IPoE：以太网承载IP协议（IP over Ethernet）
IPSec：IP安全（Internet Protocol Security）
MAC：媒体访问控制（Media Access Control）
MACSec：媒体访问控制安全（Media Access Control Security）
MD5：消息摘要算法第5版（Message Digest Algorithm 5）
M-LAG：多机箱链路聚合组 （Multi-chassis Link Aggregation Group）
NOD：新发现域名（Newly Observed Domain）
NTP：网络时间协议（Network Time Protocol）
PPPoE：以太网点对点协议（Point-to-Point Protocol over Ethernet）
RC4：Rivest加密算法4（Rivest Cipher 4）
SHA-1：安全散列算法1（Secure Hash Algorithm 1）
SNMP：简单网络管理协议（Simple Network Management Protocol）
SoC：片上系统（System on Chip）
SSH：安全外壳协议（Secure Shell）
SZTP：安全零配置部署（Secure Zero Touch Provisioning）
Telnet：终端网络（Terminal Network）
TLS：传输层安全（Transport Layer Security）
URL：统一资源定位符（Uniform Resource Locator）
VLAN：虚拟局域网（Virtual Local Area Network）
VPN：虚拟专用网（Virtual Private Network）
VRRP：虚拟路由器冗余协议（Virtual Router Redundancy Protocol）
WAPI:无线局域网鉴别和保密基础结构(Wireless Authentication and Privacy Infrastructure)
WEB：万维网（World Wide Web）
WPA：Wi-Fi保护接入（Wi-Fi Protected Access）
3DES：三重数据加密标准（Triple Data Encryption Standard）

5 概述

5.1 校园网网络架构

校园网网络架构，通常包括接入区、核心交换区、分校互联区、数据中心区以及互联网出口区等，见图1。

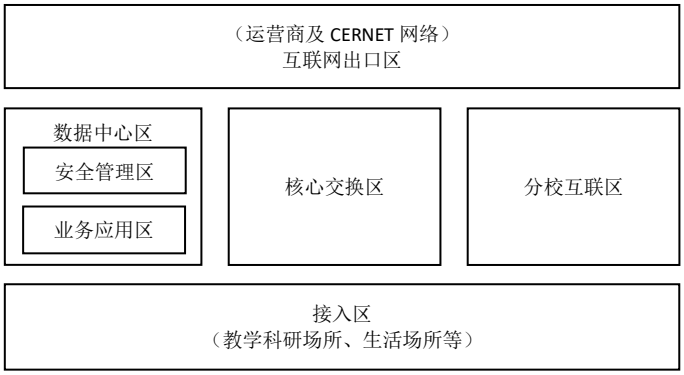

图1　校园网网络架构示意图

具备包括但不限于：

——接入区，用于教学科研（如办公室、教室、实验室、图书馆、会议室、报告厅等）和生活（如食堂、宿舍、体育馆等）等场所的终端设备接入，主要使用交换机、无线局域网AP等设备；

——核心交换区，用于校园网络各功能区的数据交换，主要使用交换机、无线局域网AC、宽带远程接入服务器（BRAS）等设备；

——分校互联区，用于分校区接入，主要使用防火墙、交换机等设备；

——数据中心区，用于承载学校教学、科研、管理和服务等多方面的数据存储、处理和管理功能，包括安全管理区和业务应用区，主要使用交换机、防火墙、抗拒绝服务攻击产品、入侵防御系统等设备；

——互联网出口区，通过运营商网络及中国教育和科研计算机网（CERNET）接入互联网和教育网，主要使用防火墙、抗拒绝服务攻击产品、路由器、入侵防御系统等设备。

5.2　校园网网络设备安全框架

5.2.1　概述

校园网网络设备包括交换机、路由器、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统。网络设备安全通常由网络设备自身安全、安全功能和安全保障构成，见图2。

图2　校园网网络设备安全框架

5.2.2　自身安全

网络设备自身具备的安全纵深防御能力，包括接入控制、通信安全、安全审计、认证凭据、证书管理、协议防攻击等，为校园网提供安全稳定的网络服务。

5.2.3　安全功能

安全功能如下：

——终端接入安全，用于终端接入的网络设备具备终端认证鉴权、接入防私接、访问控制与用户管理等能力；

——链路传输安全，网络设备具备端到端链路安全保障能力，包括无线链路（如终端到无线局域网AP）和有线链路（如无线局域网AP到无线局域网AC、接入交换机到核心交换机）；

——网络出口安全，用于互联网出口和校园网各分区出口的网络设备具备安全识别和防御能力，包括通信加密、抗拒绝服务攻击、身份认证鉴权、绿色上网、防挖矿、防勒索等。

5.2.4　安全保障

网络设备供应商符合相关安全要求，包括设备的设计与开发、生产与交付、运行与维护、供应安全等。

6 安全要求

6.1 自身安全要求

6.1.1 接入控制

网络设备应符合以下安全要求：

a) 所有在设备外部可见的能对系统进行管理的物理接口默认启用接入认证机制；
b) 所有在设备外部可见的能对系统进行管理的物理接口支持关闭；
c) 支持登录用户会话空闲超时锁定或自动退出，支持身份鉴别尝试次数限制；
d) 当鉴别失败时，设备提供无差别反馈，避免提示“用户名错误”“口令错误”等具体信息。

网络设备宜支持SZTP功能。

6.1.2 通信安全

6.1.2.1 默认安全

网络设备应符合以下安全要求：

a) 默认关闭不安全的密码算法；

示例：不安全的密码算法如 RC4、DES、3DES、AES-CBC、MD5、SHA-1 等。

b) 当启用不安全密码算法时有安全提示或告警；
c) 默认关闭不安全协议的网络管理功能；

示例：不安全协议如 Telnet、SSHv1、SNMPv1、SNMPv2、FTP、TLS1.0、TLS1.1 等。

d) 当启用不安全协议的网络管理功能时有安全提示或告警。

6.1.2.2 管理通信协议安全

网络设备应符合以下安全要求：

a) 使用 WEB 管理时，支持并默认启用 HTTPS；
b) 使用 SSH 管理时，支持并默认启用 SSHv2；
c) 使用 SNMP 管理时，支持并默认启用 SNMPv3；
d) 支持使用 a）~c）至少一种非明文数据传输协议对设备进行管理；
e) 支持使用 ACL 进行管理平面隔离，阻断从互联网或接入设备发起的请求；
f) 支持使用 NTP 等实现时间同步功能，并具备安全功能或措施防范针对时间同步功能的攻击，如提供 NTP 认证等功能。

网络设备宜支持从限定的IP接入管理平面，从限定的VPN或VLAN接入管理平面，实现管理平面隔离，阻断从互联网或接入设备发起的请求。

6.1.3 安全审计

网络设备应符合以下安全要求：

a) 支持安全日志记录功能，对用户关键操作，如增加和删除账户、修改鉴别信息、修改关键配置、用户登录和注销、用户权限修改、重启和关闭设备、软件更新等行为进行记录；
b) 在安全日志审计记录中记录必要的日志要素，至少包括事件发生日期和时间、主体（如登录账号等）、事件描述（如类型、操作结果等）、源 IP 地址（采用远程管理方式时）等，为查阅和分析提供足够的信息；
c) 在日志中不使用明文或不安全的加密算法记录敏感数据；

示例：敏感数据如用户口令、SNMP 团体名、WEB 会话 ID 以及私钥等。

d) 支持对安全日志进行防护，确保审计数据完整，防止被未经授权的查看、输出、修改或删除；
e) 支持通过管理平台等方式保留日志不少于 6 个月。

网络设备宜符合以下安全要求：

a) 安全日志单独存储，任何账号不应具备删除和修改日志的权限；
b) 支持对非法用户登录、非授权操作等疑似攻击场景记录审计日志并上报网管。

6.1.4 认证凭据

网络设备应符合以下安全要求：

a） 使用口令鉴别方式时，具备口令防暴力破解机制；

b） 使用口令鉴别方式时，支持口令复杂度检查功能，口令长度不少于 8 位且至少包含 2 种不同类型字符；

c） 使用口令鉴别方式时，不明文回显用户输入的口令信息；

d） 使用口令鉴别方式时，支持首次管理设备时强制修改默认口令或设置口令，或支持随机的初始口令；

e） 使用口令鉴别方式时，支持设置口令生存周期；

f） 认证凭据不以明文方式存储在系统介质中，支持加密保护并提供访问控制；

示例：认证凭据如口令和私钥等。

g） 认证凭据不在日志、调试信息、错误提示中明文显示；

h） 设备如存在默认口令，在产品资料中公开。

网络设备宜支持弱口令字典功能，提示用户避免使用弱口令字典中的任何口令。

6.1.5 证书管理

网络设备宜符合以下安全要求：

a） 支持和网管配合实现对数字证书的集中化、可视化的全生命周期管理；

b） 支持在数字证书即将过期前发送安全提示或者告警，提示运维人员更新证书；

c） 支持对接证书管理系统，实现数字证书的自动申请和更新功能。

6.1.6 协议防攻击

网络设备应符合以下安全要求：

a） 支持抗大流量协议报文攻击，采用限速、丢弃或优先级调度等策略；

b） 支持抗畸形报文能力，进行报文的合法性校验，丢弃针对本设备的畸形报文。

示例：畸形报文如超长包、超短包、链路层错误包、网络层错误包、上层协议错误包等。

6.2 安全功能要求

6.2.1 通用要求

网络设备应符合以下安全功能通用要求：

a） 校园网网络设备符合教育行业校园网络安全等级保护相关要求；

b） 构成网络关键信息基础设施的网络设备满足关键信息基础设施保护相关要求。

6.2.2 交换机安全要求

6.2.2.1 接入区安全

6.2.2.1.1 终端接入安全

交换机应符合以下安全要求：

a） 支持 MAC 地址认证；

b） 支持 802.1X 认证；

c） 支持 Portal 认证；

d） 支持对风险终端进行阻断，防止非授权的终端接入；

e） 支持私接行为检测。

示例：私接行为如私接 HUB、路由器、Wi-Fi 共享等。

交换机宜支持对物联终端进行被动指纹识别和主动探测扫描，实现校园物联终端识别。

示例：物联终端如门禁、闸机、水表、电表等。

6.2.2.1.2 链路传输安全

交换机宜符合以下安全要求：

a） 支持 MACSec，保障链路层数据传输安全；

b） MACSec 支持 SM4 算法（符合 GB/T 32907—2016），或国家密码管理主管部门认可的密码算法。

6.2.2.2 核心交换区安全

6.2.2.2.1 终端接入安全

交换机应支持用户准入认证及基于IP地址的身份溯源。认证方式应包括MAC地址认证、802.1X认证和Portal认证，实现权限控制，保障校园上网安全。

交换机宜支持策略联动和业务随行，简化配置，确保用户在不同位置保持一致的访问策略和权限。

6.2.2.2.2 链路传输安全

交换机应符合以下安全要求：

a) 支持堆叠或 M-LAG 跨设备链路聚合，实现设备间高可靠；

b) 支持 CPU 保护机制，防止拒绝服务攻击、非法接入以及控制平面过载等安全攻击。

示例：CPU 保护机制如协议报文识别过滤、协议报文限速、CPU 端口队列限速等。

交换机宜符合以下安全要求：

a) 支持 MACSec，保障链路层数据传输安全；

b) MACSec 支持 SM4 算法，或国家密码管理主管部门认可的密码算法。

6.2.3 路由器安全要求

6.2.3.1 互联网出口区安全

路由器应符合以下安全要求：

a) IPSec 支持 SM3 算法（符合 GB/T 32905—2016）、SM4 算法，或国家密码管理主管部门认可的密码算法，实现传输通信安全；

b) 路由协议支持 SM3 算法或国家密码管理主管部门认可的密码算法，保障路由安全；

c) 具备高可靠性，保障互联网出口路由高可靠；

示例：高可靠性如支持 VRRP。

d) 对网络链路质量具备监测手段，保障互联网出口链路高可用。

6.2.3.2 核心交换区安全

路由器作为BRAS设备时，应符合以下安全要求：

a) 支持基于 MAC 地址的 PPPoE 和 IPoE 会话负载分担，或支持 PPPoE 和 IPoE 透传；

b) 支持用户准入认证及基于 IP 地址的身份溯源，认证包括 MAC 地址认证、802.1X 认证和 Portal 认证；

c) 支持 CPU 保护机制，防止拒绝服务攻击、非法接入以及控制平面过载等安全攻击。

示例：CPU 保护机制如协议报文识别过滤、协议报文限速和 CPU 端口队列限速等。

路由器作为BRAS设备时，宜支持多校区用户会话备份，保障校园网高可靠。

6.2.4 无线局域网产品安全要求

6.2.4.1 终端接入安全

无线局域网产品应符合以下安全要求：

a) AC 支持通过内置或者外置认证服务器处理终端接入鉴权，鉴权方式包括共享密钥、账号密码、数字证书；

b) AC 支持呈现接入终端信息，信息包括但不限于鉴权方式、鉴权状态；

c) AC 支持终端接入管理控制，包括但不限于下线已鉴权终端、将终端加入黑名单等操作；

d) AC 支持对接入终端进行网络访问控制设置；

e) AC 支持接入 AP 认证鉴权，鉴权方式包括数字证书、密码、MAC 鉴权；

f) AP 支持非法热点检测与反制。

AP宜支持通过物理层防护进行空口防侦听，保障学校科研等保密信息不泄露。

6.2.4.2 链路传输安全

无线局域网产品应符合以下安全要求：

a) AP 支持 WPA2、WPA3、WAPI 安全传输协议，保障 AP 和终端的链路安全；
b) AP 支持终端二层隔离功能，阻断终端之间的二层访问流量；
c) AP 支持识别终端发起的泛洪类网络攻击，并将终端加入动态黑名单；
d) AP 支持识别终端发起的针对无线 AP 的无线协议攻击，并将终端加入动态黑名单；
e) AC 支持冗余高可靠。
AP宜支持MACSec，保障链路端到端逐跳部署MACSec保护。

6.2.5 防火墙安全要求

6.2.5.1 互联网出口区安全

防火墙应符合以下安全要求：
a) 支持已知 URL 过滤和未知恶意 URL 动态识别；
b) 支持应用、协议识别及封堵；
c) 支持恶意文件识别与阻断，并记录日志；
d) 支持 IPv4 和 IPv6 访问控制；
e) 支持 DNS 代理功能，阻止对已知恶意域名的解析请求；
f) 支持 IP 地址黑名单和白名单；
g) 支持网络层攻击防护；
h) 支持基于域名的访问控制和 URL 白名单模糊匹配功能；
i) 支持划分多个安全域，包括 Trust 域、Untrust 域、DMZ 域等；
j) 支持通过 IPSec 进行多校区安全互联，IPSec 支持 SM3 算法、SM4 算法，或国家密码管理主管部门认可的密码算法；
k) 支持冗余高可靠。
防火墙的路由协议宜支持 SM3 算法或国家密码管理主管部门认可的密码算法。

6.2.5.2 数据中心区安全

6.2.5.2.1 安全管理区安全

防火墙应符合以下安全要求：
a) 支持恶意文件识别与阻断，并记录日志；
b) 支持 IPv4 和 IPv6 访问控制；
c) 支持冗余高可靠。

6.2.5.2.2 业务应用区安全

防火墙应符合以下安全要求：
a) 支持已知勒索病毒的检测与实时阻断；
b) 支持已知挖矿病毒的检测与实时阻断；
c) 支持 IPv4 和 IPv6 访问控制；
d) 支持黑名单和白名单；
e) 支持在紧急情况下，一键关停对外发布的校园业务；
f) 支持冗余高可靠。
防火墙宜符合以下安全要求：
a) 支持未知勒索病毒的检测与实时阻断；
b) 支持未知挖矿病毒的检测与实时阻断。

6.2.6 入侵防御系统安全要求

入侵防御系统应符合以下安全要求：
a) 支持命令与控制（C&C）、挖矿域名、勒索域名、钓鱼域名、Sinkhole 域名、恶意站点、Compromised 域名、DGA 域名、NOD 域名等过滤；
b) 支持 X-Forwarded-For 识别能力；
c) 支持 tar、zip、gzip、tgz 压缩检测；

d） 支持应用识别能力；
e） 支持攻击取证、全流抓包、攻击片段取证；
f） 支持关联签名检测；
g） 支持 IPv4 和 IPv6 防护；
h） 支持基于漏洞攻击规则的防护能力；
i） 支持威胁情报联动，辅助威胁事件分析与研判。

6.2.7 抗拒绝服务攻击产品安全要求

抗拒绝服务攻击产品应符合以下安全要求：
a） 支持流量基线学习；
b） 支持异常流量清洗；
c） 支持定制差异化防护策略；
d） 支持防御策略调优；
e） 支持 HTTPS 加密攻击不解密防御；
f） 支持 IPv4 和 IPv6 防护。

6.3 安全保障要求

6.3.1 通则

网络设备的安全保障要求符合相关产品国家标准规定，具体要求如下：
a） 防火墙、抗拒绝服务攻击产品、入侵防御系统的安全保障要求应符合 GB 42250—2022 中第 6 章的规定；
b） 路由器的安全保障要求宜符合 GB/T 41269—2022 中第 6 章的规定；
c） 交换机的安全保障要求宜符合 GB/T 41267—2022 中第 6 章的规定；
d） 无线局域网产品的安全保障要求宜符合 GB/T 33565—2024 中 8.2 的规定。

6.3.2 供应安全要求

6.3.2.1 软件供应安全

网络设备的整机软件应符合以下供应安全要求：
a） 具备网络设备整机软件知识产权；
b） 具备漏洞和开源软件管理机制；
c） 设备软件和补丁不存在病毒、木马等恶意程序；
d） 设备软件和补丁不存在已知漏洞，或对已知漏洞具备补救措施。
网络设备的整机软件宜符合以下软件完整性要求：
a） 网络设备整机供应商随设备软件版本发布数字签名，并提供签名验证机制或配套流程；
b） 在设备软件更新时校验软件的数字签名，且校验不可关闭；
c） 在设备启动时校验软件的数字签名，且校验不可关闭。

6.3.2.2 硬件供应安全

网络设备核心芯片指路由器、交换机、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统等设备中负责网络报文处理的转发/交换芯片、Wi-Fi基带芯片，以及负责网络设备系统管理控制的CPU。各网络设备的核心芯片见表1。

注1：转发/交换芯片是网络设备用于报文转发交换处理的芯片，以及框式网络设备交换网板交换芯片的统称。
注2：Wi-Fi基带芯片是用于处理和传输符合IEEE 802.11系列标准的无线信号的芯片，实现设备间的无线数据通信。

表1 网络设备核心芯片

核心芯片	路由器	交换机	无线局域网产品		防火墙	抗拒绝服务攻击产品	入侵防御系统
			无线局域网AC	无线局域网AP			
CPU	√	√	√	√	√	√	√

核心芯片	路由器	交换机	无线局域网产品		防火墙	抗拒绝服务攻击产品	入侵防御系统
			无线局域网AC	无线局域网AP			
转发/交换芯片	√	√	√	—	—	—	—
Wi-Fi基带芯片	—	—	—	√	—	—	—
FPGA	√	√	√	—	√	√	√
注1：“√”表示是相关网络设备的核心芯片，“—”表示不涉及。 **注2**：上述核心芯片可以集成在SoC上，也可以是独立芯片。 **注3**：如FPGA未作为转发交换或协处理器功能使用，或整机未使用FPGA芯片，则不作要求。							

为确保安全可控，网络设备及其核心芯片供应商符合以下要求：

a） 网络设备整机供应商应提供网络设备核心芯片品牌和型号，防范核心芯片供应商出现因政治、外交、贸易等非技术因素导致产品和服务供应中断的风险；

b） 核心芯片供应商应具备芯片设计能力和知识产权。

参 考 文 献

[1] GB/T 18018—2019 信息安全技术 路由器安全技术要求
[2] GB/T 20281—2020 信息安全技术 防火墙安全技术要求和测试评价方法
[3] GB/T 21050—2019 信息安全技术 网络交换机安全技术要求
[4] GB/T 33565—2024 网络安全技术 无线局域网接入系统安全技术要求
[5] GB/T 36342—2018 智慧校园总体框架
[6] GB/T 36630.1—2018 信息安全技术 信息技术产品安全可控评价指标 第1部分：总则
[7] GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南
[8] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[9] GB 40050—2021 网络关键设备安全通用要求
[10] GB/T 41267—2022 网络关键设备安全技术要求 交换机设备
[11] GB/T 41269—2022 网络关键设备安全技术要求 路由器设备
[12] T/SSIIA 001—2024 信息技术应用创新 数据通信网络设备技术要求
[13] 高等学校数字校园建设规范（试行）（教科信函〔2021〕14号）
[14] 教育行业信息系统安全等级保护定级工作指南（试行）（教技厅函〔2014〕74号）