技术要求及说明

一、项目总体说明

1、本项目为交钥匙项目，由成交供应商出资建设，包括相关货物的供货、运输、安装调试，线缆布设施工等，建设完成后、协议期内负责日常维护、服务收费。

2、供应商根据所报方案所需软硬件设备、线缆耗材及施工、运营维护服务等情况自报基础投资额，同时在响应文件中提供投入与收益分析，详细列明各项投入与收益金额的计算过程，并进行对比（格式自拟）。

3、标注“▲”的为重要技术参数。

4、分包明细表中“是否允许进口”标记为“是”的均允许进口产品参与报价，但不限制国内同类产品；标记为“否”的不允许进口产品参与报价。

5、本项目产品功能要求中的所有名词（除国家标准、行业标准已规定的之外），仅代表采购人对功能的需求，不代表该功能的名称被指定。

6、设备、软件的各功能模块划分，仅代表系统架构和系统实现的一种合理组合，供应商可提供覆盖本项目技术需求的其他架构软件或模块组合后的产品进行报价，并逐条列明参数响应情况，单条参数主要功能相似即可。

7、参数中如涉及某产品的个性描述，均不作为对报价产品的特定要求，仅作为最低要求。供应商可提供相当于或者优于该产品参数的产品。

8、参数若涉及国标、行标等标准或者规范，如有最新版按最新版执行。

二、分包明细表

包号	分包名称	是否允许进口
A	长城路校区无线网建设与服务	否

三、基本要求

1、长城路校区无线网要求建设全光网络，免费提供出口带宽不低于 20G（单条带宽不低于 10G），并能以 1G 为单位按需增加出口带宽，确保网络带宽月均利用率不超过 80%；其中从核心机房到校内各楼宇不低于 10G 光纤线路，从楼宇内汇聚到各接入点不低于 1G。

2、该无线网络的设备要求全面支持并使用 IPv6，要求满足 WiFi6 或以上无线网络标准，支持目前主流的手机、笔记本电脑、平板电脑和台式机使用该无线网络。

3、项目建设提供的网络设备，包括核心设备、无线控制器、汇聚或接入设备要求使用同一品牌。

4、本项目采用的涉及用户数或许可数的所有软、硬件，要求许可数量至少满足2万用户、每用户允许三台设备同时在线的条件，具体如：

独立无线AC需要同时管理AP数量不低于7000个，要求双机保护，可以多组AC同时工作，同时配备不低于7000个AP的管理授权，无线认证平台需要支持最大60000个终端同时在线。

5、项目建设需详细进行实地勘察，确保各场所（各楼宇的所有房间、室外涉及体育场、篮球场、北运动场、中心广场、主干道及班车候车点等）都有设备及较好的信号覆盖，同时要求楼宇内的所有AP布放都要入室，AP都有相应网络接口，必要时作为有线网络使用，教室、报告厅、会议室等人员密集区域需根据规模布设多台设备，教学楼走廊、门厅等部位需要全覆盖。供应商应承诺根据采购人发展，为采购人新建楼宇和场所提供新的网络接入设备，保证这些场所的联网需求。

6、本项目建设长城路校区无线局域网，要求配套建设相应的网管系统，能有效管理整个系统的设备。系统产生的数据归采购人所有，未经采购人同意，成交供应商不得私自向第三方提供校园网用户信息，确保数据安全；同时要求建设相应的网络安全管理系统，防火墙、上网行为管理、多元组的日志采集及审计设备，满足用户访问的完整日志记录存放至少6个月的数据存储空间且有冗余，网络安全设备除了防范外部攻击或外部木马病毒的入侵，还要重点关注内部用户中毒、中木马或主动向外的攻击，能够有效定位并采取阻断措施。本项目设计的各系统或平台提供免费对接及开发服务，可以和学校现有管理平台进行对接，实现网络的统一管理管控。

7、响应文件提供详细的整体设计方案（含详尽的网络拓扑），具体接入点详细点位，要有所有设备（含软件）的清单（包含设备品牌、名称、型号、主要性能参数、单价以及综合布线的方案、线路图、使用各种线缆的品牌、型号、参数性能、单价及预算长度等）及总价，有详细的施工方案及日期进程安排，确保与现有合同的有效衔接，能承诺给原来的网络用户办理免费转网，确保学生权益和使用的无感过渡。成交后，供应商提供深化设计方案，报经采购人相关部门审核签字同意后实施。

8、采购人对此校企合作服务项目实行严格的考核机制与退出机制，通过招标确定合作方后，与采购人签署正式合同，合同约定（签订合同之日起开始计算）协议期为5+3年。采购人每协议年度末按考核标准对成交的合作方进行考核，年内考核不合格，依照退出机制采购人有权终止协议，责令成交供应商退出，整套无线网络设备及系统由采购人接手使用，前五年考核均合格，且满足继续良性运营条件的前提下，则协议继续执行三年，每年仍按考核标

准及退出机制执行，考核标准与退出机制详见附件1。

9、建设完成后由成交供应商负责运营维护，采购人负责综合管理和监督，且拥有成交供应商投资建设的各类软硬件资源的长期无偿使用权；成交供应商需日常派驻至少2名网络维护工程师提供驻场维护维修服务，驻场工程师的管理、薪资以及人力资源部门规定的保险等有成交供应商承担，成交供应商应加强运维人员的安全管理和培训，尽量避免发生人身伤害等安全问题，驻场期间发生的人身伤害等由成交供应商负责，学校不承担任何责任。

10、成交供应商需建设统一的校园网络运营管理体系，能与学校的网络以及与多家市场主流运营商（包含但不限于电信、联通、移动）基于此平台进行认证运营对接，对接或运行的费用问题有合作方与对接方协商确定。服务中提供的校园网络应实现基于用户属性的自动路由策略，即用户在使用互联网时能根据用户注册时选定的运营商自动选择出口线路。当校园网管理要求变动时，如特殊时期的网络资源管控等，成交供应商应及时作出调整。确保教职工通过该无线网络上网访问互联网免费，师生通过该无线网络访问校园网网内资源免费，学生上网访问互联网资费不高于同期同类其他高校标准。

11、为保证项目落实，成交供应商在签订合同前需向采购人缴纳50万人民币作为履约保证金。无线网建成并验收合格后，无息退付履约保证金。

12、成交供应商须提供园区光缆链路和室内综合布线等相关施工，具体要求为：

（1）楼宇之间敷设不少于24芯的单模光缆进行连通，其中学生宿舍区各宿舍楼及物业楼、餐厅就近汇聚到樱花园汇聚机房；放射楼、体育场、大学生活动中心就近汇聚到行政办公楼；国教学院各楼汇聚一条到荷园；樱花汇聚机房、行政办公楼、教学南楼、教学北楼、综合实验楼、物理楼、化学楼、荷园等分别敷设一条光缆连通到网络中心机房。

（2）室外无线信号发射点位的光缆由就近的楼宇敷设不少于8芯的光缆进行连通（单模或多模根据具体设备的需要确定）。

（3）各楼宇内根据设备型号采用配套的光缆、电缆或光电复合缆进行综合布线，充分利用楼内配电间、管廊、桥架等将信号链路接入室内。

（4）本项目统一组织现场踏勘。供应商根据踏勘情况，在响应文件中提供具体线缆敷设线路图和施工方案，方案中细化具体使用的各种线缆材料的品牌、型号、性能参数以及估算其长度等，对整个综合布线施工工程进行报价，作为项目总报价的一部分。成交后，供应商须深化线路图及施工方案，提供详细工程量清单及施工图纸，报经采购人相关部门审核签字同意后方可进场施工，监理公司实施监理。

（5）室外光缆建成后，采购人拥有长期无偿使用权。

（6）供应商需在响应文件中明确项目负责人，如施工过程有变更，项目负责人须签字确认。

四、项目设备、系统、平台等技术参数及数量要求

序号	设备名称	技术参数	单位	数量
1	核心区核心交换机	1、交换容量≥3800 Tbps，包转发率≥460000 Mpps； 2、支持主控板槽位数≥2，独立交换网板数≥6，业务板槽位数≥12，风扇槽位数≥3，电源模块槽位数≥8，严格前后风道设计，支持主控、网板、风扇框、电源、电源总开关等关键器件冗余设计； 3、采用 CLOS 无中板交换架构； 4、支持在 IPv4、IPv6 协议栈下通过微分段 EPG/组策略实现 ServiceChain，满足全软数据中心服务链调用特性； 5、支持 IPv4/IPv6 硬件 BFD，最小时间间隔为 3ms，支持 sflow 类流量统计和分析功能； 6、支持基于 IPv4/IPv6 Underlay 的 VxLAN 三层 Anycast 分布式网关，支持 VXLAN VRF 的数量≥4K，VSI（VNI、VXLAN Bridge Domain）数量≥64K； 7、支持 COPP，支持 CPU 保护，支持 ARP 防攻击，支持自动防御，支持 IP source guard（MAC 地址攻击防范），支持 Attack source tracing，支持 DAI，支持 DDOS 攻击防御，支持 ND Snooping，支持协议报文黑名单； 8、本次实配：主控≥2，交换网板≥2，40G 端口≥4，万兆光口≥48，≥3 个电源，≥3 个风扇，40G 堆叠线缆≥1 条。	台	2
2	智能运维管理平台	1、平台支持整体网络健康度监控； 2、平台支持分析网络问题，可识别问题，包括接入类、认证类、IP 地址类、漫游类、无线信号类、无法上网类、上网慢类、无线环境类、设备类问题，部分问题支持自动优化，并记录优化日志； 3、平台支持告警功能，支持多种告警方式，可通过微信、短信、邮件、钉钉、企业微信推送告警消息，告警时间、告警类别、告警阈值都可自定义； 4、平台支持一键诊断功能，针对设备的多个指标进行诊断，对有问题的诊断项提供修复建议； 5、平台支持 AP、终端连接分析，可查看连接记录，认证失败终端、上线失败终端的失败原因，支持解析功能，可查看终端上下线的详细报文交互，定位终端再上线失败原因； 6、平台支持快速定位故障，可快速模糊搜索故障终端、AP，查看其接入平台后的日志，日志中可查看发生问题的时间，可查看该 时间点 AP 和终端的详细参数，包括重传率、丢包率、时延、信号强度、信道利用率等； 7、平台支持 WIPS 功能，支持攻击检测、SSID 扫描、仿冒 MAC	套	1

序号	设备名称	技术参数	单位	数量
		检测功能，攻击检测支持畸形报文、蜜罐 AP、泛洪攻击、AP 扮演者攻击等多种检测项； 8、平台支持无线终端统计功能，支持终端接入趋势图、总流量趋势、人均流量趋势、平均接入时长、接入时长占比、接入次数占比、终端统计、基于接入 SSID 统计等； 9、移动客户端支持远程管理，并且可以修改交换机网络配置。 ▲10、移动端提供多种远程运维小工具，包括重启设备、升级版本、配置备份还原、文件管理等； 11、移动端支持点位验收功能，将不同点位的 wifi 检测数据上报云平台，生成点位验收报告，点位验收数据包括信号强度、频段、潜在 信道干扰数、网关时延、网络时延、wifi 质量评分等； 12、移动端支持网络监控功能，支持设备运行信息、端口状态等监控，支持 AP 流量、接入终端数、离线监控，支持终端接入趋势、驻留时长等监控，可查看告警消息。 13、有线设备运维授权：实配≥100 个网络设备授权，≥1600 个无线 AP 管理授权，≥5400 个 PON AP 设备管理授权。		
3	无线控制器	1、吞吐≥160G，管理 AP 数≥10240； 2、为了满足设备的稳定性，要求所投产品满足双电源冗余供电； 3、满足雷达检测 SSID 逃生功能：AC、AP 满足 SSID 自主逃生，当 AP 射频检测到雷达信号时，会将本射频的 SSID 迁移到其他射频，保障关键业务正常通信； 4、满足 Portal 在线用户与 DHCP 租约联动功能：AC 满足根据 DHCP 租约信息联动 Portal 用户自动下线； 5、满足防 PSK 暴力破解，当用户密码错误超过预设的阀值之后，能够将该用户加入动态黑名单，一段时间内禁止其接入网络； 6、满足 1+1 热备，对外呈现一个 IP 地址； 7、能够有效拦截 Protal 用户重定向攻击； ▲8、本次实配：两台控制器做主备可靠性设计，无线 AP 总授权≥7000；两台控制器可共享 AP 授权。满足任意一台设备宕机后不影响整个无线网络使用。如无法共享 AP 授权，需每台单独配置足量授权。 9、千兆电口≥8，万兆光口≥8，QSFP+端口≥2，万兆多模光模块≥8，电源≥2。	台	2
4	出口防火墙	1、采用多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块； 2、吞吐量不低于 45Gbps，并发连接数至少 4000 万，新建连接数至少 40 万，开启 IPS 及 AV 后，吞吐性能至少 20 Gbps； ▲3、实配：≥8 个千兆电口，≥8 个万兆光口，≥8 个千兆光口，≥4 个千兆 combo 口；内存≥32G，≥2 个风扇，≥2 个交	台	1

序号	设备名称	技术参数	单位	数量
		流电源，AV 防病毒安全 License，IPS 特征库升级服务； 4、支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析,支持基于应用风险的策略调优,可根据流量、应用、风险类型等细粒度展示； 5、能够防范 DOS/DDOS 攻击：Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、SYN Flood、ICMP Flood、UDP Flood、HTTP Flood（cc）攻击、ARP 欺骗、TCP 报文标志位不合法、超大 ICMP 报文、地址扫描的防范、端口扫描的防范、DNS Flood、ACK Flood、FIN Flood、分片 Flood、Tiny-Fragment； 6、支持流量自学习功能,可设置自学习时间,并自动生成 DDoS 防范策略； 7、HA Track 方式支持 BFD/NQA/接口/路由多种类型，支持 Track 检测链路状态，来及时触发链路切换； 8、支持一对一、多对一、多对多等多种形式的 NAT，支持 DNS、FTP、H.323、RTSP、ILS、PPTP、SIP、SQLNET、MGCP、RSH、ICMP 差错报文、TFTP、RTSP、SCTP、XDMCP、NBT、SCCP、HTTP 等多种 NAT ALG 功能； 9、支持 DNS 透明代理功能，可基于负载均衡算法代理内网用户进行 DNS 请求转发,避免单运营商 DNS 解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。		
5	48 口光主机	1、交换容量≥12Tbps，包转发≥600Mpps； 2、支持 IPv6 静态路由、RIPng、OSPFv3、ISISv6、BGP4+； 3、支持 SAVI 功能； 4、支持 EVPN 分布式网关二三层互通功能； 5、支持跨设备链路聚合技术 DRNI/M-LAG； 6、支持全端口 MACsec 加密功能； 7、支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2； 8、支持 SNMP V1/V2/V3、RMON、SSHV2； 9、支持 OAM(802.1AG，802.3AH)以太网运行、维护和管理标准；10、实配：千兆光口≥48，万兆光口≥4，40G 端口≥2，支持≥48 个 PoE++接口,具备对外光电混合缆供电能力。	台	25
6	24 口光主机	1、交换容量≥12Tbps，包转发≥500Mpps； 2、支持 IPv6 静态路由、RIPng、OSPFv3、ISISv6、BGP4+； 3、支持 SAVI 功能； 4、支持 EVPN 分布式网关二三层互通功能； 5、支持跨设备链路聚合技术 DRNI/M-LAG； 6、支持全端口 MACsec 加密功能； 7、支持 IGMP Snooping v1/v2/v3，MLD Snooping v1/v2； 8、支持 SNMP V1/V2/V3、RMON、SSHV2； 9、支持 OAM(802.1AG， 802.3AH)以太网运行、维护和管理标准；	台	16

序号	设备名称	技术参数	单位	数量
		10、实配：≥24 个 1G/2.5G SFP，，万兆光口≥6，支持≥24 个 PoE++接口具备对外光电混合缆供电能力。		
7	8 口 POE 交换机	1、固化≥8 个千兆 POE 电口，≥2 个千兆光口； 2、交换容量≥3Tbps，包转发≥100Mpps； 3、支持 802.3x 流控及半双工背压流控； 4、支持静态、动态、黑洞 MAC 地址； 5、支持多控制器（EQUAL 模式、主备模式）； 6、支持 802.1Q VLAN。	台	11
8	光 AP 下行 4 口	1、采用整机双频 4 流设计，可同时工作在 802.11a/b/g/n/ac/ac wave2/ax 模式，整机协商速率≥ 2.975Gbps，其中 5G 射频速率≥2.4Gbps，2.4G 射频速率≥ 0.575Gbps。 2、满足壁挂、吸顶和面板安装方式； 3、在网络拥塞情况下，通过对终端发送的报文进行识别，在多业务并行处理时，可以对关键业务（如视频会议、时延敏感类游戏等）优先处理从而实现应用加速。 4、在自动功率调整基础上，支持检测信号覆盖黑洞功能，并对 AP 功率做出修正，保证处于特殊位置的终端接收到增强的 AP 信号； 5、本次实配：≥1 个 2.5G SFP，≥4 个 10/100/1000M 电口。	台	456
9	放装光 AP	1、采用整机双频 4 流设计，可同时工作在 802.11a/b/g/n/ac/ac wave2/ax 模式。 2、整机协商速率≥2.975Gbps，其中 5G 射频速率≥2.4G，2.4G 射频速率≥0.575G。 3、固化接口数≥2 个，包括 1 个 100/1000M/2.5G 光口，1 个 10M/100M/1000M 电口。 4、支持内置 BLE 不低于 5.0 功能模块。 5、满足光、电同时上行且满足上行链路备份功能。 6、在 5GHz 关联 30 个真实终端，2.4GHz 关联 20 个真实终端，即整机关联 50 个真实终端的情况下，整机无线转发总性能可达到 750Mbps。	台	518
10	高密 AP	1、三频六流，可工作在 802.11a/b/g/n/ac/ac wave2/ax 模式，接入速率≥5.375Gbps； 2、支持外置物联网模块链式扩展，支持内置 BLE 不低于 5.0 功能模块； 3、在 AP 的每个射频各接入 1 个 WiFi6 真实终端，整机无线转发总性能极限可达到 2.2Gbps 以上； 4、在自动功率调整基础上，支持检测信号覆盖黑洞功能，并对 AP 功率做出修正，保证处于特殊位置的终端接收到增强的 AP 信号。 5、本次实配：≥1 个 2.5G 光电合一接口，≥2 个 10/100/1000Mbps 电口。	台	38

序号	设备名称	技术参数	单位	数量
11	单光口AP	1、采用整机双频4流设计，可同时工作在802.11a/b/g/n/ac/ac wave2/ax模式，整机协商速率≥2.975Gbps，其中5G射频速率≥2.4Gbps，2.4G射频速率≥0.575Gbps。 2、满足壁挂、吸顶和面板安装方式； 3、在网络拥塞情况下，通过对终端发送的报文进行识别，在多业务并行处理时，可以对关键业务（如视频会议、时延敏感类游戏等）优先处理从而实现应用加速。 4、在自动功率调整基础上，支持检测信号覆盖黑洞功能，并对AP功率做出修正，保证处于特殊位置的终端接收到增强的AP信号，； 5、本次实配：1个2.5G SFP，1个10/100/1000M电口。	台	406
12	WIFI7 AP	1、支持802.11be/ax/ac/n/a 标准 2、整机采用双频四流设计，整机最大接入速率8.647Gbps， 3、1个射频支持6GHz/5GHz频段切换，采用2空间流，最大可协商速率5.765 Gbps，另1个射频支持5GHz/2.4GHz频段切换，采用2空间流，最大协商速率2.882Gbps。 4、配置≥1个1000M/2.5G/5G/10G电口，≥1个10G SFP光口，≥1个10/100/1000M电口,支持光电混合缆方案,支持802.3bt供电 5、支持基于流量的负载均衡，支持基于频段的负载均衡	台	10
13	40G单模光模块	QSFP+ 40G光模块(1310nm,10km,LR4,LC)	块	8
14	万兆模块	SFP+ 万兆模块	块	152
15	千兆光模块	光模块-SFP-GE-模块	块	3000
16	OLT设备	▲1、主控交换容量：≥9Tbit/s，每业务槽位最大带宽：480Gbit/s，业务扩展槽位≥10个，主控槽数量≥2，电源模块数≥4； 2、实配：冗余主控、冗余模块化电源，万兆PON口≥192个，SFP+端口≥16个，千兆光口≥24个，≥174个5dB光衰器，≥174个1分32分光器，万兆多模光模块≥8； 3、支持OLT帧过滤功能：OLT应支持基于端口或MAC地址的数据帧过滤功能； 4、支持内置智能图形化管理功能； 5、支持SDN纳管； 6、支持端口隔离； 7、支持ARP防攻击； 8、支持VLAN。 9、支持HQoS五层调度功能IPv4 和IPv6 双栈、IPv6 二层和	台	1

序号	设备名称	技术参数	单位	数量
		三层转发。 10、支持 OSPF/RIP/IS-IS/BGP。		
17	AP 设备	要求提供企业级 AP 产品，非家庭用 AP 产品。 1、PON 口（网络侧）：≥1 个 10G PON 接口 2、UNI 侧（用户侧）：≥4*GE，≥1*USB2.0; 3、具备 WIFI6 功能，采用整机双频 4 流设计，可同时工作在 802.11a/b/g/n/ac/ac wave2/ax 模式，接入速率≥2.975Gbps，空口速率：574 Mbit/s(2.4G)，2402 Mbit/s(5G)。 4、支持链路加密; 5、支持以太网数据流分类和优先级标记; 6、支持 802.1p、DSCP 优先。 7、支持无线控制器统一集中管理与调优。	台	5000
18	分光器	分光器及配套分光箱。分光比不得高于 1:32。	套	根据终端数
19	pon 光模块	万兆 OLT 光模块(1577nm,TX10G/RX10G,20km,SC/PC)	块	175
20	室外定向 AP	1、为保证整机接入用户数，要求 AP 采用双频四流设计，可同时工作在 802.11a/b/g/n/ac/ac wave2/ax 模式，接入速率≥2.4Gbps; 2、要求采用内置高增益定向天线设计，且满足外置天线; 3、采用 WiFi 6 2*2 MIMO 终端，接入 5GHz 频段 80MHz; 4、采用 WiFi 6 2*2 MIMO 终端，接入 2.4GHz 频段 40MHz; 5、支持外置物联网模块链式扩展; 6、在自动功率调整基础上，支持检测信号覆盖黑洞功能，并对 AP 功率做出修正。 7、本次实配：≥1 个 1000M SFP 光接口，≥2 个 10/100/1000M 电口。含配套的光纤 PoE 供电器及光模块。	台	30
21	室外全向 AP	1、为保证整机接入用户数，要求 AP 采用三频十流设计，可同时工作在 802.11a/b/g/n/ac/ac wave2/ax 模式，接入速率≥5.375Gbps; 2、支持外置物联网模块链式扩展; 3、要求采用内置智能天线设计，支持内置物联网 BLE（蓝牙）; 4、内置 GPS/北斗模块。 5、采用 WiFi 6 2*2 MIMO 终端，接入 5GHz 频段 80MHz; 6、采用 WiFi 6 2*2 MIMO 终端，接入 2.4GHz 频段 40MHz; 7、本次实配：≥1 个 100/1000M/2.5G/5G/10G 以太网接口，≥2 个 10/100/1000M 电口。 含配套的光纤 PoE 供电器及光模块。	台	20
22	认证计费系统	1、支持基于 B/S 方式进行操作管理端和用户自助端; 2、认证服务满足服务期内学校全部开户用户，用户授权数量≥32000。	套	1

序号	设备名称	技术参数	单位	数量
		3、支持集群部署模式，当集群发生故障时，可以确保业务系统能够正常运行； 4、为保证校内业务系统的安全，防止非法用户接入，服务系统需实现用户接入校园网先进行准入身份认证；为保证用户访问互联网行为的管控，实现用户访问互联网进行准出身份认证；且准入准出为一体化认证，不接受二次认证方式，认证方式实现有线的 802.1x、WEB 认证，无线用户实现 WEB、基于用户身份的无感知认证（非 MAC 认证方式）；实现无线用户的二维码访客认证； 5、支持用户初次登陆的时候获取信息并自动绑定；支持有线接入情况下帐号与 IP、MAC、接入交换机 IP、端口的绑定；支持无线接入方式下帐号、用户 MAC、APMAC 绑定、SSID 绑定、无线交换机 IP 绑定； 6、支持根据用户的 IP、NASIP 进行区域的划分，控制用户可以在哪些指定的区域上网； 7、支持有线、无线的客户端接入认证，支持基于 Web 的有线和无线接入方式，支持不同区域的无感知认证； 8、多链路下支持指定用户路由策略，支持按用户设定不同的出口带宽策略； 9、支持自动数据库维护（如：自动备份，异地备份），同时满足用户在线信息出现残留后，无需管理员干预，相同用户名的后一次认证能成功上线； 10、为便于学校门户页面等系统的推广，要求支持客户端强制弹出指定 URL； 11、支持访客授权二维码认证，支持访客账户信息对应接待人员账号； 12、配置硬件服务器及运营商对接组件。		
23	Portal 系统	1、支持多种业界主流浏览器进行 web 认证； 2、支持在线保活功能，动态检测用户在线情况； 3、支持认证登录页面的 LOGO 定制化，支持最多导入多个背景图片而且不限制定制页面的大小； 4、支持主页重定向功能，用户认证后除了可以弹出保活页面，还可以重定向到学校的主页上； 5、提供配套服务器。	套	1
24	智能防共享系统	1、支持对 360 随身 WiFi、猎豹 WiFi 系列、小度随身 WiFi、毒霸免费 WiFiConnectfy、NAT 代理(RP-link)、WiFi 共享精灵、Windows 系统自带共享代理等进行检测，并与认证计费系统进行联动封控； 2、支持 MAC OUI、DHCP、HTTP User-Agent 等终端类型判断方法按优先级智能分析； 3、支持互联网常见应用协议识别，支持即时通讯，网页，邮件，P2P 等；	套	1

序号	设备名称	技术参数	单位	数量
		4、防代理类型：路由防代理、代理软件防代理、系统自带共享防代理、免费 WiFi 类软件防代理、随身 WiFi 设备防代理等。		
25	路由器	1、支持主控板、业务板完全物理分离，支持分布式转发架构，所有线卡均有业务处理和转发能力； 2、交换容量≥195Tbps，包转发率≥38400Mpps； 3、整机框全物理尺寸的线卡槽位数≥8（非子卡槽位），交换网个数≥4 个； 4、支持将两台物理设备虚拟化为一台逻辑设备，虚拟组内可以实现一致的转发表项,统一的管理,跨物理设备的链路聚合。 5、支持 SR/SRv6、FlexE、iFIT、Netconf 等技术，具备完善的 SDN 能力，支持 BRAS 功能，支持代拨功能，满足学校代拨需求。 6、设备支持硬切片的 SDN 自动化管理功能、自由调整切片所经物理链路，设备支持硬切片间的流量调优功能、SRv6 业务承载在网络硬切片上。 ▲7、设备支持通过五元组识别确定性业务，支持同一接口下确定性流和非确定性流同时承载。 8、配置≥2 个独立主控，配置≥2 个交换网板，配置≥2 个电源模块，配置 1 块 BRAS 业务板，整机配置万兆光接口≥12 个，配置千兆以太网光接口≥12 个。	台	1
26	便携式终端	1、第 13 代智能英特尔® 酷睿™ i7-13620H； 2、NVIDIA® GeForce RTX™ 4050 显卡； 3、32 GB LPDDR5 内存； 4、1 TB 固态硬盘； 5、14.0 吋屏幕 2.5K (2560X1600) 90Hz。 6、预装 win11 正版操作系统软件	台	2
27	5G 专网融合接入平台	1、与运营商 5G 虚拟专网/5G 双域网的融合认证功能，实现通过 5G 虚拟专网/5G 双域网免二次认证访问校园网，支持在运营商接入环境下对 5G 校园网用户进行实名认证、实名审计、资源访问控制； 2、与学校智慧校园对接实现实名认证、审计，与学校认证计费系统与统一身份认证系统对接，实现校内访问一次认证； 3、与运营商 UPF/SMF 设备对接，实现 5G 校园专网准入； 4、带宽处理能力≥20Gbps，1 个串口，冗余交流电源；； 5、支持 5G 基站一跳分流，实现数据不出客户场地； 6、支持二层帧数据、分组数据包的路由、转发功能； 7、支持 GTL-U 分组数据的解析功能，可进行 GTL-U 分组的解包、封装； 8、支持 NAT 功能，5G 专网本地分流时，可将 5G 专网终端用户 IP 转换为企业内网 IP； 9、定义本地流量转发规则，可根据 5G 终端 PLMN、DNN、目的 IP、协议类型及端口等信息对本地流量进行控制；分流规则定	台	1

序号	设备名称	技术参数	单位	数量
		义后，可实现随时下发随时生效。		
28	主动威胁诱捕系统	1、场景化蜜网：支持自定义添加多个蜜网模拟真实网络区域。支持在蜜网内添加多个蜜罐服务，同一蜜网内的蜜罐可以互相连通。 ▲2、系统服务伪装：蜜罐支持伪装 SSH、Telnet、Samba、Remote Desktop、FTP、VPN 服务。蜜罐受到攻击后，可以查询完整的连接建立与断开记录、用户密码登录记录、用户密钥登录记录、命令执行记录、文件遗留记录等。 3、数据库服务伪装：蜜罐支持伪装 MySQL、MongoDB、Redis、PostgreSQL、Memcached、Microsoft SQL Server、MariaDB、Oracle Database、Elasticsearch 服务。蜜罐受到攻击后，可以查询连接建立与断开记录和完整的数据库操作记录。 4、蜜罐支持伪装 Jenkins、Joomla、Jboss、Wordpress、Webmin、Zabbix、Wiki、CRM、OA、企业邮箱、堡垒机、WAS、HRM、RouYi、phpMyAdmin、Solr、RabbitMQ、Apollo、Nexus3、Druid、Metabase、YApi、Grafana、Vmware ESXI 等服务或中间件。蜜罐受到攻击后，可以记录访问请求、Web 攻击和账号密码登录等事件。 ▲5、特殊缺陷伪装：蜜罐支持伪装 Shellshock、Eternalblue、Struts2、Tomcat、Shiro、Weblogic、Coremail、Fastjson、负载均衡、VMwarevCenter、RMI 反制、NBR 路由器等存在漏洞的服务，并可以通过 POC 验证。 6、操作系统伪装：支持运行模拟 300 种以上服务指纹信息的蜜罐。蜜罐受到攻击后，可以查询完整的连接建立与断开记录。 7、工控协议伪装：蜜罐支持伪装 Modbus/TCP、IEC104、IEC61850、S7、OPCUA 等工控协议。蜜罐受到攻击后，可记录攻击事件。 8、5G 核心网元伪装：蜜罐支持伪装 AMF、SMF、AUSF、NRF 等 5G 核心网元。蜜罐受到攻击后，可记录攻击事件。 9、自定义页面蜜罐：支持上传网站页面和数据库文件生成 Web 类蜜罐，当蜜罐受到攻击时，可记录 Web 攻击事件。 10、自定义蜜罐模版：支持通过蜜罐模版修改蜜罐的页面信息、用户名密码、数据库数据等内容。 11、Web 类业务学习式蜜罐：支持运行学习真实 Web 类业务服务的蜜罐。蜜罐受到攻击后，可以记录访问请求、Web 攻击和账号密码登录等事件。 12、TCP 业务学习式蜜罐：支持运行学习真实的基于 TCP 协议的业务服务的蜜罐。蜜罐受到攻击后，可以查询完整的连接建立与断开记录。 13、HTTPS 访问蜜罐：支持上传蜜罐证书。支持以 HTTPS 的方式访问 Web 类蜜罐。 14、Web 攻击记录和语义分析：具备自主研发的语义分析引擎，	套	1

序号	设备名称	技术参数	单位	数量
		可以感知攻击者对 Web 类服务蜜罐发起的攻击请求，并智能识别其 Payload 攻击类型和威胁等级。 15、蜜罐流量下载：支持实时记录蜜罐访问流量，并支持 PCAP 格式下载。 16、命令执行记录：系统服务蜜罐支持记录攻击者的 Bash 命令及其参数。 17、数据库攻击记录：支持记录攻击者在数据库蜜罐中的增、删、改、查操作。 18、文件变动记录：支持监控蜜罐内文件的新增、修改、删除，并支持变更文件的下载。 19、Docker 逃逸检测：支持检测攻击者从蜜罐 docker 逃逸的行为，并实时告警。 20、Git 反制：支持 Git 反制功能，能在 Web 蜜罐上伪装 Git 源码泄漏缺陷。能监控源码泄漏扫描和攻击行为。能实现对对应攻击机器的反制，读取攻击设备的主机名称、邮箱、文件等信息。 21、支持仿真蜜罐，支持对真实业务网站的静态资源、动态接口进行仿真学习，以生成具备一定交互能力、支持二次开发、支持溯源反制的仿真蜜罐。 22、2U 设备，内存≥64G，硬盘≥4T,≥2 个千兆电口，支持同时开启 50 个蜜罐。		
29	网络风险资产分析系统	1、支持 Http 基础认证登录、自动识别 URL 认证登录、Https 证书登录、Cookie 认证登录； 2、支持远程扫描，采用 SSH 协议对 Windows、Linux 等系统进行登录扫描； 3、支持常用端口检测端口列表快速发现目标资产；支持自定义 TCP、UDP 的端口检测范围； 4、支持基于系统扫描的结果，下发 Web 深度扫描任务，能够针对 Web 和系统扫描的结果深入的进行风险综合分析； 5、支持通过递归方式对域名进行弱口令爆破的功能； 6、支持针对域名资产进行扫描； 7、支持通过全球地图的方式展示不同单位的资产数量分布情况；支持通过资产总数、资产存活情况、资产风险等级、资产指纹（端口开放情况、服务程序、应用中间件、操作系统等）、各业务系统资产分布等多维度分析资产情况； 8、支持多维精确或模糊匹配查询定位相关资产，如 IP 地址、操作系统、资产名称、资产所属组织单位、设备系统、网络区域、业务系统、负责人、端口服务、应用及版本号、存活性、资产风险等级等； ▲9、支持通过漏洞名称、漏洞编号、漏洞风险等级、漏洞修复状态等漏洞维度，对受影响的全部资产进行查询，定位相关资产；	套	1

序号	设备名称	技术参数	单位	数量
		10、支持自定义资产展示列表的资产产指纹、风险、管理等相关属性，支持查看资产信息包括但不限于负责人、业务系统、风险风级、漏洞数量、主机名、端口、协议和服务、Web 站点、开发语言、CMS、WAF 识别等维度。； 11、持资产详情展示，包括且不限于负责人、组织单位、标签、资产指纹、端口情况、最近扫描任务等。支持端口服务近 5 次的存活情况的展示； 12、支持按天、周、月和资产的新增存活、新增不存活、波动变化的维度筛选主机资产； 13、批量任务下发：支持划分不同的下级单位，为每个单位设置不同的用户权限，支持统一的为各下级单位下发资产风险检查任务； 14、支持扫描任务结束自动提醒，通过邮件的方式实时或定时的将报告动态发送给管理员； 15、内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、web 指纹等）、漏洞（修复方案、CVSS 评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选； 16、支持 Open API，可通过接口调度任务和同步扫描数据； 17、系统支持自定义企业、产品等基本信息，支持替换公司名称、产品名称、版权信息、官方跳转 URL、系统 logo 等； 18、支持针对扫描任务，任务结果、资产数据信息、漏洞数据信息、日志审计信息等进行数据备份和还原。支持每周、每月、不定时的备份数据。 19、2U 设备，内存≥64G，硬盘≥4T,≥2 个千兆电口，扫描 IP 地址和扫描 Web 域名数量无限制，扫描任务并发数无限制。		
30	审计日志管理网关	1、双向带宽处理能力≥40Gbps； 2、支持桥接和路由部署模式； 3、日志同时支持数据库和文件两种保存方式； 4、支持与认证计费系统联动同步 IP 和账号； 5、支持指纹组合模式分析终端类型； 6、支持 MAC OUI、DHCP、HTTP User-Agent 等终端类型判断方法按优先级智能分析； 7、支持互联网常见应用协议识别，支持即时通讯，网页，邮件，P2P 等； 8、支持 DPI 七层应用识别，页面可由图表显示识别结果； 9、支持按应用协议统计出口流量使用情况； 10、支持按应用分类统计出口流量使用情况； 11、支持特征库定期升级； ▲12、支持审计日志，日志需要详细记录上网五元组和账号，时间，URL，NATIP,NAT 端口，应用类别，应用名称；	套	1

序号	设备名称	技术参数	单位	数量
		13、支持日志文件，审计日志，备份日志，系统日志自动清除功能，可定义保留天数；硬盘容量满足保存日志至少可以 6 个月以上并有冗余备份，日志文件支持自动压缩。		
31	智能 DHCP 系统	▲1、系统基于标准 DHCP 协议开发，且支持各种厂家的 DHCP 私有属性。图形化地址管理系统，毫秒级地址动态分配，支持用户自定义 DHCP OPTION；支持全局 MAC 地址黑、白名单； 2、可与计费系统进行联动，实现：三层无感知认证、不同用户组可分配指定地址段地址、取得终端特征信息，实现设备指纹识别； 3、支持配置自动备份、导入导出、手工恢复； 4、支持 IP 地址使用图形化展示，显示 IP 地址空闲、动态分配、固定分配、冲突（手工设置）等，有效的进行 IP 地址管理及分配。	套	1

注：无线信号覆盖应满足学校要求，如按照上述文件要求的设备数量不足，应根据实际情况追加适量的设备，特别如光模块和 AP 设备等。

五、线缆材料及综合布线等相关施工要求

序号	名称	技术要求	单位	数量
1	线缆材料及综合布线等相关施工	根据地勘情况确定各种线缆用量及综合布线等相关施工，根据基本要求第 12 项进行设计及预算明细报价，区分室内、室外，铺设方式等。	宗	1

附件 1

长城路校区无线网络建设及运维服务考核标准及退出机制

中标合作方在建设完成后，约定项目合作服务的协议期限为 5+3 年。期间按协议规定进行运维管理和为广大师生服务，中标合作方负责整个设备、系统的安全稳定运行。由校方按照如下考核标准，每协议年度末进行一次考核，总分 100 分，考核成绩低于 60 分或中标合作服务方出现考核表中的重大失误，则采取退出机制，学校有权解除合作协议，按协议要求所有无线网络的设备及系统收归学校无偿使用；5 年连续考核均合格，且满足继续良性运营条件的前提下，则协议继续执行三年，每年还是按考核标准及退出机制执行。

校园网建设及运维服务目标及考核标准

服务方式/项目	服务级别类型	服务级别指标	定义	分值
系统性能目标	核心交换容量	≥3800Tbps	核心性能	达不到标准扣 5 分
	核心包转发率	≥460000Mpps	核心性能	达不到标准扣 5 分
	校园无线网接入技术	支持 802.11a/b/g/n/ac/ax	无线终端兼容指标	达不到标准扣 5 分
	无线网室内覆盖范围	≥90%	服务区域内的所有楼宇（教职工宿舍除外）	达不到标准扣 5 分
	无线网室外覆盖范围	≥80%	服务区域内的所有室外区域。	达不到标准扣 5 分
	有新建筑建成使用无线网的补充扩建	≥90%	学校新建楼宇的无线覆盖	达不到标准扣 10 分
	校园网可容纳用户数	≥2 万	整网可容纳接入用户数	达不到标准扣 5 分
服务指标	用户满意度（含学生收费的评定）	≥85%	满意人数/调查总人数×100%	满意度低于 50%扣 30 分，大于等于 50%而小于 70%扣 20 分，大于等于 70%而小于 85%扣 5 分
远程支持中心	远程服务时间	7×14	每周 7 天，每天 8:30—22:30 为服务提供时间	服务时间无响应一次扣 1 分
现场服务	服务时间	6×10	每周 6 天，8:30—18:30 提供上门服务	有投诉上门服务不及时一次扣 2 分
服务响应	紧急事件响应时间	≤0.5h	接到报修到开始处理时间	超过一次扣 5 分
	紧急事件恢复时间	≤8.0h	开始处理到业务恢复	超过一次扣 3 分
	一般事件响应时间	≤2.0h	接到报修到开始处理时间	超过一次扣 2 分

服务方式/项目	服务级别类型	服务级别指标	定义	分值
	一般事件恢复时间	≤12.0h	开始处理到业务恢复	超过一次扣 2 分

注：运维期内，因中标合作方原因造成校园网无法持续运行的重大失误，如下情形之一：

1、 一个协议年度中整网连续中断时间超过 24 小时的次数大于 5 次；

2、 一个协议年度中整网连续中断时间超过 48 小时的次数大于 3 次；

3、 一个协议年度中整网连续中断时间超过 72 小时的次数大于 2 次；

4、 一个协议年度中整网连续中断时间超过 7 日；

5、 一个协议年度中整网中断时间累计超过 15 日。

校方有权解除协议，终止合作。（由不可抗力的自然因素或国家重大政策调整造成的网络中断除外）