采购需求

一、说明

1.招标文件中所要求提供的证明材料，如为外文文本的请提供中文翻译文本。

2.评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，可以要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会可以将其作为无效投标处理。

3.本采购需求中技术要求所使用的标准或应用标准如与投标人所执行的标准不一致时，按最新标准或较高标准执行。

4.招标文件中标注“▲”号的条款为实质性条款，必须满足，否则投标无效。

5.采购需求的“技术要求”中标注“★”条款为重要条款，投标文件中应提供相关证明材料，如未提供按负偏离处理。

二、技术要求

（一）管网及弱电线路改造服务

▲1.梳理及建设社湾校区的弱电主干管网资产，建设完成学校每个楼宇的房间网络接入点到校园网中心机房的点对点光纤布线并端接。

▲2.完成新建的体育馆、图书馆、国际交流中心大楼的全光弱电系统综合布线，要求每房间均配置光网络接入点。

▲3.梳理官塘校区光纤资产，建设完成学校每个楼宇的房间网络接入点到校园网中心机房的点对点光纤布线并端接。

（二）宿舍网升级服务

1.宿舍网采用无线 Wi-Fi6 协议标准的 XGPON ONU，每台 ONU 设备提供≥1 个 XGPON 上行接口,提供≥4 个下行千兆接口，提供不低于≥16 个无线终端的能力，ONU 设备需要能够被 ONT 智能管理系统或 OLT 统一管理简化设备运维，学生可以在宿舍内通过有线+无线接入方式访问互联网，同时 Wi-Fi6 的 ONU 能和学校现有的无线 AP 进行无缝漫游，校园内走动时认证切换时间小于等于 200ms，能够实现秒级内的无线切换，并且无线切换前后无需重复认证；

2.Wi-Fi6 ONU 均采用本地供电的形式，就近取电，供电无忧；上联 1:32 无源分光器，弱电井无源免维护；宿舍网基于 XGPON 协议标准，万兆带宽入室，高峰并发时不低于 300Mbps 的并发接入速率，保障学生用网体验，高清视频、直播不卡顿；

3.无源分光器件上联核心机房 OLT，能够在 POL 协议为基础的核心设备，采用 XGPON 网络实现数据传输，基于 POL 全光网保障后续可扩展性和协议的兼容性，后续可根据学校实际使用需要灵活进行带宽调整（通过调整汇聚层的分光器和 OLT 光模块数量即可）

4.宿舍整体采用 POL 全光网方式,建设骨干无源全光网络。

5.建设校园网出口，实现多运营商代拨接入，进行认证计费。

（三）校园网升级服务

1.整体建设要求：社湾校区、官塘校区教学办公区域需改造部分进行有线+无线的全覆盖，通过教室的万兆光纤入室，以保证教学办公区的网络质量，满足大带宽接入需求和未来针对智慧教室、VR 教室等建设的底座需求。计算机教室考虑到接

入终端多，涉及教室内的屏幕广播等组播广播流量，该场景建议采用以太光网的方案进行建设，通过以太网的技术让二层流量在交换机相邻端口下就近转发或广播，不再将报文上发到核心，能够减少整个网络广播包，优化整体流量，原有教室的接入交换机就近通过上行10G光口与万兆全光汇聚交换机进行互联，尽可能减少布线和施工的难度，且要支持利旧原有的计算机教室交换机。

2.教室接入设计：教室、实训室、报告厅、会议室等场景均部署1台10口交换机设备（支持8个POE接口，其中有2个2.5G/1G接口提供给Wi-Fi7 进行无线传输，8个POE接口用于其他教室或会议室内终端进行数据传输，上联至少提供1个10G 光口并采用单模单纤技术进行互联），计算机教室及多媒体教室部署1台24口万兆接入交换机（支持24口接入，上行提供4个10G光口）及1台Wi-Fi7 高密AP，技术规格不低于：高密AP需要采用不低于3射频设计，同时支持2.4GHz/5.1GHz/5.8GHz三个经过工信部批准的无线电使用频段，能够满足不低于100台的无线终端使用的需求，同时需要具备不低于1个2.5G BIDI光口（SC型），1个1G上行电口，4个1G下行电口。

3.办公室接入设计：老师办公室等办公用房均部署1台面板AP需要采用不低于2射频设计，同时支持2.4GHz/5.1GHz/5.8GHz三个经过工信部批准的无线电使用频段，能够满足不低于50台的无线终端使用的需求，同时需要具备不低于1个2.5G BIDI光口（SC型），1个1G上行电口，4个1G下行电口，实现有线无线一体化；

4.室外区域设计：室外区域按照实际使用需求部署室外全

向 AP，采用不低于 2 射频设计，同时支持 2.4GHz/5.1GHz/5.8GHz 三个经过工信部批准的无线电使用频段，整机最大速率 2.975Gbps，能够满足不低于 70 台的无线终端使用的需求，支持在重大会议或活动时提供双 5GHz 的接入方式，提高室外的设备接入并发量，采用单模单芯光纤 SFP 接口通过 1G 光纤网络实现 AP 的数据回传，保证远距离的信号覆盖，内置天馈防雷器，支持 802.1X/CA 证书/阿里钉钉/企业微信/短信/多因素多种认证方式。

5.供电方式及运维要求：室外 AP 采用本地供电的形式，就近取电，便于运维纳管；高密 AP 和面板 AP 采用 POF 光电一体化的供电方式，通过光电混合缆 300 米的距离，从弱电间统一拉光纤到每个房间光 AP 完成供电和通讯。AP 均采用 Wi-Fi6/Wi-Fi7 协议标准满足未来扩展性,高密 AP 支持无线环境感知、认证质量感知、网络质量感知、业务质量感知、边缘安全感知等技术，保障业务的连续性，支持通过网络管理平台对交换机和 AP 进行统一管理，以保障平时的设备运维管理使用；

6.光纤接入要求：教学办公区域的 AP 基于以太网的协议标准，楼宇内部的走的光纤入室，楼宇内做线路汇聚到 1 楼或 2 楼，然后统一熔纤到 ODF，通过高芯数 1 条或多条 96 芯单模光纤直连学校机房，学校机房内再直熔到 ODF，从 ODF 直接接中心机房内的汇聚交换机，汇聚交换机统一收敛端口后，通过 2 个 40G 端口与学校核心交换机进行互联，形成整个教学办公区从教室光纤点对点直接熔纤到核心机房，整个教学楼汇聚间的弱电间完全无源。

7.核心交换机要求：社湾校区、官塘校区校园网均提供 1 台高性能核心交换机，两校区之间核心交换机提供 1G 专线互

联，核心交换设备采用高密度端口设计，至少需要单台配置70个40G光口，96个万兆光口，48个千兆光口，48个千兆电口后续可进行灵活扩展；

8.网管平台要求：社湾校区、官塘校区校园网均提供1套SDN网络管理平台,针对下联接入和无线AP设备进行统一纳管，支持零配置上线、光链路诊断、终端准入认证、可视化运维及提升无线用户的使用体验、溯源与保障，提升运维管理效率，降低人力成本与老师工作量；

9.出口建设要求：建设校园网出口，优化互联网流量调度，实现互联网准出认证计费需要跟我校的统一身份认证进行对接，满足法律法规对网络日志审计的相关法规要求。

（四）网络互联链路服务

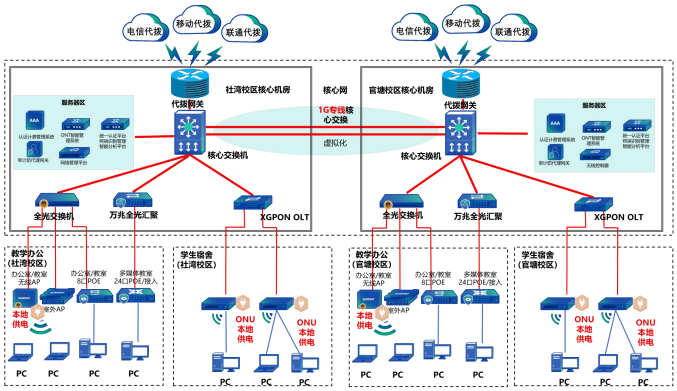
建设社湾校区到官塘校区的同城物理连接链路，提供两校万兆互联裸纤（物理光纤直连，中间不做跳转）线路。

提供10M教科网宽带线路。

（五）网络系统规划设计要求

1. 网络系统拓扑图

网络拓扑为三层结构，分为核心层、汇聚层、接入层的三层架构，其中核心机房的核心交换机和全光接入交换机设备放置在学校核心机房，本次考虑到平时的运维和管理的间接性，弱电间均采用无源架构设计，本次设计将所有楼层的 AP、交换机均回传到核心机房做接入，方便运维工作。



本期改造目标是实现有线无线网络 2.5G 到房间，无线网络 Wi-Fi6/Wi-Fi7 全覆盖，实现师生在校园内任意走动无缝漫游。

2. 终端层

终端层是指在学生宿舍接入校园网络的各种终端设备，例如台式电脑、移动平板、手机等设备。

3. 接入层

接入层是终端接入网络的第一层，为每间学生宿舍提供有线和无线两种接入校园网的连接方式。其中宿舍网络的接入层是在每个学生宿舍房间内部署 1 台 ONU 负责提供不少于 4 个有线千兆网络接口和 16 个无线终端并发接入的 Wi-Fi6 ONU，并且为保证设备的运行尽可能地减少故障点，本次的 ONU 建议采用内置天线设计，非外置天线的角度影响网络的实际使用。并

且通过每间学生宿舍有线+Wi-Fi6 无线网络的覆盖，有线无线一体化高速接入校园网络的需求。

办公区域的教室、阶梯教室等内部署 10 口 POE 接入交换机，交换机上行通过 2.5G 光口与直接核心机房的汇聚交换机相连，能够提供 2.5G 入室的接入能力，并且下行需要至少 1 个 2.5G 电接口用于与室内的高密 AP 相连,充分发挥 Wi-Fi7 AP 的高吞吐量的特点，计算机教室及多媒体教室部署 1 台 24 口万兆接入交换机（支持 24 口接入，上行提供 4 个 10G 光口）另外还需要 8 个千兆电接口满足教学区办公的需求。无线部分考虑到每个房间人数密度的不同，教室等高密度场景建议采用 3 射频的高密 AP 进行高密度覆盖。办公区的办公室考虑到终端密度相对较低，采用面板 AP 即可。

4.汇聚层

汇聚层为全光网络。主要设备包括核心机房的 POF 和 48 口万兆光汇聚交换机，所有楼栋内无汇聚设备，中间无源。POF 交换机上下行带宽一致不分光，单台汇聚 24 个下行口，可供 24 个接入交换机/无线 AP 使用,POF 交换机上自带满配光模块，上行连接至全光网核心交换机。保障 24 台接入设备超千兆速率接入。

宿舍区采用 1:32 分光器，基于 XGPON 协议，单台最大支持 32 个分光，可供 32 个学生宿舍，OLT 通过 40G 光口上联核心交换机。

5.核心层

核心层采用核心交换机，通过部署全光板卡，通过光缆直连下面接入设备。

核心层负责整个园区网络的高速互联，横向连接原校园网

核心层、网络管理区，南向联接汇聚层，北向联接安全出口区等。主要设备为核心交换机，同时旁挂无线控制器，进行宿舍区域无线设备统一管理。

本期两校区提供的核心交换机中间采用 1G 专线实现互联互通，传输网络和 IP 网络之间的转换，转发校内校园网和宿舍网之间的流量，以满足多媒体、关键应用数据的要求，满足日常教学对网络的需求。

6. 网络管理区

网络管理区是管理网络节点（例如网管系统）的区域。网管系统通过网管协议与网络设备交互，能够提供配置、管理和运维功能，本期新建一套网管平台，为校园设备提供自动化部署，可视化故障诊断、智能容量分析等功能，能有效帮助学校提高运维效率、提升资源使用率、降低运维成本，保障系统稳定运行。

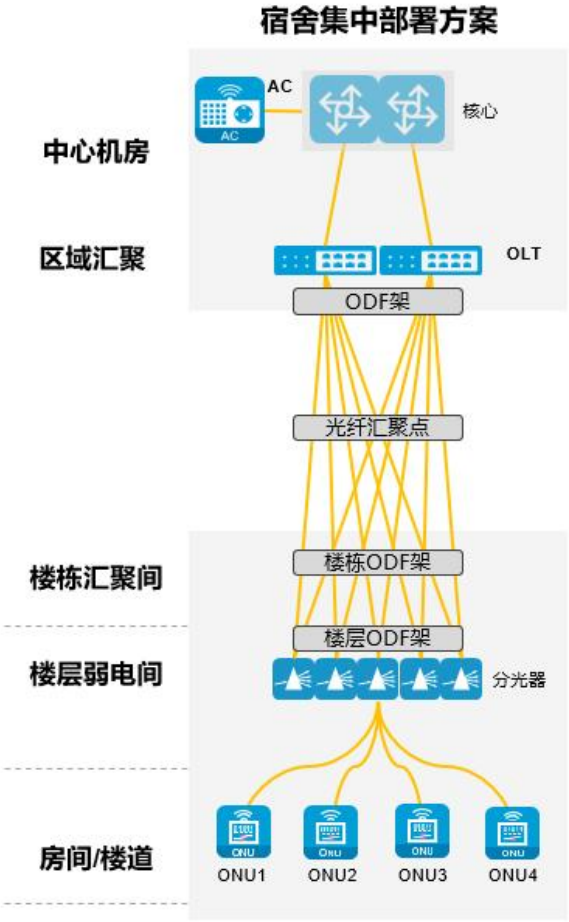
7. 安全出口区

安全出口区是作为保障校园网的安全防护体系，主要由全网行为管理、防火墙、代拔设备组成，利用现有校园网的其他安全设备共同打造符合等保 2.0 的要求的校园网安全环境。

8. 全光网设计

为满足宿舍及教学区域超千兆有线+无线覆盖的需求，将原来有线和无线融合的一张网布线，划分为相对独立的有线网络和无线网络。通过网管系统对交换机、无线设备统一管理，实现全网设备的自动化上线，有线无线的上网、认证策略统一执行。

9. 宿舍网系统结构图



10. 宿舍全光网络设计

本项目选用 XGPON 作为宿舍网光纤接入解决方案，为用户提供大容量和高带宽的数据和教育业务的接入，能够满足 FTTx 包括 FTTN、FTTC、FTTB、FTTR 等各种接入组网模式的需求。

（六）宿舍网网络规划要求

整体网络规划采取自下而上的方式，根据宿舍区房间数量以及人数选择接入 ONU-无源分光器-OLT。

（1）宿舍网规划原则

1. 光缆少，节点少，维护小；

2. 平衡网络资源最大化与成本最小化（设备成本、施工建设成本、后期维护成本）；

3.考虑网络可靠性，考虑网络保护方案；

4.考虑网络扩容扩建，满足后续网络接入的需求；

5.考虑后期新增业务建设及统一管理维护。

(2)OLT

本方案采用 XGPON OLT 为汇聚设备，支持 PON 协议，同时兼容以太网协议。

下行口为 XGPON 接口，通过 1:32 分光对宿舍的流量进行收敛，上行方向，考虑到下行流量已在分光收敛，故本次上行口不建议再收敛，否则会影响整个网络的流量大小，因此本次上行口建议采用 40G 接口,考虑到实际的部署情况和链路冗余，建议至少需要提供 4 个 40G 接口，才能较好地满足本次方案的要求。

所有主件（引擎板，业务板，电源，风扇）支持热插拔；

双主控模块冗余备份；双电源冗余备份；风扇冗余；无源背板设计，因此故障率大大降低，运营支出最大程度地降低。确保系统稳定可靠运行。

内置安全机制，可从控制、管理、转发三平面全方位保障网络设备的安全。内置协议报文攻击识别模块，防止协议报文攻击；安全的 SNMPv3 网管协议；IP、VLAN、MAC 和端口等多种组合绑定；组播/广播风暴抑制；

（3）光缆选型

光缆光纤应采用单模光纤，选型宜符合下列规定：

1.室外光缆中光纤宜采用 G.652D 类型；

2.室内光缆宜选用直径与 G.652 光纤相匹配的 G.657 类型。

光纤连接器宜采用 SC 和 LC 型。

光缆光纤设计选型符合下列规定：

1.光缆的允许拉伸力和压扁力应符合现行行业标准《宽带光纤接入工程设计规范》YD5206的相关规定；

2.室内光缆宜采用干式结构加非延燃外护层结构。

光缆芯数的配置要求应符合下列规定：

1.每ONU的接入光缆应根据用户分布情况进行配置，至少配置一条2芯光缆；

2.院区建筑物间或建筑物内布放的主干光缆应预留不小于10%的备份。

（4）配线设备选型

机架式光分路器安装架选型符合下列规定：

1.应根据安装环境选择防护等级，防护等级应不低于IP20；

2.应根据布线方式选择顶部或底部出线的机柜，出线孔宜按需调节大小；

3.宜采用宽度为600mm或800mm的机柜，800mm的机柜宜前后双开门；

4.宜选择19英寸或21英寸标准安装方式；

5.宜采用框架结构形式；

光纤配线架选型符合下列规定：

1.应符合现行行业标准《光纤配线架》YD/T778等相关配线设备标准的规定；

2.应支持预端接光缆、熔接等接入方式；

3.应具有可靠的保障室外光缆接地的接地装置；

4.宜采用抽屉式结构，并支持左右出纤要求。

19英寸或21英寸机架式跳线管理模组选型符合下列规定：

1.应符合现行行业标准《光纤配线架》YD/T778等相关配线设备标准的规定；

2.盒体表面涂覆层附着力要求应不低于现行国家标准《色漆和清漆漆膜的划格试验》GB/T9286标准2级要求；

3.应保证充足的盘纤空间和光缆的弯曲半径；

4.跳线放出程度应不小于2.5米；

5.应支持左右方向同时出纤；

6.宜采用托盘式结构模块化设计，每个配线架（1U）配置多个储纤型托盘组件，支持即插即用；

7.宜采用储线型托盘组件存储并管理光纤跳线冗长功能，每个组件含多只绕线盘，每只绕线盘容纳存储一根光纤跳线，单个托盘存储8芯～12芯跳线。

光缆交接箱及光缆配线箱选型符合下列规定：

1.光缆交接箱应符合现行行业标准《通信光缆交接箱》YD/T988的相关规定；

2.箱体孔洞应满足进出光缆管孔的需求；

3.箱体内应有光分路器的安装位置；

4.箱体内应有光缆终接、保护和跳纤的位置；

5.箱体内应设置固定光缆的保护装置和接地装置；

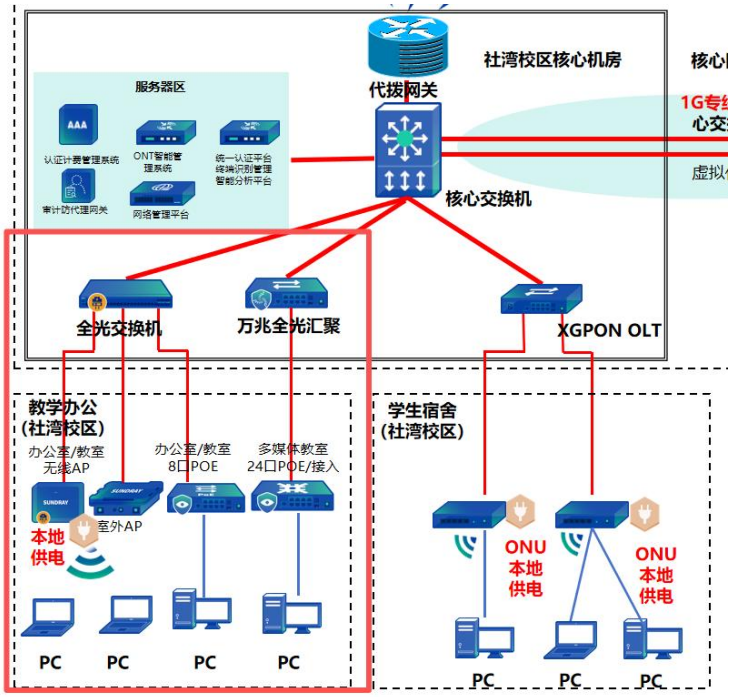
6.室外箱体应防雨、通风，光缆进、出口处应采取密封防潮措施，防护等级应不低于IP65；

7.箱体应具有良好的抗腐蚀、耐老化、抗冲击损坏性能及防破坏性能，门锁应为防盗结构；

8.箱体内宜配置熔接配线一体化模块，适配器或连接器宜采用SC或LC类型。

（七）教学、办公网系统规划要求

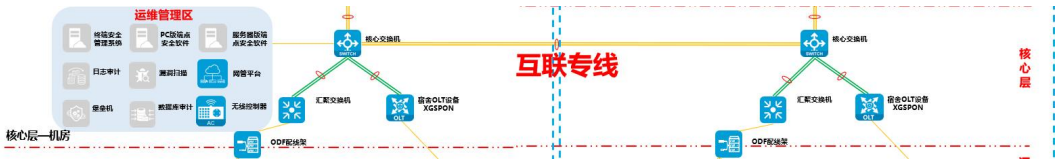
结构图



1. 核心层网络

核心层主要承载宿舍区和校园网的流量转发，根据不同的楼栋与区域设置相应的 VLAN 及 IP 地址。负责整个园区网络的高速互联，横向通过 1 条 1G 专线实现两校区间互联，1/10G 连接运维管理区的网管平台，专线对接出口代拨设备等。主要设备为核心交换机，骨干链路保障 2*40G 带宽（考虑到教学办公区均超过 40 个端口，减少核心层的带宽收敛，并且需要保证链路冗余，同时考虑到对现有业务的兼容和使用，至少需要 56 个 40G 端口，96 个万兆端口，48 个千兆光口，48 个千兆电口），才能够满足下联光纤收敛后入室的千兆入室需求，且未来 5-10 年内整个网络的架构依然处于较高的建设水准。

2. 系统结构图



3. 设计说明

本期核心交换机负责替换原有的核心交换，进行传输网络和 IP 网络之间的转换，转发各个教学楼和学生宿舍之间的流量，以满足多媒体、关键应用数据的要求，满足日常教学对网络的需求。

4. 核心交换机要求

核心交换机应根据支持的业务类型、配置场所和功能要求确定配置和选型。

核心交换机应支持堆叠负荷分担，应支持主控板、电源板、风扇模块冗余保护。宜采用插卡式设备，选型宜符合下表规定。

规格类型	大规格	中规格	小规格
交换容量	256Tbit/s	128Tbit/s	64Tbit/s
堆叠	支持	支持	支持
MAC 地址数（个）	512k	256k	128k
IPv4 路由表（条）	256k	128k	64k
IPv6 路由表（条）	64k	32k	16k
IPv4 路由协议	支持 RIP、OSPF、ISIS、BGP 等 IPv4 路由协议		
IPv6 路由协议	支持 RIPng、OSPFv3、ISISv6、BGP4+等 IPv6 路由协议		
100GE 端口数(个)	≥64	≥32	≥16

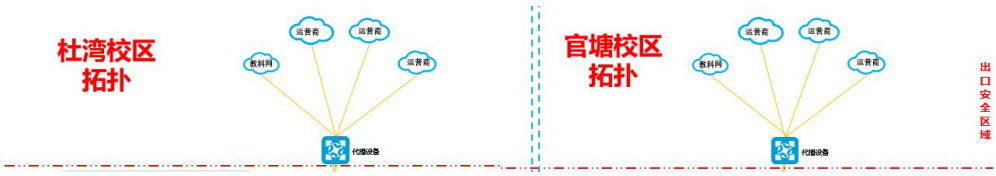
10GE 端口数（个）	≥480	≥288	≥144

核心交换机选型表

结合项目实际情况，建议选用大规格的核心交换机。

（五）互联网出口

互联网出口主要负责为学生、教职员工和其他工作人员提供上网通道。



（八）认证计费平台建设要求

1.认证计费平台

在学校中心机房部署一套认证计费平台进行校园网认证计费管理系统搭建。平台包含认证网关（vBRAS）、认证计费系统（含 Portal 系统）、防代理/行为审计。支持与学校统一身份认证系统（如有）对接，提供学生和教职工用户实名认证接入、基于用户的访问策略配置管理、基于用户身份的不同访问权限配置等管理功能，对学生有线、无线 Wi-Fi 等进行认证、计费、审计，对学生宿舍是否有电脑共享热点、私接无线路由器、私接 Wi-Fi 小设备、随身 Wi-Fi 等网络共享行为进行检测及控制，实现对宽带用户进行上网行为审计、共享上网行为监测和控制等功能。

同时，上网行为审计日志存留时间满足公安部相关要求，向学校完全开放必要的上网计费、行为审计等数据，确保学校对学生有线、无线上网行为可控、可管、可溯源。功能清单如下所示：

（1）统一身份：与学校现有的校园网融合实现互联互通，面向全校师生，可基于不同的用户身份配置上网策略。

（2）智能选路：教师可通过校园专线访问互联网；并配合校园内网路由配置实现未缴费的学生可以访问校园内网的教学资源的服务；开通宽带的学生则走出口上网。

（3）统一认证：所有接入校园网学生有线、无线 Wi-Fi 皆需进行认证、计费、审计，校园网、学生宿舍有线/无线网融为一体，实现统一认证、统一计费和统一上网行为管理。

（4）共享控制：认证网关、认证计费系统、防代理/行为审计联动，对学生宿舍是否有电脑共享热点、私接无线路由器、私接 Wi-Fi 小设备、随身 Wi-Fi 等网络共享行为进行检测及控制，实现对宽带用户进行上网行为审计、共享上网行为监测和控制等功能。

（5）审计安全：审计日志存留最少 180 天，满足公安部 82 号令，且学校可审计数据，用于用户上网行为追踪。

（6）管理权限：学校对本地的认证计费系统拥有超级管理员权限，可随时查看认证系统的所有数据，包括用户上网清单、开户数据、各项统计报表等。

（7）认证方式：本地网络采用 PORTAL 认证，本地网络与运营商网络之间采用 PPPOE 认证。

2.认证网关

本期项目投入的认证网关，是基于 NFV/SDN 架构的认证网关产品，产品采用了多 CPU 并发工作流技术和集群技术，具有高可靠和高性能特点；同时产品还能够灵活地进行新功能定制，能够协助用户快速开展新业务。

部署一台高吞吐量的认证网关，采用高可靠集群部署，联

动认证计费管理系统，实现校园账号身份有线无线统一认证，学校内网认证与运营商外网认证无缝融合，做到一次点击完成二次认证。具备 DHCP Server、支持 IPV4/IPV6 双栈认证、多终端接入控制、时段接入控制、黑白名单控制、无感知认证控制、智能选路、智能 DNS 等功能；支持 portal、PPPoE、portal 转 PPPoE ，PPPoE 转 PPPoE 等多种认证接入方式。

（1）认证接入区域

对学校入网用户的宽带接入认证进行控制和管理。同时满足准入认证和互联网出口认证一次完成。

（2）认证接入流程

校内用户（学生/老师）在认证界面，使用学号/工号认证上网，内网认证成功后，认证计费系统会识别账号角色，为运营商宽带用户则自动关联到运营商账号，与对应的运营商服务器进行 PPPOE 代拨，完成外网认证；免费教师账号无需开通运营账号，直接走校园专线出口上网。

（3）校园出口选路

校园目前存在两个上网出口，一个是固定专线的办公出口，主要用于教学资源；一个宽带运营商出口，主要用于学生的上网出口。认证网关联动认证计费系统，通过识别用户角色，根据角色智能选择出口，大大提高不同区域的用户上网体验。

（4）组网接入设计

扁平化大二层网络建设，采用 QINQ 技术，把接入网络通过 vlan 进行物理隔离， 减少相互干扰。在无线接入环境，把无线接入进行细化 vlan 隔离，在 QinQ 环境下，用户接入不同 vlan 下的无线，能够实现一个 IP 地址不变。vBRAS 能够很好地适应这些网络建设要求，实现用户在 QinQ 相互物理隔离

的同一接口网络环境下同一个 IP 接入的要求。

（5）用户接入方式

支持多种用户接入方式:web Portal,PPPOE,WEB 转 PPPOE,webPortal。能够并发 5 万重定向连接，能够抗干扰，过滤非浏览器定向。支持 PPPOE 代拨号服务，能够根据用户身份代拨不同端口，能够锁定用户虚拟 MAC 地址，能够控制代拨连接单会话独享或多会话共享。

以下是本次投入认证网关的详细功能设计:

1）高性能、多接入设计

具备 4 个千兆端口+8 个 10G SFP+万兆光口；双向吞吐量 40G，支持 DNS 智能分流器功能，支持多合作方选路。支持标准 Radius 协议和扩展协议，支持 PPPoE/PPPoE 代拨/WEB/Client 认证方式。

2）快速部署设计

支持基于 NFV/SDN 架构，实现快速部署

3）相同账号不同终端宽带共享设计

支持 PPPOE 代拨上网，相同账号不同终端（1PC+1 手机）并发在线时支持共享账号带宽

4）无感知认证设计

支持 IPoE 二/三层无感知接入。联动认证计费系统，对已经登录过的用户 mac，再次发起外网请求的时候，vBRAS 自动向计费系统发起 mac 认证请求，认证计费系统收到认证请求，找到匹配此 mac 对应的用户信息，则自动完成认证。无需用户再次手动触发认证登录。

vBRAS 支持二层 MAC 无感知认证，配合 DHCP 服务器，支持三层无感知认证。

5）高并发、高承载设计

支持用户高并发条件下的承载能力，单台设备可支持 2 万并发用户。

6）还支持以下功能：

支持集群部署。

支持冗余，单台硬件宕机，其他用户能够自动切换至其他设备。

支持用户自动负载均衡。

支持灵活调度功能，能够在不断网的情况下，实时增加 vBRAS 的数量，增加后，通过调度系统激活新增设备后，能够自动加入 vBRAS 集群中工作。

支持 QinQ，能够根据外层 VLAN 给用户分配指定的地址池的 IP 地址。

支持多运营商选路，和 AAA 系统配合，能够选择不同的互联网出口路由，支持校内外账号自助绑定、不同运营商用户自动选择不同出口，支持 PPPoE 代拨认证，支持运营商双认证、双计费等功能。

支持 Portal 认证转运营商 PPPoE 认证，和 AAA 系统配合，用户 Portal 认证后，能够自动向外网的运营商的 BRAS 发起 PPPoE 认证请求，不需要再通过其他方式和运营商的 AAA 系统对接。

支持 MAC 认证，无线用户只要在 AAA 后台记录对应的 MAC 地址，连接上网，就可以自动认证，不需要再输入密码。

3.认证计费系统

在本次项目上投入认证计费管理系统部署在学校的中心机房，用户上网账号实现本地化管理，负责统一认证计费系统

实现校内用户的账号开户、收费、资料变更、销户、管理等。配合认证网关向用户提供差异性收费策略、控制用户的接入时间与速率、统计账务报表以及上网清单等。

认证计费系统软件基于标准Radius协议和Portal协议开发，并具备良好的标准性、兼容性、开放性，实现有线无线认证计费和管理平台一体化。满足教育信息系统安全等级保护要求。

（1）认证接入区域

对学校的宽带接入认证进行控制和管理。同时满足准入认证和互联网出口认证一次完成。

（2）认证接入流程

校内用户（学生/老师）在认证界面，使用学号/工号认证上网，内网认证成功后，认证计费系统会识别账号角色，为运营商宽带用户则自动关联到运营商账号，与对应的运营商服务器进行PPPOE代拨，完成外网认证；免费教师账号无需开通运营账号，直接走校园专线出口上网。

（3）防共享控制流程

防代理/行为审计通过配置检测对上网数据做分析，发现有账号行为时，通知认证计费系统，认证计费系统做出对该用户的决策行为，包括冻结、强制下线、一定时间内禁止登录等命令，认证计费系统下发命令给认证网关进行接入拦截控制。

（4）组网接入设计

◆认证对接校园统一身份平台，实现账号统一管理，账号实名制。

◆认证计费系统联动认证网关实现有线、无线统一接入认证。

◆认证计费系统联动认证网关实现智能选路,识别不同用户走不同出口。

◆认证计费系统联动认证网关，识别开通运营商账号用户，实现 web 转 PPPoE 认证，用户只需点击一次登录即可自动完成二次认证，提升用户上网体验。

◆认证计费系统联动防代理/行为审计设备实现共享行为控制。

◆认证计费系统配置灵活的控制策略，是区域接入控制、无感知控制、时段接入控制、终端接入控制、黑白名单控制等等，可根据校园管理的需要进行配置。

◆联动统一运维管理平台实现业务开通与管理。

以下是本次投入认证计费管理系统的功能支持与设计：

◆认证计费管理系统支持多种认证方式，二层 PPPOE，802.1X，三层的 WEB Portal,L2TP 认证、PPPoE 代拨认证，认证授权都有以下的功能：

◆支持对同一帐号可同时使用人数多少的认证；

◆同一账户认证成功后再次认证,后认证用户可自动踢前一次认证用户下线；

◆根据接入设备传送的用户信息,把用户的账号和 IP 地址、MAC 地址、接入设备 IP、接入设备端口、VLAN ID 进行认证绑定；

◆黑名单功能，黑名单的 MAC，IP 不能认证；

◆控制用户认证的服务,不同策略的账号只能使用指定的服务；

◆下发策略定义的多服务，配合 BAS 实现各种域的控制；

◆支持 IPV4,IPV6 的混合认证；

◆支持对用户上下行带宽，本地上下行带宽的授权；

◆支持时段控制和时段速率控制功能；

◆支持对用户地址池的授权；

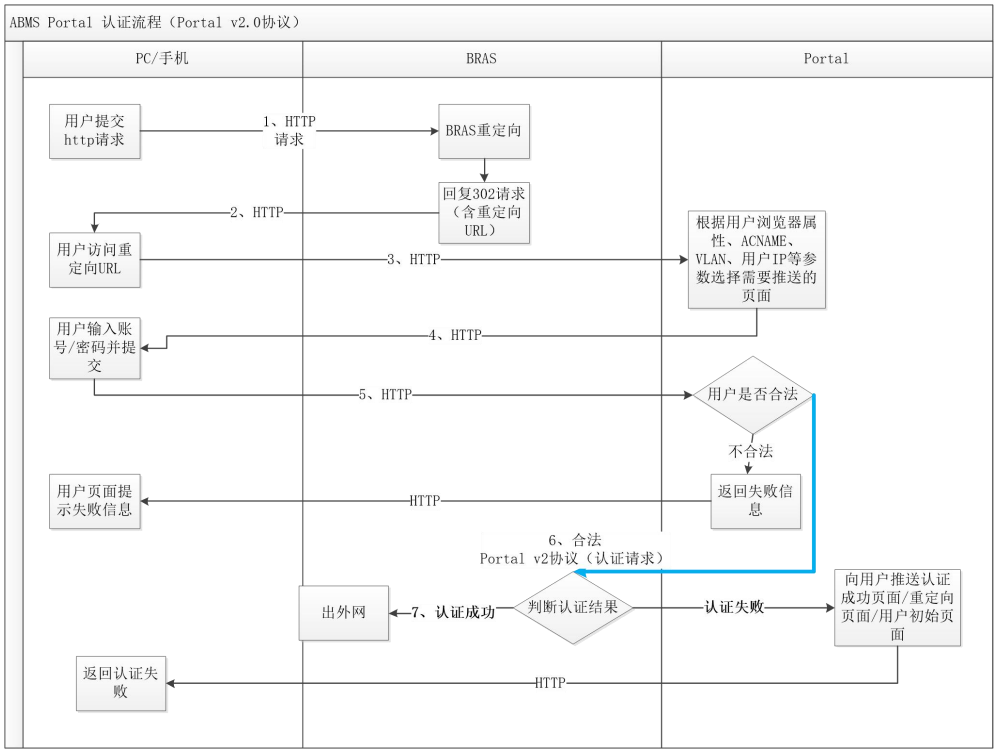
◆支持欠费账号宽限使用：即欠费的用户也可以宽限使用指定的天数

◆以计时长、计流量、包月、包天、包年、分层计费、免费为模板的 7 种计费策略类型。

4.Portal 系统

部署 Portal 系统，实现提供个性化 Portal 登录页面，支持在登录页面上发布信息公告。

Portal 认证交互流程如下



以下是本次投入 Portal 系统的功能支持与设计：

◆本期投入的 Portal 系统，外置 WEB Portal Server，实现通过网关、AC、ONU 推送 WEB Portal，支持按照不同的账号/SSID/VLAN/NASIP 推送不同的页面；支持 PORTAL2.0 协议规范，

支持短信提醒，短信验证认证。

◆支持个性化认证页面推送：针对不同的SSID/VLAN ID/IP地址段/网关所在区域推送不同的用户认证页面，为不同区域用户定制个性化的登陆页面。

◆支持无感知的MAC认证；

◆支持根据接入设备名称、SSID、VLAN、IP值推送个性化Portal页面；

◆支持自定义Portal和模板化Portal页面；

5.防代理/行为审计

本期投入一台基于NFV/SDN架构的防代理/行为审计，主要对宽带用户进行防共享控制。实现对校园场景下不同类型的共享设备（如小路由器、代理软件、系统自带共享、免费Wi-Fi类软件、随身Wi-Fi设备）实现防共享接入控制，实现网络实名制，上网用户一人一号，防止上网共享行为。

防代理系统通过cookie检测、应用特征检测等手段来判断出用户是否存在共享上网行为，识别共享终端数量、终端的设备类型、操作系统类型等信息，最终核实用户是否存在共享宽带转售行为，并在一定的时间段内对检测到共享上网行为的用户进行提醒和封锁，从而实现防代理。

系统设备抓取用户的上网日志，URL日志既是执法部门常用的审计手段，又是监管部门衡量网络整体效率的依据。审计系统具有准确完善的URL分类库和强大的URL日志收集及加工能力，这些分类库是根据国内用户当前情况进行的合理采集和分类，符合我国用户的网络使用环境的需求，分类结果基本覆盖了在国内用户中有一定访问量的URL地址。

防代理/行为审计组网说明：

◆旁路部署在交换机上，与认证计费系统网络可达

◆认证网关串接在网络上，整体大二层接入

◆认证计费系统部署在服务器集群位置，保证与认证网关、防代理/行为审计可网络通信

◆把交换机与认证网关设备互连的端口的上行数据,镜像至交换机与防代理互联的端口

◆防代理/行为审计通过配置检测对上网数据做分析，发现有账号行为时，通知认证计费系统，认证计费系统做出对该用户的决策行为，包括冻结、强制下线、一定时间内禁止登录等命令。

优势：

◆可针对账号做管控，避免用户更换 IP 后，共享拦截失效。

◆不影响正常用户的上网行为,只对有代理行为的用户起到控制作用，如若网络故障，也不会影响用户的正常上网。

◆记录用户的上网行为数据，保存 180 天以上，满足公安 82 号令，实现对宽带用户进行上网行为审计、共享上网行为监测和控制。

◆对当前主流的共享设备接入具备有效的判断控制,防代理/行为审计已在多校稳定运行。

◆以下是本次投入防代理/行为审计的功能支持与设计：

◆本期设计的防代理/行为审计万兆光口*2；千兆电口*6，支持 20G 吞吐量， 满足 2 万人以下用户规模使用；非关系型大型数据库进行数据管理。

◆支持监控 6.4 万个并发 IP

◆支持监控 200 万个连接

◆支持和计费系统互动，根据账号停用用户，避免用户频繁

更换 IP

◆支持内容审计，满足公安部 82 号令，可增加硬盘本地存储审计内容，并和认证计费系统互动，直接获取用户账号信息

◆支持直接配置黑名单，禁止黑名单用户上网

◆支持配置白名单，不监控用户

◆支持配置门限参数，根据门限参数判断代理行为

◆支持通过小路由特征判断代理行为

◆支持串接部署

◆支持通过镜像端口盘路部署

（九）IT 运维服务

1. 网络管理系统

网络管理系统的建设，一是要满足全光网网管管理的需要。同时建议融合现有学校校园网网管系统，形成统一的运营维护一体化平台，将平台做成集“监-控-管-视-析”于一体，统一监控，智能分析，自动运维，流程高效，实现监、控、管、营、服全生命周期管理。

统一网管系统对在校多层级设备进行统一监管，校园网络设备在线情况直观可视。多种图像图表可对园区内数据、资源、故障实时感知，并且告警、报错，可实现运维操作自动化。平台可以有线、无线、波分一体化运维，有利于设备间联动问题查找，方便管理员实时查看。

设备支持即插即用，即换即通，分钟级上线，接入设备可配置模板统一下发，缩短设备上线与开通时间，从而降低设备部署成本。

2. 运维服务

网络维护服务负责学校所有网络、网络设备的日常维护、

维修工作。办公和教学场所的网络设备及耗材由采购人提供。

网络设备服务方案负责维护校园信息化设备，包括但不限于教学、实训、办公用信息化设备等。

建设统一的 IT 运维服务体系，将网络整合成一张网，并提供网络运维服务以及校园信息设备（教学、实训、办公用信息化设备）运维，保障教学、行政办公活动能够正常开展，保障学生宿舍网络正常。

3.维护内容

（1）校园网络巡检

◆负责学校所有网络、网络设备的日常维护、维修工作。办公和教学场所的网络设备及耗材由采购人提供。

◆负责学校网络维护、维修工作。包括宿舍、教室、实训室、行政办公、一卡通、安防、消防、监控、门禁、广播及其他公共区域网络日常维护、维修。

◆进行定期巡检（每月一次），有巡检记录（报告）。

◆配置维护所需人员，自备维护网络检查、检修所需的常规仪器如熔纤机、OTDR、光功率等设备和工具。

◆对校园网络进行规范化管理。

（2）学生宿舍区网络建设

负责学生宿舍宽带网络规范化建设和管理，实现单链路和光猫接入。

◆负责学校建设中、后续建设的学生宿舍宽带网络建设（含到宿舍楼栋主干光缆布设、到房间网络布设与相关设备安装调试、配套供电等，并自行承担相关费用。

◆学生宿舍宽带网络铜改光工程，并自行承担相关费用。

（3）开学迎新等活动服务

◆免费提供不少于10次/年的开学、迎接新生、各类校内外考试、重大会议、开放日及各二级学校开展的重大活动等的临时网络布设（布设网线等）与网络保障服务（包括临时增加带宽等），其中的设备、耗材除外。

（4）固话网络建设及维护

免费负责学校固话网络建设及维护，并规范管理。

（5）网络零星综合布线服务

免费提供400个点/年（校园内非学生宿舍区域房间内）的网络零星综合布线工程，工程规范并符合国家相关标准（材料费除外），超出部分的费用按当时市场最低价结算。

4.服务目标

保障教学、行政办公活动能够正常开展，保障学生宿舍网络正常。

◆做到故障报修及时响应，及时解决，保证全校教学及行政办公的正常运转。

◆每月进行网络设备检测、巡检，发现风险隐患及时整改，并形成报告，提交给采购人。

◆保障各种考试、比赛活动正常进行（包括语言类考试、各种考证、比赛、竞赛及期末考试等等）。

◆重大会议、活动保障有力，全年重大会议、活动网络保障事故为零。

5.服务质量要求

建立全面的网络维护工作计划（含上课、寒暑假和节假日）、定期巡检工作方案、应急预案，形成完备的工作记录，并定期报告（月报、学期总结、年度总结）。保证全校范围内的教学场所教学和行政办公能够正常开展，完成开学迎新、单

招、各种考试、竞赛以及采购人主办或承办重大活动的网络保障工作。

（1）业务受理

1）设立固定报修热线：座机或手机和报修网站，必须有专人处理，每天工作时间内确保能及时地响应和处理各类网络故障。

2）报修网站应有报修平台（有报修流程），平台应公布主管人员、维护人员等个人信息、联系方式（定期更新或人员更迭后更新），定期发布病毒预警、补丁升级的温馨提示，定期发布运维统计数据和分析结果（月报、期末汇总、年度总结，电子表格形式，特殊需要另计）。

3）实施值班经理制度，保证突发事件应急处理的及时有效性。

4）接到报修反映的问题后，应在 10 分钟内响应，30 分钟内通过远程或到达现场进行处理解决。

（2）网络故障响应

1）中标人维护的主干网络，网络线路修复要求标准不低于各运营商相关的标准要求，重大故障 1 小时内响应，4 小时抢通或修复，不能及时抢通或修复的也要告知采购人不能修复故障原因，普通故障 2 小时内响应，24 小时抢通或修复，核心主干平均抢通或修复时长低于 12 小时，重点保障区域平均抢通或修复时长低于 24 小时,普通故障修复时间低于 48 小时(因不可抗力或采购人原因影响如备件缺失，以及校园施工导致等原因的除外）。

2）由中标人负责维护的教学、实训区域各信息点线路，紧急故障 10 分钟内响应，0.5 小时内修复，不能及时修复的也

要告知采购人不能修复故障原因；普通故障20分钟内响应，普通故障修复时间低于2小时（因不可抗力或采购人原因影响如备件缺失，及校园施工导致等原因的除外）。

（3）学生宿舍网络管理

每年寒暑假期间，对学生宿舍网络进行巡检，特别是秋季学期新生宿舍，需检查每一间宿舍的网络设备和线路情况，确保新生宿舍网络设备可用，网络线路整齐、美观。

（4）投诉处理

1）直接受理的投诉，应在一个工作日内核实情况并作回复处理，最长不超过三个工作日；如有直接向有关部门投诉的，应查明事实，确认证据，分清责任后如实上报书面材料至采购人，并协助有关部门做好相应工作。

2）所有投诉的受理、处置应保留记录，并确保真实有效。

（5）档案管理

须建立网络维护服务管理档案，要求档案完整、真实，并更新及时。档案内容必须包括：人员管理、报修记录、工作记录、巡检记录、各种分析报表、月报、年度总结、培训记录（时间、地点、照片）、设备资产表等。服务期满后移交采购人。

（6）设备、配件更换

网络维护中发现需要更换、更新的网络设备、配件应做好记录并注明原因，向采购人申请领用更换（须有领用、更换记录）；换下来的设备、配件应交还采购人留存，所有配件、耗材均由采购人提供。每学期末应提前一个月做好下一学期的配件、耗材计划，报采购人处理。

（7）安全保密（信息安全）

中标人必须签署信息安全保密协议，并确保实施过程中设

备原有数据的完整性和安全性。

中标人对参与网络运维的全部人员进行安全保密、信息安全培训，每年2次，并提供培训记录和相关文档资料。

（8）工作人身安全

参与现场的服务人员，需由中标人开展工作安全培训，保障其自身安全，如出现伤亡事故，需承担竞标人全部责任。

（9）其他服务

1）配合采购人完成各种重大活动的技术保障、支援工作（如开学迎新、在采购人召开的重要会议、重大活动、各种比赛、考试活动等，完成网络设备安装、网络的连接、调试活动，并按照要求执行活动期间的技术保障工作，所需设备、耗材由采购人提供）；

2）在采购人需要时，提供所管辖范围内网络设备的免费送修服务（含送去与取回，维修费用按实际收取）。

3）协助完成管辖区域内资产管理，包括设置资产标签，按要求统计设备资产数据，每学期进行资产盘点等。

6.服务规范要求

（1）建立完善的管理制度、制定工作流程、人员考核制度（月度考核），确定驻场人员岗位职责，能够对驻场人员的工作进行跟踪及质量监督，有完备的文档资料存档。

（2）编制运维手册，建立完备的运维过程文档资料，统一格式、做好分类，最终建成运维文档库（利用日常积累的网络故障及解决方案对问题预先判断），并采用管理软件进行过程管理和运维状态管理。

（3）应有网络出现大面积中断的应急预案，若出现人手紧缺，可能影响响应和处理时间时，中标人需给予全力支持，

及时调整人力资源。

1）制订教学突发情况应急预案。防止因病毒侵袭导致网络大面积瘫痪、数据丢失，考试期间断电、断网、考试数据无法上传、数据丢失或其他突发事件，造成事故。

2）制订行政办公突发情况应急预案。防止因病毒侵袭导致网络大面积瘫痪、数据丢失，极端恶劣天气造成设备损坏，网络突发故障导致重要会议中断、断网、数据丢失或其他突发事件，造成事故。

3）制订开学突发情况应急预案。防止因意外情况导致无法正常开学。

4）暑假期间根据上一年度工作总结，酌情对各应急预案进行修订完善。

（4）确保和提高设备的使用率，做好各类网络设备运行状况的记录工作，保证运维工作快速有效，制定定期检修及所有网络设备的巡检计划（按区域分类，每月一次），巡检报告以文档形式提交给采购人，每月月初（5 号前）提交上月的运维报告给采购人。

（5）定期对交换机设备进行配置备份，并进行必要的软件版本升级和配置优化，发现风险隐患及时整改。服务期满后移交采购人。

（6）每次更换的所有设备或零配件应同时做好设备更换记录，填写有关设备信息存档。对所有设备进行分类登记形成文档，做好设备的管理、分配、调拨等工作，协助做好固定资产登记的工作。项目实施三个月内需形成采购人网络设备、信息点基础信息库，并及时更新。服务期满后移交采购人。

（7）数据分析与总结

1）根据报修记录进行统计，报修网站应定期发布运维报表和维修维护分析数据（月报、期末汇总、年度总结，一般以电子表格形式，特殊需要另计），每学期提交整个学期的分析报告及改进意见给采购人。

2）每年暑假期间对上一年度管理工作进行总结，提出整改意见及落实时间表。

（8）驻场人员行为规范必须合法合规，且遵守采购人规定规范。

（9）人员要求

1）项目经理（管理人员）1 人，网络维护技术人员不少于 6 人（上班时间，社湾、官塘校区必须保证每个校区各有不少于 3 名技术人员同时值班），如有员工离职，应提前不少于 1 个月提出申请，在配齐合格人员并做好工作交接后方可离职。

2）中标人人员有三次及以上违反采购方规章制度或造成一次及以上重大教学事故的，除了按学校规章制度办理之外，中标人必须更换涉事人员，且需经过采购人考核认可。

3）重大活动期间（如开学迎新、单招考试、校园开放日、采购人主办或承办的重大比赛、重要活动等），根据采购人要求增加可以临时支援的技术人员不少于 1 人，每次时间不超过 2 天。

（10）工作时间

每天 8:00-22:00，保证社湾、官塘校区每个校区各有不少于 2 名技术人员同时驻点，响应网络维护、维修，如遇突发情况，应及时安排人员支援。

节假日采购人如需临时安排工作，应提前不少于 1 天通知项目经理安排人员值班，正常节假日应安排有不少于 2 人在待

命（不出柳州市区），需要的话可以在 1 个小时内赶到学校。

7.其他重要事项要求

在开展网络维护服务过程中须特别重视安全工作，必须做到但不限于做到以下几点：

（1）应制定校内维护维修安全条例，明确安全事项；与采购人签订安全目标责任书，并自觉接受采购人的监督与指导；制订安全管理责任制度、安全工作标准及发生安全事故的应急预案等，并不断修订完善。

（2）中标人应教育员工注意安全，中标人的雇员在履行职务中的人员伤亡，责任由中标人承担，采购人不承担任何责任；

（3）维护、维修操作涉及用电安全，均须严格按照国家和地区相关安全操作规程执行，如发生违规操作现象，所产生的后果全部由中标人承担，如造成经济损失，全部损失由中标人赔偿。

（4）若因中标人原因而造成的被盗事件，责任由中标人全权承担，中标人须按丢失物品账目价值赔偿；如造成教学事故，还应视情节严重程度，处以罚款，罚款金额由双方沟通确定。

（5）处置紧急突发事件时中标人工作人员必须服从采购人的指令，及时配合参与处置。

在开展网络维护服务过程中必须遵规守纪守法，必须做到但不限于做到以下几点：

（1）在签订网络维护服务合同中须与采购人签订廉政责任书，遵守廉政约定。

（2）遵守现行《中华人民共和国劳动法》《中华人民共

和国劳动合同法》及柳州市相关规定，与服务人员签订劳动合同，为服务人员提供工资、保险等正常待遇，若出现劳动纠纷、劳动违法现象，由中标人全部负责。

（3）不得擅自占用校区内的公共设施或改变使用其功能，如需扩建或完善配套项目，需与采购人协商经批准后方可实施；中标人不得将管理责任及利益转让给其他单位或个人，不得在校区内开展与本网络维护服务无关的活动，不得干涉或影响采购人进行各种合法活动。

（4）中标人在做好设备维修维护服务的同时，还应遵守采购人各项管理制度，积极配合采购人搞好管理、服务、育人工作，共同维护校园安定稳定；不得透露校区有关重要消息和情况，对外不得损害采购人名誉，和校区师生进行正常交往，不得散布流言蜚语。

8.其他重要事项

1）中标人在开展设备维护服务过程中须特别重视安全工作，必须做到但不限于做到以下几点：

（1）应制定校内维护维修安全条例，明确安全事项；与采购人管理部门签订安全目标责任书，并自觉接受采购人的监督与指导；制订安全管理责任制度、安全工作标准及发生安全事故的应急预案等，并不断修订完善。

（2）中标人应教育员工注意安全，中标人的雇员在履行职务中的人员伤亡，责任由中标人承担，采购人不承担任何责任。

（3）维护、维修操作涉及用电安全，均须严格按照国家和地区相关安全操作规程执行，如发生违规操作现象，所产生的后果全部由中标人承担，如造成经济损失，全部损失由中标

人赔偿；采购人发现中标人有违规操作现象或出现事故可直接进行经济处罚，酌情给予每次200元至2000元。

（4）若因中标人原因而造成的被盗事件，责任由中标人全权承担，中标人须按丢失物品账目价值赔偿；如造成教学事故，还应视情节严重程度，处以合同金额1%—3%的罚款。

（5）处置紧急突发事件时中标方工作人员必须服从采购人的指令，及时配合参与处置。

9.关于项目重要说明

（1）本项目所有人员均为现场驻点人员，能够及时响应各种报修。

（2）本项目中所有服务按要求进行考核。

10.中标人在开展维保服务过程中须遵规守纪守法，必须做到但不限于做到以下几点：

（1）在签订维保服务合同中须与采购人签订廉政责任书，遵守廉政约定。

（2）遵守现行《中华人民共和国劳动法》《中华人民共和国劳动合同法》及柳州市相关规定，与员工签订劳动合同，为员工提供工资、保险等正常待遇，若出现劳动纠纷、劳动违法现象，由中标人全部负责。

（3）不得擅自占用校区内的公共设施或改变使用其功能，如需扩建或完善配套项目，需与采购人协商经批准后方可实施；中标人不得将管理责任及利益转让给其他单位或个人，不得在校区内开展与本设备维护服务无关的活动，不得干涉或影响采购人进行各种合法活动。

（4）中标人在做好设备维修维护服务的同时，还应遵守采购人各项管理制度，积极配合采购人搞好管理、服务、育人

工作，共同维护校园安定稳定；不得透露校区有关重要消息和情况，对外不得损害采购人名誉，和校区师生进行正常交往，不得散布流言蜚语。

11.中标人在开展维保服务过程中须重视提高服务质量，必须做到但不限于做到以下几点：

（1）加强制度建设，经常听取服务对象的意见；中标人在项目运行过程中需逐步导入ISO9001:2008国际质量管理体系、ISO 27001:2022信息安全管理体系，逐步实现科学化的管理；以“国优”为工作目标，在双方的共同努力下，使得本项目在三年内达到信息设备维保优秀示范项目的标准；自觉接受校区管理部门的监督、考核。

（2）加强队伍建设，保持服务队伍的相对稳定；项目经理、各部门负责人、技术骨干等重要岗位人员必须经采购人管理部门审核同意后方可上岗，未经采购人管理部门许可不得更改；管理人员、从事维护服务的技术人员应按照国家有关规定取得人社部、工信部的计算机技术与软件专业技术资格证书（中级：网络工程师，信息安全工程师，高级：网络规划设计师、系统架构设计师、信息系统项目管理师）或国内知名IT企业认证：（华为认证HCIAHCIPHCIE；新华三认证（H3C）H3CNEH3CSEH3CIE）（如技术良好且服务质量优良者经采购人同意可以适当放宽要求），且须保证在合同服务期内保持持证人员的在岗数量；所有工作人员必须无犯罪记录。

（3）加强文化建设，经常开展员工培训活动；所有工作人员应具有良好的仪态，仪表及职业素养，佩戴服务标志，行为规范，服务主动、热情。

12.中标人在开展设备维护服务过程中须重视档案管理工

作：

（1）中标人应建立健全的管理服务档案，并负责及时记载有关变更情况，形成电子档案，年终考核时作为考核材料汇总至采购人。

（2）在设备维护服务合同终止时，中标人应当向采购人管理部门移交全部管理档案等资料；采购人管理部门如选聘了新的信息设备维保服务企业的，服务企业之间应当做好相关交接工作；若中标人未按约定完成移交事宜，采购人有权没收履约保证金。

13.除采购人明确要求的外，中标人不得将项目分包或转包给任何单位和个人。否则，采购人管理部门有权即刻终止合同，没收履约保证金，并要求中标人赔偿相应损失。

14.投标人必须承诺，中标后按《中标人须投入的设备清单》列出所投入本项目的设备，投标人必须提供设备名称、型号规格（或主要技术性能、参数）、生产厂家、数量、价格、购买年份等资料；如全部或部分设备为中标后新购的，投标人应作出承诺，在中标后进行采购；投标人必须承诺所有投入设备在服务期间仅限于本项目使用，且服务期间如设备损坏、丢失，投标人均需提供同类同性能设备供本项目使用。

15.投标人所提供的人员配置如在上述采购需求中有证件要求的，须在项目进场时提供证件原件至采购人处核验。

16.其他未尽事宜参照采购人管理部门相关管理规定。

17.系统配置及软硬件选型原则

为实现本项目的系统建设目标，实现系统高效、可靠、安全运行和管理，减少技术风险，确保信息安全，主要软硬件选型应遵循以下原则：

（1）先进成熟

根据总体设计的要求，采用较为先进、成熟的网络和信息安全厂商和产品。性能指标要满足业务系统的需求，产品线长，具有先进、完善的功能，稳定的运行效果和良好的可扩展性。选用国内生产厂商，确保信息安全。

（2）安全可靠

设备应符合安全方面的要求，符合有关国家标准、国际标准，以保证不同厂家系统设备之间的互操作性和系统的开放性。所有设备必须选用国产设备。所有设备都应具备自主知识产权、具备高效、成熟和低故障率，能长时间稳定运行。

设备采用环保材料，支持节能技术，减少环境污染和能源、资源损耗。

（3）支持服务

本项目在追求项目完整性和设备适应性的同时，要求供应商应具有完善的服务体系，提供专业、标准、多元化的服务和持续、高效、快捷的技术支持。要选择技术、资金实力雄厚，具有良好信誉并长期致力于政务领域发展的专业厂商，与其在信息化建设方面进行长期合作。

另一方面，还要考虑所选设备与现有系统所用设备兼容性和易操作性。应尽量保持与现有设备一致，可减少因设备间的兼容性而造成的故障，同时，更易于系统的集成和技术人员的熟练操作与维护。

（4）安全可信

本项目所采购的软硬件设备应选用安全可控的国产产品。

（十）中标人须投入的设备清单

序号	设备名称	功能及技术参数	数	单

			量	位
1	社湾核心交换机（社湾校区 ）	一、单台配置 1、主控引擎与业务板卡完全物理分离，采用全分布式转发处理架构，独立主控槽位≥2，业务槽位≥12，整机支持≥6个电源模块； 2、为了减少流量跨业务板卡进行传输，影响使用稳定性，要求所提供的实配总装机箱 1 套，主控板 2 块，交流电源模块 2 块，满配风扇框，单台配置≥70 个 40G 光口，≥96 个万兆光口，≥48 个千兆光口，≥48 个千兆电口； 3、设备交换容量≥1000Tbpss，包转发率≥230000 Mpps； 4、▲支持单槽位最大扩展 12 个 100G 业务接口； 二、参数要求 1、支持静态配置和动态学习 MAC 地址，支持查看和清除静态 MAC 地址； 2、支持静态路由、支持 RIP v1/v2、OSPF，支持策略路由、支持 VRRP； 3、支持 L2(Layer 2)~L4（Layer 4）包过滤功能，提供基于源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、TCP/UDP 协议、源/目的端口号、协议、VLAN 的非法帧过滤功能；	1	台

		4、支持交换机可视化呈现设备 IP 地址、MAC 地址、软件版本、多主检测状态、ARP 表项、路由表项、ACL 表项等资源利用率、电源状态、风扇状态等主要信息，方便直观运维 5、▲支持芯片级系统级 Flash 双启动，避免因 FLASH 芯片故障导致交换机无法启动； 6、为保障核心冗余，设备需支持横向 N:1 虚拟化（N≥2），可以将多台物理设备虚拟化为逻辑上的一台设备； **7、★支持配置静态 IP 地址、DNS 域名等多种方式上线网管平台（投标文件中提供功能截图）。** 8、▲支持业务板卡一键复位、下电、移除等功能，并支持可编辑板卡名称； 9、支持交换机板卡面板及可视化，整体机框状态直观可视，电源风扇、风扇状态可视，异常情况直观可视； 10、支持交换机电源系统冗余、1+1 冗余方式选择，并且可一键设置业务板上电优先级； 11、▲支持快速定位板卡功能；		
2	网络管理平台（社湾校区 ）	1、支持管理无线 AP 数≥3500 颗，管理交换机数≥800 台； 2、本次配置交换机管理授权 405 套。	1	套

		AP 管理授权 740 套； 3、支持最大在线用户数≥95000； 4、▲为保障数据读写效率和可靠性，需采用双硬盘设计，提供不少于 1TB 固态硬盘数据存储； 5、为保障设备运行可靠性，需支持双电源冗余； **6、★支持预配置部署上线，可以通过导入无线 AP 的 MAC 地址和 SN 码，AP 联网后无需任何配置即可发现无线控制器；（投标文件中提供功能截图）** 7、兼容设计：兼容的软件系统开发商包括但不限于华三、华为、锐捷、思科、信锐等； 8、支持分级管理的架构，总部控制器可以统一管理下属所有的分支控制器和 AP，配置能够自动同步，并且在总部控制器上能够查看整个无线网络的信息； 9、支持主流终端类型识别，例如：摄像头、路由器、办公设备、移动终端等 10、▲支持关闭终端不必要的端口服务，创建交换机和无线 AP 的东西向流量安全策略，实现全网安全风险拦截，实现内网终端之间风险拦截； 11、支持将核心业务区域设置成重点区		

		域，重点保障重点区域的接入体验； 12、▲支持智能无线自动调优功能，在不影响业务的情况下，能够基于历史无线数据，进行射频资源调优，支持查看调优记录； 13、▲为了方便后续管理与维护，须与光 AP、光交换机需统一品牌，提供承诺函。		
3	上网行为管理平台（社湾校区）	1、支持旁路部署和串联部署两种方式 2、支持识别邮件、游戏、P2P 流媒体、WEB 流媒体、金融交易、办公 OA、移动终端应用等主流应用； 3、可识别 6000 种网络应用，海量预分类的 URL 地址。 4、▲支持上网行为审计，可审计用户访问的 URL、网络应用类型、FTP 上传和下载的文件名、TELNET 执行的命令等 5、支持基于多元化应用识别管控，包括用户、接入位置、终端类型、终端 MAC 地址、时间段； 6、支持免审计策略，排除指定用户，对该用户的上网行为不进行审计； 7、▲支持与本地公安网监平台对接，按网监要求将审计数据上传至公安的网监平台 8、▲为了方便后续管理与维护，须与	1	套

		光 AP、光交换机需统一品牌，提供承诺函。		
4	代拨网关（社湾校区）	1、至少提供满足 30G 出口网关。 ★2、产品架构：系统支持通用 X86 平台（包括虚拟机）部署以及热备部署。**（标文件中应提供第三方检测机构出具的检测报告复印件证明材料）** 3、支持 PPPOE 代拨上网，支持最少 8 个终端共享账号带宽，支持拨号账号池工作模式，支持绑定拨号账号 MAC。 4、支持 https/http 定向，定向能判断浏览器 http 访问，减少无效其他软件 http 通信定向。 5、QINQ 功能：QINQ 环境下支持 PPPOE 认证接入、支持 IPoE 接入。 ▲6、WEB 管理功能，通过 HTTPS 实现 web 远程管理： ①支持实时配置、升级版本、配置文件管理、log 信息查看等功能。 ②支持实时查看在线用户、在线用户的带宽使用情况，提供历史信息和图表。 ③支持在不重启系统情况下，单独重启虚机实现带外管理。 ④支持实时查看宽带接入设备上认证计费的统计信息，包括认证总数、认证成功数、认证失败数等信息。	1	台

		⑤支持实时查看宽带接入设备上Portal 协议的统计信息，包括 Portal 协议数量、Portal 认证成功数量等。 7、支持用户异常断线处理： ①PPPOE 用户异常断线，宽带接入服务器可判断用户异常，将用户踢下线； ②IPoE 用户异常断线，宽带接入服务器可判断用户异常，将用户踢下线； ③PPPOE 代拨用户异常断线，外网 PPPOE 链路故障，宽带接入设备可判断用户异常，将用户踢下线（IPoE,PPPOE 代拨）。 8、下线清除 MAC 策略：支持用户在 portal 页面点击下线即可自动清除 mac； 9、5G 双域查询功能：支持针对 5G 接入终端以及接入用户进行在线状态查询、流量使用情况查询； 10、5G 双域管理功能：支持针对 5G 接入终端远程管理，包括远程重启、掉线告警（通过短信或者企业微信通知）； 11、支持自定义会话断线频度，下发会话数断线后重启服务或者重启系统。		
5	认证计费管理系统	1、认证性能：radius 认证效率：系统吞吐率(>3000 次/秒）；IPoE(Portal 认证）全流程压力测试：IPoE 认证压力测试：系统吞吐率(>1200 次/秒）；	1	台

		2、支持不同的认证接入： ①支持 PPPoE 认证，支持 PoE 认证。 ②支持 PPPoE 代拨认证。 ③支持 MAC 认证。 3、支持集中式管理与对接： ①提供自助开户页面，实现宽带开通、在线信息、绑定终端管理、修改密码、充值缴费、故障上报等支撑服务。 ②提供统一大屏，展示不同接入区域的用户开户数、在线用户数、在线终端数、活跃数；带宽实时速率等。 ③支持同时与多个统一身份平台进行对接，支持基于 LDAP 统一身份认证，支持 CAS、OAUTH 等协议，集成主流厂家（金智、东软等）的 API，实现统一认证或单点登录。 4、支持 radius coa 协议修改在线用户带宽、时长，以及下发强制下线操作。 5、支持第三方平台/设备对接； ①对接第三方接口，下发上下线认证记录，如审计设备。 须支持国内外主流厂商网关、多功能宽带接入路由器或者 AC 实现认证计费、带宽控制和强制下线等功能，同时须支持在内外层混合环境下实现用户一次登录多次认证通过。		

		②支持与校园一卡通系统对接 ③支持到期提醒功能，可通过短信/邮件/APP/企业微信等多种渠道通知上网用户。 6、支持对接防代理服务器，针对 ip 下线控制或限速限制. 支持白名单解控或管理人工解控， 并支持记录查询。 7、支持运营商对接与管理： ①支持运营商接入，与宽带接入控制联动实现用户身份智能选择运营商出口以及 DNS。 ②支持不同运营商认证失败信息自定义错误提示，将系统提示的登录错误转换为中文提示，用于学生识别报错类型，告知运维人员快速排除故障。支持批量导入 error code 列表。 ③支持多运营商用户统计，统计指定时间内所有运营商用户中使用过运营商服务的用户数量。 ④提供运营商月统计报表，展示每月不同运营商开户数、销户数、活动用户数趋势图。		
6	审计防代理网关	1、支持在 X86/Power 平台部署，支持物理硬件加速。 2、支持通过镜像端口旁路部署。 3、认证对接：支持和认证计费管理系	1	台

		统互动，根据账号停用用户，避免用户频繁更换IP，如对接产生费用，由中标人承担。 4、白名单配置：支持配置白名单，不监控用户。 5、支持多种行为代理控制； ①支持通过TTL特征判断代理行为。 ②支持通过小路由特征判断代理行为。 ③支持通过TCP windows大小判断代理行为。 ④支持通过User-Agent特征判断代理行为。 ⑤支持通过注入Cookie判断代理行为。 ⑦支持通过单IP的网络连接数判断代理行为。 6、防共享要求：支持检测校园目前主流共享设备（如GSWIFI）实现防共享接入控制，实现网络实名制，上网用户一人一号，防止上网共享行为。		
7	统一认证平台	1、系统采用B/S架构，适配主流浏览器 2、平台最大管理账号数不低于50000，在线用户数量可达8000 3、平台应持802.1x、Portal、MAC地址认证、CA证书认证、802.1X WEP等企业认证；	1	套

		4、平台应支持二维码审核认证、短信认证、APP 认证、临时访客账号等访客认证方式； 5、★支持对接钉钉、企业微信等做基于 OAuth2.0 协议的用户认证，以实现多用户认证可靠、安全且高效的认证管理。**（投标文件中提供功能截图）** 6、为保障无线认证体验统一，平台需支持兼容多品牌设备统一认证，兼容的软件系统开发商包括但不限于华三、华为、锐捷、思科、信锐、Aruba、Ruckus 等至少 3 家 7、▲为更好地保障用户认证体验，支持用户业务随行，将用户和 IP 解耦，实现用户移动到不同位置可以获取相同的访问权限； 8、为更好地为用户提供认证推广服务，支持灵活的设置 Portal 认证页面内容，可基于接入位置、终端类型、用户名、运营商等信息呈现不同的 Portal 认证页面。 9、▲为了方便后续管理与维护，须与光 AP、光交换机需统一品牌。		
8	终端识别管理	1、系统采用 B/S 架构，适配主流浏览器 2、支持终端类型库，基于指纹自动识	1	套

		别PC、路由器、摄像头设备、无线AP等 3、支持基于终端类型进行准入控制，可对非指定类型终端非法接入，通过短信通知、手机APP通知，并同时将终端加入黑名单冻结； 4、支持自定义终端指纹特征，可快速添加新类型终端入库，保证终端识别的准确性； 5、支持基于时间、逻辑区域、服务类型、访问状态、攻击类型等多个维度统计访问终端和被访问终端的详细信息 6、★支持东西向流量安全策略，实现全网安全风险拦截，实现内网终端之间风险拦截。**（投标文件中提供功能截图）** 7、▲为了方便后续管理与维护，须与光AP、光交换机需统一品牌。		
9	智能分析平台	1、系统使用B/S架构，基于主流Web浏览器进行界面展示呈现，方便管理员实时掌握网络状况； 2、★支持通过独立扫描硬件射频模拟终端，对无线网络服务进行检测，包括网络接入、DHCP、网关、DNS、网络地址等阶段的时延和质量检测，预警网络风险；**（投标文件中提供功能截图）** 3、支持查看接入用户列表，用户信息	1	套

		主要包括用户 MAC、用户名、接入次数、质差时长、接入类型、最近上线状态、总体验时长、平均速率、总流量等； 4、支持将核心业务区域设置成重点区域，重点保障重点区域的接入体验；5、支持至少 1000 巡检项，便于对网络进行更全面的巡检 6、支持基于用户接入的关联、认证（802.1x 认证、Portal 认证、MAC 认证）、DHCP 三个阶段，进行协议级别的过程呈现，通过细化各个协议交互阶段结果与耗时，提供用户接入过程问题的精细化分析； 7、▲支持 7*24 小时主动巡检功能，覆盖设备、网络状态、设备运行情况、服务状态等巡检项目 8、★支持一键调优、定时调优、无线自动调优等至少三种方式，以便用户在不同场景使用，来保障用户在使用网络时始终处于最优；**（投标文件中提供功能截图）** 9、支持至少 1000 个异常处置建议，帮助用户精准识别异常问题并给出针对性的修复建议 10、支持识别至少 6000 种主流应用，海量预分类的 URL 地址；		

		11、▲为更好地保障关键业务/应用体验，系统支持对关键业务的访问质量进行评估，包括但不限于丢包、抖动、延时、连通性、服务器繁忙等指标，从而帮助用户对关键业务进行排障； 12、▲为了方便后续管理与维护，须与光AP、光交换机需统一品牌，提供承诺函。		
10	光交换机	1、▲1G/2.5G光口≥24个，10G/25G SFP28光口≥4，配置10G/25G SFP28光模块1个，40G QSFP+光口≥2个；满配2.5G光模块； 2、交换容量≥2Tbps，包转发率≥750Mpps； 3、支持MAC地址≥32K,支持4K个VLAN，支持MAC地址自动学习，支持源MAC地址过滤，支持接口MAC地址学习个数限制； 4、支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； 5、▲支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计； 6、支持静态IP地址、DNS域名发现网	48	台

		管中心平台； 7、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换； 8、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 9、支持终端类型库，基于指纹自动识别 PC、路由器、摄像头设备、无线 AP 等； 10、★为提高系统兼容性对接，需支持联动第三方安全设备或平台，通过联动实现从系统及接入层交换机对风险终端 MAC 地址进行封堵；**（投标文件中提供功能截图）**		
11	万兆光汇聚	1、▲万兆光口≥48 个，满配万兆光模块，40G/100G QSFP28 光口≥8 个，配置 40G/100G QSFP28 光模块 2 个； 2、设备的交换容量≥8Tbps，包转发率≥3000Mpps； 3、支持电源数量≥2 个，冗余风扇≥5 个； 4、支持 MAC 地址≥160K； 5、支持静态路由、RIPv1/2、OSPF、策略路由； 6、★支持基于优先级的流量控制（PFC），显示拥塞通知（ECN）；**（投标文件中提供功能截图）**	4	台

		7、支持堆叠、M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； 8、支持在交换机上创建东西向安全策略，实现全网安全风险拦截； 9、支持联动第三方安全设备或平台，通过联动实现从系统及接入层交换机对风险终端 MAC 地址进行封堵； 10、支持通过配置静态 IP 地址、DNS 域名发现网管中心平台； 11、▲为保证设备在受到外界机械碰撞时能够正常运行，要求所投交换机防护测试等级至少达到 IK06； 12、支持 SNMPv1/v2c/v3、支持 Console、Telnet、SSH； 13、支持通过 APP 进行远程管理，并且可以修改交换机网络配置；		
12	24 口 POE 交换机	1、设备的交换容量≥670Gbps，包转发率≥120Mpps（每台配 2 个万兆单模光模块）； 2、千兆 POE 电口≥24 个，10G SFP 光口≥4 个，配置 10G SFP 光模块 1 个； 3、支持 IEEE802.3af/at 供电标准，单端口最大输出功率≥30W，整机最大输出功率≥370W； 4、支持 MAC 地址≥16K，支持 MAC 地址	56	台

		自动学习；支持源 MAC 地址过滤； 5、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 6、上线方式：支持静态 IP 地址、DHCP Option 43、DNS 域名等多种方式上线网管平台； 7、支持通过在网管中心平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息； 8、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换；9、支持 IEEE802.3az 标准的 EEE 节能技术：当 EEE 使能时，大幅度减小端口在该阶段的功耗，达到节能目的； 10、支持通过网管中心平台图形化操作对交换机端口状态的开启与关闭； 11、支持通过网管中心平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作； 12、支持通过网管中心平台查看交换机处于工作端口的发送与接收的流量趋势；		
13	8 口 POE 交换机	1、设备的交换容量≥670Gbps，包转发率≥100Mpps 2、千兆 POE 电口≥8 个，1G/2.5G 光口≥2 个，配置 1G/2.5G 光模块 1 个。	218	台

		3、支持 IEEE802.3af/at 供电标准，单端口最大输出功率≥30W，整机最大输出功率≥125W； 4、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 5、支持配置静态 IP 地址、DNS 域名等多种方式上线网管平台； 支持通过在网管中心平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息 7、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换。 8、支持 IEEE802.3az 标准的 EEE 节能技术：当 EEE 使能时，大幅度减小端口在该阶段的功耗，达到节能目的； 9、支持通过网管中心平台图形化操作对交换机端口状态的开启与关闭； 10、支持通过网管中心平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作； 11、支持通过网管中心平台查看交换机处于工作端口的发送与接收的流量趋势；		
14	24 口交换机	1、千兆电口≥24 个,10G 光口≥4 个（每台配 2 个万兆单模光模块）； 2、设备的交换容量≥670Gbps，包转发	76	台

		率≥120Mpps； 3、支持静态路由、RIPv1/2、OSPF、策略路由； 4、设备支持M-LAG技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； 5、支持终端IP-MAC绑定，当IP+MAC不对应时，可以将终端加入黑名单实现断开终端流量； 6、★支持在交换机上创建东西向安全策略，实现全网安全风险拦截；**（投标文件中提供功能截图）** 7、支持IEEE802.3az标准的EEE节能技术：当EEE使能时，大幅度减小端口在该阶段的功耗，达到节能目的； 8、支持SNMPv1/v2c/v3、支持Console、Telnet、SSH； 9、支持防网关ARP欺骗，支持端口保护、隔离、防止ARP泛洪攻击功能； 10、支持DHCP Snooping，支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应DHCP报文； 11、支持基于终端类型自动识别结果，禁止非法终端（例如私接路由器）接入； 12、支持联动第三方安全设备或平台，		

		通过联动实现从系统及接入层交换机对风险终端MAC地址进行封堵； 13、支持通过配置静态IP地址、DNS域名发现网管中心平台； 14、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换；		
15	光AP	1、▲产品需支持802.11be 协议，兼容802.11a/b/g/n/ac/ax协议，支持2.4G和5G同时工作； 2、整机无线空间流≥4条，理论无线传输速率＞3.5Gbps； 3、▲2.5G上行光口≥1个，配置2.5G光模块一个，千兆上行网口≥1个，同时提供额外的千兆以太网口≥4个，可供有线终端直接接入；提供1个USB2.0接口； 4、支持Fat和Fit 两种工作模式，可根据网络规划需要灵活切换； 5、支持虚拟AP技术，单射频SSID数量最高支持≥16，整机≥32； 6、支持静态IP地址、DNS域名发现网管中心平台； 7、支持逃生模式，AP与控制器连接中断后，原有用户在线、新用户正常接入，业务不中断； 8、▲支持联动安全策略，通过安全策	644	台

		略可以实现对疑似感染病毒或已感染病毒的无线客户端进行识别、监控与隔离等多种方式的处理；		
16	高密吸顶AP	1、▲支持802.11be 协议，兼容802.11a/b/g/n/ac/ax协议，支持2.4G和5G同时工作； 2、整机采用三射频设计，理论无线传输速率＞3.7Gbps； 3、Wi-Fi 7单终端接入时，在多链路操作特性下吞吐量≥2.3Gbps； 4、▲内置独立扫描硬件射频，可在不影响业务接入前提下支持实时检测并反制环境非法Wi-Fi； 5、▲2.5G上行光口≥1个，配置对应2.5G光模块一个，下行千兆以太网口≥4个，可供有线终端直接接入； 6、支持Fat和Fit 两种工作模式，可根据网络规划需要灵活切换； 7、支持AP零配置上线，支持二三层发现、DNS、域名等多种自动发现机制； 8、支持无线带宽平均分配，让不同协商速率终端占用相等无线信道时间，防止低速终端拉低网络整体速度； 9、具备无线网络环境指标检测功能，包括信道总利用率、Wi-Fi 信道利用率、非 Wi-Fi 信道利用率、同频 AP 数	119	台

		量等； 10、为了降低无线网络优化难度，AP 结合管理平台可实现无线网络信道自动优化功能； 11、▲主动对无线网络服务检测，包括网络接入、DHCP、网关、DNS、网络地址等阶段的时延和质量检测； 12、▲为了保障内网无线流量安全，AP 结合管理平台可实现识别记录异常终端访问行为，并执行策略阻断风险终端访问动作；		
17	室外 AP	1、▲支持 802.11ax 协议，兼容 802.11a/b/g/n/ac 协议，支持 2.4G 和 5G 同时工作； 2、整机采用双射频四空间流设计，理论无线传输速率＞2.9Gbps； 3、整机最大接入终端数≥1000； 4、▲配置≥1 个千兆网口，≥1 个千兆光口，配置对应光模块一个 5、为适应室外环境，具备 IP68 防护等级，可工作在-40-70° 宽温环境 6、支持 Fat 和 Fit 两种工作模式，可根据网络规划需要灵活切换； 7、支持虚拟 AP 技术，单射频 SSID 数量最高支持≥16，整机≥32； 8、支持静态 IP 地址、DNS 域名等多种	36	台

		自动发现机制； 9、▲支持逃生模式，AP 与控制器连接中断后，原有用户在线、新用户正常接入，业务不中断； 10、支持无线带宽平均分配，让不同协商速率终端占用相等无线信道时间，防止低速终端拉低网络整体速度； 11、▲为了保障内网无线流量安全，AP 结合管理平台可实现识别记录异常终端访问行为，并执行策略阻断风险终端访问动作； 12、▲具备无线网络环境指标监测功能，包括信道总利用率、Wi-Fi 信道利用率、非 Wi-Fi 信道利用率、同频 AP 数量等；		
18	2.5G 光模块	1、产品类型：SFP 2.5G 光模块 2、光纤类型：单模 3、传输模式：单纤双向 4、发送波长：TX 1310 nm 5、接收波长：RX 1550 nm 6、最大传输距离：10 km	253	套
19	40G 光模块	1、光纤类型：单模双纤； 2、光接口类型：LC； 3、速率：40Gbps； 4、波长：1310nm 发送；1310nm 接收； 5、传输距离：10km。	104	套

20	XGPON OLT（社湾宿舍区）	1、下行接口：提供XG-PON接口≥72个（含XGPON模块）,整机最大支持≥144个XGPON接口；上行接口：提供8个25G/10G 光接口,提供4个100G/40G 光接口 （提供4个40G多模光模块）； 2、设备带宽：每业务槽位最大带宽不低于200 Gbit/s，主控板交换容量不低于8Tbit/s,二层包转发率≥50000Mpps； 3、地址表项:整机MAC地址表项≥570K，整机ARP地址表项≥90K； 4、双栈：支持IPv4与IPv6双栈转发，支持三层RIP、OSPF、ISIS、BGP等路由协议，支持MPLS OAM/RSVP-TE/VxLAN等特性； 5、流氓ONU：支持ONU下挂AP查询，支持流氓ONU检测功能，可实现秒级实时检测和流氓ONU自动隔离； 6、SRV6特性：支持SRv6功能，可以通过扩展IPv6报文的头域，实现类似标签转发的处理，便于IPv6转发路径的流量调优，保障现有网络平滑演进到SDN网络； 7、工作环境：设备的运行环境温度范围0° C 到 +45° C,设备的运行环境湿度范围 5% RH 到 95% RH；	1	台

		8、虚拟化：支持堆叠功能或虚拟化功能，最大支持 4 台 OLT 虚拟化，主备 OLT 的上行链路可以跨框聚合，实现负荷分担，主备 OLT 的管理界面、管理 IP 统一，登录主设备后就能对整个系统进行管理； 9、DHCP：设备支持 DHCP Option82 标识接入线路标识，支持根据 DHCP Option60 选择 DHCP Server 主备服务器； 10、提供设备软硬件 3 年维保；		
21	分光器 1x32	1、支持进行机架式上架使用 2、光分路器-单模-1×32 均分-SC/UPC； 2、插入损耗（dB）<17； 3、回损耗（dB）>50； 4、工作波长 1260~1360nm & 1480~1560nm； 5、输入输出接头类型 SC/PC； 6、工作温度-10℃～70℃；	59	个
22	4 口 ONU Wi-Fi6	1、上行口：为保证设备性能，要求提供 XG-PON 接口≥1 个； 2、下行口：提供下行千兆以太网接口≥4； 3、无线性能：为保证设备性能所提供的 ONU 为内置天线，无外置天线，无线支持 2.4G/5G Wi-Fi6 工作模式	1279	个

		4、支持接入ONT智能管理系统，实现集中管理、集中配置； 5、配合宽带接入网关，提供终端用户统一管理、认证、审计等服务； 6、支持IPV4/IPV6双协议栈；多SSID（8个SSID）；支持桥接组网等； 7、提供设备3年维保；		
23	ONT智能管理系统	ONT智能管理系统作为无源光局域网中ONT网管设备，统一管理配置ONT设备，提高运维效率。 设备功能：远程下发ONT配置、Wi-Fi信道管理、功率设置、批量升级、状态查询，告警功能等； 硬件参数：1U主机机箱，6个固定100/1000M RJ45电口，1个串口，1个交流电源模块1个风扇模块,电源线缆,安装配件）。ONT系统管理license授权1500个。	1	套
24	网络管理平台（官塘校区）	1、支持管理无线AP数≥3500颗，管理交换机数≥800台； 2、本次配置交换机管理授权405套。AP管理授权740套； 3、支持最大在线用户数≥95000； 4、为保障数据读写效率和可靠性，需采用双硬盘设计，提供不少于1TB 固态硬盘数据存储；	1	台

		5、为保障设备运行可靠性，需支持双电源冗余； 6、支持预配置部署上线，可以通过导入无线 AP 的 MAC 地址和 SN 码，AP 联网后无需任何配置即可发现无线控制器； 7、兼容设计：兼容的软件系统开发商包括但不限于华三、华为、锐捷、思科、信锐等； 8、支持分级管理的架构，总部控制器可以统一管理下属所有的分支控制器和 AP，配置能够自动同步，并且在总部控制器上能够查看整个无线网络的信息； 9、支持主流终端类型识别，例如：摄像头、路由器、办公设备、移动终端等 10、支持关闭终端不必要的端口服务，创建交换机和无线 AP 的东西向流量安全策略，实现全网安全风险拦截，实现内网终端之间风险拦截； 11、支持将核心业务区域设置成重点区域，重点保障重点区域的接入体验； 12、支持智能无线自动调优功能，在不影响业务的情况下，能够基于历史无线数据，进行射频资源调优，支持查看调优记录； 13、为了方便后续管理与维护，须与		

		光 AP、光交换机需统一品牌，提供承诺函。		
25	上网行为管理平台（官塘校区）	1、支持旁路部署和串联部署两种方式 2、支持识别邮件、游戏、P2P 流媒体、WEB 流媒体、金融交易、办公 OA、移动终端应用等主流应用； 3、可识别 6000 种网络应用，海量预分类的 URL 地址 4、支持上网行为审计，可审计用户访问的 URL、网络应用类型、FTP 上传和下载的文件名、TELNET 执行的命令等 5、支持基于多元化应用识别管控，包括用户、接入位置、终端类型、终端 MAC 地址、时间段； 6、支持免审计策略，排除指定用户，对该用户的上网行为不进行审计； 7、支持与本地公安网监平台对接，按网监要求将审计数据上传至公安的网监平台； 8、为了方便后续管理与维护，须与光 AP、光交换机需统一品牌；	1	套
26	代拨网关	1、至少提供满足 30G 出口网关。 2、产品架构：系统支持通用 X86 平台（包括虚拟机）部署以及热备部署。 3、支持 PPPOE 代拨上网，支持最少 8 个终端共享账号带宽，支持拨号账号池	1	台

		工作模式，支持绑定拨号账号 MAC。 4、支持 https/http 定向，定向能判断浏览器 http 访问，减少无效其他软件 http 通信定向。 5、QINQ 功能：QINQ 环境下支持 PPPOE 认证接入、支持 IPoE 接入。 6、WEB 管理功能，通过 HTTPS 实现 web 远程管理： ①支持实时配置、升级版本、配置文件管理、log 信息查看等功能。 ②支持实时查看在线用户、在线用户的带宽使用情况，提供历史信息和图表。 ③支持在不重启系统情况下，单独重启虚机实现带外管理。 ④支持实时查看宽带接入设备上认证计费的统计信息，包括认证总数、认证成功数、认证失败数等信息。 ⑤支持实时查看宽带接入设备上 Portal 协议的统计信息，包括 Portal 协议数量、Portal 认证成功数量等。 7、支持用户异常断线处理： ①PPPOE 用户异常断线，宽带接入服务器可判断用户异常，将用户踢下线； ②IPoE 用户异常断线，宽带接入服务器可判断用户异常，将用户踢下线； ③PPPOE 代拨用户异常断线，外网 PPPOE		

		链路故障，宽带接入设备可判断用户异常，将用户踢下线（IPoE,PPPOE 代拨）。 8、下线清除 MAC 策略：支持用户在 portal 页面点击下线即可自动清除 mac; 9、5G 双域查询功能：支持针对 5G 接入终端以及接入用户进行在线状态查询、流量使用情况查询; 10、5G 双域管理功能：支持针对 5G 接入终端远程管理，包括远程重启、掉线告警（通过短信或者企业微信通知）; 11、支持自定义会话断线频度，下发会话数断线后重启服务或者重启系统。		
27	审计防代理网关	1、支持在 X86/Power 平台部署，支持物理硬件加速。 2、支持通过镜像端口旁路部署。 3、认证对接：支持和认证计费管理系统互动，根据账号停用用户，避免用户频繁更换 IP，如对接产生费用，由中标人承担。 4、白名单配置：支持配置白名单，不监控用户。 5、支持多种行为代理控制 ①支持通过 TTL 特征判断代理行为。 ②支持通过小路由特征判断代理行为。 ③支持通过 TCP windows 大小判断代理	1	台

		行为。 ④支持通过User-Agent特征判断代理行为。 ⑤支持通过注入Cookie判断代理行为。 ⑦支持通过单IP的网络连接数判断代理行为。 6、防共享要求：支持检测校园目前主流共享设备（如GSWIFI）实现防共享接入控制，实现网络实名制，上网用户一人一号，防止上网共享行为。		
28	统一认证平台（官塘校区）	1、系统采用B/S架构，适配主流浏览器 2、平台最大管理账号数不低于50000，在线用户数量可达8000 3、平台应持802.1x、Portal、MAC地址认证、CA证书认证、802.1X WEP等企业认证； 4、平台应支持二维码审核认证、短信认证、APP认证、临时访客账号等访客认证方式； 5、支持对接钉钉、企业微信等做基于OAuth2.0协议的用户认证，以实现多用户认证可靠、安全且高效的认证管理 5、支持Portal认证页面自定义，包括页面展示信息、页面标题、文字描述、免责声明等信息	1	套

		为更好地帮助单位推广媒体，平台应提供认证推广功能，可以支持抖音、快手、B 站等主流媒体平台跳转 6、为保障无线认证体验统一，平台需支持兼容多品牌设备统一认证，兼容的软件系统开发商包括但不限于华三、华为、锐捷、思科、信锐、Aruba、Ruckus 等至少 3 家 7、为更好地保障用户认证体验，支持用户业务随行，将用户和 IP 解耦，实现用户移动到不同位置可以获取相同的访问权限； 8、为更好地为用户提供认证推广服务，支持灵活的设置 Portal 认证页面内容，可基于接入位置、终端类型、用户名、运营商等信息呈现不同的 Portal 认证页面		
29	终端识别管理	1、系统采用 B/S 架构，适配主流浏览器 2、支持终端类型库，基于指纹自动识别 PC、路由器、摄像头设备、无线 AP 等 3、支持基于终端类型进行准入控制，可对非指定类型终端非法接入，通过短信通知、手机 APP 通知，并同时将终端加入黑名单冻结；	1	套

		4、支持自定义终端指纹特征，可快速添加新类型终端入库，保证终端识别的准确性； 5、支持基于时间、逻辑区域、服务类型、访问状态、攻击类型等多个维度统计访问终端和被访问终端的详细信息 6、支持东西向流量安全策略，实现全网安全风险拦截，实现内网终端之间风险拦截； 7、为了方便后续管理与维护，须与光AP、光交换机需统一品牌。		
30	智能分析平台	1、系统使用B/S架构，基于主流Web浏览器进行界面展示呈现，方便管理员实时掌握网络状况； 2、支持通过独立扫描硬件射频模拟终端，对无线网络服务进行检测，包括网络接入、DHCP、网关、DNS、网络地址等阶段的时延和质量检测，预警网络风险； 3、支持查看接入用户列表，用户信息主要包括用户 MAC、用户名、接入次数、质差时长、接入类型、最近上线状态、总体验时长、平均速率、总流量等； 4、支持将核心业务区域设置成重点区域，重点保障重点区域的接入体验； 5、支持至少100巡检项，便于对网络	1	套

		进行更全面的巡检 6、支持基于用户接入的关联、认证（802.1x 认证、Portal 认证、MAC 认证）、DHCP 三个阶段，进行协议级别的过程呈现，通过细化各个协议交互阶段结果与耗时，提供用户接入过程问题的精细化分析； 7、支持 7*24 小时主动巡检功能，覆盖设备、网络状态、设备运行情况、服务状态等巡检项目 8、支持一键调优、定时调优、无线自动调优等至少三种方式，以便用户在不同场景使用，来保障用户在使用网络时始终处于最优； 9、支持至少 100 个异常处置建议，帮助用户精准识别异常问题并给出针对性的修复建议 10、支持识别至少 6000 种主流应用，海量预分类的 URL 地址； 11、为更好地保障关键业务/应用体验，系统支持对关键业务的访问质量进行评估，包括但不限于丢包、抖动、延时、连通性、服务器繁忙等指标，从而帮助用户对关键业务进行排障； 12、为了方便后续管理与维护，须与光 AP、光交换机需统一品牌。		

31	光交换机	1、1G/2.5G 光口≥24 个，10G/25G SFP28 光口≥4，40G QSFP+光口≥2 个，满配 40G QSFP+光模块；满配 2.5G 光模块； 2、交换容量≥2Tbps，包转发率≥ 750Mpps； 3、支持 MAC 地址≥32K，支持 4K 个 VLAN，支持 MAC 地址自动学习，支持源 MAC 地址过滤，支持接口 MAC 地址学习个数限制； 4、支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面；5、支持查看安全事件记录、终端类型异常记录、终端在端口迁移次数、终端地址异常记录等安全事件的记录统计； 6、支持静态 IP 地址、DNS 域名发现网管中心平台； 支持通过网管中心平台一键替换“按钮”即可完成故障设备替换； 8、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 9、支持终端类型库，基于指纹自动识别 PC、路由器、摄像头设备、无线 AP 等； 10、为提高系统兼容性对接，需支持联动第三方安全设备或平台，通过联动实	60	台

		现从系统及接入层交换机对风险终端MAC 地址进行封堵；		
32	万兆光汇聚	1、万兆光口≥48 个，满配万兆光模块，40G/100G QSFP28 光口≥8 个，配置40G/100G QSFP28 光模块 2 个； 2、设备的交换容量≥8Tbps，包转发率≥3000Mpps； 3、支持电源数量≥2 个，冗余风扇≥5 个； 4、支持 MAC 地址≥160K； 5、支持静态路由、RIPv1/2、OSPF、策略路由； 6、支持基于优先级的流量控制（PFC），显式拥塞通知（ECN）； 7、支持堆叠、M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； 8、支持在交换机上创建东西向安全策略，实现全网安全风险拦截； 9、支持联动第三方安全设备或平台，通过联动实现从系统及接入层交换机对风险终端 MAC 地址进行封堵； 10、支持通过配置静态 IP 地址、DNS 域名发现网管中心平台； 11、为保证设备在受到外界机械碰撞时能够正常运行，要求所投交换机防护测	7	台

		试等级至少达到 IK06； 12、支持 SNMPv1/v2c/v3、支持 Console、Telnet、SSH； 13、支持通过 APP 进行远程管理，并且可以修改交换机网络配置；		
33	24 口 POE 交换机	1、设备的交换容量≥670Gbps，包转发率≥120Mpps； 2、千兆 POE 电口≥24 个，10G SFP 光口≥4 个，配置 2 个万兆单模光模块； 3、支持 IEEE802.3af/at 供电标准，单端口最大输出功率≥30W，整机最大输出功率≥370W； 4、支持 MAC 地址≥16K，支持 MAC 地址自动学习；支持源 MAC 地址过滤； 5、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 6、上线方式：支持静态 IP 地址、DHCP Option 43、DNS 域名等多种方式上线网管平台； 7、支持通过在网管中心平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息； 8、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换； 9、支持 IEEE802.3az 标准的 EEE 节能技术：当 EEE 使能时，大幅度减小端口	52	台

		在该阶段的功耗，达到节能目的； 10、支持通过网管中心平台图形化操作对交换机端口状态的开启与关闭； 11、支持通过网管中心平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作； 12、支持通过网管中心平台查看交换机处于工作端口的发送与接收的流量趋势；		
34	8 口 POE 交换机	1、设备的交换容量≥670Gbps，包转发率≥100Mpps 2、千兆 POE 电口≥8 个，1G/2.5G 光口≥2 个，满配光模块。 3、支持 IEEE802.3af/at 供电标准，单端口最大输出功率≥30W，整机最大输出功率≥125W； 4、支持通过 APP 进行远程管理，并且可以修改交换机网络配置； 5、支持配置静态 IP 地址、DNS 域名等多种方式上线网管平台； 支持通过在网管中心平台的 Web 页面对交换机进行可视化管理查看，包括交换机的端口状态及配置、vlan 信息 7、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换 支持 IEEE802.3az 标准的 EEE 节能技	329	台

		术：当 EEE 使能时，大幅度减小端口在该阶段的功耗，达到节能目的； 9、支持通过网管中心平台图形化操作对交换机端口状态的开启与关闭； 10、支持通过网管中心平台查看交换机面板端口工作状态，通过端口颜色显示状态即可判断端口是否在线工作； 11、支持通过网管中心平台查看交换机处于工作端口的发送与接收的流量趋势；		
35	24 口交换机	1、千兆电口≥24 个,10G 光口≥4 个（每台配 2 个万兆单模光模块）； 2、设备的交换容量≥670Gbps，包转发率≥120Mpps； 3、支持静态路由、RIPv1/2、OSPF、策略路由； 4、设备支持 M-LAG 技术，跨设备链路聚合（非堆叠技术实现），要求配对的设备有独立的控制平面； 5、支持终端 IP-MAC 绑定，当 IP+MAC 不对应时，可以将终端加入黑名单实现断开终端流量； 6、支持在交换机上创建东西向安全策略，实现全网安全风险拦截； 7、支持 IEEE802.3az 标准的 EEE 节能技术：当 EEE 使能时，大幅度减小端口	79	台

		在该阶段的功耗，达到节能目的； 8、支持 SNMPv1/v2c/v3、支持 Console、Telnet、SSH； 9、支持防网关 ARP 欺骗，支持端口保护、隔离、防止 ARP 泛洪攻击功能； 10、支持 DHCP Snooping，支持交换机端口设置为信任端口或非信任端口，非信任端口也可设置白名单响应 DHCP 报文； 11、支持基于终端类型自动识别结果，禁止非法终端（例如私接路由器）接入； 12、支持联动第三方安全设备或平台，通过联动实现从系统及接入层交换机对风险终端 MAC 地址进行封堵； 13、支持通过配置静态 IP 地址、DNS 域名发现网管中心平台； 14、支持通过网管中心平台一键替换“按钮”即可完成故障设备替换；		
36	光 AP	1、产品需支持 802.11be 协议，兼容 802.11a/b/g/n/ac/ax 协议，支持 2.4G 和 5G 同时工作； 2、整机无线空间流≥4 条，理论无线传输速率＞3.5Gbps； 3、2.5G 上行光口≥1 个，配置 2.5G 光模块，千兆上行网口≥1 个，同时提供额外的千兆以太网口≥4 个，可供有线	986	台

		终端直接接入；提供1个USB2.0接口； 4、支持Fat和Fit 两种工作模式，可根据网络规划需要灵活切换； 5、支持虚拟AP技术，单射频SSID数量最高支持≥16，整机≥32； 6、支持静态IP地址、DNS域名发现网管中心平台； 7、支持逃生模式，AP与控制器连接中断后，原有用户在线、新用户正常接入，业务不中断； 8、支持联动安全策略，通过安全策略可以实现对疑似感染病毒或已感染病毒的无线客户端进行识别、监控与隔离等多种方式的处理；		
37	高密吸顶AP	1、支持802.11be 协议，兼容802.11a/b/g/n/ac/ax协议，支持2.4G和5G同时工作； 2、整机采用三射频设计，理论无线传输速率＞3.7Gbps； 3、Wi-Fi 7单终端接入时，在多链路操作特性下吞吐量≥2.3Gbps； 4、内置独立扫描硬件射频，可在不影响业务接入前提下支持实时检测并反制环境非法Wi-Fi； 5、2.5G上行光口≥1个，配置2.5G光模块，下行千兆以太网口≥4个，可供	172	台

		有线终端直接接入； 6、支持 Fat 和 Fit 两种工作模式，可根据网络规划需要灵活切换； 7、支持 AP 零配置上线，支持二三层发现、DNS、域名等多种自动发现机制； 8、支持无线带宽平均分配，让不同协商速率终端占用相等无线信道时间，防止低速终端拉低网络整体速度； 9、具备无线网络环境指标检测功能，包括信道总利用率、Wi-Fi 信道利用率、非 Wi-Fi 信道利用率、同频 AP 数量等； 10、为了降低无线网络优化难度，AP 结合管理平台可实现无线网络信道自动优化功能； 11、主动对无线网络服务检测，包括网络接入、DHCP、网关、DNS、网络地址等阶段的时延和质量检测； 12、为了保障内网无线流量安全，AP 结合管理平台可实现识别记录异常终端访问行为，并执行策略阻断风险终端访问动作；		
38	室外 AP	1、支持 802.11ax 协议，兼容 802.11a/b/g/n/ac 协议，支持 2.4G 和 5G 同时工作； 2、整机采用双射频四空间流设计，理	38	台

		论无线传输速率＞2.9Gbps； 3、整机最大接入终端数≥1000； 4、配置≥1 个千兆网口，≥1 个千兆光口，配置对应光模块。 5、为适应室外环境，具备 IP68 防护等级，可工作在-40-70°宽温环境 6、支持 Fat 和 Fit 两种工作模式，可根据网络规划需要灵活切换； 7、支持虚拟 AP 技术，单射频 SSID 数量最高支持≥16，整机≥32； 8、支持静态 IP 地址、DNS 域名等多种自动发现机制； 9、支持逃生模式，AP 与控制器连接中断后，原有用户在线、新用户正常接入，业务不中断； 10、支持无线带宽平均分配，让不同协商速率终端占用相等无线信道时间，防止低速终端拉低网络整体速度； 11、为了保障内网无线流量安全，AP 结合管理平台可实现识别记录异常终端访问行为，并执行策略阻断风险终端访问动作； 12、具备无线网络环境指标监测功能，包括信道总利用率、Wi-Fi 信道利用率、非 Wi-Fi 信道利用率、同频 AP 数量等；		
39	2.5G 光模块	1、产品类型：SFP 2.5G 光模块	369	套

		2、光纤类型：单模 3、传输模式：单纤双向 4、发送波长：TX 1310 nm 5、接收波长：RX 1550 nm 6、最大传输距离：10 km		
40	40G 光模块	1、光纤类型：单模双纤； 2、光接口类型：LC； 3、速率：40Gbps； 4、波长：1310nm 发送；1310nm 接收； 5、传输距离：10km。	134	套
41	XGPON OLT（官塘校区宿舍区）	1、下行接口：提供 XG-PON 接口≥96 个（含 XGPON 模块）,整机最大支持≥144 个 XGPON 接口；上行接口：提供 8 个 25G/10G 光接口,提供 4 个 100G/40G 光接口 （提供 4 个 40G 多模光模块）； 2、设备带宽：每业务槽位最大带宽不低于 200 Gbit/s，主控板交换容量不低于 8.3Tbit/s,二层包转发率≥ 50000Mpps； 3、地址表项:整机 MAC 地址表项≥570K，整机 ARP 地址表项≥90K； 4、双栈：支持 IPv4 与 IPv6 双栈转发，支持三层 RIP、OSPF、ISIS、BGP 等路由协议，支持 MPLS OAM/RSVP-TE/VxLAN 等特性； 5、流氓 ONU：支持 ONU 下挂 AP 查询，	1	台

		支持流氓ONU检测功能，可实现秒级实时检测和流氓ONU自动隔离； 6、SRV6特性：支持SRv6功能，可以通过扩展IPv6报文的头域，实现类似标签转发的处理，便于IPv6转发路径的流量调优，保障现有网络平滑演进到SDN网络； 7、工作环境：设备的运行环境温度范围0° C 到 +45° C，设备的运行环境湿度范围 5% RH 到 95% RH； 8、虚拟化：支持堆叠功能或虚拟化功能，最大支持4台OLT虚拟化，主备OLT的上行链路可以跨框聚合，实现负荷分担，主备OLT的管理界面、管理IP统一，登录主设备后就能对整个系统进行管理； 9、DHCP：设备支持DHCP Option82标识接入线路标识，支持根据DHCP Option60选择DHCP Server主备服务器； 10、提供设备软硬件3年维保；		
42	分光器1x32	1、支持进行机架式上架使用 2、光分路器-单模-1×32均分-SC/UPC； 2、插入损耗（dB）<17； 3、回损耗（dB）>50； 4、工作波长1260~1360nm &	96	个

		1480~1560nm; 5、输入输出接头类型 SC/PC; 6、工作温度-10℃～70℃;		
43	ONT 智能管理系统	ONT 智能管理系统作为无源光局域网中 ONT 网管设备，统一管理配置 ONT 设备，提高运维效率。 设备功能：远程下发 ONT 配置、Wi-Fi 信道管理、功率设置、批量升级、状态查询，告警功能等; 硬件参数：1U 主机机箱，6 个固定 100/1000M RJ45 电口，1 个串口，1 个交流电源模块 1 个风扇模块,电源线缆,安装配件），ONT 系统管理 license 授权 2500 个。	1	套
44	4 口 ONU Wi-Fi6	1、上行口：为保证设备性能，要求提供 XG-PON 接口≥1 个; 2、下行口：提供下行千兆以太网接口≥4; 3、无线性能：为保证设备性能所提供的 ONU 为内置天线，无外置天线，无线支持 2.4G/5G Wi-Fi6 工作模式 4、支持接入 ONT 智能管理系统，实现集中管理、集中配置; 5、配合宽带接入网关，提供终端用户统一管理、认证、审计等服务; 6、支持 IPV4/IPV6 双协议栈；多 SSID	2486	个

		（8 个 SSID）；支持桥接组网等； 7、提供设备 3 年维保；		
45	教室门禁一体机	人脸认证：采用深度学习算法，支持单人识别，支持照片、视频防假 二维码认证：支持学校端二维码认证开门 多重认证：设备支持本地认证、本地+远程开门认证、本地+超级密码认证三种认证模式。每种模式最大支持 20 个认证组，每个认证组最多支持 128 人多重认证（每个认证组支持 8 个群组，每个群组支持 16 个人） 门禁计划配置：支持计划模板管理，支持常开、常闭时段管理 视频预览：支持管理中心远程视频预览，支持接入 NVR 设备，实现 7*24H 视频监控录像 口罩检测：支持戴口罩检测，可配置提醒戴口罩、强制戴口罩（未戴口罩不开门） 报警功能：支持防拆报警、门被外力开启报警、胁迫卡和胁迫密码报警、事件联动报警等 联动配置：支持事件联动、卡号联动、工号联动，可配置联动门开关、联动报警输出、联动抓拍等功能	200	套

		本地功能：支持本地注册人脸、查询、设置、管理设备参数等操作 Web 端管理：可进行人员管理、参数配置、事件查询、系统维护等操作 含配套开关电源、磁控门锁、出入开关、发卡器。		
46	教室门禁管理平台	基础门禁管理通过接入多种门禁设备，利用卡片、人脸、指纹介质，实现人员身份辨别、出入管控等智能应用，主要提供门禁权限管理、事件管理、门禁状态查看、门禁远程控制、人员出入记录实时展示、远程呼叫对讲等应用。 【门禁管理】 一、提供门禁权限管理应用 1、支持按组织、设备、设备分组、人员、人员分组、规则 6 种方式完成通行权限配置 2、支持设置权限有效期、计划模板、假日计划； 3、支持按人员特征属性生成人员分组，如证件类型、性别等； 4、支持权限自动下发、增量下发、初始化下发； 5、支持按时段配置门的常开常闭状态； 6、支持认证方式设置，可按不同时段设置不同的认证方式，如刷卡+人脸、	1	套

		刷卡+指纹； 7、支持首卡常开，刷首卡可使门保持常开至常开时间段结束，若此期间再次刷首卡，门恢复正常状态； 8、支持限制出入名单管理（名单内人员无法进入）、胁迫卡（正常开门并上报胁迫报警）、超级用户（不受限于门常闭、刷卡+密码认证需要密码确认的规则，刷卡直接开门）； 9、针对刷卡开门方式，即使卡片权限未同步到设备，也可通过中心平台完成权限认证开门。 10、支持按门禁点、人员、组织、区域等多维度，综合查询权限配置、下发状态等信息； 11、支持根据平台及设备的权限数据进行门禁权限一致性核对 12、支持在权限任务中心中查看下载进度，包括正在计算设备数、正在下发设备数、当前下发进度、当前下发速度(个/分钟）、剩余下发时间 13、支持设置人员N天未进出时自动冻结权限 二、提供门禁事件管理应用 1、支持配置平台接收到事件类型； 2、支持配置事件保存时长；		

		3、支持人员出入事件和设备事件的查询、断网续传； 三、提供门禁状态查看及远程控制应用 1、支持查看门禁状态，包括开关状态、在离线状态； 2、支持对门禁点反控，包括对门进行开、关、常开、常闭的反控操作； 3、支持远程呼叫应用，门禁一体机呼叫中心发起开门请求，cs 客户端弹窗显示一体机视频，中心可选择接听、拒绝、开门； 四、提供人员出入记录实时展示应用 1、支持人员进出事件实时展示，包括人员基础信息、抓拍图片、进出时间、设备名称等，可全屏展示		
47	建设施工	包含管网及及弱电线路改造服务、宿舍网全光网施工服务、教学区施工服务；包含材料	1	项

三、▲商务要求

（一）服务期限

项目建设期为签订合同之日起 2 年内完成建设，最长的 8 年运维期（实际运维期根据中标人的投标文件确认，但最长不超过 8 年）包含 2 年的建设期。

（二）服务地点

柳州职业技术大学指定地点

（三）合同签订时间

自中标通知书发出之日起30日内完成合同签订。

（四）其他服务与承诺

1.服务期内，由中标供应商统一对接各ISP运营商的业务及运维工作，合作模式和政策按照上级主管部门的文件要求执行。

2.学校在社湾校区以及官塘校区提供不小于20平方米的运维场所，便于学生办理网络、售后保障等事宜。

3.中标供应商按本文件要求需投入的设备清单，投入的所有资产,在2年建设期完成后由第三方专业审计机构审计价格，捐赠给学校。捐赠的资产经第三方专业审计机构审计价格不足中标供应商承诺的投入价格的，中标供应商应根据学校的需求补齐投入。软件如果也参与第三方审计计价，则一同作价捐赠。合作期内涉及软件升级维护费用的，由中标供应商负责，合作期结束后的捐赠软件的升级维护费用校方自行负责。

4.在合同有效期内，若供应商无重大违约违规情形，学校不得单方面终止服务合同。

5.学校承诺，在合作有效期内，协助供应商在约定的合作区域内进行校园基础网络建设、运维、宽带接入工作，如有除甲方、乙方以外的其他主体进行本项目范围内学生公寓的网络建设、运维工作必须经过学校、中标供应商双方书面同意。学校应全力配合中标供应商进行项目施工，向中标供应商提供合同范围内通信电缆线路管道的开挖权和使用权，负责协调可能对中标供应商工作产生影响的相关组织机构，为中标供应商提供建设的施工便利，并配合中标供应商进行相关工程实施。学校负责配合中标供应商进行相关的调试工作，保证工程的顺利

实施。

6. 其他约定，双方在协议中另行协商补充。