基于 EPON 与 PPPOE 技术的校园网设计

校园网是为学校师生提供教学、科研和综合信息服务的宽带多媒体网络服务平台。随着信息技术的快速发展，当今的校园网功能已经不再局限于只向师生提供网络接入服务，许多弱电工程项目也融入到校园网建设当中。南京信息职业技术学院校园信息化建设主要包括：

1、校园楼宇房间内部提供电话和计算机网络接入业务，会议室与宾馆区域增加电视业务。

2、公共场所覆盖校园无线网。

3、视频监控校园全覆盖。

基于 EPON 技术的校园网建设与改造方案，通过 PPPOE 协议对上网用户进行认证与计费，该方案不仅解决了校园信息资源共享中的安全问题，而且通过与中国电信合作共建的方式，实现电话、计算机网络与电视业务的融合。

方案设计

1、楼宇内部采用综合化布线方案。

在综合布线系统中，信息插座和管理子系统(即中间配线架)之间的连接实现是水平子系统的功能，水平干线的设计包括水平子系统的传输介质与部件集成。选择水平子系统的线缆，要根据建筑物内具体信息点的类型、容量、带宽和传输速率来确定。从系统的兼容性和信息点的灵活互换性角度出发，水平子系统考虑采用同一种布线材料。超五类双绞线用于语音传输和最高传输速率为 1000Mbps 的数据传输，因为电话和网络接口都执行 RJ 标准(RegisteredJack：注册插孔，是美国电子工业协会和电信工业协会确立的一种以太网连接器的接口标准)，设计语音(电话)信息点与数据信息点均采用非屏蔽超五类双绞线，从而方便楼宇内部语音与数据端口功能的灵活切换。

2、与中国电信合作共同建设，校园网宽带接入采用 EPON 链路与 PPPOE 认证相结合。

传统交换式局域网采用三层模型架构。在校园网改造过程中，利用原有校园网构建校园业务网，主要提供认证计费服务数据库、服务器与存储、联网打印机资源和校园 IP 视频监控资源等。

EPON(以太网无源光网络)是一种新型的光纤接入网技术，其典型的拓扑结构为树型，它采用点到多点结构、无源光纤传输，在以太网之上提供多种业务。在物理层采用了 PON(无源光网络)技术，在数据链路层使用以太网协议，利用 PON 的拓扑结构实现了以太网的接入。因此，它综合了 PON 技术和以太网技术的优点：

低成本、高带宽、扩展性强、灵活快速的服务重组、与现有以太网的兼容性和方便的管理等特性，是目前以太网最佳的组网方式。

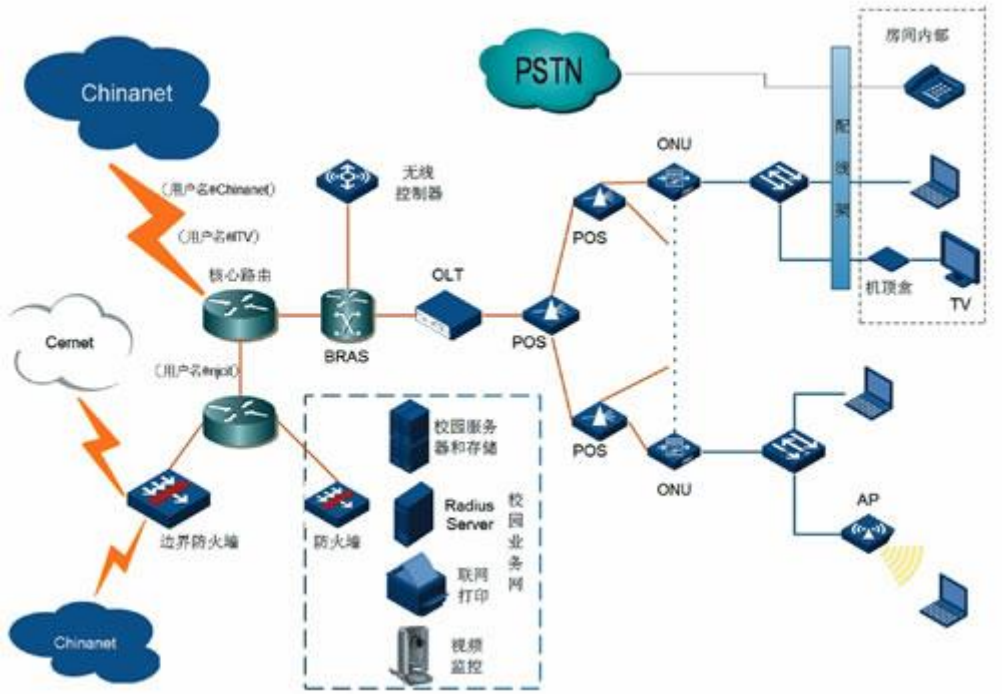

图 1 EPON 链路与 PPPOE 认证拓扑结构

图 1 是设计的校园网新的拓扑结构图，其中，EPON 链路主要由 OLT(光线路终端)、POS(无源分光器)和 ONU(光网络单元)和组成。

OLT 放在中心机房，是 EPON 整个链路的控制中心，OLT 一方面承载各种业务的信号在局端进行汇聚，按照一定的信号格式送入接入网，以便向终端用户传输，另一方面将来自终端用户的信号按业务类型分别送入各种业务网中。POS(无源光纤分支器)，是一个连接 OLT 和 ONU 的无源设备，它的功能是分发下行数据和集中上行数据。

POS 的部署相当灵活，由于是无源操作，几乎可以适应于所有环境，一般一个 POS 的分线率为 8 和 16，并可以进行多级连接。

ONU(光网络单元)位于远端接入侧，EPON 中的 ONU 采用以太网协议，在通信过程中不需要进行协议转换，实现 ONU 对用户数据的透明传送，保障从 OLT 到 ONU 之间高速的数据转发[3]。校园网采用 EPON 网络结构的优点：

⑴在原有交换式三层结构网络基础上易于升级改造。在南京信息职业技术学院学生宿舍原先没有布置局域网的情况下，设计直接建设 EPON 网络；在办公、教学等原先已经按照三层结构布置局域网的情况下，原有接入层交换机可以继续使用。

⑵相对成本低，维护简单，容易扩展，易于升级。从 OLT 端到 ONU 端之间仅有光纤、POS 等光无源器件，无需租用机房、无需配备电源、无需有源设备维护人员，可有效节省建设和运营维护成本。采用单纤波分复用技术(下行 1490nm，上行 1310nm)，仅需一根主干光纤和一个 OLT。

⑶能够提供比较高的带宽。EPON 目前可以提供上下行对称的 1.25Gb/s 带宽，并且随着以太网技术的发展可以升级到 10Gb/s。

⑷服务范围大。EPON 作为一种点到多点网络，以一种扇形的结构节省有限的光缆资源，能够服务大量用户。

PPPOE(基于以太网的点到点连接协议)，可以使以太网主机通过一个简单的桥接设备连接到一个远端的接入集中器上。

通过 PPPOE 协议，远端接入设备能够实现对每个接入用户的控制和计费。PPPOE 由 BRAS(宽带接入服务器)配合 Radius(远程用户拨号认证系统)服务器实现对用户的认证、计费。

使用 PPPOE 协议,BRAS 设备必须位于用户子网中或同一个 VLAN(虚拟局域网)中，以确保二层广播能够正确使用，在图 2 中 BRAS 作为 RadiusClient 位于 OLT 与核心路由设备之间，到用户之间是纯二层链路。Radius 服务器位于校园业务网中，设计校园每个用户有一个上网用户名，用户名后面可以跟不同域名，同一个用户名加上不同域名构成账号(用户名@域名)进行认证，认证通过后根据域名采用虚拟路由技术进行不同的网络路由。

采用 PPPOE 认证，由于网络接入设备只有在认证通过以后才能上网，AP(无线接入点)未经认证与无线控制器之间数据不能交互，设计在认证计费系统中设置，将所有 AP 设备设置为“直通”即免登录的联网方式。采用 PPPOE 方式认证的优点：

⑴有效控制网络广播风暴：PPPOE 上网方式由于采用二层认证，所有链路设备都工作在二层，故不存在网络第三层广播风暴的问题。

⑵有效防止 ARP 攻击行为。ARP 攻击一直是高校传统局域网的安全威胁，通过采用 PPPOE 认证上网模式，在用户认证过程中上网主机获取 BRAS 服务器(网关)MAC 地址不再使用 ARP 协议，而是通过在认证发现阶段的 PADI 报文和 PADO 报文的交换获得 MAC 地址(物理地址)，从而杜绝 ARP 攻击行为的发生。

⑶防止 IP 地址冲突。PPPOE 接入方采用动态分配 IP 地址，不存在用户自行更改 IP 地址而产生地址冲突的问题。

⑷支持 QOS(服务质量)，方便管理。采用 PPPOE 接入方式支持 QOS 业务，对不同的上网用户进行不同的流量控制和计费策略，能够实现基于时间或流量的上网计费以及基于帐号的用户管理。

⑸有效地阻止病毒蔓延和网络盗号的安全威胁。PPPOE 协议是把 PPP(点对点)协议移植到以太网上应用的一种协议，用户之间在逻辑上互不相通，这种点对点通信可有效防范网上病毒、木马和蠕虫感染其它用户的机器。此外，网络监听软件通常是利用以太网的广播特性或 ARP 协议来实现监听，而采用 PPPOE 认证接入方式，网络用户间通信是点对点通信，不适合监听软件的工作环境。

IPTV(交互式网络电视)是一种集合宽带有线电视网、互联网、多媒体、通讯等多种技术于一体，面向家庭用户提供的包括数字电视在内的多种交互式服务，用户在家中应用 IP 机顶盒加普通电视机就可以享受到 IPTV 所提供的电视业务。与传统的数字机顶盒相比，IP 机顶盒实现了视频、语音、数据三者的融合，即三网融合业务。

在会议室、宾馆等区域，一个房间内部至少有三个 RJ-45 端口，一个端口接电话，连接 PSTN(公共交换电话网)；一个端口用于用户电脑连接，通过上网账号用户可以访问 Internet 或者校园业务网；还有一个端口连接机顶盒，机顶盒与电视机相连，用户使用中国电信分配的账号(用户名@ITV)直接收看电视节目，IPTV 的认证计费服务由中国电信管理。

IP 监控系统设计

IP 监控是以 IP 网络摄像机及其编码器为硬件核心设备，视频信号从前端便被编码压缩，并以网络为传输载体，基于 TCP/IP 协议，采用流媒体技术实现视频数据在网络上传输，并通过网络及软件来实现对整个监控系统的调用、存储和控制等功能。IP 监控系统具有前端一体化、传输网络化、处理数字化、管理智能化及系统集成化的特点，能够满足大容量、大跨度的应用需求。

原有的校园网经过改造后，运用原有二层和三层交换设备组建的交换式局域网供 IP 监控系统使用。设计将 IP 摄像机连接接入层交换机，视频存储设备直接连接核心交换，保障 IP 摄像机数据能够快速、实时地传输到存储设备上。校园网安防管理人员通过 EPON 链路使用 user@njcit 类型的上网账号登陆，访问校园业务网的视频监控资源：可以直接根据 IP 视频摄像机的 IP 地址访问指定摄像机的实时监控视频；也可以远程连接视频存储服务器查看之前的视频内容。

基于 EPON 与 PPPOE 技术的校园网改造项目方案设计与实施，保留了原有校园网主干设备与信息资源，解决了传统交换式局域网存在的网络安全威胁，在保障校园网安全的同时，实现了信息资源共享，通过与中国电信共同建设的模式，不仅减少了网络建设与改造的开支，而且实现了电话、计算机网络与电视业务的融合。