



学校校园网建设方案



北京融讯光通科技有限公司

2023 年 12 月

目 录

一、设计概述	1
1.1 现状分析	1
1.2 网络需求分析	1
1.3 校园网特点	1
二、网络系统设计	2
2.1 设计思想	2
2.2 设计目标	2
2.3 设计原则	2
2.4 网络三层架构设计	3
2.4.1 核心设备选型	4
2.4.2 汇聚设备选型	4
2.4.3 接入设备选型	4
2.5 网络总体规划	4
2.6 网络安全管理	5
2.6.1 威胁网络安全因素分析	5
三、整体方案	6
3.1 核心交换机 RT-S5800-64H（根据项目按需选配）	6
3.2 汇聚交换机 RT-S3900-54（根据项目按需选配）	7
3.3 接入交换机 RT-S2900-48P6X（根据项目按需选配）	7
3.4 运营级软 AC 系统 RT-WSC6100-OS	7
3.5 无线 AP（室内） RT-WAP2100-T630	8
3.6 无线 AP（室外） RT-WAP2100-I630-Q	8
3.7 多合一防火墙 RT-F5100H	9

一、设计概述

1.1 现状分析

校园网络建设的目的在于提供信息的传递速率和效率，在于使教师能更有效，更方便地教学，学生能更主动，更积极地学习，从而提升整个学校的现代化教育，教学水平。校园网是“数字化校园”的传输平台，一个可靠，高效，安全的网络是建设数字化校园的坚实基础。随着高校信息化的深度发展，学校的教学办公和管理等活动将越来越依赖校园网络。因此构建一个高效，实用，稳定可靠，安全的网络平台，是高校网络建设考虑的重点。

1.2 网络需求分析

校园网是学校进行教育教学、科研、各项管理工作和各类信息交流沟通的应用平台，是一个集成相关软件系统和硬件设备于一体的具有综合功能的宽带计算机局域网，为学校提供了一个日常教学、科研、管理和通讯的综合性网络应用环境。进入信息时代需要培养学生的一种重要能力就是获取信息和处理信息的能力，网络正是架起了一座交流和获取信息的桥梁。毋庸置疑，在 21 世纪，中国每一所学校都应该建立起自己的校园网。通过校园网将计算机应用于教学的各个环节，从而师生可以通过校园网络进行备课、教学、查阅资料、多媒体教学软件开发与演示、师生之间互相通信、浏览因特网等，所以它对于提高教学质量，推动教育现代化起着不可估量的作用。毫无疑问，校园网是学校提高管理水平、工作效率、改善教学质量的有力手段，是实现教育现代化的基本工具。

1.3 校园网特点

（1）高速的局域网连接

校园网的核心为面向校园内部师生的网络，因此园区局域网是该系统的建设重点，由于参与网络应用的师生数量众多，而且信息中包含大量多媒体信息，故大容量、高速率的数据传输是网络的一项基本要求；

（2）信息结构多样化

校园网应用分为电子教学（多媒体教室、电子图书馆等）、办公管理和远程通讯（远程教学、互联网接入）三大部分内容：电子教学包含大量多媒体信息，办公管理以数据库为主，远程通讯则多为 WWW 方式，因此数据成分复杂，不同类型数据对网络传输有不同的质量需求；

（3）安全可靠

校园网中同样有大量关于教学和档案管理的重要数据，不论是被损坏、丢失还是被窃取，都将带来极大的损失；操作方便，易于管理——校园网面向不同知识层次的教师、学生和办公人员，应用和管理应简便易行，界面友好，不宜太过专业化；

(4) 经济实用

学校对网络建设的投入有限，因此要求建成的网络应经济实用，具备很高的性能价格比。

(5) 操作方便，易于管理

校园网面向不同参差的教室、学生和办公人员，应用和管理应简便易行，界面友好，不宜过于专业化。

二、网络系统设计

2.1 设计思想

校园网总体设计方案的科学性，应该体现在能否满足以下基本要求方面：

- (1) 整体规划安排；
- (2) 先进性、开放性和标准化相结合；
- (3) 结构合理，便于维护；
- (4) 高效实用；
- (5) 能够实现快速信息交流、协同工作和形象展示。

2.2 设计目标

具体的设计目标是：建设一个以办公自动化、计算机辅助教学、现代计算机校园文化为核心，以现代网络技术为依托、技术先进、扩展性强、覆盖全校主要楼宇的校园主干网络，将学校的各种 PC 机工作站、终端设备和局域网连接起来，并与有关广域网相连；系统总体设计本着总体规划、分布实施的原则，充分体现系统的技术先进性、高度的安全可靠性和良好的开放性、可扩展性，以及建设经济性。

2.3 设计原则

(1) 实用性和经济性

充分集成现有的各种计算机和网络设备，使建设的系统适用、安全、可靠且易管理、维护和扩展，具有最高的性价比。

(2) 开放性

构造一个开放的网络系统，是当前世界计算机技术发展的潮流。在整个系统设计中采用的规范和设备，具有较强的兼容性，便于与外界异种机平滑互联。

（3） 先进性

当今计算机网络技术发展日新月异，把握不准方向则可能导致在很短的时间内技术落伍，从而面临被淘汰的危险。因此在坚持实用性的前提下尽量采用国内外先进成熟的网络技术和设备，以适于未来的发展和需要，做到一次规划长期受益。

（4） 可扩充性

所选择的联网方案及设备要能适应网络规划不断扩大的要求，以便于将来设备的扩充；要能适应信息技术不断发展的要求，平稳地向未来新技术过渡。

（5） 可靠性

系统设计除采用信誉好、质量高的设备外，还采用一系列容错、冗余技术，提高整个系统的可靠性。

为了保证骨干网络平台的健壮性和链路冗余性，建议网络实施时在学校启用千兆备份线路。在学校启用物理链路冗余机制，保证任何一条线路出现故障后骨干网络平台的可用性。

（6） 安全性

包括两个方面：网络用户级的安全性，数据传输级的安全性。网络用户级的安全性应在网络的操作系统中予以考虑，而数据传输的安全性则必须在网络传输时解决。

在网络设计中，既要考虑信息资源的充分共享，更要注意信息的保护和隔离，因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括端口隔离、路由过滤、防 DDoS 拒绝服务攻击、防 IP 扫描、系统安全机制、多种数据访问权限控制等，有多种的保护机制，如划分 VLAN、IP/MAC 地址绑定（过滤）、ACL、路由过滤、防 DDoS 拒绝服务攻击、防 IP 扫描、认证机制、SSH 加密连接等具体技术提升整个网络的安全性。

2.4 网络三层架构设计

校园网网络整体分为三个层次：核心层、汇聚层、接入层。为实现校区内的高速互联，核心层由 1 个核心节点组成，包括教学区区域、服务器群；汇聚层设在每栋楼上，每栋楼设置一个汇聚节点，汇聚层为高性能“小核心”型交换机，根据各个楼的配线间的数量不同，可以分别采用 1 台或是 2 台汇聚层交换机进行汇聚，为了保证数据传输和交换的效率，现在各个楼内设置三层楼内汇聚层，楼内汇聚层设备不但分担了核心设备的部分压力，同时提高了网络的安全性；接入层为每个楼的接入交换机，是直接与客户相连的设备。本实施方案从网络运行的稳定性、安全性及易于维护性出发进行设计，以满足客户需求。

2.4.1 核心设备选型

通常将网络主干部分称为核心层，核心层的主要目的在于通过高速转发通信，提供可靠的骨干传输结构，因此核心层交换机应拥有更高的性能和吞吐量。

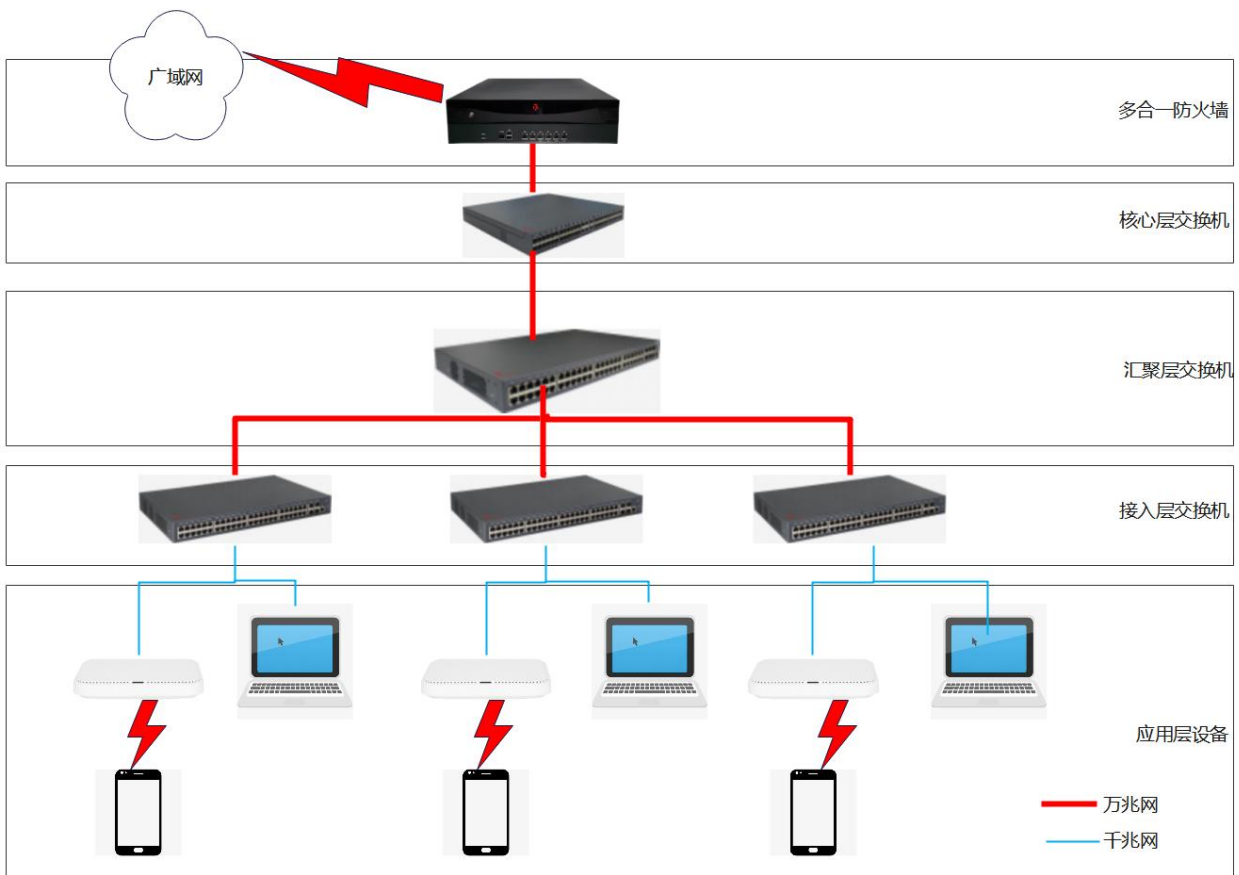
2.4.2 汇聚设备选型

通常将位于接入层和核心层之间的部分称为分布层或汇聚层，汇聚层交换层是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路，因此汇聚层交换机与接入层交换机比较，需要更高的性能和更高的交换速率。

2.4.3 接入设备选型

通常将网络中直接面向用户连接或访问网络的部分称为接入层，接入层目的是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性。

2.5 网络总体规划



2.6 网络安全管理

校园网的安全威胁主要来源于两大块，一块是来自于网内，一块来自于网外。来源于网内的威胁主要是病毒攻击和黑客行为攻击。据统计，威胁校园网安全的攻击行为大概有 40% 左右是来自于网络内部，如何防范来自于内部的攻击是校园网网络安全防护体系需要重点关注的地方。

2.6.1 威胁网络安全因素分析

计算机网络安全受到的威胁包括：

1. “黑客”的攻击；
2. 计算机病毒；
3. 拒绝服务攻击（Denial of Service Attack）。

安全威胁的类型：

1、非授权访问。指对网络设备及信息资源进行非正常使用或越权使用等。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享。

2、冒充合法用户。主要指利用各种假冒或欺骗的手段非法获得合法用户的使用权限，以达到占用合法用户资源的目的。

3、破坏数据的完整性。指使用非法手段，删除、修改、重发某些重要信息，以干扰用户的正常使用。

4、干扰系统正常运行，破坏网络系统的可用性。指改变系统的正常运行方法，减慢系统的响应时间等手段。这会使合法用户不能正常访问网络资源，使有严格响应时间要求的服务不能及时得到响应。

5、病毒与恶意攻击。指通过网络传播病毒或恶意 Java、active X 等，其破坏性非常高，而且用户很难防范。

6、软件的漏洞和“后门”。软件不可能没有安全漏洞和设计缺陷，这些漏洞和缺陷最易受到黑客的利用。另外，软件的“后门”都是软件编程人员为了方便而设置的，一般不为外人所知，可是一旦“后门”被发现，网络信息将没有什么安全可言。如 Windows 的安全漏洞便有很多。

7、电磁辐射。电磁辐射对网络信息安全有两方面影响。一方面，电磁辐射能够破坏网络中的数据 and 软件，这种辐射的来源主要是网络周围电子电气设备产生的电磁辐射和试图破坏数据传输而预谋的干扰辐射源。另一方面，电磁泄漏可以导致信息泄露。

三、整体方案

校园网建设要求覆盖学校的教学楼、办公楼和实验楼和宿舍楼等各场地，要求数据、图形、图像、语音、视频等信息能在网络上较好的传输，考虑需求分析中收集的师生员工规模的信息，在网络设计事将学校分为主干网络和各区子网，主干带宽 10000Mbps, 子带宽 1000Mbps，网络支持 VLAN 管理、IP 组播、第三层交换以及多种路由协议；在网络的选型上，采用目前主流的快速以太网技术。

3.1 核心交换机 RT-S5800-64H（根据项目按需选配）



RT-S5800-64H 交换机支持 48 端口万兆光+2 个 40G 光+4 端口 100G 光，以太网路由交换机(一个 console 口，1 个带外管理千兆电口+48 个万/千兆 SFP+光口+4*100G/40G 光口（QSFP28 封装，可适应 40GE QSFP+ 或配置成 4 个 10GE）+2 个 40G QSFP+光口（每个 40G 端口可扩展成 4 个 10G 端口使用）；两个电源槽位，标配 2 个 AC220V 电源, 4 个风扇槽位，标配包含 4 个风扇, 风扇散热，支持前后/后前风道设计，1U 高度，

19 英寸机架式安装)

3.2 汇聚交换机 RT-S3900-54 (根据项目按需选配)



RT-S3900-54 交换机支持 48 端口千兆电+6 端口万兆光，以太网路由交换机 (1 个 RJ45 型 CLI 口，48 个千兆电口，6 个万兆/千兆自适应 SFP+光口；标配一个可热插拔电源 AC220V，可拓展双电源；风扇散热，1U 高度，标准 19 英寸机架式安装)

3.3 接入交换机 RT-S2900-48P6X (根据项目按需选配)



RT-S2900-48P6X 交换机支持 48 端口千兆电，6 端口万兆光，以太网 POE 交换机 (1 个 CLI 控制口，48 个千兆 POE 电口，6 个万/千兆 SFP+光口；标配双电源 AC220V+DC48V，AC 输入 POE 功率 370W，DC 输入 POE 功率 740W，风扇散热，1U 高度，标准 19 英寸机架式安装)

3.4 运营级软 AC 系统 RT-WSC6100-OS

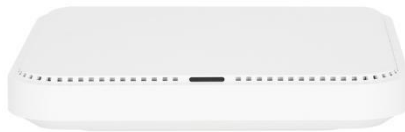


RT-WSC6100-OS 适应力强、可靠性高、简单易用的无线 AC 控制器产品，支持 CAPWAP 标准协议，可提供强大的 WLAN 接入管理与控制能力，支持 AP 自动信道管理、无线射频调整、用户负载均衡等功能，提供良

好的用户漫游及切换等能力。

RT-WSC6100-0S 作为大型无线网络的承载者，支持 AC 的分级部署和管理。通过分级可有效减少中心设备的压力，降低结构性风险，提高管理效率。RT-WSC6100-0S 还支持支持丰富的认证与平台接口，与业界主流 Radius、Portal 平台对接组网。

3.5 无线 AP（室内） RT-WAP2100-T630



RT-WAP2100-T630 采用高性能射频芯片方案设计，无线吞吐率高、并发接入能力强。配合内置的全向 MIMO 大功率天线，可最大程度的满足 WLAN 无线覆盖，避免信号死角。RT-WAP2100-T630 支持 POE 和 Adaptor 两种供电方案，外形美观大方，可广泛用于石膏板、水泥顶等各种场合的吸顶安装。

3.6 无线 AP（室外） RT-WAP2100-I630-Q



RT-WAP2100-I630-Q 系列室外型采用高性能射频芯片设计，无线吞吐率高、并发接入能力强。内置大功率 MIMO 天线和防雷模块，可满足各种复杂室外场景的无线覆盖，并大幅降低施工难度。RT-WAP2100-I630-Q 系列支持 IP67 防护和宽温设计，使用标准 POE 远程供电，给 AP 规划和选址提供了极大的灵活性，是您组建各种室外高密无线网络的理想选择。

3.7 多合一综合防火墙（根据项目按需选配）



T 比特级 7 层防火墙以保障用户应用安全为目标，立足于高性能的矢量操作系统和一体化引擎，通过 L2-L7 层全面威胁防御及强大应用安全管控技术，为用户提供超高性能的网络安全解决方案。