金陵中学智慧校园云防护项目

2020年7月

目 录

[金陵中学智慧校园云防护建议 1](#_Toc46431691)

[1 项目背景 3](#_Toc46431692)

[2 项目目的 3](#_Toc46431693)

[2.1 金陵中学现有网络情况 4](#_Toc46431694)

[2.2 校园网络存在不足 5](#_Toc46431695)

[2.2.1 校园接入层不足； 5](#_Toc46431696)

[3 优化与升级项目 5](#_Toc46431697)

[3.1 校园网络结构优化服务 6](#_Toc46431698)

[3.1.1 网络区域划分 6](#_Toc46431699)

[3.1.2 网络子网规划 7](#_Toc46431700)

[3.1.3 有线云防护 9](#_Toc46431701)

[3.1.4 物联网规划预留 9](#_Toc46431702)

[3.1.5 优化调整计划 10](#_Toc46431703)

[3.2 优化升级后整体结构 12](#_Toc46431704)

[4 预算清单 13](#_Toc46431705)

[4.1 校园网络云结构防护服务 13](#_Toc46431706)

# 项目背景

通过建设智慧校园提高学校教育的信息化水平，逐步解决校园教学的全向交互、校园环境的全面感知、校园管理的高效协同、校园生活的个性便捷，最终实现建成完整统一、技术先进，覆盖全面、应用深入，高效稳定、安全可靠的智慧校园。具体目标就是实现“五个智慧化”和“一站式教育服务”。

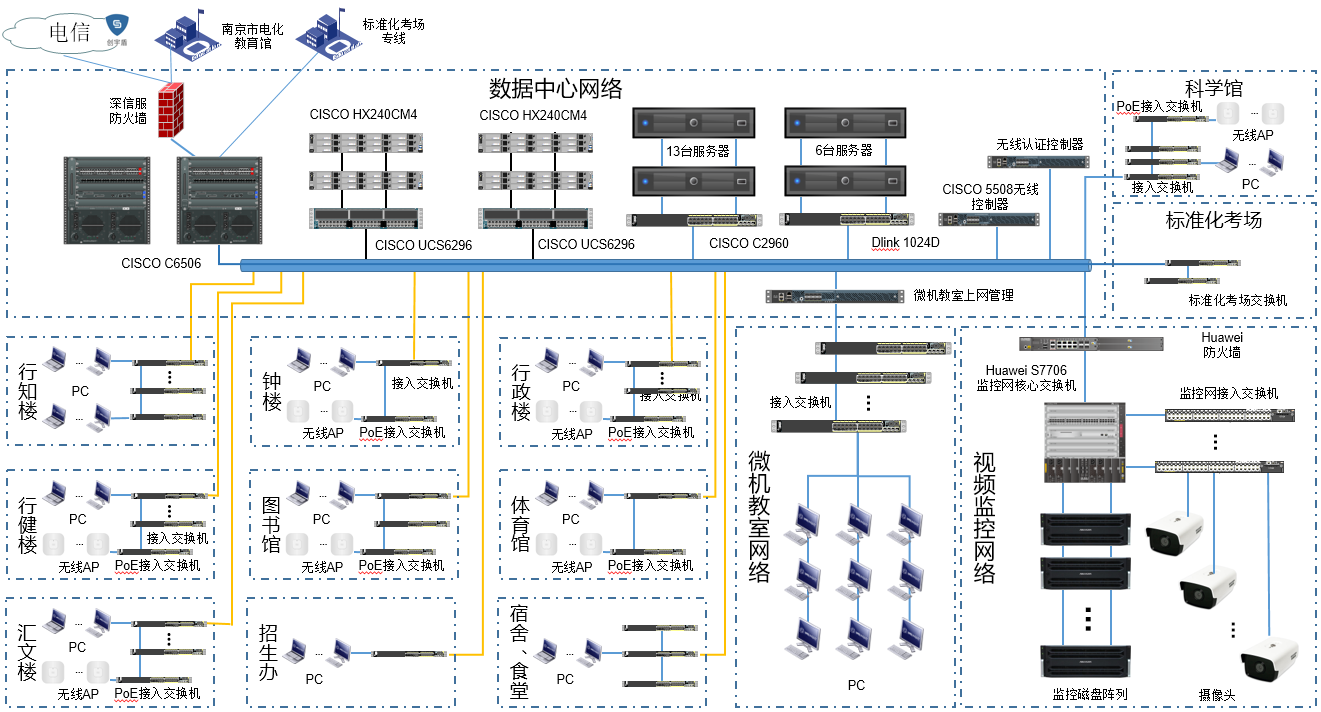
随着智慧校园建设，学校教育信息化水平越来越高，校园信息化的复杂程度也随着增加。利用云计算技术，很多学校数据中心实现了计算资源、网络资源、存储资源的虚拟化和服务化，同时学校数据中心的安全威胁和防护要求也产生了新的变化，诸多的业务系统运行在数据中心云服务平台上，保障数据中心的业务连续性和安全性将是一个巨大的挑战。

同时在智慧校园的建设中，校园内接入网络存在众多类型设备，如：教学终端、智能设备、PC、无线网络设备、监控设备、以及物联网设备等，造成现有网络结构复杂，极易出现网络流量干扰或拥塞问题，大大影响校园网络的稳定和安全使用。

# 项目目的

通过本次项目的优化和提升，将智慧校园网络基于功能和类别进行单独划分，保证不同类型网络逻辑隔离，互不干扰，各尽其职。并提升数据中心网络安全性，保障校内各应用系统的安全和稳定运行，为全校师生提供高效、安全的教学服务。同时可以为未来智慧校园建设提供充分的扩展性和标准化。

## 金陵中学现有网络情况



通过学校整体的网络拓扑可以看到，目前学校网络主要分为三个部分，数据中心网络、校园接入网络和视频监控网络。数据中心网络与校园接入网络使用同一台核心交换机，另一台核心交换机作为冷备份核心运行，监控网络与核心交换机之间使用一台华为防火墙进行隔离。网络出口方面，由一条电信千兆出口提供互联网接入服务，另一条千兆城域网出口连接南京教育城域网，还有一条标准化考场专线，连接至标准化考场专网。

校园网接入部分，目前每栋教学楼或功能楼的都有一个设备间，设备间内部署有楼层接入交换机和PoE交换机，无线AP接入PoE交换机。

## 校园网络存在不足

### 校园接入层不足；

1. 楼宇内接入网络未进行隔离，一栋楼的网络都在一个广播域中，存在安全隐患和网络干扰；
2. 针对智慧校园建设缺少网络扩展性和专用网络。

# 优化防护与升级项目

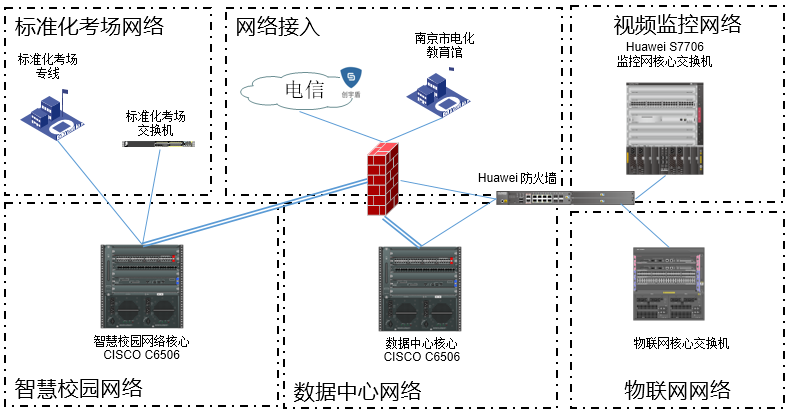
本次金陵中学智慧校园云防护依照对校园网络整体结构进行梳理和优化调整，使整个校园网络更加合理和高效。

## 校园网络云结构防护服务

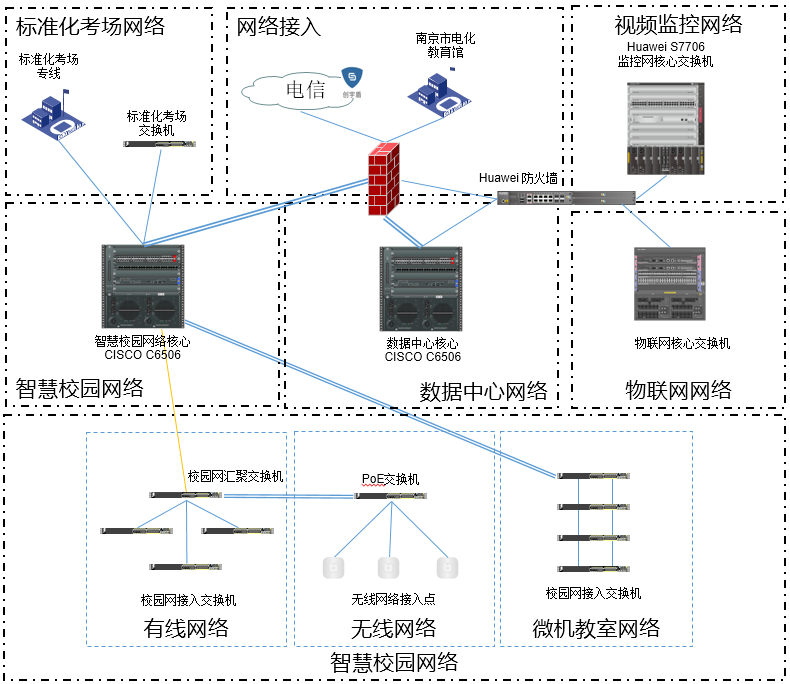
### 网络区域划分

依照网络功能性进行划分，将校园网络划分为：数据中心网络区域，网络接入区域，数据中智慧校园网络区域，监控网络区域，物联网区域以及标准化考场网络区域。不同网络区域之间使用安全设备进行隔离和可控制访问管理。

如下图所示



其中，智慧校园网络区域根据接入网络设备类型又可以分为，无线网络区域，有线网络区域，微机教室网络区域。如下图所示



### 网络子网规划

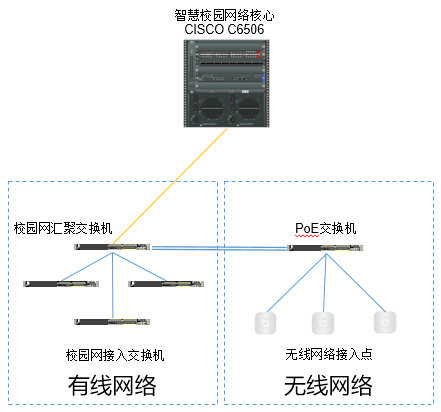
建议数据中心网络划分一个C类地址段，监控网络保持原有地址段，标准化考场使用原有地址段，无线网络使用原地址段，划分一个C类地址段给物联网网络使用，校园有线网络和微机教室网络重新划分新的网络地址段，可以考虑使用南京教育城域网分配给学校的地址段，对有线网络和微机教室网络进行多网段划分，可根据年级教室，年级组办公室，行政办公室，校长室等不同类型功能房间进行网段细分。例如：

|  |  |  |
| --- | --- | --- |
| 类型 | VLAN | 地址段 |
| 数据中心 | 100 | 192.168.10.0/24 |
| 监控网络 | 200-299 | 172.16.X.0/16 |
| 无线网络 | 300-363 | 192.168.64.0/18 |
| 物联网网络 | 500-531 | 192.168.32.0/19 |
| 高一年级教室 | 400 | 10.69.65.0/24 |
| 高二年级教室 | 401 | 10.69.66.0/24 |
| 高三年级教室 | 402 | 10.69.67.0/24 |
| 国际部教室 | 403 | 10.69.68.0/24 |
| 高一年级组办公室 | 404 | 10.69.69.0/24 |
| 高二年级组办公室 | 405 | 10.69.70.0/24 |
| 高三年级组办公室 | 406 | 10.69.71.0/24 |
| 行政办公室 | 407 | 10.69.72.0/28 |
| 校长室 | 408 | 10.69.72.16/28 |
| … … | … … | … … |

使用城域网段地址的终端可以直接通过教育城域网专线访问南京市教育城域网资源，使用其他私有地址段的终端可以在出口防火墙上进行源地址转换后访问南京市教育城域网资源。

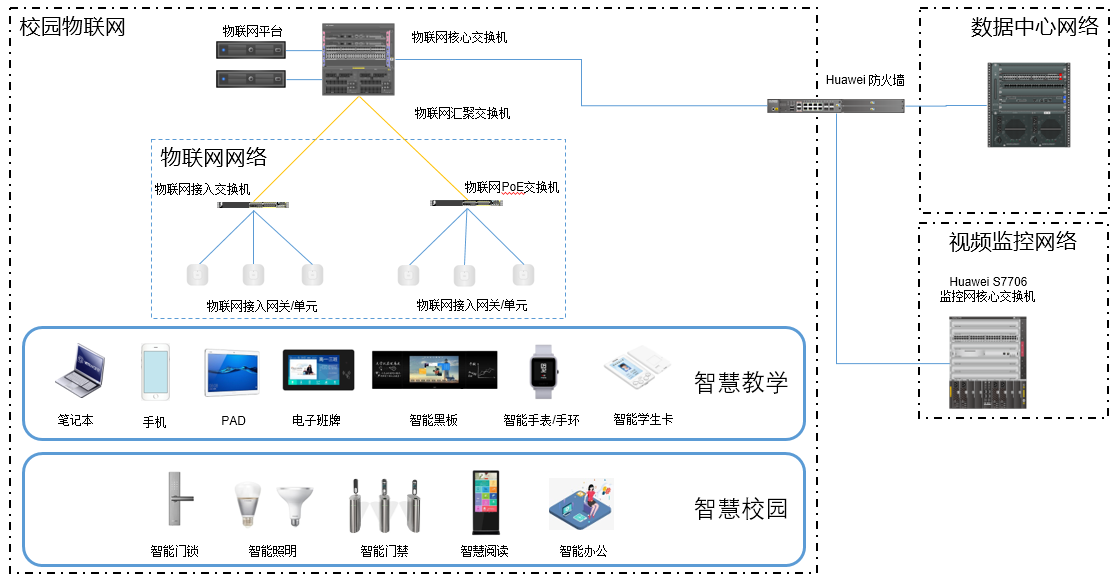
### 有线云防护

现有有线网络存在楼层交换机串联接入，需要将连接方式改为星型连接，可以减少故障点，并能够充分使用上行链路带宽。



### 物联网规划预留

针对智慧校园建设中，校园物联网应用越来越广泛，物联网接入设备越来越丰富多样，如果在原有校园网基础上进行扩展建设，易造成网络结构复杂，网络流量干扰等问题。建议预留一组物联网IP地址，物联网网络核心接入现有华为防火墙，与其他网络进行隔离控制，保证物联网内安全。后续建设的物联网平台，可以部署于物联网网络区域，直连至核心交换机。



### 优化调整计划

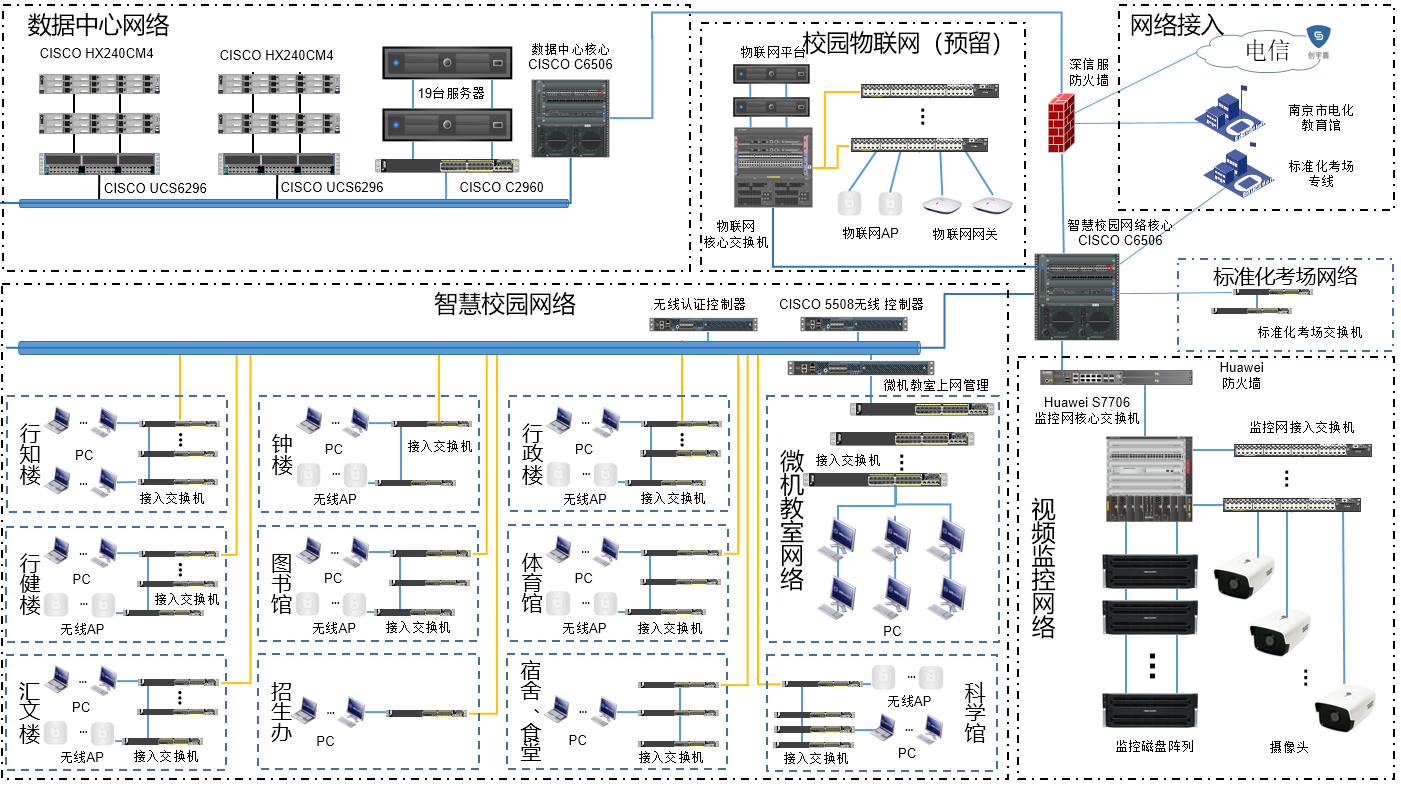
1. 现有网络接入情况摸底排查，方便后续接入网络划分VLAN。按照目前接入交换机的统计，总的接入点数量约为1500个。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 24口POE | 24口 | 48口POE | 48口 |
| 钟楼 | 1 |  |  | 1 |
| 行政楼 | 1 | 1 | 1 | 3 |
| 汇文楼 | 1 | 2 |  | 2 |
| 行知楼 |  | 1 |  | 2 |
| 图书馆 | 1 | 4 |  | 1 |
| 教师宿舍 |  |  | 1 |  |
| 行健楼 | 2 | 2 |  |  |
| 小卖部 |  | 1 |  |  |
| 学生宿舍 |  |  | 1 |  |
| 体艺楼 | 1 |  |  | 1 |
| 体育馆 | 1 |  |  |  |
| 二食堂 |  | 1 |  |  |
| 科学馆 | 1 | 6 | 1 | 2 |
| 招生办 | 1 |  |  |  |
|  | 10 | 18 | 4 | 12 |

1. 网络调整配置计划

|  |  |  |
| --- | --- | --- |
| 调整内容 | 实施人数 | 天数 |
| 数据中心网络情况摸底 | 2 | 1 |
| 防火墙网络配置 | 2 | 1 |
| 核心交换机分离  服务器接入调整 | 2 | 1 |
| 数据中心网络联调 | 2 | 2 |
| 楼层网络接入交换机配置 | 2 | 4 |
| 调整后网络运行保障 | 2 | 1 |
|  | 总计 | 20人/天 |

## 优化升级后整体结构



# 预算清单

## 校园网络云结构防护服务

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备 | 说明 | 数量 |
| 1 | 网络云结构防护服务 | 现有网络接入点摸底，点位测试，确定接入交换机连接信息 | 1500 |
| 接入线路故障处理，辅材 | 1 |
| 网络调整配置（人/天） | 20 |