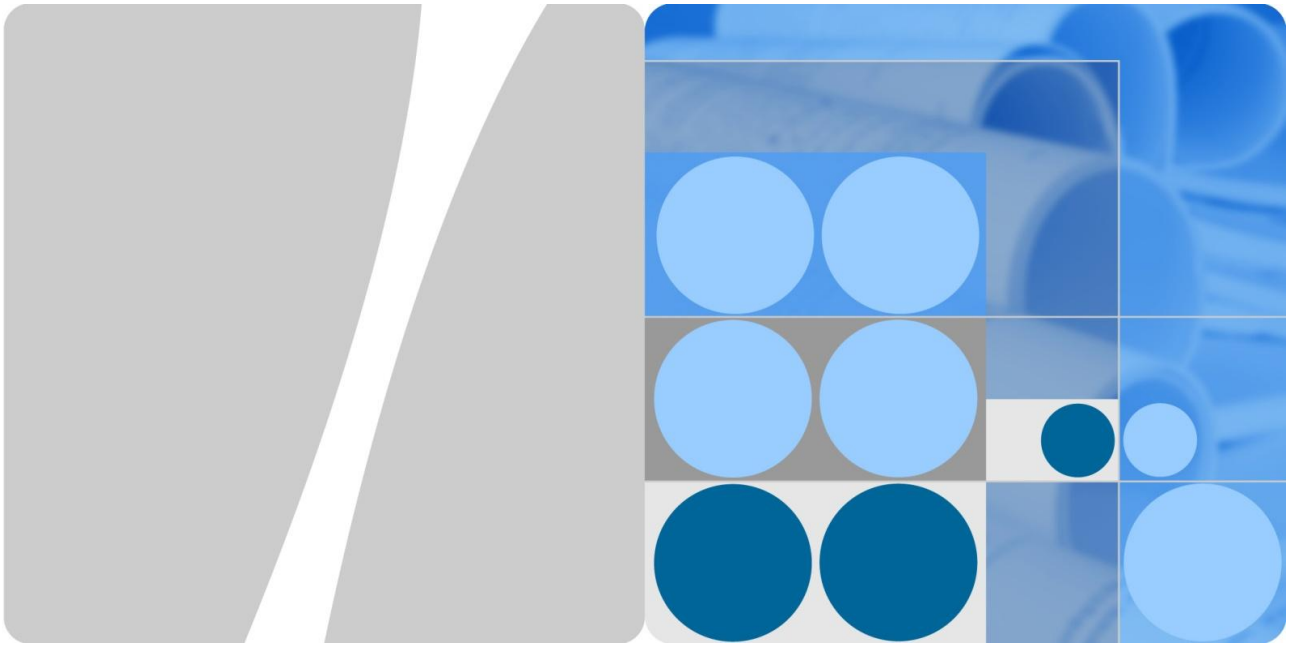


# 区域云教育解决方案技术建议书

教育规划设计组

作者：毕元堂　张幸元　王丽兵

## 华为技术有限公司

地址：　　深圳市龙岗区坂田华为总部办公楼　　邮编：518129

网址：　　http://www.huawei.com

客户服务邮箱：　　support@huawei.com

客户服务电话：　　0755-28560000　4008302118

客户服务传真：　　0755-28560111

# 目录

# 1 本文档说明

## 1.1 目的

本文从技术角度，对 XX 区域云教育项目提出规划和建议，本文的目的如下：

1) 对 XX 区域云教育进行总体设计，明确设计原则、总体需求和总体方案，界定需要建设的各子系统；

2) 对各组成子系统进行高层设计，明确子系统功能、组网方案、关键参数、设备配置和对外接口。

## 1.2 缩略语

表 1.1 缩略语列表

| Abbreviations | Full Spelling |
|---|---|
| VDI | Virtual Desktop Infrastructure |
| MPLS | Multi-Protocol Label Switching |
| VLAN | Virtual Local Area Network |
| CSS | cluster switch system |
| TC | thin computer |
| VRRP | Virtual Router Redundancy Protocol |
| FRR | fast reroute |
| CIDR | classless inter-domain routing |

## 1.3 依赖条件与假设

本文设计中存在的依赖条件与假设如下：

1) 假设云教育的云数据中心为新建，并且各学校连接到云数据中心的网络（不是基于现有的 Cernet 网和教育城域网建设）；

2) 假设暂无云教育既有系统。

## 1.4 文档范围及结构

本文分 8 章，各个章节的内容简要介绍如下：

第一章对全文进行概述，包括本文的目的、存在的假设，以及文档范围和结构等。

第二章描述项目背景，包括项目的概要说明、问题与挑战、建设意义等。

第三章描述总体需求，从业务角度，对需求进行分析，总结其各子系统的需求。

第四章描述项目总体方案，包括设计原则，总体方案组成等。

第五章分别对各个子系统进行设计，从 5.1 到 5.2 分别是对云数据中心(含桌面云)、教育区域网络子系统的设计，各个子系统从设计依据、子系统功能、组网方案、关键参数、设备配置、方案亮点等多个纬度展开描述。

第六章分别描述各个子系统对外的接口。

第七章详细阐述整体方案亮点。

第八对各个子系统中包括的主要设备进行介绍。

# 2 项目背景

## 2.1 项目概述

### 2.1.1 区域教育的问题与挑战

教师是地区教育质量保障的核心，教师的再教育是必要的。时代在变，社会在飞速发展，知识日新月异，不能总是凭老经验教学。要想成为新时期的合格教师、优秀教师，就应该不断地去自学或培训自己各方面的能力，活到老，学到老，与时俱进，做学生喜爱的称职的好老师。

传统的教师教育传统的方法有集中面授、函授或脱产进修等多种形式，这些教育方法对教师教育的确起到了一定的效果。但由于传统的方法很多局限性：

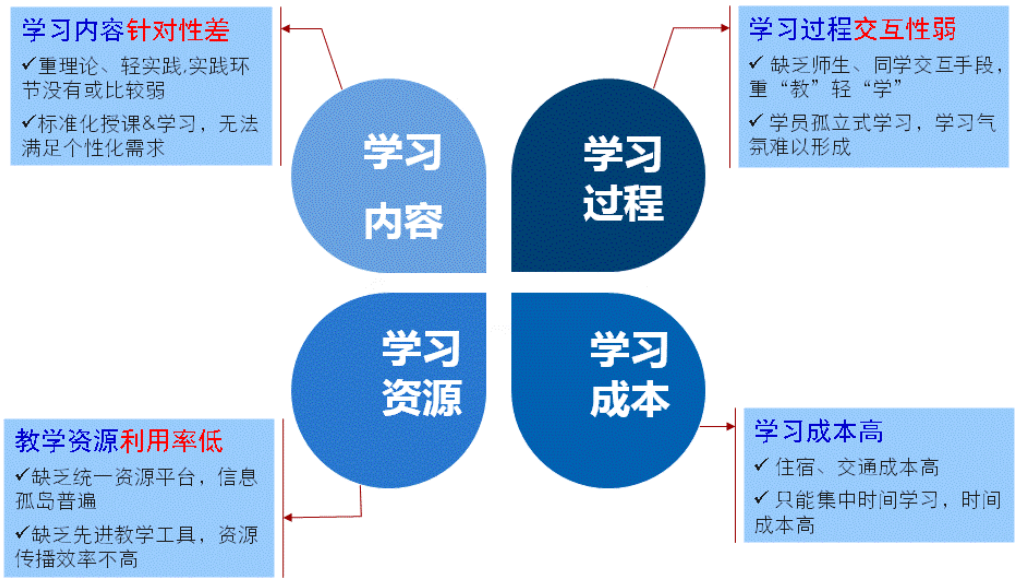



图 2.1 教师教育传统方法的问题

（1）学习内容主要是理论上的学习，缺乏教学技能实践，如模拟实际课堂教学的实践、模拟班主任的一些实践；

（2）教学活动多由教员做主，学员只能是被动学习。学习的主动性和独立性受到一定程度的限制；

（3）时间、地点、内容和进程都程序化、固定化，难以在教学活动中容纳更多的内容和方法；由于以“课”为活动单元，而“课”又有时间限制，因而某些完整的教材内容被人为地割裂以适应“课”的要求；

（4）教学面向全班学员，步调统一，难以照顾学员的个别差异；

### 2.1.2 政策牵引

2003 年 9 月教育部启动实施全国教师教育网络联盟计划。

2004 年 9 月，教育部印发了《教育部关于加快推进全国教师教育网络联盟计划，组织实施新一轮中小学教师全员培训的意见》（ 教师[2004]4 号）和《2003-2007 年中小学教师全员培训计划》。

2005 年全国大部分省（区、市）结合本地实际,认真研究制定了落实“意见”和“计划”的实施意见和工作方案。

2009 年 6 月，教育部下发了《教育部关于“教师教育创新平台项目”实施工作的意见》，提出要努力促进资源共享，建设教师教育创新平台。

### 2.1.3 项目建设意义

(1)、教师教育模式创新，采用网络学习+实训两者结合的模式。

教师教育的核心是“人网”、“天网”、“地网”的融通,本项目的建设有利于地网（网络学习）、人网（实训）两者结合，优势互补。

(2)、有利于资源共享，整体提高教师的素质。

建立统一学习资源管理平台，使不同地区、不同层次的教师能够共享优质教育资源，从整体上提高教师的素质。一般的网络学习资源比较分散，优质资

源存在但是利用率很低，并且仅对部分学员开放,并没有实现真正的优质资源的共享，有效的区域学习平台应该是一个完全开放的系统,能够实现全部资源的共享。

(3)、教师教育形式多样化,学员学习兴趣高、学习成本低。

与传统的教师培训方式相比，区域云教育的形式更加灵活新颖。它作为其中一种促进教师教育发展、提高教师专业化水平的教育形式有着非常重要的意义和强大的生命力，我们期待这种新的教师教育形式有更好的发展。

## 2.2 项目范围

### 2.2.1 项目总体目标及阶段说明

整个方案的设计基于 XX 区域教育发展战略，在满足当前 XX 区域需求的同时，充分考虑到将来整个系统的投资保护和对新应用的支持。以公共云教育为最终目标，设计 XX 区域云教育平台，分阶段实施。具体来说项目的建设将分三阶段进行：

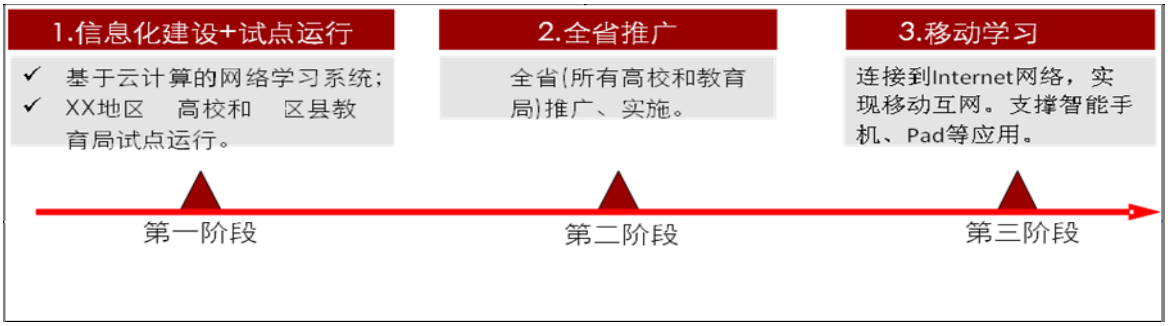



图 2.2 项目的三个阶段

➢ 第一阶段建设内容：

（1）由 XX 牵头建设云教育平台，用云计算平台解决教师再教育信息化需求。

（2）在 XX 地区的高校及教育局试点运行。

➢ 第二阶段建设内容：

在 xxx 地区内推广实施、应用。

➢ 第三阶段建设内容：

连接到 Internet 网络，实现移动互网。支撑智能手机、Pad 等应用。

### 2.2.2 本方案的建设范围

项目目前处在第一阶段，本方案是以 XX 地区为试点，由 XX 建设和运营云教育平台，为 XX 范围内的高校教师和中小学教师提供网络再教育服务。

XX 区域云教育项目主要包括三子系统建设：

- 云教育数据中心子系统

云数据中心总体架构设计遵循面向业务需求的设计思路，基于模块化的设计方法，实现云教育数据中心基础架构模块与业务模块松耦合，保证地区教育业务动态扩展和新业务快速上线。

- 桌面云子系统

VDI 替代传统 PC，多用于在学生机房，多媒体教室、教师办公使用，提供虚拟桌面，通过端到端的虚拟化平台解决方案，支持瘦终端 TC，软终端 PC，笔记本和手机可以通过软终端访问。

- 教育区域网络子系统

教育区域网实现 XX 市内高校和各区县教育局连接到云数据中心，满足教师教育远程教学等业务需求。

暂不用现有的 Cernet 或教育城域网络，重新建设教育区域网络。将 XX 范围内的高校(高校内部的校园网络不属于本方案范围)和区县教育局连到云数据中心（中小学校到教育局之间的互联不属于本方案范围）。

# 3 XX 区域云教育总体需求

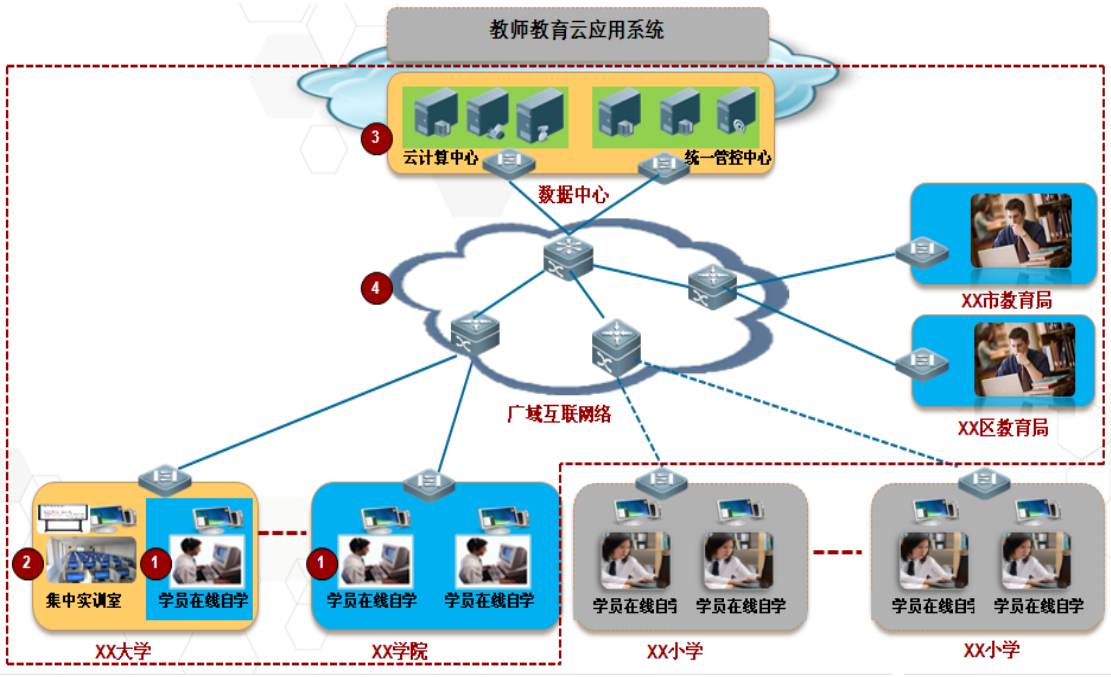
## 3.1 需求综述

本项目是以 XX 地区为试点，由 XX 建设和运营，为地区内的高校教师和中小学教师提供网络再教育服务。

下图是教师网络教育的一个应用场景图， 教师主要通过两种方式进行学习：

(一)、**学员（教师）在线自学**：学员在课余时间通过学校电脑登录云教育平台进行自学；

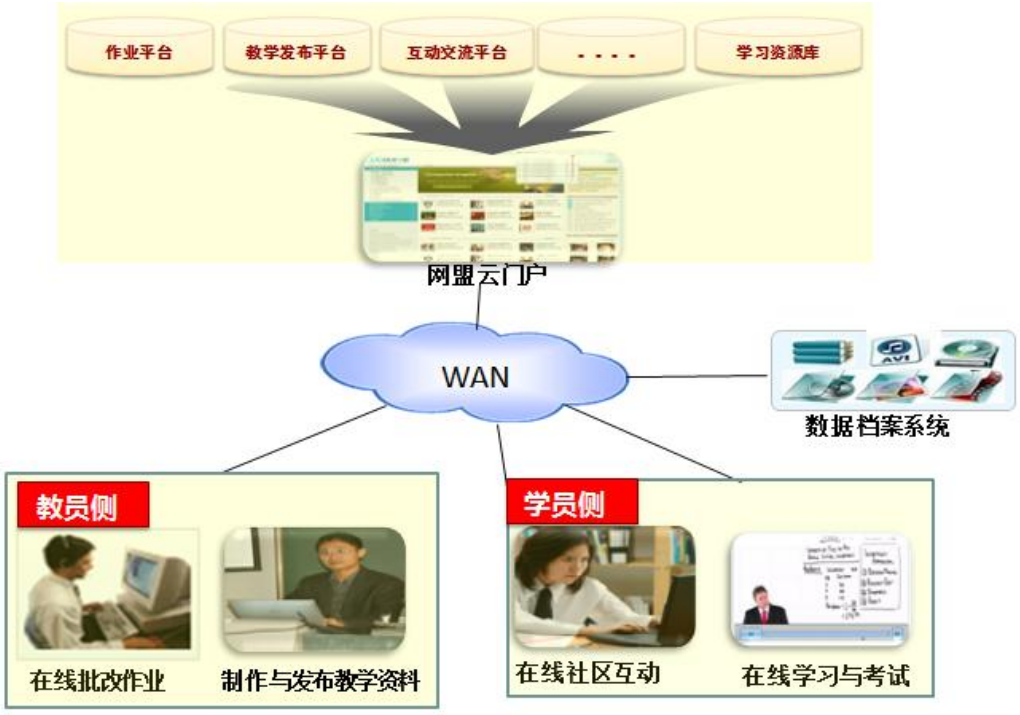
(二)、**集中实训学习**：有些课程需要集中实训，才能够有效提高实践能力，学员需要集中到多媒体实训教室进行统一学习。




在该项目中，重点聚焦实现数据中心、集中实训室、教育区域网络三大系统。

## 3.2 学员在线学习

教师大部分时间是利用自己的课余时间进行远程学习。远程网络应用系统包括：教育门户子系统、课程管理子系统、教学资源共享平台、作业管理子系统、教学发布子系统、学习管理子系统、社区互动学习子系统、数据档案子系统、综合管理子系统等九大系统。




总结起来，教师再教育具有以下特点：

（1） 学习时间不固定：大多数情况下，教师是利用自己的课余时间进行学习。

（2） 集中学习：在暑期、寒假或其它节假日，教师有可能自发或有组织地进行集中学习。

（3） 在学习过程中，大部分的学习课件是视频资料。

（4） 在社区互动学习的很多应用中要求实时互动性强。

## 3.3 集中实训室

一、集中实训室简介

在教授一些交互实践性较强的课程时，需要把教师集中到一起，进行统一授课。这就需要一个多媒体实训室，每人一台电脑，进行实践操作。这就是文中提到的“集中实训室”。如下图所示：

二、集中实训室的电脑终端选择

从技术选型上看，电脑桌面终端可以是 PC，也可以是 VDI。两种方案的比较如下：

| 方案 | 优点 | 缺点 |
| --- | --- | --- |
| PC | 1、 符合传统使用习惯<br>2、 不受网络限制 | 1、 数据难于共享<br>2、 信息安全难于保证<br>3、 扩容升级麻烦<br>4、 运维成本高<br>5、 资源利用低<br>6、 高能耗、高排放、高噪音<br>7、 高 TCO |

| | | |
|---|---|---|
| VDI | 1、 桌面随行、移动办公<br>2、 绿色安全<br>3、 高效运维<br>4、 低 TCO | 1、 受限于网络<br>2、 需培训新的用户习惯 |

三、 集中实训室需求

| 分类 | 需求描述 |
|---|---|
| 业务需求 | 学生机房(需要终端 xxx 台)、x 个实验室(需要终端 xxx 台)、xx 个多媒体教室（每个教室一台） |
| | xxx 个电脑帐号，xxx 台桌面终端 |
| | 每个虚拟机操作系统内存 2GB，用户个人数据存储空间不低于 80GB |
| | 要支持常用办公软件，如：Microsoft office、图片浏览、杀毒软件、内部通讯软件、网上下载工具等。 |
| | 在 xxx 个终端同时登录时，不降低用户体验 |
| 维护需求 | 支持集中管理能力，如：对操作系统镜像统一管理、软件补丁统一分发、TC 终端统一管理。 |
| | 支持通过扩容存储与计算资源实现用户平滑扩容 |
| 技术需求 | QoS 的要求达到时延<100ms，抖动<50ms，丢包<0.1% |
| | 支持高可用性、动态迁移等特性 |
| | 每用户平均 IOPS 不低于 12（读写比例 60％RR,40%RW，数据块大小为 64KB） |

## 3.4 云教育中心

一、 云教育中心简介

云教育中心即整个项目中的云数据中心，它将为云教育应用提供 ICT 的支撑平台。本项目中，云教育中心特指数据中心的 L2 层，如计算、存储、网络和安全设备，以及对这些设备的调度和管理等。

二、 数据中心的选择

根据目前数据中心的发展趋势及其技术成熟度，本项目建议采用云数据中心解决方案。云数据中心与传统数据中心的对比如下：

| 方案 | 优点 | 缺点 |
| --- | --- | --- |
| 传统数据中心 | 1、 符合传统运维技能<br>2、 初期投入较低 | 1、 运维效率低，维护成本高<br>2、 高能源消耗，低资源利用率<br>3、 平台支撑能力差，水平扩展性差<br>4、 信息共享弱<br>5、 服务策略（如安全策略、业务优化策略）不一致<br>6、 高 TCO |
| 云数据中心 | 1、 统一管理<br>2、 虚拟化、自动化<br>3、 弹性扩展<br>4、 安全节能<br>5、 高效运维 | 1、 需要整合传统遗留系统<br>2、 初期投入要高于传统数据中心<br>3、 用户需要学习云管理技能 |

| | | |
|---|---|---|
| | 6、 低 TCO | |

三、 云教育中心的需求

| 分类 | 需求描述 |
|---|---|
| 业务需求 | 支持应用系统的 7*24 小时的正常运行 |
| | 支持将来扩展到 xxxx 个云桌面的正常运行 |
| | 支持 xxxxx 个用户的同时在线并发访问 |
| | 支持 xxxx 个用户同时在线视频互动 |
| 维护需求 | 能够集中管理、自动化管理、基本满足 1 个人可以维护 1000 台虚拟机的要求 |
| 技术需求 | 支持弹性扩展，在不影响业务系统运营的情况下，可以根据业务需求灵活扩展服务器、存储等容量大小。 |
| | 数据中心网络需要支持 IPsec VPN、SSL VPN、MPLS VPN 等多种安全访问方式，从而保证数据中心的高安全性。 |
| | 稳定性要达到 99.999% |
| | 全方位的安全策略，以保证数据安全、网络安全、用户安全 |
| | 支持未来多数据中心互联互通 |
| 带宽需求 | ● 上行带宽：xxxM;<br>● 下行带宽：xxxG<br>（详细计算过程如下） |

带宽计算如下：（选取分散远程学习及集中实训带宽要求最大的值作为带宽需求）

*注：业务并发率：同一时间在线用户会同时使用某业务的机率；*

*用户并发率：同一时间所有用户同时在线的比率；*

*实际带宽冗余量：在计算带宽的基础上加乘30%，以更好支持业务体验。*

1) 分散远程学习

| 业务类型 | 平均每用户上行带宽(Kbps) | 平均每用户下行带宽(Kbps) | 用户数 | 业务并发机率 | 用户并发机率 | 上行带宽需求(Kbps) | 下行带宽需求(Kbps) |
|---|---|---|---|---|---|---|---|
| 教育门户子系统 | | | | | | | |
| 课程管理子系统 | | | | | | | |
| 教学资源共享平台 | | | | | | | |
| 作业管理子系统 | | | | | | | |
| 教学发布子系统 | | | | | | | |
| 学习管理子系统 | | | | | | | |
| 社区互动学习子系统 | | | | | | | |
| 数据档案子系统 | | | | | | | |
| 综合管理子系统 | | | | | | | |
| 总带宽 | | | | | | | |

- 分散自学的带宽需求：（在净载荷基础上，加乘 20%的实际冗余量）

  上行带宽：xxxM ； 下行带宽：xxxG

2) 集中实训

| 业务类型 | 平均每用户上行带宽(Kbps) | 平均每用户下行带宽(Kbps) | 用户数 | 业务并发机率 | 用户并发机率 | 上行带宽需求 | 下行带宽需求 |
|---|---|---|---|---|---|---|---|
| 教育门户子系统 | | | | | | | |
| 课程管理子系统 | | | | | | | |
| 教学资源共享平台 | | | | | | | |
| 作业管理子系统 | | | | | | | |
| 教学发布子系统 | | | | | | | |
| 学习管理子系统 | | | | | | | |
| 社区互动学习子系统 | | | | | | | |
| 数据档案子系统 | | | | | | | |
| 综合管理子系统 | | | | | | | |
| 总带宽 | | | | | | | |

- 集中实训的带宽需求：（在净载荷基础上，加乘 20%的实际冗余量）

  上行带宽：xxxM； 下行带宽：xxxM

## 3.5 教育区域网络

一、 教育区域网络的简介

XX 市内学员分布比较广，XX 区域云教育项目要满足 XX 市内教师再培训，同时 XX 市教育区域网络承载多种教学业务应用，必须实现 XX 市内各个区和县级市内高校、教育局网络互联。

二、 教育区域网络的需求分析

| 分类 | 需求描述 |
| --- | --- |
| 业务需求 | 能够支持多种业务的承载，如：语音、数据、视频等 |
| | 即使在网络繁忙时，也能够保证语音业务及实时视频业务的用户体验。 |
| 维护需求 | 支持集中管理，远程维护、降低维护复杂度 |
| 技术需求 | QoS 可设置：实时语音业务 > 实时视频 > 网页数据 > 非实时数据（如文件下载、邮件、消息等） |
| | 可靠性要达到 99.999% |
| | 要基本解决常见安全问题，如：病毒，非法攻击和恶意的业务盗用等。 |
| 带宽需求 | ● 数据中心侧带宽需求：<br>上行带宽：xxxM<br>下行带宽：xxxG<br>● XX 大学侧带宽需求：<br>上行带宽：xxxM<br>下行带宽：xxxG |

| | |
|---|---|
| | ● 其它学校侧带宽需求：<br>上行带宽：xxxM<br>下行带宽：xxxG |

# 4 XX 区域云教育总体方案设计

## 4.1 设计原则

区域云教育平台是一个复杂的系统工程，不可能一蹴而就，必须遵循“统一规划、分步实施”和“以需求为导向，以应用促发展”的原则。

除了要遵循高性能、高可靠性和高安全性的设计原则外，还应遵循如下设计原则：

- 遵循教育部政策，借鉴成功经验

在建设过程中，应借鉴国内外，特别是其它省市的成功经验，从本地的教育现代化实际情况出发，充分了解教育部关于《教育部关于“教师教育创新平台项目”实施工作的意见》，重点梳理共性需求和个性化需求，应用先进成熟的理论和技术，确定分阶段的建设目标、建设任务，正确把握教育现代化的发展方向。

- 成熟性与发展性的统一的原则

工程建设应首先采用符合目前计算机及应用系统发展趋势的主流技术，技术先进并趋于成熟的，被公众认可的优质产品。既要保证当前系统的高可靠性，又能适应未来技术的发展，满足多业务发展的要求。要本着“有用、适用和好用”的原则，不片面追求硬软件设施的先进性，强调整个系统的可连接性和整体布局、应用的合理性。

- 先进性与实用性的统一

工程建设方案要面向未来，技术必须具有先进性和前瞻性和实用的原则，在满足性能价格比的前提下，坚持选用符合标准的，先进成熟的产品和开发平台。

- 独立性与开放性的统一

教师再教育涵盖高校教师、中小学教师的再培训，主要是在网上学习为主，必然是多种传统终端、新型的智能终端需要接入。因此，在规划和设计本系统时，强调尽可能保证系统的开放性和数据、资源的完全共享。

- 可配置性

由于整个系统涉及的部门比较多，业务种类比较复杂，因此系统的灵活配置性就显得非常重要，系统的可配置性应包括部门配置、人员角色配置、公文样式配置、处理流程配置等。

- 标准化

现有信息技术的发展越来越快，为了使该系统在未来运行过程中其技术能和整个信息技术的发展同步，系统应具有备灵活适应性和良好的可扩展性，系统的结构设计和产品选型要坚持标准化，首先采用国家标准和国际标准，其次采用广为流传的实用化工业标准。

可实现服务器的负载均衡，支持服务器线性扩展。

软件采用组件化设计，可方便地与用户其他的应用系统集成。

- 可靠性、安全性、保密性

教育信息化涉及面广，设计上要充分考虑其大量硬件设备、软件系统和数据信息资源的实时服务特点，要保证网络、系统、数据的安全，保证系统运行的可靠，防止单点故障，对涉密信息应充分保证其安全。对安全管理要充分考虑安全、成本、效率三者的权重，并求得适度的平衡。对整个系统要要有周密的系统备份方案设计。对系统主要的信息实行自动备份，以保证系统的

异常情况的补救，并设有系统自动恢复机制。采取必要措施防止数据丢失，保证数据的一致性，保证系统运行过程中的高可靠性。

系统中的各个服务均采用了先进的多线程结构，优化的 I/O 系统，在 Linux 服务器上充分利用操作系统的高度并发和异步完成的高效性，在充分利用硬件提供的有限资源的前提下，实现最大流量的课件点播输出和高效的事务处理。

## 4.2 设计理念

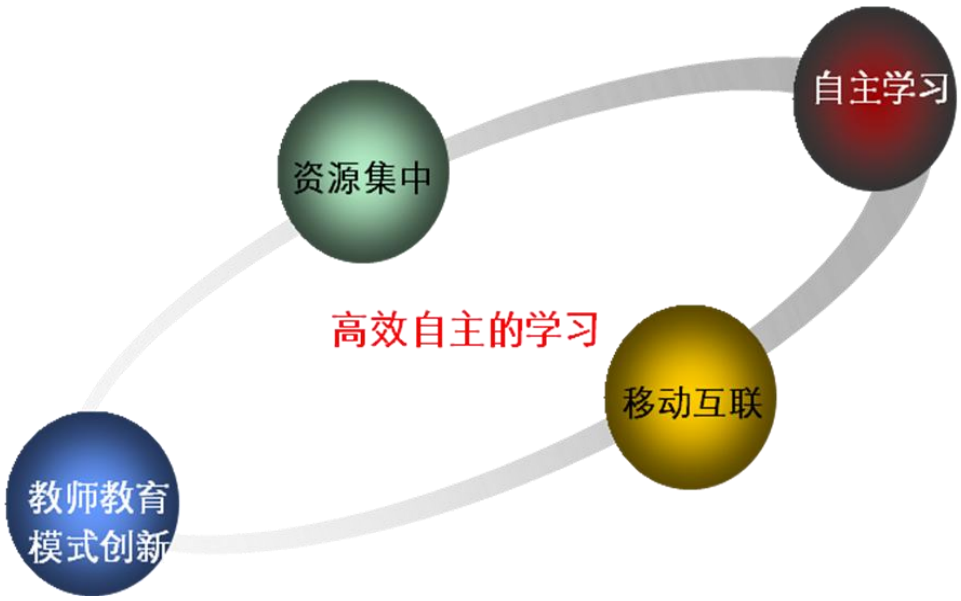



图 4.1 设计理念

设计理念的描述，如下表

| 理念 | 描述 |
| --- | --- |
| 资源集中 | 基于云计算的数据中心<br>教学资源集中存储<br>数据安全、运维快捷 |

| | |
|---|---|
| 自主学习 | 被动学习变主动学习<br>冲破时空的自由学习<br>按兴趣选择性的学习<br>阅读方式的多样性 |
| 移动互联 | 随时随地的上网<br>移动的教与学<br>网络教学、工作协同 |
| 教师教育模式创新 | 虚拟环境的创建,带领教育的创新<br>实现量化评估，更为科　学的管理 |

表 4.1　设计理念描述

## 4.3 总体方案

### 4.3.1 系统上下文

本项目是独立、新建的系统，包括底层的数据中心、教育区域网及上层应用系统都是独立的系统，也是新建的系统，跟其他系统没有关联。

### 4.3.2 总体逻辑架构

云教育平台以公共云教育为最终目标，设计 XX 云教育平台，分阶段部署为指导：首先在 XX 实施教育私有云，用云计算平台解决新教师再教育信息化需求。未来平滑融合到统一的市公共云教育。

总体逻辑架构主要包括资源池层、管理调度层、平台层、业务层和接入层等。具体结构如图所示。

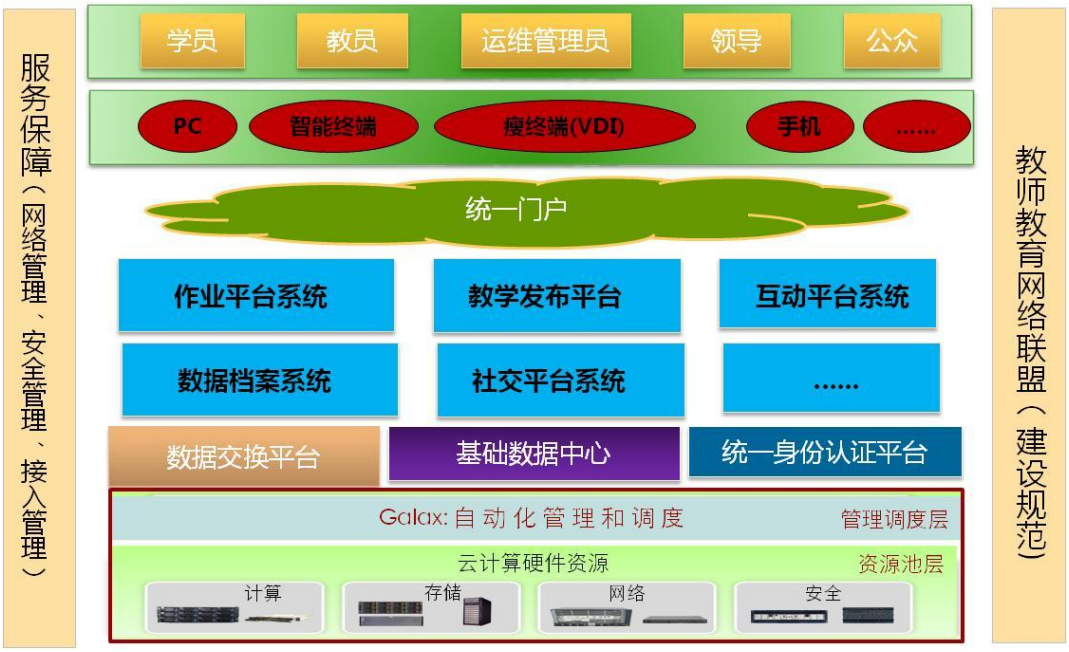



图 4.2 总体逻辑架构

总体架构主要包含：

资源池层：数据中心系统相关的硬件基础设施，包括服务器、存储设备、交换设备、安全设备等。

管理调度层：把物理资源虚拟化成多种虚拟资源包括计算资源、存储资源和网络资源等; 并实现资源管理、弹性调度以及操作维护等综合管理功能，为上层应用平台提供按需获取、可管理的物理和虚拟资源。

平台层: 面向教师教育的软件支撑平台，包含基于标准的基础数据库，教育资源库，统一身份认证，内容管理，数据交换，教育应用中间件，搜索引擎等。实现统一的数据定义与相关标准、规范的数据环境，资源共享和数据交换的教育支撑平台。

业务层: 是用户直接面对并使用的业务，包括作业平台系统、教学发布平台、互动平台系统、数据档案系统、社交平台系统等。

接入层：广大学员、教员通过统一门户系统接入。

### 4.3.3 总体物理架构

云教育平台的物理架构：云数据中心布署在 XX 机房、之后将 XX 地区高校和教育局通过专网接入到数据中心，学员通过校园网进行网络学习。各高校校园网及中小学校园网的建设不在本项目范围内，中小学与当地教育局之间互联也不在本项目范围内。

总体物理架构如下图所示：

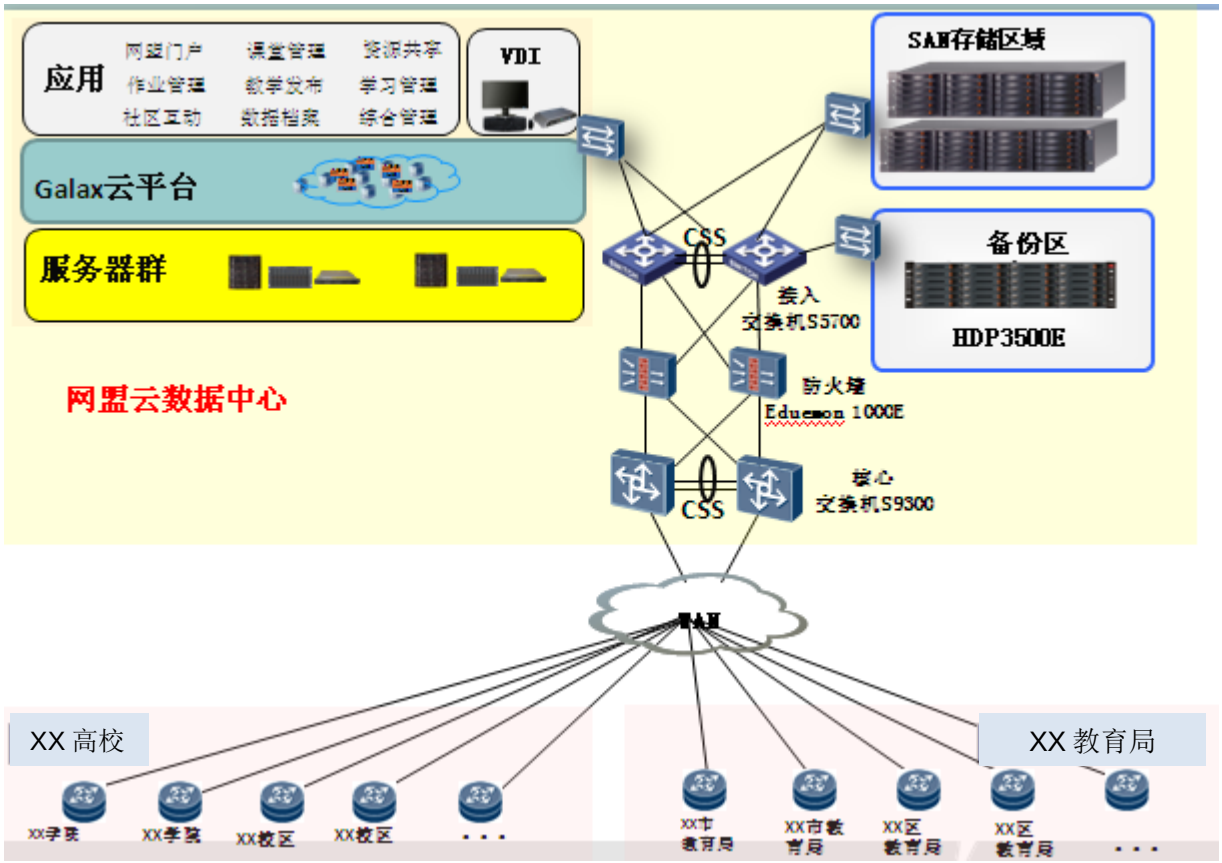



图 4.3 总体物理架构

# 5 XX 区域云教育各子系统设计

## 5.1 云数据中心子系统

### 5.1.1 设计依据

- GB50174-2008 《电子计算机机房设计规范》
- GB50462-2008 《电子信息系统机房施工及验收规范》
- TIA-942 数据中心的通信基础设施标准

### 5.1.2 子系统功能

本文中的云数据中心子系统是基于云计算技术的数据中心的 L2 层，即数据中心 IT 系统，如各类计算、存储、网络和安全设备，以及对这些设备的调度和管理。L3 层的应用系统部署在服务器上，但 L3 层不属于项目的建设范围。

本项目云数据中心子系统主要包括两个功能：

- 为应用软件系统提供服务器及安全支撑；
- 提供桌面云虚拟机。

### 5.1.3 XX 区域云教育数据中心子系统设计方案

#### 5.1.3.1 云数据中心 IT 基础架构设计

云数据中心的 IT 基础架构作为数据中心方案的总体架构的核心内容之一，主要包含网络子系统、计算与存储子系统、云平台子系统、安全子系统、备份子系统、运维管理子系统，以及机房子系统。机房子系统不属于本项目建设范围，本方案不展开描述。

XX 区域云教育（以下简称“云教育”）数据中心总体架构设计遵循面向业务需求的设计思路，基于模块化的设计方法，实现云教育数据中心基础架构模

块与业务模块松耦合，保证地区教育业务动态扩展和新业务快速上线。云教育数据中心解决方案 IT 基础架构设计方案如下图：

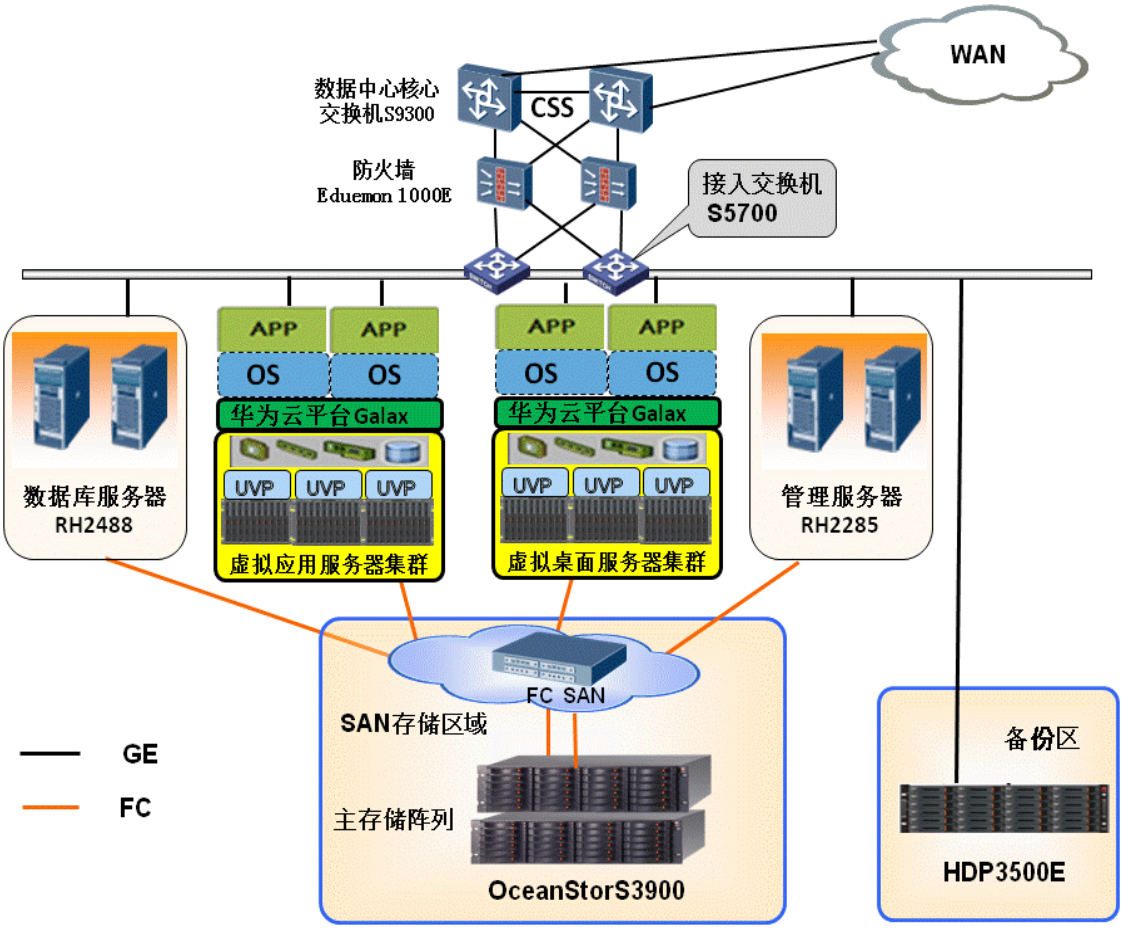



图 5.1 数据中心 IT 基础架构

**网络：**本方案数据中心网络架构采用扁平化二层网络架构（核心层、接入层），使用网络虚拟化技术，核心交换机承担着核心层和汇聚层的双重任务。

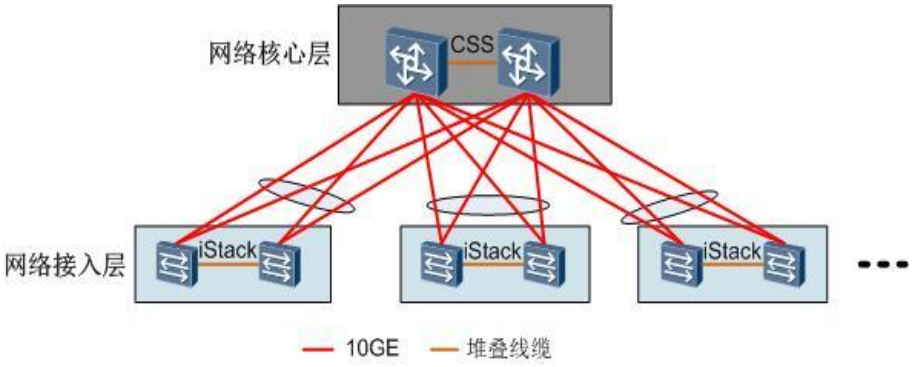



图 5.2 数据中心网络架构

**计算：**本解决方案所提供的计算系统的设备为华为自研服务器，本方案中推荐使用华为服务器 RH2285 和 RH2488。该服务器配合华为的云平台，可以为用户提供高计算密度、高资源利用率、以业务为导向的易管理的计算系统。根据实际业务需求，结合安全和管理需求，除数据库服务器(RH2488)和管理服务器(RH2285)不虚拟化外，其他服务器将充分采用虚拟化技术分两个区：虚拟应用服务器集群和虚拟桌面服务器集群。

**存储:**存储与计算分离，存储采用 FC SAN 连接主存储阵列 OceanStor3900。通过虚拟化集中部署，动态分配和调用资源，实现计算和存储资源的高效管理。

**备份：**备份系统相对容灾系统具有性能低，成本低的特点。本备份方案中采用华为备份一体机 HDP3500E。

**华为云平台 Galax：**Galax 是华为提供的虚拟化管理软件，每朵云部署一套 Galax 软件，Galax 主要包括管理节点有：MCNA、ESC、OMM、CRM、IMG。Galax 采用三层架构，第一层是弹性业务节点 ESC，ESC 是针对整朵云的管理与调度；第二层是集群管理节点 CRM，一朵云下可有多个集群，一对 CRM

只负责管理一个集群；第三层就是计算与存储资源池。ESC 有附属的 OMM 节点对外提供管理 Portal，IMG 节点保存镜像。

**虚拟化平台：**华为虚拟化平台 UVP 通过对服务器物理资源的抽象，将 CPU、内存、I/O 等服务器物理资源转化为一组统一管理、可灵活调度、动态分配的逻辑资源，并基于这些逻辑资源在单个物理服务器上构建多个同时运行、相互隔离的虚拟机执行环境。

**运维管理：**云教育数据中心运维管理采用开放的管理架构和模块化的设计思路，根据云教育数据中心管理需求配置运维管理模块。主要管理模块包括服务管理、统一管理门户、服务流程管理、综合监控管理以及云计算平台管理。为了保证方案的开放性和可扩张性，运维管理架构采用业界成熟管理产品与华为管理产品相结合：

- 统一管理门户采用华为 SingleCLOUD 门户方案；
- 综合监控管理采用华为 U2000 和华为 ISM 监控方案；
- 云平台管理采用华为 SingleCLOUD 管理方案。

#### 5.1.3.2 组网方案

网络架构设计采用“分区+分层”的设计思路：

- 根据云教育数据中心不同业务功能区域的隔离需求，将云教育数据中心网络分成多个业务区域，各业务区域之间在实现网络逻辑隔离；
- 根据云教育数据中心网络动态扩展的需求，将云教育数据中心网络设计中分为核心层与接入层，实现扁平的二层网络架构。

根据云教育数据中心网络高效交换的需求，将云教育数据中心存储网络和业务网络分离，保证业务数据与存储数据之间互不影响。

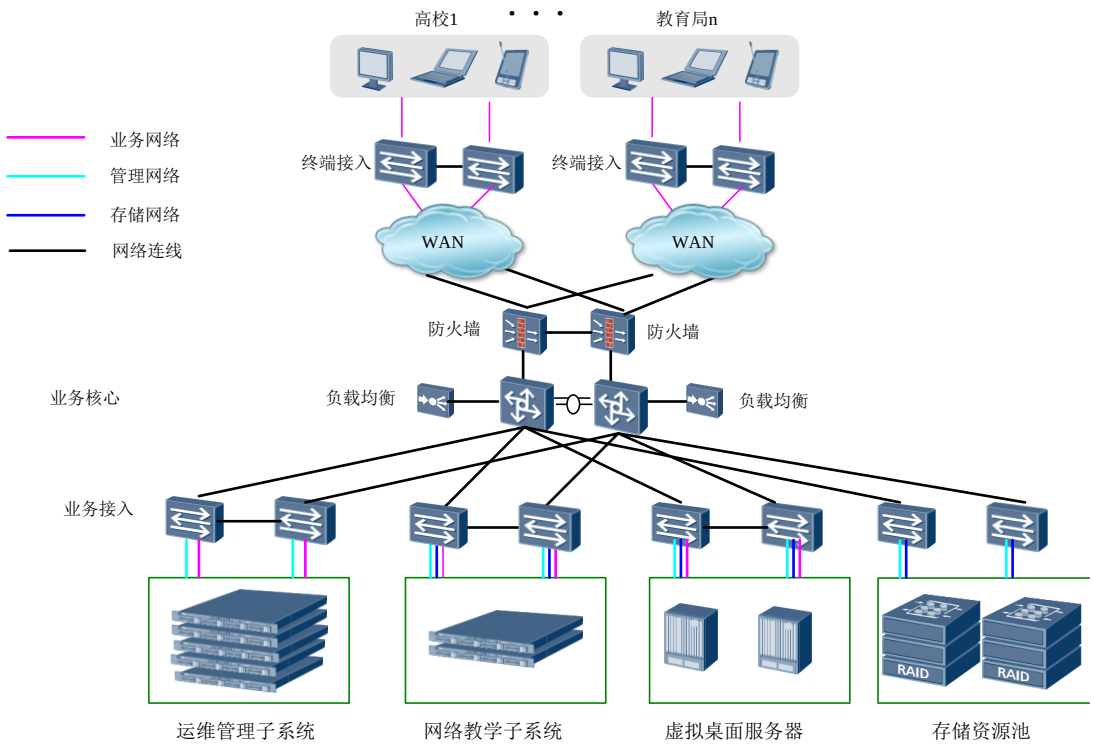



图 5.3 数据中心组网方案

本云教育数据中心主要提供以下两个应用：

- 教育区域的网络教学系统
- 虚拟桌面办公系统（VDI）

各成员单位通过广域网连接到数据中心，可以通过在线访问网络教学系统进行学习和管理。

虚拟桌面办公系统（VDI）主要是 XX 使用。通过 TC(桌面云瘦终端)访问云教育数据中心的桌面云，实现高效安全的办公方式，实现 IT 基础架构的统一管理。

项目中主要涉及的组件：

- TC：为用户提供用户桌面的显示输出，以及键盘鼠标输入，TC 通过 ICA 协议访问对应的桌面，可以通过策略开放或者禁止 TC USB 等外设至虚拟机的重新定向；用户通过在 TC 上输入域用户名和密码访问对应桌面。
- 负载均衡：对接入桌面云提供负载均衡功能。
- 桌面会话管理 VDesktop：VDesktop 是华为提供的桌面管理与投送软件。负责显示基于 Web 的界面，当用户顺利通过身份验证后可以看到自己可用的虚拟应用。还要负责计算负载量和分配连接的应用发布服务器。
- 云管理 Galax：Galax 是华为提供的虚拟化管理平台，采用物理机形式部署，主要包括以下管理节点：主要完成整个虚拟桌面的资源管理与调度，为每个虚拟机分配相应的虚拟计算资源等。
- 计算资源池：为用户虚拟机提供计算资源。
- 存储资源池：为用户虚拟机提供存储空间，包括系统数据和用户数据。
- 网络安全：为数据中心各出口位置部署统一安全网关，以及日志审计设备，提高整网的安全性。根据安全级别的高低和系统的特点，本方案安全部署的建议分为三个部分，第一部分，首先考虑的是广域网内网的中心与各节点之间部署统一安全网关，实现核心域与其他域之间的隔离；其次是云教育数据中心边界安全网关部署；再次在功能分区（如业务服务器区、运维管理区）接入侧部署防火墙设备提高整网安全能力。同时，在核心区域出口位置增加日志管理系统，提高网络审计报表功能。

#### 5.1.3.3 数据备份方案

本方案中的备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。备份最多表现为通过备份软件使用磁带机或者磁带库将数据进行备份，也有用户使用磁盘、光盘作为存储介质。备份系统相对容灾系统具有性能低，成本低的特点。

本备份方案中采用华为备份一体机 HDP3500E，它能提供云或非云场景下的数据备份，如下图所示：

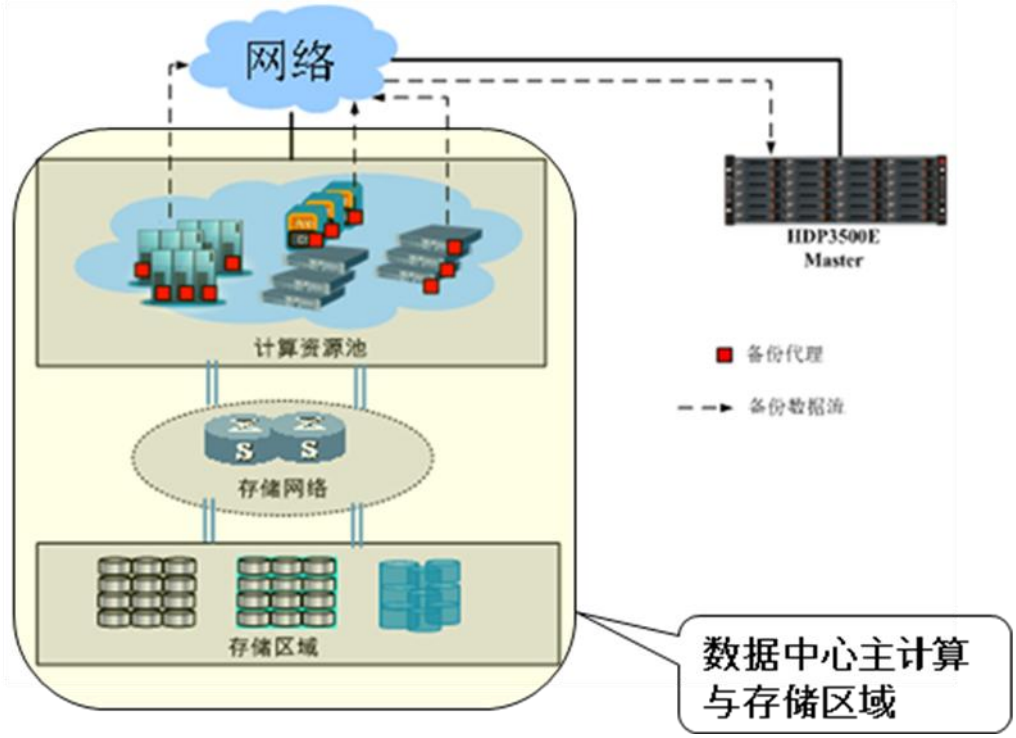



图 5.4 数据备份方案

华为 HDP3500E 是一款集备份服务器、存储设备和备份软件于一体的高密度、高性能备份产品。它集成最新的 NetBackup 7.1 备份软件，能够为关键业务提供无可匹敌的数据保护。通过备份设备的横向扩展组建基于 HDP3500E 的备份域，可实现备份容量和备份性能的线性增长。

#### 5.1.3.4 安全方案

数据中心面临内部恶意攻击和外部非法入侵威胁，同时经常安全审计不及时，所以加强数据中心的安全管理是必要的。

加强数据中心的边界安全管理、阻击恶意流量清洗是数据中心安全管理的重中之重。另外，随着网络业务的迅速发展而出现了越来越多的远程接入需求，这也是本方案中重点设计的内容之一。

常见的安全风险见下图（图中红色）：

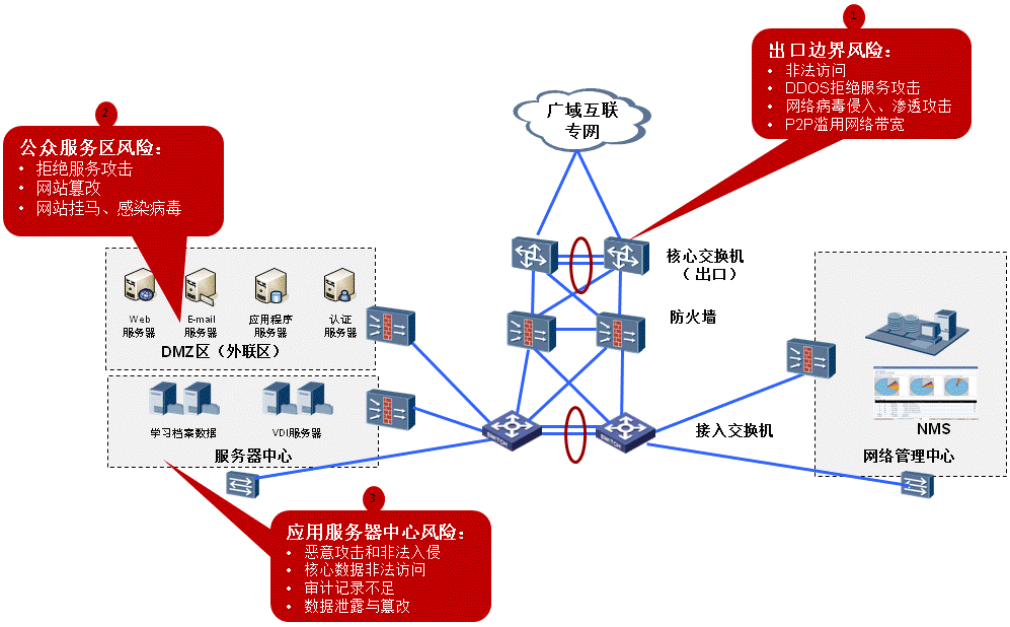



图 5.5 数据中心 IT 基础架构

**出口边界**的安全防范措施主要有：安全域划分、实时入侵防御、网络防病毒安全和上网行为的管理。

**公众服务区**风险和**应用服务器中心**的风险防范主要是措施：防止恶意流量的清洗和实时入侵防御。

本方案中的安全产品主要采用华为 Eduemon 1000E 防火墙。

### 5.1.3.5 应用服务器虚拟机关键指标参数设计

**应用服务器虚拟机主要配置参数**

| | 计算单元 | 内存（GB） | 存储(T) |
|---|---|---|---|
| 参数 | 8VCPU | 8 | 10 |

**规格配置说明：**应用服务器配置 8VCPU+8GB 内存可以满足区域内教学需求。按平均每个系统 xxxT 存储，共 xx 个应用系统，一共 xxxT 存储。

**总体规划原则：**采用 E6000 进行虚拟化。

#### 5.1.3.6 主要物理设备配置方案

云平台管理节点：xx 台 RH2285（单台配置：2 路 6 核 CPU，32G 内存，2*600G 硬盘）。

应用服务器（xx 个应用）：xx 台 RH2285，每台可虚拟出 12 个虚机，其中 10 个部署应用，2 个作为热迁移备份（单台配置：2 路 6 核 CPU，72G 内存，2*1T 硬盘）。

数据库服务器（xx 个数据库）：xx 台 RH2488 服务器，数据库服务器不建议使用虚拟环境，一般是部署在物理机上（单台配置：4 路 8 核 CPU，64G 内存，4*1T 硬盘，做 RAID 5）。

### 5.1.4 设备配置清单

| 硬件设备 | 型号 | 数量 |
|---|---|---|
| 应用资源服务器 | RH2285服务器（2路6核CPU、72G内存） | |
| 应用管理服务器 | RH2285服务器（2路6核CPU、32G内存） | |
| 数据库服务器 | RH2488服务器(4路8核CPU，64G内存,4*1T硬盘，做RAID 5) | |
| 接入交换机 | S5700 | |
| 汇聚/核心交换机 | S9306 | |
| 应用存储 | S3900（1控制框，600G SAS硬盘） | |
| 防火墙 | Eduemon 1000E | |
| 负载均衡 | MPX9500-1*2.33G(四核)CPU-8GB RAM | |
| 机柜 | IDCU机柜(4路16A交流220V输入) | |
| 出口统一安全网关 | USG5550，VPN隧道数(10 隧道)，SSL VPN并发用户数(100个)，IPS-AV-URL-AS功能集36个月 | |
| 数据中心安全网关 | USG5550，IPS-AV-URL-AS功能集36个月 | |

| | | |
|---|---|---|
| 日志管理系统 | 日志管理系统 | |

### 5.1.5 方案亮点


图 5.6　数据中心方案亮点

- 高效

云计算的动态基础架构，通过虚拟化技术，将数据中心的服务器、存储、网络等资源进行池化，使数据中心能够灵活扩展、动态调度，提高资源使用效率。通过统一的运营平台，分权分域运维，提高运营效率。

- 节能

云计算通过虚拟化技术，将硬件资源池化进行资源共享，提高硬件资源使用率，降低单位能耗；资源管理平台通过动态资源调度、负荷均衡、分布式电源管理等技术使 IT 设备与基础设施联动，按需调度，降低能耗。

- 安全

统一安全管理平台中心，支持全网设备日志统一采集，分析，呈现；支持对海量审计日志关联分析，并逐级响应；可视化的安全配置和展现；将一些非关键业务应用云化部署迁移，多业务整合，统一出口、统一安全管理。

## 5.2 桌面云子系统

### 5.2.1 XX 区域云教育桌面云的总体架构设计

桌面云解决方案在云的功能实现基础上，它还实现高安全、高可靠、高性能、易远程集中运维、平滑扩容等功能，采用业界主流成熟的虚拟化技术，实现虚拟桌面、应用发布、服务器虚拟化等要求，其体系结构图如下图所示：


图 5.7 桌面云总体架构设计

- **终端接入层：**

在远端用于访问桌面云中桌面云的特定的终端设备，包括瘦终端、软终端软件和各种手持终端等。

- **桌面和应用交付层：**

负责对桌面云使用者的权限进行认证，保证桌面云的使用安全，并对系统中所有桌面云的会话进行管理。并对终端的接入访问进行有效控制，包括接入网关，防火墙，负载均衡器等设备。接入控制设备不是桌面云解决方案所必须的组成部分，可以根据实际需求进行裁减。

- **虚拟化及云平台层：**

云资源管理是指根据桌面云的要求，把桌面云中各种资源分配给申请资源的桌面云，分配的资源包括计算资源、存储资源和网络资源等。

虚拟化平台是指根据桌面云对资源需求，把桌面云中各种物理资源虚拟化成多种虚拟资源的过程，这些虚拟资源可以供桌面云使用，这些资源包括计算资源、存储资源和网络资源等。

- **硬件资源层：**

硬件是指组成桌面云系统相关的硬件基础设施，包括服务器、存储设备、交换设备、机架、安全设备、防火墙、配电设备等。

### 5.2.2 利用 vDesktop 架构实现虚拟桌面化

VDI 方式下指的是每个用户都有一个独立的虚拟机（独享或资源池），虚拟机系统盘和数据盘都通过 IP SAN 加载。系统需要在 Galax8800 云平台的基础上，部署至少一套桌面管理组件（包括 DDC,Web interface 等）。Galax8800 云平台产生虚拟机，而这些虚拟机将被桌面管理组件所管理，并被通过远程桌面协议推送给终端用户。此方案可替代目前学校机房和办公室中广泛使用的 PC。

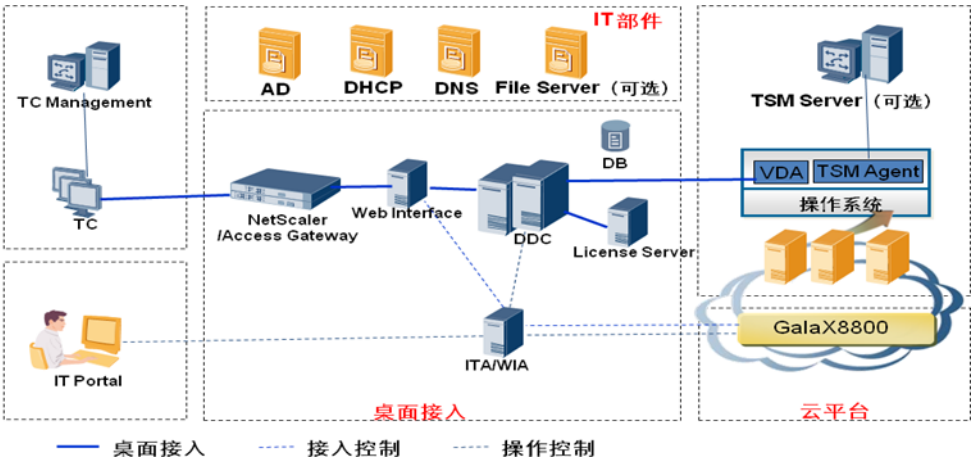



图 5.8　VDI 解决方案架构

基于 VDI 方案的桌面基础架构包含以下部件：

**IT 部件：**如果教育系统当前已有 AD/DHCP/DNS 等基础设施，华为桌面云支持与已有的 IT 系统对接，充分利用已有的 IT 应用。比如利用已有的 AD 系统进行桌面云用户鉴权；在桌面云上使用已有的 IT 工作流；通过 DHCP 给虚拟桌面分配 IP 地址；通过已有的 DNS 来进行桌面云的域名解析等。如果没有则需在设计时规划；

**桌面接入：**桌面接入由多个不同功能的部件组成，除 Netscaler/Access Gateway 是硬件设备外，其他都可部署在虚拟机上。

Netscaler：在两个或多个 web 服务器间做负载均衡作用；

Access Gateway：通过接入网关可将接入网络和虚拟机网络分离；

Web Interface：负责显示基于 Web 的界面，当用户顺利通过身份验证后可以看到自己可用的虚拟应用；

Desktop Delivery Controller: 负责计算负载量和分配连接的应用发布服务器的角色叫做 Data Collector；

License Server: 用于终端用户接入桌面云提供 License 控制；

Data Base: 数据库服务器集群用来记录用户与虚拟机的对应关系等信息；

ITA/WIA:虚拟桌面业务管理组件

**TSM:**对桌面策略进行统一管理，还有软件分发、文件分发、远程协助等功能

**TCM:**统一管理机房或办公室的瘦终端

桌面虚拟机化有以下主要功能特性：

**用户驱动的桌面重新启动：** 如果桌面无法启动或花费很长时间才能连接，用户可以使用桌面重新启动选项关闭并重新启动桌面。

**多媒体支持：**HDX 融合了多种技术，专用于为桌面云的用户提供可与本地 PC 相媲美的高清晰度音频与视频体验。 例如，HDX MediaStream 可确保流畅、无缝的多媒体内容体验，为 Windows Media Player 使用的 Media Foundation 提供支持。 HDX MediaStream for Flash 能让 Adobe Flash 内容在用户设备上进行本地播放，从而为用户提供高清晰度播放效果。 HDX Plug-n-Play 简化了与 USB、多监视器、打印机和其他外设，以及本地计算机资源的连接。 其他 HDX 技术可确保桌面云的传输能针对任何网络（无论本地还是远程）进行优化。

**即开即用：** vDesktop 虚拟机在空闲池中保持运行状态，以便在用户登录时可以使用新的桌面云，从而节省了冗长的物理计算机启动时间并提高了工作效率。

**通用打印机驱动程序：** vDesktop 为用户提供了一致、快速的打印体验，而无需特定的本地打印机驱动程序。 用户只需将 USB 兼容的打印机插入其用户设备即可进行打印。

**虚拟机基础结构：**vDesktop 使用 SmartUVP（一个集成的基于半虚拟化的 64 位虚拟机管理程序）来实现桌面云的可伸缩经济型承载。 SmartUVP 提供实

时迁移和集中式多服务器管理，将静态、复杂的数据中心环境转换为动态、易于管理的 IT 服务交付中心，从根本上降低数据中心成本。

**桌面分配**：vDesktop 允许管理员将不同类型的桌面云分配给不同用户，包括基于刀片式 PC 的桌面、基于专用虚拟机的桌面以及各组用户的池桌面。

**会话管理**： vDesktop 允许管理员管理处于活动状态和非活动状态的桌面云连接。 管理员可以查看用户连接的服务器，如有必要还可以将其注销。

**会话可靠性**：此功能可在网络中断期间维护用户的桌面云。重新建立网络连接后，用户可以继续他们的工作，不会存在任何中断。

**高可用性/故障转移**：vDesktop 通过提供故障转移功能来避免发生单点故障。即使单个服务器失败，用户也可以继续访问和使用其桌面云。

**即需即用桌面**： vDesktop 允许管理员将资源配置到池中，以便根据池范围应用常见配置设置，从而极大简化了重新配置任务。

对于教育行业，采用桌面云能有效提升教室办公和学员用机的使用效率，从而达到降低成本，提升教学质量的目的：

- 提供基于虚拟机级别的隔离，安全性高；
- 支持丰富的外设类型；
- 用户体验接近传统 PC；

使远程教学和移动办公成为可能，提供随时随地多种终端方便的桌面接入。

### 5.2.3 子系统功能设计

#### 5.2.3.1 桌面云业务

桌面云子系统也叫虚拟个人桌面系统，是基于云计算的虚拟办公桌面系统。也就是说我们只需要一个瘦客户端设备，或者其他任何可以连接网络的设备，

通过专用程序或者浏览器(软终端)，就可以访问驻留在服务器端的个人桌面以及各种应用，并且用户体验就象我们使用传统的个人电脑（PC）一样。

除了有 PC 机用户体验外，桌面云还有可移动、安全、节能、维护方便等优点。

#### 5.2.3.2 功能设计

云教育系统需要 xxxx 台桌面云，同时应实现以下功能目标。

1） 每个虚拟机操作系统内存 2GB，用户个人数据存储空间不低于 80GB。

2） 虚拟桌面站点需接入互联网，允许进行互联网的浏览、文件上下载等常见操作。

3） 要支持常用办公软件，如：Microsoft office、图片浏览、杀毒软件、内部通讯软件、网上下载工具等。

4） 系统要支持集中管理能力，如：对操作系统镜像统一管理、软件补丁统一分发、TC 终端统一管理。

5） 系统要支持互联网终端接入桌面云需求

6） 系统要支持安全架构设计，具有完善的安全防护能力。

7） 系统支持高可用性、动态迁移等可靠性设计。

8） 系统支持通过扩容存储与计算资源实现用户平滑扩容。

### 5.2.4 性能设计

网络延时设计原则要求：QoS 的要求达到时延<100ms，抖动<50ms，丢包<0.1%。

虚拟机体验性能设计原则：主要性能指标（VM 连接时间、VM 重启时间、VM 热迁移时间、VM 故障迁移时间、打开 PPT 文件响应时间、打开 VISIO

文件响应时间、打开 WORD 文件响应时间、语音延时、高清视频延时）不影响用户体验。

存储性能设计原则：每用户平均 IOPS 不低于 12。

总体用户性能设计原则：当上线总人数超过设计容量的 85%时，必须扩容。

### 5.2.5 关键指标参数设计

建设 xxxx 虚拟机桌面规划，桌面云终端建设数量为 xxx 个。桌面配置规格如下：

| 场景 | 规格 |
| --- | --- |
| 培训室或学员机房 | VCPU=2 MEM=2G 存储=80G 网络=共享100M IOPS＝12 |

xxxx 个用户(也就是一个虚拟机)，服务器采用 E6000 刀片式服务器，每台 E6000 刀片服务器上配置 xxx 个用户 VM。

### 5.2.6 设备配置

建设 xxxx 虚拟机桌面规划，桌面云终端建设数量为 xxx 个。

**资源服务器计算：**xxxx 桌面虚拟机，需要 xxx 台计算服务器；

**存储计算：**通过容量和 IOPS 两个维度计算存储设备配置，每个 600G SAS 硬盘的极限 IOPS 为 200，有效 IOPS 为 60（创建 RAID5 后，考虑写惩罚因素），创建 11+1 的 RAID5。（其中 1 表示热备盘，11 为 10 个数据盘加 1 个检验盘）一个 11+1 的 RAID5，可提供容量为 10*600G＝6000G，可提供 IOPS 为 11*60＝660.

| 设备类型 | 型号 | 单位 | 数量 |
|---|---|---|---|
| 资源服务器 | E6000 服务器（2 路 6 核 CPU、72G 内存） | 台 | |
| 管理服务器 | E6000 服务器（包括桌面会话管理和终端网关服务器） | 台 | |
| 负载均衡器 | 共用云数据中心的设备 | 台 | |
| 接入交换机 | S5352 | 台 | |
| 核心交换机 | 共用云数据中心核心交换机 | 台 | |
| 存储 | S3900（配置 240 块 600G SAS 硬盘） | 套 | |
| 云终端 | 瘦客户机 CT2000 华为海思 3716C，ARM Cortex A9 1.0GHz-Linux-内存 512M | 台 | |

## 5.3 教育区域网络子系统

### 5.3.1 设计依据

本次网络项目的网络设计完全符合国家网络建设的相关标准和规范。

1） 网络标准与规范

- RFC 1661：The Point-to-Point Protocol (PPP)
- RFC 1990：The PPP Multilink Protocol (MP)
- RFC 1994：PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC791：Internet Protocol. (IP)
- RFC792：Internet Control Message Protocol (ICMP)
- RFC793：TRANSMISSION CONTROL PROTOCOL (TCP)
- RFC768：User Datagram Protocol (UDP)
- RFC 826：An Ethernet Address Resolution Protocol (ARP)
- RFC2328：OSPF Version 2
- RFC1793：Extending OSPF to Support Demand Circuits
- RFC1771:：A Border Gateway Protocol 4(BGP-4)
- RFC1965：Autonomous System Confederations for BGP

- RFC1966：BGP Route Reflection
- RFC1997：BGP Community Attribute
- RFC2439：BGP Route Flap Damping
- RFC2138：Remote Authentication Dial In User Service (RADIUS)
- RFC2139：RADIUS Accounting
- RFC2784：Generic Roouting Encapsulation
- RFC2401：Security Architechure for the Internet Protocol
- RFC1157：Simple Network Management Protocol (SNMP)
- RFC2474：DS Field in the IPv4 and IPv6 Headers
- RFC2475：An Architecture for Differentiated Service
- RFC2615：POS
- RFC2547：MPLS VPN
- IEEE 802.3u：100Base 规范
- IEEE 802.3z：1000Base-X(GBIC)规范
- IEEE 802.3ae：10G 规范
- IEEE 802.1Q/1P：Virtual Bridged Local Area Networks
- IEEE 802.3ad：Link Aggregation
- IEEE 802.17：RPR

2） 国家安全标准与参考规范

- GB/T18336-2001
- GB/T18019-1999
- GB/T18020-1999
- UL 1950
- EN 41003
- AS/NZS 3260
- AS/NZS 3548 Class A
- CSA Class A
- FCC Class A
- EN 60555-2
- VCCI (ClassII )
- 抗干扰性
- IEC 1000 4 2 (ESO )
- IEC 1000 4 3 (辐射敏感性)

### 5.3.2 子系统功能

- 网络互联

XX 市区域云教育网络涉及范围包括 XX 市内 xx 个区和 xx 个县市，涵盖 xx 多高校（含职业院校）和市区教育局,以及县市教育局互联。

实现 XX 市内高校之间、高校和区教育局、高校和县市教育局网络互联。

- 多业务承载

教育区域网络是一个全 IP 网络，将承载多种业务数据，如语音、数据、视频、图等。从实时性来说，业务又可分为实时业务、非实时业务；从重要性来说，可可分为关键业务、非关键业务；

- 业务保障

业务对 QoS 的要求是不一样的，比如关键业务要求快速转发对带宽要求不高，比如办公的数据业务对时延要求不高，但有一定的带宽要求。

如何在一张广域网上去承载所有的这些业务是构建 IP 承载网的关键。这也是教育区域网络需要具备的业务保障能力。

- 业务安全保证

IP 网络的开放性决定的其相对传统网络更易受到攻击，所以如何保障这张 IP 承载网的安全性成了关键点。

✓ 通信内容保密，关键业务与非关键业务隔离

✓ 提供安全防范手段保护逻辑网络内部关键系统安全，防止业务盗用；

✓ 承载网基础网络（设备）能够有效防范各种非法攻击和病毒冲击，保证网络持续稳定运行，且性能不会劣化。

### 5.3.3 组网方案

#### 5.3.3.1 组网设计

从学校或教育局接入教育数据中心有两种方式：一、租用电信传输线路，自建交换网络，搭建从学校或教育局到数据中心的数据网络；二、利用原有CERNET 网络接口，接入数据中心。

由于各个学校或教育局的出口网络现状各不相同，总结有以下几种情况：

一、 已有 CERNET 出口，并且带宽能够满足教育新业务：建议延用现有CERNET 接入数据中心；

二、 已有 CERNET 出口，并且带宽满足不了教育新业务：建议新增出口路由直接接入教育区域网络，最终连入数据中心；

三、 无 CERNET 出口：新增出口路由直接接入教育区域网络，最终连入数据中心；

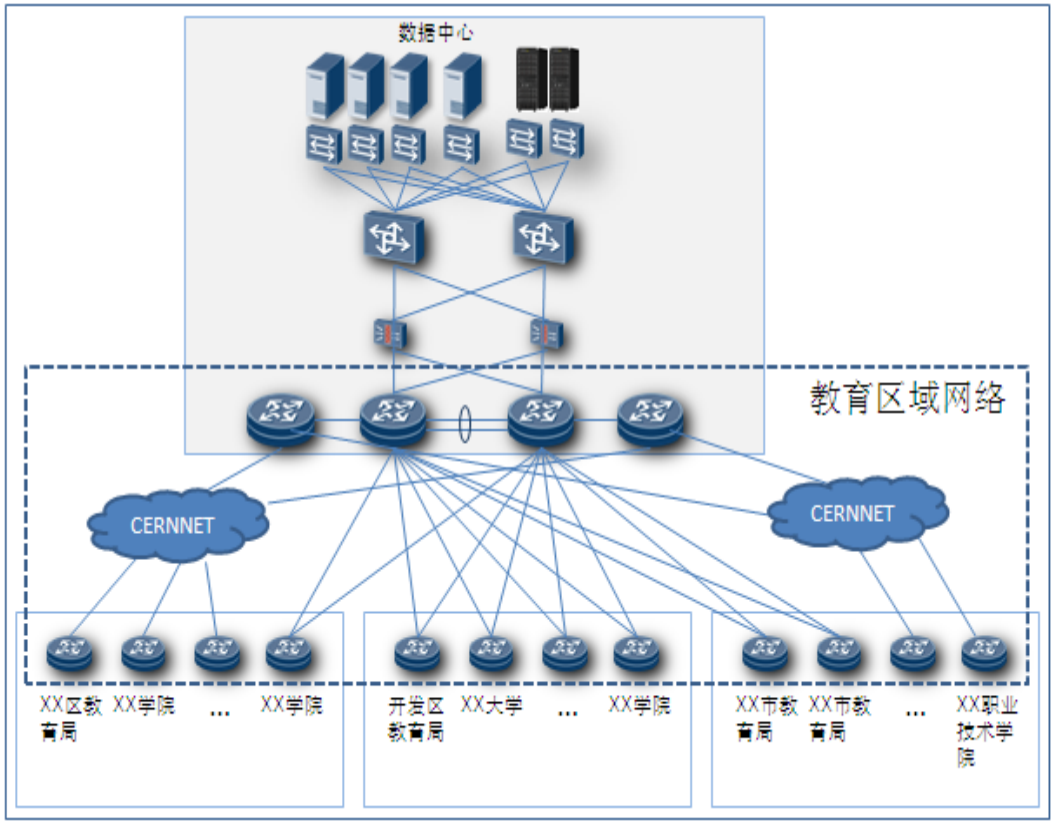
其中，网络带宽计算可参照 3.5 节进行计算。其中，学校及教育局带宽计算如下：

上行带宽：xxx（数据中心的上行总带宽）

下行带宽：xxxx（数据中心的下行总带宽）

由于底层传输网络是租用电信公司的，并且网络横向交换需求较少，教育区域网络将采用两层网络：即，接入网及核心网。

具体拓扑图如下，XX 地区的高校及教育局由接入网接入：




### 5.3.3.2 IP 地址规划

一、 IP 地址规划原则

IP 地址空间的分配与合理使用与网络拓扑结构、网络组织及路由政策有非常密切的关系，将对城域网的可用性、可靠性与有效性产生显著影响，应充分考虑本地网对 IP 地址的需求，以满足未来业务发展对 IP 地址的需求。城域网 IP 地址规划遵循以下原则：

- IP 地址的规划与划分应该考虑到城域网业务的飞速发展，能够满足未来发展的需要；既要满足工程现状对 IP 地址的需求，同时要充分考虑未来业务发展，预留相应的地址段。
- IP 地址的分配需要有足够的灵活性，能够满足各种用户接入如拨号、专线用户等的需要。

- 地址分配是由业务驱动的，按照业务量的大小分配各地的地址段。
- IP 地址的分配必须采用 VLSM 技术，保证 IP 地址的利用效率。
- IP 地址的规划应尽可能和网络层次相对应，采用自顶向下的分配原则，同时应充分体现分层管理的思想。
- 充分合理利用已申请的地址空间，提高地址的利用效率。

二、 IP 地址规划建议

整个区域教育网络基本上还是在教育系统中使用，而在教育系统中一般优先使用 CERNET 的 IP 地址。当然，如果要出口到外部 Internet 的话，还需要单独申请电信公网 IP 地址，在这不讨论。

根据上图所示，各学校或教育局内部皆视为局域网，在各自出口路由可设置 NAT，对 LAN IP 进行转换到公网 IP（CERNET 或 Internet）。

- 决定延用现有 CERNET 出口设备的学校或教育局

  延用原有 IP 地址规划即可。

- 新增出口路由，并连入教育区域网络的学校或教育局

  向 CERNET 申请新的公网地址

- 数据中心出口路由及需要发布到公网上去的服务器

  向 CERNET 申请新的公网地址

#### 5.3.3.3 路由规划

**1. 路由协议选择**

在大型网络中，选择适当的路由协议是非常重要的。目前常用的路由协议有多种，如 RIP、OSPF、IS-IS、BGP、DVMRP、PIM 等等。不同的路由协议有各自的特点，分别适用于不同的条件之下。

在目前，可以用于大规模网络部署同时又基于标准的路由协议有 OSPF 和 IS-IS。两种路由协议均是基于链路状态计算的最短路径路由协议，采用同一种最短路径算法（Dijkstra）。两种协议在实现方法、网络结构上均相似，在大型网络中都有成功案例。在 IGP 路由协议的选择上，不采用扩展性差的(如 RIP)和厂家的私有路由协议(如 IGRP 和 EIGRP)，建议采用 OSPF 或 IS-IS。从对两者的比较结果看，OSPF 更加适合教育教育区域网建设。下面是两种协议的具体比较。

OSPF 协议对比 IS-IS 协议

| 序号 | 比对项目 | 描述 | 比对结果 |
|---|---|---|---|
| 1 | 基本原理 | 基本原理相同，都是基于链路状态算法的路由协议。OSPF只用于IP，IS-IS除了支持IP之外还支持ISO的CLNP(支持二层和三层协议)。 | 教育教育区域网只考虑三层部署 |
| 2 | 灵活性 | IS-IS结构严谨，OSPF更加灵活。OSPF协议是基于接口的，而IS-IS路由器只能属于一个Area，并且不支持NBMA网络。 | OSPF占优势 |
| 3 | 适合的网络 | IS-IS占用网络资源相对较少，支持网络规模大于OSPF，在网络规模庞大时（比如：运营商网络）占优势。但对宽带城域网来说，OSPF和IS-IS无大的差异。对于网络的稳定性、可扩展性，两种协议都能很好的支持。 | 对规模不大的教育教育区域网来说，两者旗鼓相当 |
| 4 | 设备支持度 | 从目前很多厂商的设备来看，很多用户的中低端路由器及三层交换机不支持IS-IS，但所有的主流路由器及三层交换机都支持OSPF。 | OSPF有更好的设备支持度 |
| 5 | 业界部署 | 相比IS-IS，OSPF更常被选用做内部IGP。 | OSPF更适合教育区域网 |

2. 路由部署方案

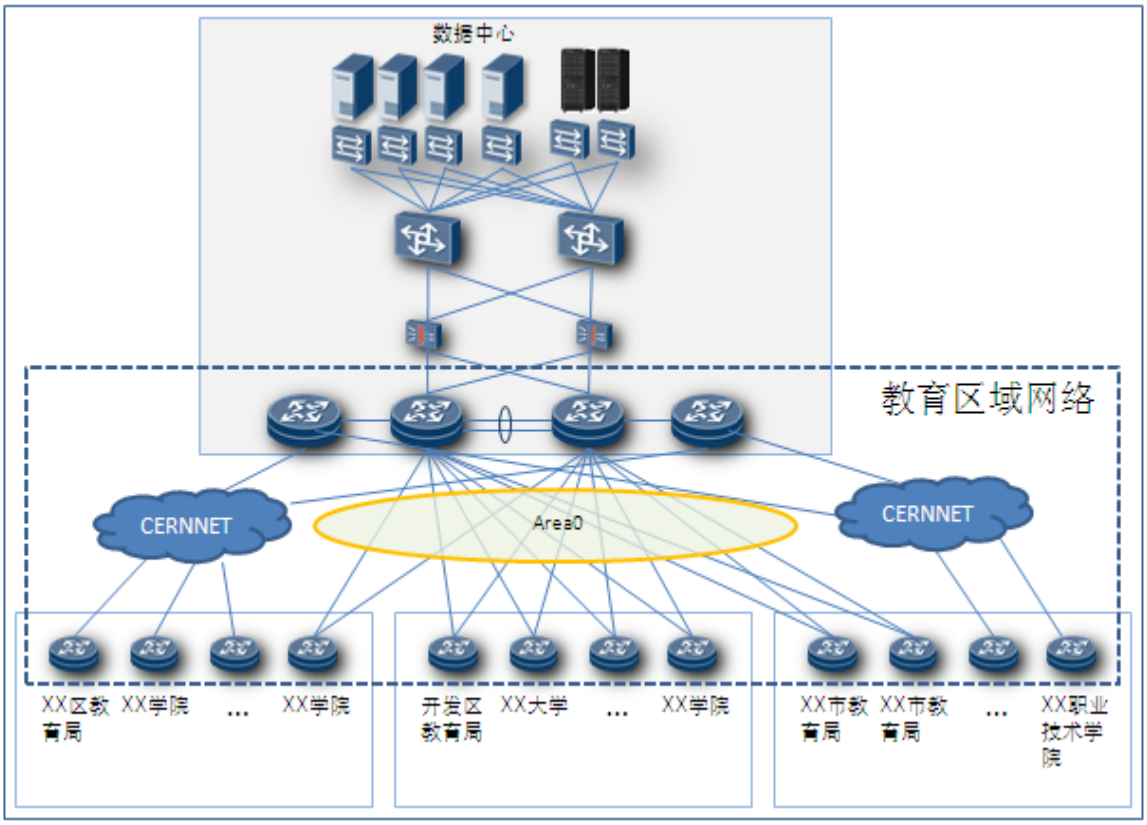
本节给出基于 OSPF 的路由协议部署方案。

- 规划合理的 RouteID

  RouteID 建议采用 Loopback 接口 IP 地址。

- OSPF 核心区域规划

  由于采用两层架构，且接入路由器设备数量较少，所以接入网与核心网之间设置一个区域即可，即 Area0。




### 5.3.3.4 IP 承载层可靠性规划

网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中应选用已规模商用的高可靠性网络产品，合理设计网络架构，制订可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持系统的正常运行，承载层设备本身必须达到 99.999%可靠性要求。

华为公司在业界首家提供“可真正部署的端到端 ms 级倒换方案”，满足电信业务承载的可靠性要求（50ms ~ 500ms），解决标准技术在扩展性、可部署性等方面的不足，降低运营维护成本、保障业务运营效果。

## 一、 故障检测技术

传统的故障检测技术是通过检测设备接口的状态来发现故障，这种方式只能检测简单的物理故障，而对于更深层的故障（如转发引擎故障、链路单通等）只能依靠上层的路由协议通过 Keep alive 或 Hello 报文来发现故障。这种机制不仅检测时间慢、开销大，而且存在应用场景的限制（不能跨协议）。

因此，为了提高 IP/MPLS 层的故障检测时间和效率，需要使用检测速度快、支持各种协议的故障检测机制。目前主要采用的机制有 MPLS OAM 和 BFD 技术。

- BFD

BFD（Bi-directional Forwarding Detection）是一个简单的交互检测协议，用于快速检测系统之间的通信故障，并在出现故障时通知上层应用。

BFD 具有如下特性：

✓ 可以对相邻转发引擎之间的通道提供轻负荷、快速故障检测。这些故障包括接口故障，数据链路故障，甚至有可能是转发引擎本身故障。BFD 的故障检测时间一般在 50ms 以内。

✓ 提供一个单一的机制，能够用来对任何媒介、任何协议层进行实时地检测。实现 BFD for Everything，例如 IS-IS/OSPF、BGP、LSP、TE 等等。

在目前网络中，BFD 已经被广泛应用于各种链路、协议的故障检测。

## 二、 业务保护技术

IP/MPLS 网络的每个部件都有可能出现故障，而采取的网络保护手段也有所不同。例如：

✓ 应用主控冗余、单板热插拔、GR 等保证设备层故障。

- ✓ 应用 VRRP、GLBP 等技术提高网关节点可靠性。
- ✓ 通过 IGP 快速收敛、TE FRR 保证网络路径的可用性。
- ✓ 通过 VPN FRR 保证 PE 节点可靠性。

下面就对各种常见的保护技术进行简单的说明。

- IGP 快速收敛

IGP 快速收敛的目的在于当网络发生故障时，提高 IGP 重新计算和路由收敛的速度。IGP 快速收敛是由多项技术结合而成的，主要包括如下特性。

- ✓ I-SPF（Incremental SPF）：增量路由计算，它每次只对变化的一部分路由进行计算，而不是对全部路由重新计算。
- ✓ PRC（Partial Route Calculation）：PRC 的原理与 I-SPF 相同，都是只计算变化的那一部分。但 PRC 不需要计算节点路径，而是根据 I-SPF 算出来的 SPT 来更新叶子（路由）。
- ✓ LSP 快速扩散：路由器收到一个或多个比较新的 LSP 时，在路由计算之前，先将小于指定数目的 LSP 扩散出去，加快 LSDB 的同步过程。这种方式在很大程度上可以提高整个网络的收敛速度。
- ✓ 智能定时器：智能定时器可以根据路由信息变化的频率自动调整延迟时间，既保证了路由快速收敛，且不影响路由器效率。智能定时器包括 SPF 智能定时器和 LSP 生成智能定时器。

- IP FRR

传统的 IP 网络中，从检测出故障，到路由系统完成路由收敛，一般需要几秒钟的时间。对于网络上某些对延时、丢包等非常敏感的业务来说，这种收敛速度无法容忍。比如 VoIP 业务所能容忍的网络中断时间为毫秒级。

IP FRR 特性能够保证转发系统快速地对于这种故障进行检测并采取措施，尽快让业务流恢复正常。IP FRR 的主要实现思想如下：

- ✓ 在主链路可用时，通过 Route-Policy 设置 IP FRR 策略，把备份路由的转发信息同时提供给转发引擎。
- ✓ 当转发引擎感知到主链路不可用时，能够在控制平面路由收敛前直接使用备份路径转发信息。

- IGP Auto FRR

  IP FRR 的备份下一跳是通过手工配置生成的，配置复杂，且需要依靠人为规划避免环路问题，容易出错。为了克服 IP FRR 的技术缺陷，引入了 IGP Auto FRR。

  IGP Auto FRR 是 IGP 利用收集到的链路状态信息动态决策出 IP FRR 备份的技术，其 IP 备份下一跳完全由路由协议根据链路状态信息结合公式自动生成，无需人工干预，极大的节约了维护的成本。

- BGP FRR

  IGP /LDP FRR 技术对链路故障的情况，可以做到快速的路径切换，但是当 BGP 节点发生故障时，需要 BGP 控制层面收敛，然后重新下转发表，收敛时间可能达到秒级，BGP 下一跳分离技术可以加快控制层面的收敛速度，但仍然无法达到电信级的可靠性要求。

  BGP FRR 技术采用转发层面的直接切换的方式，将次优 BGP 邻居的 LDP Label/BGP Label 直接作为备份放置到转发表中，当 BFD 等快速检测机制检测到最优 BGP 邻居故障时，直接切换到备份的表项，实现业务的快速收敛。

#### 5.3.3.5 QoS 规划

一、 QoS 设计

教育区域网中，除了基础数据业务外，还包括语音和视频业务。这些业务的特点是对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如在线学习需要高带宽的保证。语音业务虽然不一定要求高带宽，但非常注重时延，在拥塞发生时要求优先获得处理。

服务质量 QoS 是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方对客户的服务需求提供支持的能力，目的就是向用户的业务提供端到端的服务质量保证。一般情况，QoS 度量指标如下：

- 吞吐量（Throughput）

  又可称为带宽，表示一定时间内业务流的平均速率。通常通过流量监管（CAR）、流量整形（GTS）实现带宽调度。

- 时延(Latency)

  表示业务流穿过网络时需要的平均时间。对于网络中的一个设备来说，一般将不同时延的业务分为几种优先级，通过队列调度保证业务需求。

- 抖动(Jitter)

  表示业务流穿过网络的时间的变化，可通过拥塞避免等技术防止流量抖动。

- 丢包率（Drop Ratio）

  在网络中传输数据包时丢弃数据包的最高比率。数据包丢失一般是由网络拥塞引起的。

针对带宽、时延、抖动、丢包率等要求，QoS 可以通过优先级映射、流量监管、流量整形、队列调度、拥塞避免等技术提升网络服务质量，满足用户在有限的资源限制情况下，获得多业务部署的最佳体验。

## 二、 QOS 部署模型

QoS 部署模型规定了多种 QoS 技术如何组合满足用户网络服务需求，当前主要存在以下两种部署模型：

- Int-Serv 模型

Int-Serv（Integrated Service）模型是一个综合服务模型，它的特点是在发送报文前要先向网络提出申请，一般通过资源预留协议 RSVP 实现。

- Diff-Serv 模型

Diff-Serv（Differentiated Service）模型是一种多服务模型，它通过携带在报文头部的优先级参数（802.1P、DSCP、EXP）来告知网络节点它的 QoS 需求，这样，Diff-Serv 在提供服务时，可以为属于同一需求类别的分组提供同样的服务策略，而无需通过信令协议再去申请资源。

正是由于拥有“带内”信令和基于流进行服务的特点，在网络部署中，Diff-Serv 具有良好的可扩展性，成为区域网络部署的主流方案。

## 三、 用户业务分类

可以根据设备在整个网络架构中的位置来采取不同的 QoS 标记策略，边缘区域可能采用 IP Precedence、IP DSCP 或 802.1p 标识 QoS 等级，骨干可能采用 IP Precedence、IP DSCP、MPLS EXP 标识 QoS 等级。IP Precedence、MPLS EXP 和 802.1p 等字段均为 3 位 8 个等级，IP DSCP 则有 8 位 64 个等级。这就需要有一种对应机制，以便不同标记字段之间进行相互转换。转换方法是使用 IP DSCP 的前三位来标识 8 个等级，后三位均设为 0，这样形成与 3 位 8 个等级的一一对应关系。

用户业务的优先级

| 业务名称 | 优先级 | 业务描述 | IP Precedence | DSCP 定义 | 802.1p |
|---|---|---|---|---|---|
| 网络控制信息 | 高 | 适用于网络维护与管理报文的可靠传输，要求低丢包率。 | 7 | 5（CS7） | 7 |
| 运行管理信息 | | | | | |
| 实时消息 | 高 | 对时延、抖动较敏感；带宽需求低。 | 6 | 46（EF） | 6 |
| VoIP | | | | | |
| 视频会议、流媒体等 | 较高 | 对时延、抖动较敏感；带宽需求高；需要可预计的时延和 | 5 | 34（AF41） | 5 |

| | | | | | |
|---|---|---|---|---|---|
| | | 丢包率。 | | | |
| 网页浏览 | 中 | 对时延、抖动相对不敏感。 | 2 | AF31 | 2 |
| 其他 | 低 | 与公司业务无关，多是娱乐性的业务。如BT、eMule、YouTube等非组织性的内容。 | 0 | BE | 0 |

业务流量的识别和区分由最靠近用户的接入设备完成，根据以太网 802.1p 对业务流进行保障，保证从用户侧进入 IP 网络时 802.1P 可以映射到 IP DSCP，在路由器上对业务进行业务带宽保障，从网络层发向用户侧的数据由 IP DSCP 优先级映射到 802.1P，这样交换机可以根据 802.1P 对业务双向保障。

用户业务的队列调度和丢弃方式

| 业务名称 | 优先级 | 业务描述 | DSCP 定义 | 队列调度 | 丢弃方式 |
|---|---|---|---|---|---|
| 网络控制信息<br>运行管理信息 | 高 | 适用于网络维护与管理报文的可靠传输，要求低丢包率。 | 56（CS7） | PQ | WRED/SRED |
| 实时消息<br>VoIP | 高 | 对时延、抖动较敏感；带宽需求低。 | 46（EF） | PQ | WRED/SRED |
| 视频会议、流媒体等 | 较高 | 对时延、抖动较敏感；带宽需求高；需要可预计的时延和丢包率。 | 34（AF41） | WRR | WRED/SRED |
| 网页浏览 | 中 | 对时延、抖动相对不敏感。 | AF31 | WRR | WRED/SRED |
| 其他 | 低 | 与公司业务无关，多是娱乐性的业务。如BT、eMule、YouTube等非组织 | BE | WRR | WRED/SRED |

| | | | | | |
|---|---|---|---|---|---|
| | | 性的内容。 | | | |

#### 5.3.3.6 网络管理规划

一、 网管方案选择

在进行网络管理系统方案设计时，应遵循以下原则：

- 开放性、兼容性原则
- 整体性原则
- 模块化原则
- 易操作性原则

eSight 是华为推出的新一代面向区域网络的管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。

eSight 支持对 IT&IP 以及第三方设备的统一管理，同时对网络流量、接入认证角色等进行智能分析，自动调整网络控制策略，全方位保证企业网络安全。同时 eSight 提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

二、 eSight 运维部署方案

华为 eSight 提供多种应用，包括：多厂商的设备管理；企业资源统一管理；可视化的企业统一视图；全方位的企业故障监控；机房精细化监控；辅助智能楼宇安防监控；企业网络监控性能管理；分权-分域-分时的用户管理。

- 多厂商的设备管理

eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升管理效率。

eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 企业资源统一管理

如下图所示，华为 eSight 提供全方位的企业资源管理，针对不同网络设备、不同业务、不同服务器、工作站等 PC 资源进行管理。


- 可视化的企业统一视图

IP 网络是开放的，各厂商混合组网成为企业组网普遍情况。大部分企业不会像运营商一样建设综合网管，新厂商进入导致企业运维人员将面对多套厂商管理系统分而治之的情况。如果不具备全网设备统一监控的能力，出现网络故障后需要登录到多个网管查看状态，会导致管理效率低下。

eSight 预集成业界主流设备，默认已包含 Cisco20 个系列 140 余款设备、H3C14 个系列 130 余款设备、其他厂商 100 余款设备、以及数十款打印机、服务器。企业运维人员不做任何配置，即可管理全网设备，大大提升了管理效率。

eSight 拥有厂商新款设备自动配套能力，通过 eSight 厂商类型自动识别能力，对于友商新发布的设备也可实现拓扑、告警、性能等管理能力。

- ✓ 自动发现：自动发现网络资源，网络链路自动创建。
- ✓ 统一视图：提供 IT&IP 一体化拓扑视图，全面管理企业资源。
- ✓ 实时呈现：呈现子图、网元、链路、网元状态，实时了解网络的运行情况。
- ✓ 灵活定义：按用户信息保存网元位置，支持拓扑背景图和自定义图标功能。各种 Tips 信息，企业结构一目了然。

针对业界主流设备深入分析，不仅支持标准的流量采集，还同时支持设备面板、设备 CPU 利用率等私有属性的管理。

- 全方位的企业故障监控

华为 eSight 提供全方位的故障监控，提供包括基于 IP 设备、基于 IT 设备、基于业务应用等丰富的告警，同时提供 7*24 不间断的故障监控，实时故障提醒和实时故障远程通知，同时也能提供丰富的故障统计功能。

- 企业网络监控性能管理能力

华为 eSight 提供强大的企业网络监控管理能力、提供图形方式呈现性能数据，可以直观了解企业设备、服务器等资源设备性能情况；提供性能阈值告警能力，可以对企业网络健康度实时了解，保障企业业务承载网络健康性；自动创建设备基本性能监控；支持批量创建同类性能监控实例，方便客户轻松操作。

- 分权-分域-分时的用户管理

为不同用户分配不同权限，并记录操作日志；设置用户管理区域；限定用户管理范围；限定用户帐户有效时间、有效期。

### 5.3.4 关键指标参数

- 业务 QoS

QoS 就是针对各种不同的需求，提供不同的、可预测的服务质量的能力。可用性、延迟、抖动以及丢包率是衡量 IP 网络 SLA 的四个技术标准。

- ✓ 可用性（Availability）：指用户能够使用业务的时间占业务全部工作时间的百分数。在连续 5 分钟内，如果一个 IP 网所提供业务的丢包率≤5%，则认为该时间段是可用的，否则是不可用的。
- ✓ 延迟（Latency）：指在两个参考点间某一 IP 包从发送到接收之间的时间间隔。
- ✓ 抖动（Jitter）：指不同分组之间在延迟上的偏差。
- ✓ 丢包率（Packet loss）：指在两个参考点间传输时丢失的 IP 包数与已发送的 IP 包总数的比值。丢包主要是由网络拥塞引起的。

不同的用户及业务对 QoS 技术指标的要求是不同的。通过有效地实施各项 IP QoS 技术，能够有效地控制网络资源及其使用，能够在单一 IP 网络平台上融合语音、视频及数据等多种业务，能够在现有网络上细分客户、针对不同的客户需求提供特色的差别业务，以便能迅速获得利益回报，从而进一步扩大市场占有率、提高市场竞争力。

IP 广域网建设应能满足各种电信业务及信令的 QoS 要求。目前，IP 广域网承载的主要业务中对于 QoS 要求较高的是教育实时关键业务，因此 IP 广域网 QoS 建设目标是满足教育多业务统一承载及实时业务的 QoS 的综合要求。

- 业务可靠性

传统 IP 网络尽管有动态协议、冗余连接等可靠性技术，但是其程度远没有达到电信级要求，从可靠性的指标看，一个普通的 IP 网络故障，将导致业务中断几秒到分钟量级，这种指标可以满足传统 Internet 业务承载要求，但是无法满足实时话音、视频业务的服务质量需求。

电信级业务对于承载网可靠性要求为：

- ✓ 网络设备的可用性达到 99.999%

- ✓ 网络的可用性达到 99.999%
- ✓ 故障保护倒换时间：骨干网推荐链路保护小于 50ms（达到 SDH 要求）
- ✓ 网络设备的关键部件冗余，接口板件支持热插拔
- ✓ 关键的节点采用双节点冗余备份
- ✓ 关键的链路采用双归属链路

- 业务安全性

要想提高业务的安全性，使其达到电信级的要求，IP 广域网必须要满足以下几点要求 ：

- ✓ 业务安全隔离：物理网络隔离，或者单一的物理承载网实现基于业务的逻辑网络，逻辑网络之间以及逻辑网络到基础网络任何情况下没有泄漏；
- ✓ 逻辑网络内部：承载网提供安全防范手段保护逻辑网络内部关键系统安全，防止业务盗用；
- ✓ 基础网络可靠性：承载网基础网络（设备）能够有效防范各种非法攻击和病毒冲击，保证网络持续稳定运行，且性能不会劣化。

- 业务可运营可管理

IP 网络具有承载网和业务网双重属性。随着教育广域网中业务全面 IP 化的发展趋势，要求 IP 网能够承载更多更丰富的教育级业务，必然要求其能够为客户提供一套方便的网络业务运营管理手段。

所谓可管理，不仅仅指通常意义上的网络设备管理，更重要的是对于业务的管理能力，其中包括对于用户的管理能力、业务质量的管理能力、业务安全性的管理能力等等。这些业务管理功能如果仅仅体现在 BSS/OSS 中的一个模块上，而没有在网络设备和网络结构上加以考虑，是不可能实现的。因此，教育广域网的规划必须要考虑承载网具备开展各种灵活的用户管理、业务管理和安全性管理能力。

### 5.3.5 设备配置

| 序号 | 设备名称 | 推荐型号 | 数量 | 备注 |
|---|---|---|---|---|
| 1 | 核心交换机 | S9300 | | 用于数据中心 |
| 2 | 多业务路由器 | AR3260/ AR2240 / AR220 | | 根据项目情况定 |

### 5.3.6 方案亮点

- 多业务承载的质量保证，满足 QOS 需求
- IP 设备和网络可靠性强，故障保护倒换时间短。
- 业务安全隔离，逻辑网络内部，有效防止业务盗用；基础网络有效防范非法攻击和病毒攻击
- 可视化运营管理
- 多业务接入路由器支持丰富的广域网接口，提供高密度以太、语音等用户接入，支持 IPSec VPN 和防火墙等安全功能，可充分满足企业分支互联、中小企业广域接入和运营商转售等多种场合的需求

# 6 总体方案亮点

## 6.1 方案整体优势概述

华为公司基于 SOA 和云计算理念和技术（如服务器虚拟化、存储虚拟化、网络虚拟化、并行计算、分布式计算等）设计的新一代教育行业数据中心解决方案，为教育客户提供集中、共享、标准化、模块化的、虚拟化、自动化、面向服务的基础设施环境和应用支撑环境，它资源利用率高，业务灵活性强，能适应不断变化和不断增长的电子政务需求，让教育客户获得最大的投资回报。具体体现在：

- 实现电子政务的灵活扩展与平稳升级

华为的教育行业数据中心解决方案采用开放融合的体系架构，可兼容多厂家硬件产品，融合 UVP、VMWare、BC-EC 等多种虚拟化软件，利于教育客户现有 IT 资源的利旧、应用系统的平滑迁移以及将来对数据中心的灵活扩展。云数据中心可以跟传统数据中心进行融合，并进行统一的管理，利于教育客户实现现有电子政务系统平稳、有序向政务云过渡。

- 实现 IT 资源共享和高效利用

华为的教育行业数据中心解决方案通过服务器虚拟化、存储虚拟化、网络虚拟化等技术实现计算、存储、网络资源的集中和共享，形成一个共享资源池，为用户提供统一的服务器空间、虚拟服务器、存储空间、集中备份等服务，各教育单位可以按需、动态申请与回收计算、存储与网络资源。系统通过对共享资源池的自动化调度，实时动态满足业务系统高峰时段或突发高负荷时段对计算资源的弹性扩容需求，以保证系统的运行性能；同时，系统通过资源错峰、分时复用等策略和技术，提高资源利用率。

- 提升 IT 资源运行性能

华为的教育行业数据中心解决方案通过架构优化、CPU 调度优化、内存优化、I/O 优化、QoS 优化、弹性共享、负载均衡、温度平衡等技术有效提升资源运行性能。

- 支持应用的快速开发部署与静默升级

华为的教育行业数据中心解决方案可以快速虚拟化和创建政务系统所需的服务器资源、存储资源、网络资源及终端计算资源，快速部署和推广政务系统，当政务系统需要升级和扩容时，可以实现业务不中断的静默升级，降低服务成本和升级风险。

- 提供全方位安全保障

华为的教育行业数据中心解决方案提供了分层防护、纵深防御的安全技术方案，提供安全加固、安全巡检、应急响应等安全服务，提供安全管理制度咨询服务，从而为教育客户提供全方位的安全解决方案，确保数据中心、政务系统、数据的安全。

- 实现 IT 运维管理高效

华为的教育行业数据中心解决方案对数据中心的服务器、存储、网络、安全设备以及系统软件、应用软件等所有 IT 资源进行集中的监、管、控。各教育单位业务系统都能得到统一标准的运维管理服务，各教育单位信息中心可以将精力投入到各自业务系统中，不必再过分关注备份恢复、安全管理、运行维护等细节中，从而可有效降低 IT 运维难度和工作量，进而降低 IT 运维成本。

- 实现绿色节能

华为的教育行业数据中心解决方案综合运用多种节能方案与优化措施结合高效节能设备，最终达到绿色节能的目标。

## 6.2 自主研发能力

经过多年技术积累和产品研发，华为已经形成了丰富的云计算产品线，覆盖了云计算解决方案中的主要核心产品。主要核心产品线包括：

丰富的高中低端的服务器设备、存储设备、虚拟磁带库等计算存储产品；

丰富的核心网络设备、接入网路设备、无线网络设备等网络产品；

自主研发的电信级云计算虚拟化平台；

自主研发的云计算平台综合监控管理系统

丰富的高中低端防火墙、入侵监测、DDoS、VPN 等安全接入产品；

在核心产品的支撑的基础上，华为针对数据中心需求开发出针对性的云计算解决方案，各组件之间无缝集成，确保了解决方案的稳定性、完备性和安全性。

## 6.3 先进的云计算架构

华为云计算方案架构设计采用 SOA 的架构设计理念，从业务需求的角度设计匹配的 IT 基础架构，确保 IT 架构的可扩展性、灵活性和可演进性。同时，实现业务设计和 IT 基础架构松耦合，确保 IT 架构对业务多样性的支持和业务快速上线的支持。华为云计算方案架构设计的优势主要体现在以下几点：

电信级的网络设计方案。云计算网络方案借鉴华为在电信行业网络设计的多年经验和技术积累，采用先进的网络设计方法、技术、产品，确保数据中心网络架构满足未来长期的业务发展需求

成熟的云计算设计方案。云计算平台方案设计采用华为自主研发的虚拟化产品，总结华为丰富的云计算项目经验，经过华为 IPD 流程的严格开发，确保了云计算方案的先进性和可靠性

先进的电信级管理方案。华为云计算管理方案设计覆盖网元管理、网络管理、云平台计算资源管理，以及和业界先进产品合作的服务管理等多方位管理系统，满足大规模数据中心运维管理的需求，形成了完整的数据中心管理体系。

## 6.4 电信级安全架构

华为安全解决方案是华为在传统数据中心和云计算数据中心建设过程中的经验总结，体现了华为的竞争力。华为安全解决方案体现以下特点：

以华为丰富的电信级数据中心安全产品为依托；

对电信行业安全规范的深入理解；

结合华为公司自身数据中心安全管控的丰富经验；

深入总结电信网络安全管理方面的项目经验；

基于以上积累，华为提出了数据中心安全框架，并针对安全架构提出整体解决方案，覆盖了数据中心的完整安全需求。

## 6.5 上线即用

华为云计算解决方案不仅为教育部门数据中心打造先进的云计算计算资源平台，而且在云计算平台上为私有云上提供了功能完善的云计算服务产品。主要包括以下典型业务：

虚拟主机资源申请自助服务。虚拟主机资源申请自助服务给最终用户提供自助申请管理界面，帮助最终用户快速、灵活、方便地申请所需资源；

虚拟桌面业务。虚拟桌面业务为客户提供完整、安全的办公桌面解决方案，简化桌面管理；

云存储业务。云存储业务为最终用户提供集中方面的在线存储功能，使得用户在任何地点，以任何方式都可以方便存取个人的相关数据；

联合通讯业务。联合通讯业务为客户提供即时通信、在线会议等典型服务，满足客户基本办公需求；

BMS 门户。BMS 门户为数据中心运维管理人员提供基础的云服务门户功能，数据中心管理人员只需要根据自身需求做定制开发就可以快速对外提供云服务。

## 6.6 敏捷管控，维护效果高

维护效率提升 90%，并且可以对对电教室教学软件实现统一管理，限制学生乱安装软件和游戏；

云平台可对服务器进行整合，提高服务器资源利用率；

对于传统 PC 机，一个人最多维护 100 台 PC 机；面对于桌面云，一个人可以维护 3000 台虚拟机。所有 PC 都需要技术人员现场维护 。而桌面云无需到现场，采用统一资源管理平台，维护效率高。

## 6.7 绿色、安全、按需部署

节能且资源利用率高：桌面云 TCO 比传统 PC 节省 32%，其中电费节省 70%。云数据中心的 CPU 利用率高到 60%。

安全性高。云数据中心采用统一出口、统一安全管理；

采用云计算架构，可以一次规划，多次部署。

# 7 设备介绍

## 7.1 数据中心及桌面云主要设备介绍

### 7.1.1 华为 E6000 服务器介绍

本次管理服务器和资源服务器拟采用华为刀片服务器 E6000。E6000 服务器具有如下特点：

- **散热好：**

华为刀片散热架构先进：每个模块独享风道；刀片采用“对称布局”设计，相对“影子布局”，散热更均匀。

- **可靠性**

架构可靠性高：背板采用无源背板；全冗余设计；所有模块（刀片/硬盘/交换/管理/风扇/电源）支持在线热插拔；

- **管理维护简单**

“免下架”维护：机箱上架后，终生“免下架”维护。机箱所有模块拔出后，只剩下免维护的无源背板和结构件。ZeroTouch 零接触管理，所有管理维护操作都可以远程完成。

➢ **技术规格**

| 系统 | 类别 | 描述 |
|---|---|---|
| E6000 主机 | 尺寸 | 8U 机架（HxWxD：353mm×447mm×810mm） |
| | 刀片槽位 | 10 |
| | 交换机模块 | 6，可配置为 6 个 GE 交换机或 4 个 GE 交换机+ 2 个 FC 交换机。136Gbps 交换容量 |
| | 电源 | 6 个 110V/220V 80plus 电源 |
| | 风扇 | 9 个热插拔风扇模块 |
| BH620 刀片 | CPU | 2×CPU（Intel Nehalem），支持 CPU 单配，80W/95W CPU |
| | 内存 | 12 个 DIMM 插槽，DDR3 1GB/2GB/4GB/8GB，最大支持 96GB |
| | 硬盘 | 支持 2.5 寸 SAS/SATA 热插拔硬盘<br>支持 4 个硬盘配置 |
| | 扩展 | 2 个 8x PCIe 扩展卡接口，用于安装扣卡，无法外接 |
| 管理 | 管理 | 板上支持单板管理模块 BMC 提供对服务器的智能监控功能，符合 IPMI2.0 标准<br>支持远程 KVM，虚拟媒体等功能 |

### 7.1.2 华为 RH2285 服务器介绍

华为 Tecal RH2285 服务器具有如下特点：

➢ **性能高**

华为通过高速信号 SI（信号完整性）优化和自主研发的 BIOS 调优技术，使得服务器在同类服务器中性能更好。

- **能耗低**

关键部件如 VRD 电源、风扇等采用低能耗部件，系统电源采用 80Plus 金牌电源，单机静态功耗最低仅 75W；

- **存储容量大**

2U 12 个 3.5’盘架构，单机最大支持 24T（采用 2T 硬盘），单机磁盘 IO 带宽高于 1000MB/s；

- **管理维护简单**

ZeroTouch 零接触管理，所有管理维护操作都可以远程完成。

- **技术规格**

| 类别 | 描述 |
|---|---|
| CPU | 2 颗四核或六核 Intel Westmere-EP 5600 处理器，支持 95W、80W、60W 系列； |
| 内存 | 12 个 DDR3 800/1066/1333 RDIMM / UDIMM 内存插槽，系统最大支持 96GB |
| 硬盘 | 最多支持 12 个 3.5 英寸 SAS/SATA 硬盘<br>最多支持 12 个 2.5 英寸 SAS 硬盘，支持 300GB SAS 硬盘，最高存储容量为 3.6TB； |
| 扩展 | 2 个 PCIe 扩展卡接口 |
| 尺寸 | （HxWxD）：87.5 mm×448 mm×700 mm； |
| 管理 | 板上支持单板管理模块 BMC 提供对服务器的智能监控功能，符合 IPMI2.0 标准<br>支持远程 KVM，虚拟媒体等功能 |

### 7.1.3 华为 OceanSto S3900 网络存储

针对本次项目需求分析，我们拟采用 OceanStor S3900 存储为用户提供系统空间和数据空间，存储特点如下：

- **高性能、高扩展性**

高速部件/高速总线：配备 64 位多核处理器以及高速大容量缓存，最高 36GB/s 的系统内部交换带宽，支持 SAS2.0 宽端口后端通道。

支持多种不同种类的硬盘：SAS/SATA/SSD。

支持最大 2 块 I/O 接口卡：最大 12 个 IO 接口（包括前端与后端接口）。支持 4/8Gb FC、1/10G Ethernet 与 6Gb SAS2.0 接口。

三重性能加速技术：依靠强大硬件支撑的固有性能，使用 SmartCache 技术持续监测系统热点数据并缓存至 SSD 盘片，最高可获得数倍的读性能提升；利用纯 SSD 将系统性能再次大幅提高。三重性能加速机制，稳固按需提升系统性能，全面降低整体拥有成本。

高镜像带宽：双控之间的 Cache 镜像采用专用高速 8GB/s 通道，消除双控间数据交换的瓶颈。

- **高可靠、高可用性**

接口模块化热插拔设计： TurboModule 技术使得 I/O 接口卡可在线热插拔而无需关闭存储控制器，对业务主机完全透明，实现真正的在线 I/O 扩容

掉电数据保护：系统掉电后内置电池模组自动将 Cache 数据写入数据保险箱，保证数据不丢失。

硬盘预拷贝技术：提前发现即将故障的硬盘，主动迁移故障盘数据，规避系统降级的风险，有效降数据丢失的风险。

硬盘坏道修复技术：最大限度修复硬盘坏道，将硬盘故障率降低 50%以上，延长硬盘的可使用周期。

高级数据保护技术：利用 HyperImage 以及 HostAgent 实现针对应用系统数据的一致性快照，并能从快照中瞬间恢复数据；跨存储平台卷拷贝技术实现异构存储间的数据保护。远程复制技术实现数据异地备份容灾保护。

- **低总体拥有成本**

统一的 IO 接口模块：本系列全线产品使用统一的 IO 模块，极大降低总体拥有成本。

24 盘位高密设计：2U/4U 高密度硬盘框（24 块/框），平均 1U 空间最高可容纳 12 块硬盘（2.5 英寸），相对于低密度盘框设计来讲，扩容成本降低 60%。

易用的管理维护工具：通过 ISM 统一管理界面，5 步即可完成基本配置。支持声音、灯光、手机短信、邮件等多种告警手段；一键式双控在线 Firmware 升级，有效地降低用户运维成本。

- **低功耗**

硬盘节能技术：依据业务负载，实现硬盘智能休眠，可降低 40%的能耗。

智能风扇调速技术：根据系统当前温度智能调节风扇转速，降低风扇功耗及噪音，(风扇占整机功耗 15%左右)，增强设备环境适应能力。

CPU 智能变频：根据业务压力智能调节 CPU 工作频率，在业务压力小时，降低 CPU 工作频率，大大降低系统功耗。

- **技术规格**

| 型号 | S3900 |
|---|---|
| 硬件特性 | |
| 存储处理器 | 多核多处理器组 |

| | |
|---|---|
| 缓存 | 16GB |
| 控制器数 | 2 |
| 前端通道端口类型 | 8Gb FC、1/10GE(iSCSI) |
| 后端通道端口类型 | 24Gb SAS宽端口 |
| 板载IO端口数 | 8×8Gb 前端FC及4×24Gb 后端SAS宽端口 |
| 最大IO模块数 | 2 |
| 最大硬盘数量 | 288 |
| 硬盘规格 | SAS、SATA、SSD |

| | |
|---|---|
| RAID 支持 | 0,1,3,5,6,10,50 |
| 连接主机数量 | 512 |
| Luns | 2048 |
| 支持快照数量 | 1024 |
| TurboBoost | 支持 |
| TurboModule | 支持 |
| 其他功能软件 | HyperImage（快照）、HyperCopy（LUN拷贝）、HyperMirror（同步/异步远程复制）、HostAgent（主机端快照/复制管理模块）、UltraPath（多路径软件）、Diskguard（主机端数据保护软件）、SmartCache（TurboBoost中的动态数据缓存技术） |
| 操作系统兼容性 | AIX、HP-UX、Solaris、Linux、Windows等 |

### 7.1.4 负载均衡器选型方案

为了实现用户连接负载均衡要求以及 Internet 接入安全需求，需要配置 Netscaler 设备（企业版），Netscaler 可以起到下面两个作用：

功能一：网络负载均衡器（LB）：将某一应用的流量根据负载均衡算法重定向到多台服务器上，并能监控服务器的可用性；

功能二：接入网关（AG）：集中所有用户的认证、单点登录；负责用户和服务器之间的 ICA 连接。

由于用户规模大于 2500，所以配置 2 台 MPX9500

| 类别 | 项目 | MPX 9500 |
|---|---|---|
| 物理参数 | 高度 | 1U |
| | 重量 | 21kg |
| 环境参数 | 工作温度 | 0℃～40℃ |
| | 工作湿度 | 10％ RH～90％ RH（无冷凝） |
| 电源参数 | 电源模式 | 双电源 |
| | 输入电压 | AC：100V～240V |
| | 最大功率 | 450W |
| 系统配置参数 | 处理器 | Intel Xeon L5410（4核） |
| | 内存（GB） | 8 |
| | 接口 | 8×10/100/1000M网口 |
| | 系统吞吐量（Gbit/s） | 3 |
| | 每秒HTTP请求数 | 200,000 |
| | 每秒新建SSL连接数 | 20,000 |
| | SSL吞吐量（Gbit/s） | 3 |
| | 压缩吞吐量（Gbit/s） | 2 |
| | SSL VPN：并发用户数 | 10,000 |

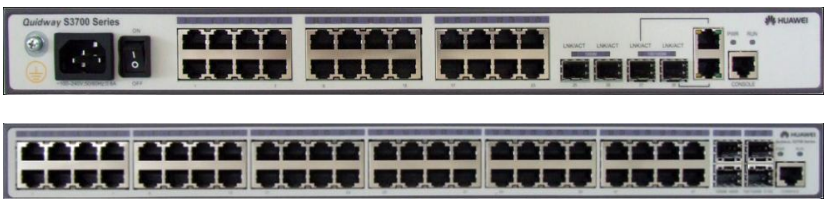
### 7.1.5 数据中心主要网络设备

## 接入交换机 S5700

Quidway S5700 系列以太网交换机（简称 S5700）是华为公司推出的集接入、汇聚和传送功能于一身的以太网交换机，满足企业网对多业务可靠接入和高质量传输的要求。

S5700 定位于企业网接入和汇聚层，具有大容量、高密度、高性价比的分组转发能力。借助 S5700 可构建高可靠的环形网络拓扑，具有多业务接入能力、良好的扩展性、QoS（Quality of Service）、强大的组播复制能力和运营级的安全性。

| 产品 | S5700-28C-EI<br>S5700-28C-PWR-EI | S5700-52C-EI<br>S5700-52C-PWR-EI | S5700-28C-EI-24S |
|---|---|---|---|
| 端口配置 | 24*10/100/1000BASE-T | 48*10/100/1000BASE-T | 24*100/1000BASE-X + 4* GE Combo |
| 可选配插卡 | 1个灵活子卡，支持 4*GE SFP、2*10GE SFP+、4*10GE SFP+ | | |
| 交换容量/转发性能 | 128G / 96Mpps | 176G /132Mpps | 128G /96Mpps |
| 电源 | 内置双电源模块，实现1+1备份 | | |
| 堆叠 | 专用堆叠卡堆叠（插卡插入专用堆叠卡槽位），，48G双向堆叠带宽 | | |



S3700-28 设备提供 24 个 FE 接口（S3700-28TP 为 24 电接口，S3700-28TP-24S 为 24 光接口）、2 个 GE 光接口和 2 对 COMBO 接口，并提供一个 Console 口用于本地配置，S3700-28TP-EI-MC 还提供两个监控口用于输入开关量检查和输出开关量控制。S3700-28 包括 1 个交换主控板称为 SCU（Switch Control Unit），支持 12.8Gbps 的交换能力。

S3700-52 设备提供 48 个 FE 接口（S3700-52P 为 48 个电接口，S3700-52P-24S 为 24 光接口和 24 个电接口，S3700-52P-48S 为 48 光接口）、2 个 GE 光接口和 2 个 GE/FE 光接口，并提供一个 Console 口用于本地配置。S3700-52 包括 1 个交换主控板称为 SCU（Switch Control Unit），支持 17.6Gbps 的交换能力。

绿色节能设计方面，S3700-28TP-SI/EI 采用自然散热，无噪声污染，产品可靠性高；节省风扇功耗，并避免定期维护风扇，节省维护费用；无风扇等额外功耗，使产品达到更好的能效功耗比；还可以有效的避免单板腐蚀。

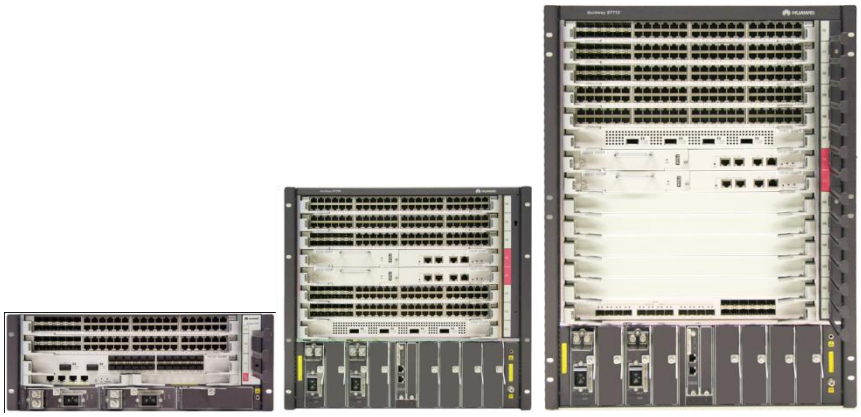
## 核心汇聚交换机 S9300

S9300 单槽位支持 12×10GE 线速转发，整机支持 2T 的交换能力。系统预留向更大交换容量升级的能力，满足未来 100GE 的需求。支持扩展到 5.12T 交换容量，48×10GE 高密度 10G 线卡，充分考虑未来 3～5 年的用户增长需求，提供带宽平滑扩展能力。

核心汇聚交换机选择说明：

- 每个S9303提供3个接口板，每个接口板可以提供12个10GE或者48个GE接口，接口可以达到线速转发；
- 每个S9306可提供6个接口板，每个接口板可以提供12个10GE或者48个GE接口，接口可以达到线速转发；
- 每个S9312可以提供12个接口板，每个接口板可以提供12个10GE或者48个GE接口；需要注意的是，当采用S9312提供10GE接口的时候，总流量只能达到840G的转发能力，即部分接口需工作在收敛的模式；

综上所述，因为核心/汇聚交换机的端口数量有限，需根据业务需求、网络出口、增值业务需求以及设备互联之间的端口需求，计算出各端口数量之后，选择对应的设备，同时也可以根据客户实际情况，配置多对汇聚交换机和一对核心交换机，采用分层交换的方式，完成网络互联。S7700 交换机如下图：



| 产品型号 | 说明 |
| --- | --- |
| S7703 | 支持3块LPU<br>交换网容量288Gbit/s<br>背板容量1.2Tbit/s<br>转发能力215Mpps |
| S7706 | 支持6块LPU<br>交换网容量1.536Tbit/s<br>背板容量2.4Tbit/s<br>转发能力432Mpps |
| S7712 | 支持12块LPU<br>交换网容量1.536Tbit/s<br>背板容量4.8Tbit/s<br>转发能力864Mpps |

S7700 系列产品有如下特点：

- 先进体系结构，高性能，配置灵活
- S7700系列交换机采用先进的全分布式体系结构设计，采用业界最新的硬件转发引擎技术，所有端口支持的业务能够线速转发，业务包括IPv4/MPLS/二层转发等。支持ACL线速转发。
- S7700系列交换机实现组播线速转发，硬件完成两级复制：交换网板复制到接口板和转发引擎复制到接口。
- S7700支持1.536Tbps交换容量，支持多种高密度板卡，满足核心、汇聚层设备大容量、高端口密度的要求，可以满足用户日益增长的带宽需求，能够极大的保护和节约用户投资。

- 完善的安全机制
- S7700系列交换机支持OSPF、RIP v2及BGP v4报文的明文及MD5密文认证，支持安全的SSH登录、命令行分级保护、基于用户安全策略的SNMP V3、DHCP Snooping、IP Source Guard、DAI、层次化CPU通道保护，并提供以下几种用户认证方式：本地认证、RADIUS和HWTACACS认证。

  支持防网络风暴攻击、防 DOS/DDOS 攻击、防扫描窥探攻击、防畸形报文攻击、防网络协议报文攻击等安全技术。

- 全面的可靠性

  S7700 系列交换机最大支持 128 个汇聚组，每个汇聚组内支持最多 8 个成员端口，支持跨单板端口间的汇聚。

  支持 DLDP，可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

  支持 RRPP 及多实例，相比其他以太环网技术，RRPP 具有以下优势：拓扑收敛速度快，低于 50ms。收敛时间与环网上节点数无关，可应用于网络直径较大的网络。

  支持标准 STP/RSTP/MSTP 二层环网保护协议。

  支持 SmartLink 及多实例。

  支持 BFD for 单播路由/VRRP/FRR/PIM。

### 7.1.6 桌面云瘦终端介绍

学员机房可选择 CT2000 TC 终端，技术规格如下：

| 项目 | CT2000产品指标 |
| --- | --- |
| 尺寸 | 37×130×156.4 |
| 功耗 | 6W |
| 处理器 | 海思3716C，ARM Cortex A9 1.0GHz |
| 内存 | Linux: 512M |
| 存储 | Linux:512M DOM卡 |
| 显示特性 | 本地最大支持24位颜色数显示，分辨率最高支持1920×1200 |
| 显示接口 | 1个DVI-I |
| USB端口数量 | 4个 |
| PS2 | 无 |
| 串口 | 无 |
| 并口 | 无 |
| 网口 | 千兆网口 |
| 音频IO端口 | 2 个音频端口（麦克风输入端口/音频输出端口） |

## 7.2 教育区域主要设备介绍

### 7.2.1 AR 系列

Quidway®AR12/22/32 系列路由器是华为公司为满足新一代企业分支、中小企业的 WAN 接入和运营商转售市场多业务承载需求而推出的新一代接入路由器产品。

AR12/22/32 系列路由器基于新一代高性能硬件和华为公司统一的 VRP 软件平台，支持丰富的广域网接口，提供高密度以太、语音等用户接入，支持 IPSec VPN 和防火墙等安全功能，可充分满足企业分支互联、中小企业广域接入和运营商转售等多种场合的需求。

Quidway®AR12/22/32 分为 AR12、AR22 和 AR33 三个系列产品。

| 产品型号 | 设备外观 | 备注 |
| --- | --- | --- |
| AR2220 |  | 整机容量：32Gbps<br>转发性能：1Mpps/500Mbps(64byte) |
| AR2240 |  | 整机容量：80Gbps<br>转发性能：2Mpps/1333Mbps(64byte) |
| AR3260 |  | 整机容量：160Gbps<br>转发性能：3.5Mpps（SRU80 高性能主控板）/2000Mbps(64byte) |

AR 系列产品的特点如下：

- 高性能

  华为 AR 产品采用最新的 ASIC 芯片和多核 CPU。LAN 模块内接口之间线速转发，LAN 模块之间具有高带宽 Fabric。CPU 采用 500MHz 两核到 750MHz12 核的 MIPS 处理器，25M 到 1G 的 WAN 转发性能，CPU 内置高性能加解密模块，具有 25M 到 300M 的加解密性能。

- 多业务集成

  华为 AR 产品除了提供对数据业务的支持外，还可以同时作为 IP PBX、IPSec VPN 网关和防火墙使用，AR12 还有支持 WLAN AP 的型号，真正做到数据、语音、视频、安全、无线等多业务的统一集成。

- 强大的 QoS

  华为 AR 产品支持 3 级 HQoS，其中 3260 通过 TM 硬件提供更强的转发性能。

- 高密度接入

  华为 AR 提供高密度的语音和数据接入，通过不同类型的插卡组合，可以充分满足各种场景下语音和数据的混合接入。

- 丰富的广域网接口

  华为 AR 提供丰富的广域网接口，包括 E1/T1、ISDN BRI、FR、3G 等各种主流接口，并支持作为 MPLS VPN 的 CE 和 PE 设备。