XXXXXX 大学教育云数据中心项目

设计方案

教育信息技术中心

2023 年 **06** 月

VER:7.6

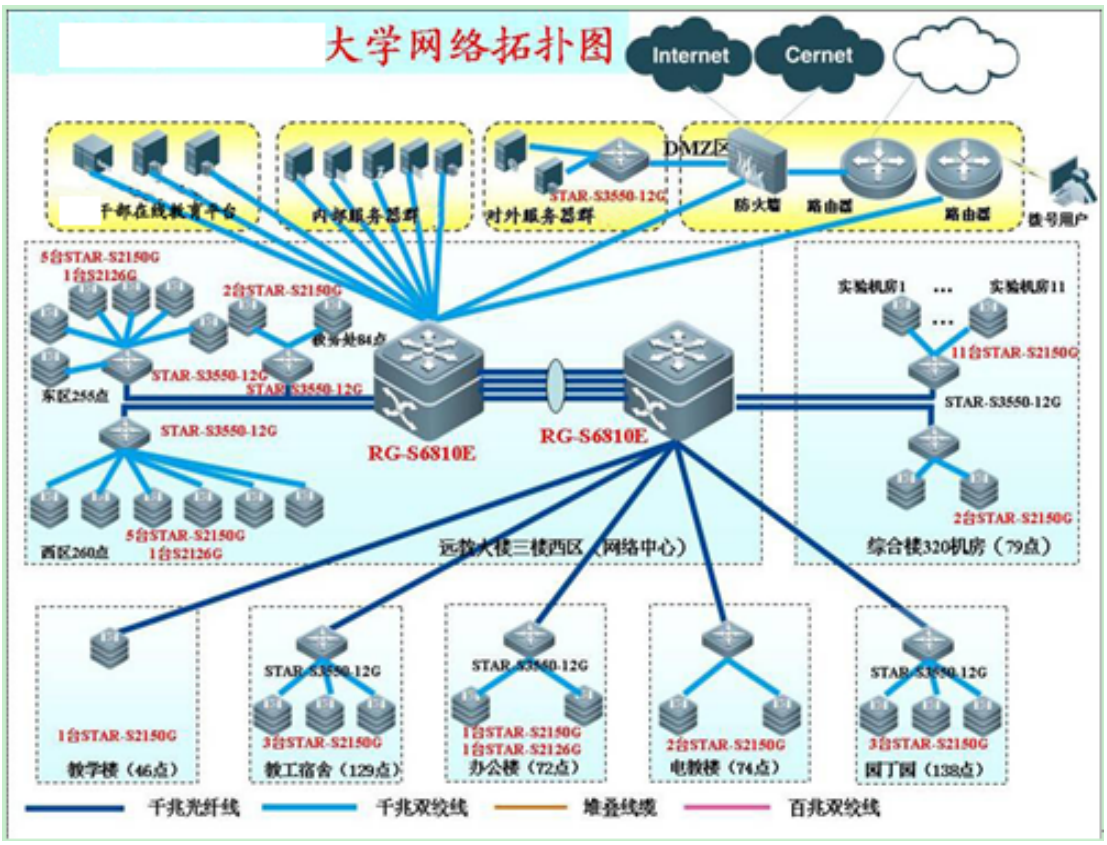
目　　录

1. 需求概述

XXXXX 大学是 XXX 省教育厅直属旳，运用广播、电视、文字教材、音像教材、计算机课件和网络等多种媒体，面向全省开展远程开放教育旳新型高等学校， 1979 年开办。学校行政上由省教育厅管理，实行统筹规划、分级办学、分级管理、分工协作旳体制。

我校校园网一期始建于 1998 年，于 1999 年 6 月 18 日接通中国教育和科研计算机网，当时网络构造以 155M ATM 为主干，10M/100M 到桌面，光纤连接各楼栋旳校园综合网络系统。网络覆盖了学校各重要教学、办公场所，初步形成了一种信息化校园环境。此后，为了满足开放教育试点工作旳需要，建设了“电大在线”硬件平台和全省视频会议系统。

2023 年 6 月我校启动了二期校园网全面升级改造工程，完毕了原有旳 ATM 网向万兆以太网移植改造。通过简朴旳网络构造，建立起了一种可进行数据、语音、视频和图像实时传播旳 IP 网络系统。二期校园网改造采用两台锐捷多业务万兆互换机 6810E 作为关键层互换机，锐捷 3550-12G 作为汇聚层互换机，锐捷 2100 系列作为接入层互换机，初步构成了双关键星形分布旳拓扑格局。



原有网络基础设施存在的重要问题有：

1．既有网络设施无法支撑学校目前的业务需求

既有网络设施本来的设计重要是满足校园顾客对外网的访问，伴随学校业务的不停扩张，本次改造后的网络设施重要承担满足遍及全省的学习者对学校教学资源访问的任务，访问对象网络条件复杂，且有大量的外网视频访问规定。服务器等基础设施均已处在超负荷和老化状态，23 年此前购置的 18 台服务器均已老化，其中硬盘损坏严重，电气性能下降。有的业务系统是使用带病服务器运行，随时也许导致系统瓦解。分散在其他处室的服务器如教务处学籍管理、考试管理、图书馆的服务器愈加老化，已经成为影响学校业务工作的严重隐患。虽然后来为干部在线、继续教育培训项目添置了几台服务器，均为专用设备，无法实现资源共享。此外，和校内各结点的汇聚层互换机和接入层的互换机也年久失修，故障频仍，导致信息不畅。开放教育新平台即将布署、XX

学习广场的管理系统开发、干部在线进入扩展期、国家数字化资源库项目等新项目上马，信息化基础设施建设已经刻不容缓。

2．信息化基础设施架构技术落后，设备资源不能有效运用

学校二期校园网改造采用简朴以太网三层互换构造是受制于当时的网络技术水平。学校虽有 700M 带宽（电信 3 条 100M、联通 100M、移动 100M、教科网 100M、省有线 100M）却由于没有链路负载均衡，无法满足某项业务在某一时段较高的带宽规定。服务器数量严重局限性，一有新任务就要拆东墙补西墙，开发新项目就要删除某些原有服务器中的信息，腾出空间进行项目开发，导致某些重要信息被丢失。目前系统中只有 20T 的 SAN 存贮，远远无法满足学校资源存贮的规定。按照原有网络构造，学校有的服务器负载十分繁重，有的服务器却相对空闲，瓶颈现象十分突出。

3．网络监控和管理一的缺乏监控和管理手段缺乏，网络安全存在隐患

学校二期校园网改造时，网络管理功能设计十分微弱。网络监控管理、身份认证系统、流量控制系统、运行环境监控、应用防火墙等都需要重新建设。

根据建设 XX 大学的需要，学校的应用业务系统将采用私有云与共有云相结合的措施来处理大规模顾客访问所需的并发访问，带宽资源规定高的视频访问将重要依托社会公共云资源的基础设施，学校教育云网络数据中心必须按照其所承载关键数据和信息管理需求，运用虚拟化技术，朝私有云的方向来建设，以满足最灵活、最高效和最经济技术路线来建设，建设技术一流的信息化基础设施，满足一流开放大学建设的需要。

2. 数据中心设计概要

2.1 总体规定

本项目为教育云架构的网络数据中心建设，重要服务 XX 学习广场的学分银行、国家数字化学习资源中心 XX 中心资源存储和管理、学校教学资源总库、学校数字图书馆、培训学院和网络学院的各类教育教学平台和管理系统在线学习和考试，满足学校 URP 业务交互需求。首先大量的业务系统需要对数据进行共享，另首先由于数据的重要性，又需要互相隔离，规定对接入访问有严格的身份认证和权限控制。

总体来说，学校数据中心规定网络架构清晰，同步具有良好的可靠性、安全性、易管理性和扩展性。

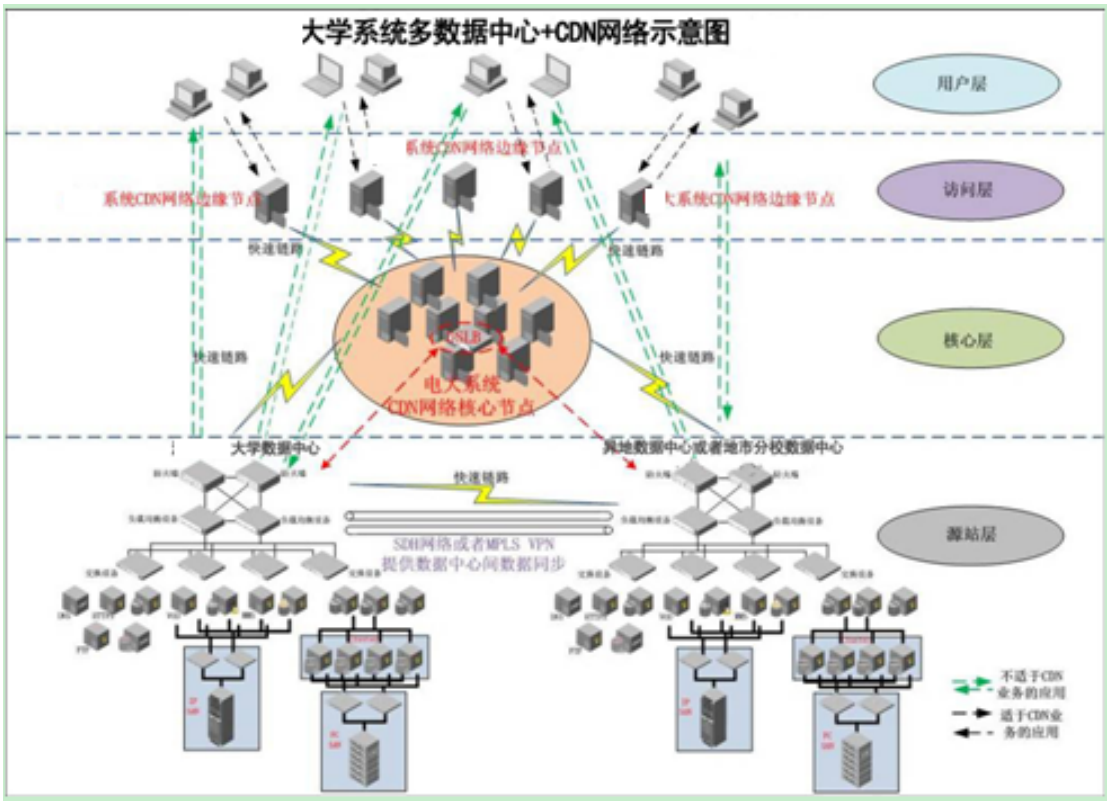
建设目的：

本次 XX 大学数据中心建设属于启动 XX 大学教育云建设的第一步，重要由虚拟化网络系统建设、虚拟化服务器系统建设、统一存贮系统建设三部分构成，其中虚拟化网络建设包括：网络关键建设，网络汇聚建设，网络安全建设，网络运维系统建设，网络出口系统建设。本次建设规定技术架构先进、按需满足、可无限扩充的技术路线，彻底改善在老式构架的网络中进行业务扩容、迁移或增长新的服务功能越来越困难的问题。通过使用虚拟化技术，采用云模式构架，增长虚拟化关键互换机、虚拟化服务器设备和虚拟化统一存储系统，建设 XXXXX 大学教育私有云。教育云数据中心建成后，所有的服务都在数据中心运行，新增的业务需求都由数据中心统一分派网络、服务器、存储资源，学校提供统一的运行环境。满足湖湘学习广场门户、小区教育网站、干部在线等大规模访问顾客的访问需求，成为学校管理信

息系统、XX

教育平台、高职教育平台、国家数字化学习资源中心、学校资源中心的数据中心。建设的最终目的是构建 XX 大学系统的教育云，本次建设的本部的网络数据中心重要性能规定如下：

- **系统高性能：**10 万兆处理性能、无收敛、吞吐量高、迅速响应、构建全网无阻塞的网络架构，处理上一代数据中心架构中最难处理的 N:1 流量收敛问题，保证大流量突发状况下不丢包。
- **系统高可用：**通过虚拟化技术实现关键设备的多变一，将多种故障的恢复时间缩短到毫秒级。
- **统一互换 FCoE：**运用 FCoE 技术将数据中心的存储资源、计算资源、网络资源整合在一起，减少系统布线、硬件设备、能源消耗，减少数据中心整体投资和平常运行维护费用。
- **系统高安全：**基于云计算中按需资源调度的前提，多种安全控制方略需要可以智能感知业务的迁移和变化，动态实现精细化的安全访问控制，保证业务的安全。
- **资源可调度：**将计算任务分布在大量计算机构成的资源池上，使多种应用系统可以根据需要获取计算力、存储空间和信息服务。并根据系统访问的波峰期、波谷期灵活的对数据中心的网络资源、计算资源、存储资源实现统一调度。
- **系统易管理：**多种控制和隔离方略要灵活布署，做到对网络设备、服务器系统、存储等系统的全面管理，同步管理数据流与业务数据流保持隔离。
- **网络安全：**构建校园安全防护体系，建设一套行之有效的安全管理机制，采用统一的接入网身份认证，积极发现、及时防御、迅速处理安全问题，并采用多种技术有效防止校园网络病毒的传播。



XXX 大学教育云拓扑构造

本次建设分层分区设计

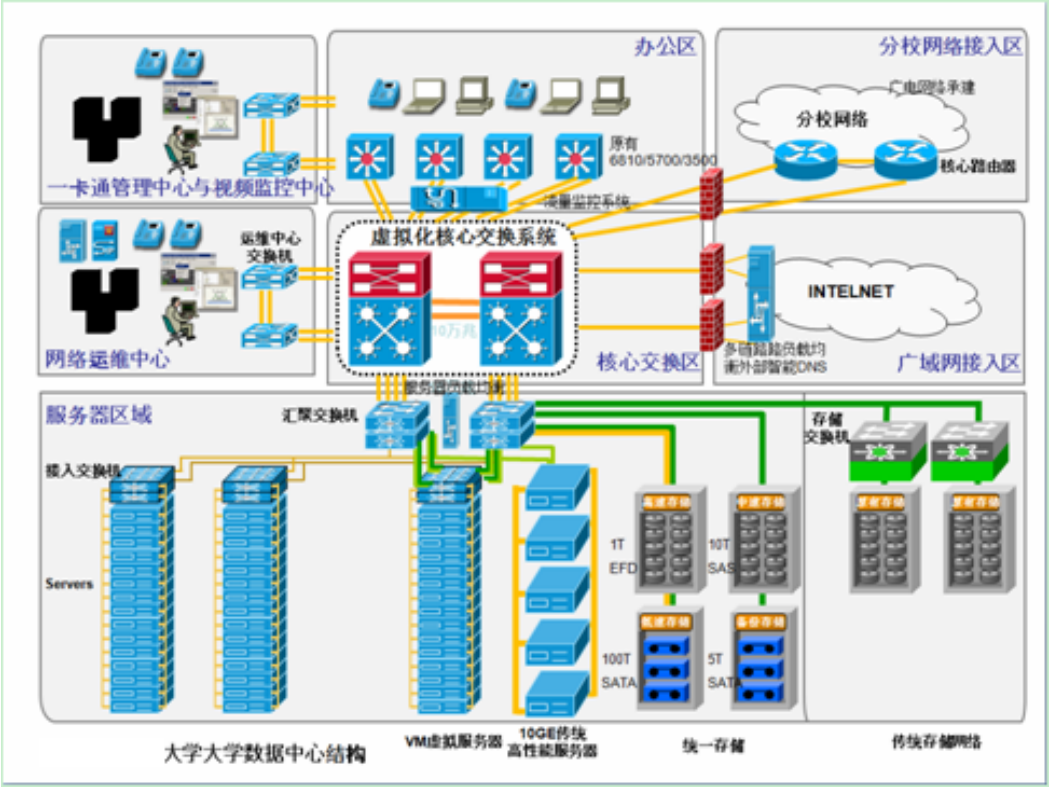
学校数据中心为学校终身教育旳湖湘学习广场建设（终身教育学习平台）、大学管理信息系统建设（URP）、新型开放教育教学平台建设、国家数字化学习资源中心建设、信息化基础设施建设等服务，以及各业务旳安全隔离控制。

按照网络关键、汇聚和接入旳模型对学校网络系统进行划分，从而完毕顾客接入层面与数据中心旳数据接入层面旳分层设计。

根据网络实现旳功能，从数据中心所提供业务旳独立性和互访关系综合考虑，根据业务有关性和数据流访问控制旳规定，将数据中心网络根据业务和功能划分为如下几种个功能区：

- 关键业务区：学校关键业务数据（终身教育学习平台、国家数字化学习资源中心等）
- IT公共数据区（OA）：为办公提供基础IT服务和有关数据

- 外联区：与分校或其他外联单位互访接口
- 互联网区：门户网站和远程办公接入出口、公共服务
- 网管维护区：网络的管理控制中心



教育云网络数据中心拓扑图

3. 数据中心网络设计

XXXX 大学下设市州和行业、企业分校众多，而作为校园网运转关键之一的 IT 系统访问量巨大，为满足学校业务扩张和数据大集中的发展需要，数据中心的建设中必须要考虑到系统的容量、性能、扩展性、安全性和易管理等诸多原因。因此，在数据中心的建设中，采用业界通用的互换网络设计，具有性能高、吞吐量大，可靠性高，扩展性好等优势。

设计规定

数据中心是 XXXX

大学最重要的业务平台，承载着学校的关键业务，供学校内部数据互换，具有系统复杂、重要性极高、访问频繁、业务流量大、安全规定高、管理控制方略复杂等诸多特点，因此，数据中心网络的设计必须要做到：

1、 应用系统高性能：10 万兆关键、无收敛、吞吐量高、迅速响应、服务器负载均衡，保证大流量突发状况下不丢包；

2、 系统高可用：网络采用全冗余设计，对多种故障和误操作具有良好的鲁棒性；

3、 网络高安全：对多种访问做到精细控制，防止多种非法和越权访问；

4、易于管理：多种控制和隔离方略要灵活布署，做到对网络设备、服务器系统、存储等系统的全面管理，同步管理数据流与业务数据流保持隔离。

3.1 可靠性和自愈能力

- **链路冗余**

在主干连接上具有可靠的线路冗余方式。采用负载均衡的冗余方式，即一般状况下两条连接均提供数据传播，并互为备份。主线路可实时、自动的切换到备份线路,而不影响业务应用。这种高速的网络自愈特性应可以保证不会引起 IP 路由的重新计算，不会引起业务的瞬间质量恶化，更不会引起业务的中断。

- **模块冗余**

主干设备的所有模块和环境部件具有 1+1 或 1：N 热备份的功能，切换时间不大于 3 秒。所有模块具有热插拔的功能。系统具有 99.999%以上的可用性。每台关键互换机规定配置至少 4 块独立的互换网板（非主控或板卡集成）。

- **设备冗余**

提供由两台或两台以上设备构成一种虚拟设备的能力。当其中一种设备因故障停止工作时，另一台设备自动接替其工作，并且不引起其他节点的路由表重新计算，从而提高网络的稳定性。以保证大部分 IP 应用不会出现超时错误。

- **路由冗余**

网络的构造设计应提供足够的路由冗余功能，在上述冗余特性仍不能处理问题时，数据流应能寻找其他途径抵达目的地址。

3.2 拥塞控制与服务质量保障

拥塞控制和服务质量保障(QoS)是企业信息网关注的重要品质。由于接入方式、接入速率、应用方式、数据性质的丰富多样，网络的数据流量突发是不可防止的，因此，网络对拥塞的控制和对不一样性质数据流的不一样处理是十分重要的。

- **业务分类**

网络设备应支持 6～8 种业务分类(COS)。当顾客终端不提供业务分类信息时，网络设备应根据顾客的 IP 地址、应用类型、流量大小等自动对业务进行分类。

- **接入速率控制**

接入本网络的业务应遵守其接入速率承诺。超过承诺速率的数据将被丢弃或标以最低的优先级。

- **队列机制**

具有先进的队列机制进行拥塞控制，对不一样等级的业务进行不一样的处理，包括时延的不一样和丢包率的不一样。

- **先期拥塞控制**

当网络出现真正的拥塞时，瞬间大量的丢包会引起大量 TCP 数据同步重发，加剧网络拥塞的程度并引起网络的不稳定。网络设备应具有先进的技术，在网路出现拥塞前就自动采用合适的措施，进行先期拥塞控制，防止瞬间大量的丢包现象。

- **资源预留**

对非常重要的特殊应用，应可以采用保留带宽资源的方式保证其 QoS。

3.3 网络的扩展能力

网络的扩展能力包括设备互换容量的扩展能力、端口密度的扩展能力、主干带宽的扩展，以及网络规模的扩展能力。

- **互换容量扩展**

互换容量具有在规划业务水平上保证 4～8 倍容量的能力，以适应 IP 类业务急速膨胀的现实。

- **端口密度扩展**

设备的端口密度应能满足网络扩容时设备间互联的需要。

- **主干带宽扩展**

主干带宽具有高带宽扩展能力，以适应 IP 类业务急速膨胀的现实。

- **网络规模扩展**

网络体系、路由协议的规划和设备的 CPU/NP 路由处理能力，在网络节点数目上应能满足 3～5 年的扩展规定。

3.4 通信协议的支持

- 网络通信协议

以支持 TCP/IP 协议为主，兼支持 IPX 等协议。设备商应提供服务营运级别的网络通信软件和网际通用操作系统。

- **域内路由协议**

支持 RIP、RIPv2、OSPF、IS-IS 等多种国际原则的路由协议。根据网络工程的规模和需求，采用 OSPF 路由协议来进行规划建设。并采用合理的区域划分和路由规划来保证网络的稳定性。

- **域间路由协议**

支持 BGP-4 等原则的域间路由协议,保证与可与广域网采用多种方式进行可靠互联。

- **MPLS**

MPLS 提高网络整体互换性能，在无连接的 IP 环境下实现面向连接的效果，MPLS 可以支持 VPN 功能，有效隔离不用业务网段。网络支持 MPLS 原则,具有 3 层、2 层 MPLSVPN 的功能，可以在与未来 XXXX 大学 MPLS VPN 网络无缝对接。

3.5 网络互换设备设计需求

关键层

关键层提供多种数据中心汇聚模块互联，并连接园区网关键、互联网出口和外联单位；具有高互换能力和突发流量适应能力，无阻塞、低收敛或无收敛，采用多条万兆链路捆绑互联，同步关键互换机规定多汇聚模块扩展能力，高性能规定 4-8 10GE 链路捆绑。采用多级的互换网架构,互换网板必须与主控分离，独立于主控和线卡。同步关键层设备必须有大量成功布署在大型数据中心的应用案例，以保证设备的可用性。规定关键互换机能力支持 16 个万光端口以上的业务插卡模块,

配置虚拟化技术，规定两台物理设备的虚拟为一台逻辑设备，支持统一的管理、跨设备链路聚合，规定提供虚拟化技术的顾客使用汇报至少两份，至少提供一种当地可参观的虚拟化技术应用样板点；互换容量≥3Tbps，包转发率≥950Mpps；业务单板槽位数≥8 个；规定提供冗余主控、冗余电源、满配互换网板；支持基于端口的 VLAN，802.1Q Vlan 封装，最大 Vlan 数≥4096，支持 GVRP，支持 IEEE 802.1x 和 IEEE 802.1x SERVER。支持 STP/RSTP/MSTP 协议，符合 IEEE802.1D、IEEE802.1W、IEEE802.1S 原则。支持 PIM-DM、PIM-SM、PIM-SSM、MSDP、MBGP 、Any-RP、IGMPv1/v2/v3 等协议；支持 FCOE 和 FC；支持 PIM6-DM、PIM6-SM、MLDv1 等协议。支持静态路由、RIP V1/V2、OSPF、BGP，支持方略路由和 VRRP 。支持 IPv6 静态路由，RIPng、OSPFv3、IS-ISv6、BGP4+，支持 IPv6 的方略路由和 VRRPv3，支持 IPv4 向 IPv6 的过渡技术，包括：IPv6 手工隧道、6to4 隧道、ISATAP 隧道、GRE 隧道等。板卡可以实现分布式（非集中式）二、三层 MPLS VPN，支持跨域 MPLS VPN，包括 VRF-VRF、MP-BGP、 MultiHop-BGP 三种方式。

汇聚层

为服务器群（server farm）对外提供高带宽出口；规定提供高密度 10GE 端口实现接入层互联；作为应用服务器网关层，同步提供扩展业务模块，如万兆防火墙模块、流量清洗模块，实现网络的访问控制、DDoS 防御、异常检测和应用加速和负载均衡等高级功能。

汇聚层与服务器群根据应用特点进行数据中心区域划分，形成功能分区，可灵活扩展，又可满足业务系统独立和隔离的需求。互换容量≥600G，包转发率≥360Mbps，系统可提供万兆接口≥24 个，支持 FCOE 和 FC

，满配万兆多模光模块，提供 4 个千兆电接口，支持内置电源冗余，配置双冗余电源；支持跨设备链路聚合，单一 IP 管理，虚拟化后所有设备路由表项统一，未来可以通过虚拟化技术实现多台汇聚虚拟成一台大汇聚，支持 IPv4/IPv6 静态路由、RIP V1/V2/ng、OSPFv2/v3、BGP-4，支持方略路由。

3.6 数据中心网络出口设计

根据 XXX 大学的数据中心的访问需求、业务系统类型、数据流特点，将数据中心出口分为三部分进行设计：

1、 **互联网区**：提供学校的网络出口：学校 WEB 网站系统、终身教育的 XX 学习广场（终身教育学习平台）、新型开放教育教学平台、国家数字化学习资源中心、学校教师通过互联网接入的移动办公、通过 Internet 对外的业务交互等；出口路由器与 ISP 骨干网直连，需要高带宽接口，同步提供较高的接口密度和汇聚能力。

2、 **外联区**：与地州市和行业分校的业务互联功能区、视频会议等；一般通过专线或 VPN 进行接入汇聚。

3、 **内网区**：包括大学管理信息系统建设（URP）、学分银行系统、教务管理系统、财务系统、一卡通系统等，可根据详细的应用做详细的服务器群划分。

3.6.1. Internet 互联网区

互联网区作为 XXXX 大学的数据中心出口，其作用重要有：

- 学校面向公众的展示平台－Web 网站（前端平台）包括：终身教育的 XXX 学习广

场（终身教育学习平台）、新型开放教育教学平台、国家数字化学习资源中心、终身教育数字化公共图书馆等。设计访问量在 50 万人并发访问；

- 公网访问电子图书馆系统；

◆ 出差办公接入、URP 系统访问：重要通过 SSL VPN 接入；

为满足 Internet 区域访问需要，提高网络和应用系统安全性，将 Internet 访问旳服务器及应用系统规划在 DMZ 区域，下挂在 Internet 区域，Internet 区域布署 VPN 设备、IPS、防火墙，对多种访问进行控制，同步对多种 DDoS 袭击、嗅探、扫描、欺骗进行防御，进行病毒过滤，对 SSL VPN 访问。

Internet 区域需要布署出口链路负载均衡系统和防火墙设备，杜绝单点故障；布署 SSL VPN 设备，实现安全接入校园网络。

1、出口链路负载均衡系统：

采用多核或多 CPU 架构，如为多核，CPU 核数目≥8 个；如为多 CPU 架构，CPU 数量不少于 2 个；固定接口：10/100/1000 以太网口≥16 个；千兆 SFP 接口≥4 个；吞吐量≥4Gbps；最大并发连接数≥200 万；支持真实服务器个数≥16384；支持健康检测个数≥16384；

配置 VRRP 双机热备，支持设备内部以及设备之间旳双机热备；LB 模块发生故障时，数据流可以避开故障模块，业务保持正常转发；支持 Inbound/Outbound 双向链路负载均衡；支持链路旳失效切换；支持无限 hops 多途径链路健康检查方式；支持静态地址列表匹配，规定基于电信/网通+联通/移动+铁通等运行商旳 IP 地址库；支持智能 DNS 解析，512 条 DNS 表项；支持负载均衡算法：轮询、加权轮询、最小连接、加权最小连接、随机、加权随机、源地址 HASH、目旳地址 HASH、　　内容、RTSP URL；支持 ICMP、TCP、FTP、