

金陵科技学院

课程设计报告



题 目 校园网的规划与组建

课 程 名 称 计算机网络课程设计

院 部 名 称 软件工程学院

专 业 软件工程

班 级 20 软件工程嵌入式培养 4 班

学 生 姓 名 夏书恒

学 号 2012011113

课程设计地点 科技楼 2 栋 409-2

课程设计学时 20 学时

指 导 教 师 胡夏芸

金陵科技学院教务处制

目 录

- 第 1 章 网络工程项目介绍
- 第 2 章 校园局域网相关技术
- 第 3 章 企业网络工程项目设计
 - 3.1 需求分析
 - 3.2 设计原则
 - 3.3 Vlan 与子网划分
 - 3.4 路由与安全设计
 - 3.5 应用服务器设计
- 第 4 章 网络拓扑结构设计
- 第 5 章 校园网络工程项目实现
 - 5.1 交换部分的实现过程
 - 5.2 路由部分的实现过程
 - 5.3 应用服务器部分的实现过程
- 第 6 章 设备配置相关代码
- 第 7 章 校园网络工程项目测试
- 第 8 章 项目总结与展望

摘要

随着信息技术的发展，计算机网络已成为现代教育的重要组成部分。在大学校园中，校园网络已经成为教育教学、科研工作、学生生活和管理服务的重要基础设施之一。因此，设计和建设高效、安全、稳定、可靠的校园网络，对于提高教学科研质量、提升学校的影响力和声誉，具有重要的意义。本文将从学校校园网的需求出发，设计一个适合学校使用的校园计算机网络。首先，我们要对学校的需求进行分析。学校的校园网需要支持大量的学生、教职工和管理人员同时上网，要求网络带宽大、延迟低、安全可靠。此外，校园网需要覆盖校内各个区域，包括教学楼、实验室、图书馆、宿舍等等。因此，我们需要设计一个具有高带宽、强安全性、高可靠性、完整覆盖的校园网络。

为了实现这个目标，我们需要采用一些网络工程项目的设计原则和方案。首先，我们需要考虑网络的拓扑结构，采用星型拓扑或树型拓扑都可以，但需要保证每个节点都能够得到充分的网络带宽。其次，我们需要考虑网络的安全性，采用 VPN 技术或防火墙技术等，对于教师和学生的信息进行保护。同时，我们还需要考虑网络的可靠性，采用冗余路由技术和备份设备技术等，保证网络在设备故障时也能正常运行。最后，我们还需要考虑网络的管理，采用网络管理系统等工具，对网络设备进行监控和管理，及时发现并解决网络故障。

在实现校园计算机网络的过程中，我们需要运用多种技术，如路由器、交换机、服务器等，同时我们需要进行网络配置、网络连接、网络管理等一系列工作。具体地说，我们需要在校内不同的区域内部署各种网络设备，建立起相互连接的网络，然后进行网络配置和管理，保证网络的运行和可靠性。

在项目完成后，我们需要进行测试和总结。首先，我们需要对校园网络的带宽、延迟、安全性和可靠性进行测试，以保证网络达到设计要求。其次，我们需要对网络设备进行管理和维护，包括定期升级设备软件、备份重要数据、监控网络状况等。最后，我们需要对项目进行总结，总结项目的收益和成本，评估项目的实施效果，提出改进建议，为未来的校园网络建设提供参考和借鉴。

关键词：校园网；网络规划；安全性；可靠性；

第 1 章网络工程项目介绍

校园网络工程项目是一项大型的信息化建设项目，其目的是建立一个高效、安全、可靠的校园计算机网络，为学生、教师和工作人员提供各种网络服务和资源。该项目包括网络规划、网络设计、设备选型、设备配置、网络测试等多个阶段，需要涉及多种技术和工作人员的合作。

在校园网络工程项目设计中，应该遵循以下原则：首先，需要根据学校的需求进行网络规划和设计，包括网络拓扑结构、网络设备选型、网络安全策略等方面；其次，需要进行网络设备的合理配置和布局，保证网络的高效、稳定和安全运行；最后，需要进行网络的测试和优化，确保网络能够满足学校的各种需求。

在实现校园网络工程项目的过程中，需要充分运用各种技术手段，如路由器、交换机、服务器、防火墙等，同时需要进行网络配置、网络连接、网络管理等一系列工作。具体而言，需要在校内不同的区域内部署各种网络设备，建立起相互连接的网络，然后进行网络配置和管理，保证网络的运行和可靠性。

在项目完成后，需要进行测试和总结。测试包括对网络的带宽、延迟、安全性和可靠性进行测试，以保证网络达到设计要求。同时，需要对网络设备进行管理和维护，包括定期升级设备软件、备份重要数据、监控网络状况等。最后，需要对项目进行总结，评估项目的实施效果，提出改进建议，为未来的校园网络建设提供参考和借鉴。

总之，校园网络工程项目是一项具有重要意义工程项目，需要充分考虑学校的需求，设计合理的网络结构和安全策略，合理选择网络设备和技术手段，并进行充分测试和优化。通过实施校园网络工程项目，可以为学生、教师和工作人员提供高效、稳定、安全的网络服务，为学校的信息化建设提供有力的支撑。

第 2 章 校园网局域网相关技术

相关技术：端口聚合 EtherChannel、动态路由 OSPF 协议、VLAN 与 TRUNK、VTP、NAT、DHCP、snooping STP

1. 端口聚合 EtherChannel

端口聚合是一种将多个物理接口组合成一个逻辑接口的技术。通过端口聚合可以提高网络的带宽和可靠性，同时还可以提高网络的可扩展性和灵活性。使用端口聚合技术，我们可以将多个物理接口绑定成一个逻辑接口，这个逻辑接口可以处理更多的数据流量，并且在其中任意一个物理接口出现故障时，其他物理接口可以顶替它的工作，保证网络的可靠性和稳定性。

2. 动态路由 OSPF 协议

OSPF 是一种开放式链路状态协议，可以用于在企业级网络中路由 IP 数据包。OSPF 可以根据不同的带宽、成本、网络拓扑等因素计算出网络中最短的路径，并能够实现快速收敛。与其他路由协议相比，OSPF 具有更快的收敛速度、更高的网络可靠性和更好的可扩展性，因此被广泛应用于企业网络中。

3. VLAN 与 TRUNK

VLAN 技术可以将一个物理网络分成多个逻辑网络，提高网络的隔离性和安全性。TRUNK 则是将多个 VLAN 通过一个物理链路传输的技术。VLAN 技术可以帮助网络管理员更好地管理网络，并且可以提高网络的隔离性和安全性。通过使用 TRUNK 技术，网络管理员可以通过一个物理链路实现多个 VLAN 的传输，提高网络的可扩展性和灵活性。

4. VTP

VLAN Trunking Protocol (VTP) 可以帮助网络管理员在一个网络中统一管理 VLAN，并实现 VLAN 的自动配置和传输。通过使用 VTP 技术，网络管理员可以将 VLAN 的配置信息在整个网络中进行传播，并且可以在任意一个交换机上进行 VLAN 的配置，提高网络的管理效率和可靠性。

5. NAT

Network Address Translation (NAT) 技术可以将私有网络中的 IP 地址转换成公共网络的 IP 地址，提高网络的安全性和隔离性。通过使用 NAT 技术，网络管理员可以隐藏私有网络的 IP 地址，提高网络的安全性和隔离性，同时可以避免 IP 地址冲突等问题。

6. DHCP snooping

Dynamic Host Configuration Protocol (DHCP) snooping 技术可以通过对 DHCP 消息的监控和验证，保证 DHCP 服务器分配的 IP 地址是合法的。DHCP snooping 技术可以帮助网络管理员提高网络的安全性和稳定性，防止恶意攻击和网络故障。

DHCP snooping 技术通过在交换机上开启 DHCP snooping 功能，对 DHCP 消息进行过滤和验证，只允许 DHCP 服务器向指定的端口分配 IP 地址。同时，DHCP snooping 技术可以记录 DHCP 消息，保留 MAC 地址、IP 地址和端口等信息，用于网络故障排查和追踪。

DHCP snooping 技术的工作原理是通过交换机上的 DHCP snooping 数据库，对 DHCP 消息进行验证。当 DHCP 客户端请求 IP 地址时，交换机会将该消息发送到 DHCP snooping 数据库进行验证。如果该 DHCP 请求是合法的，则交换机会向该端口转发 DHCP 消息，并将 MAC 地址、IP 地址和端口等信息保存到 DHCP snooping 数据库中。如果 DHCP 请求是非法的，则交换机会

将该消息过滤掉，并向管理员发送警报信息。

DHCP snooping 技术可以防止恶意攻击和网络故障。例如，如果一个攻击者在网络中发布 DHCP 服务器并分配虚假的 IP 地址，DHCP snooping 技术可以通过验证 DHCP 消息，防止攻击者成功分配虚假的 IP 地址。另外，如果一个 DHCP 客户端通过欺骗攻击发送虚假的 DHCP 消息，DHCP snooping 技术可以过滤掉非法的 DHCP 消息，保证网络的安全性和稳定性。

7. STP

STP (Spanning Tree Protocol) 是一种用于在交换机网络中防止环路的协议。当交换机之间存在多条连接时，会产生环路，这会导致网络出现广播风暴和数据包不断重复转发，最终导致网络崩溃。STP 就是为了解决这个问题而被设计出来的。

STP 的工作原理是通过选择一个交换机作为根交换机，然后在整个网络中选择最短路径到达根交换机的路径，其他路径都会被阻塞。当一条路径出现故障时，STP 会重新计算路径并选择一条新路径来替代故障的路径，从而保证网络的连通性和稳定性。

在 STP 中，每个交换机都有一个优先级，根据优先级来选择根交换机。当优先级相同时，MAC 地址较小的交换机会被选为根交换机。STP 还会将交换机之间的连接形成一个树形结构，其中根交换机位于树的顶部，其他交换机位于树的底部。STP 会将所有不必要的路径阻塞，只保留根交换机到每个交换机的最短路径。

STP 可以有效地防止网络中的环路，提高网络的稳定性和可靠性。但是，在大型网络中，STP 可能会导致网络的收敛速度变慢，从而影响网络的性能。因此，在设计网络时，需要综合考虑网络规模、带宽、拓扑结构等因素，选择合适的 STP 版本和参数配置，来满足网络的需求。

第 3 章 校园网络工程项目设计

3.1 需求分析

随着信息技术的不断发展，计算机网络已经成为现代教育的重要组成部分。作为一所现代化高等学府，大学需要一套高效、稳定、安全、可靠的校园计算机网络，为学校师生提供优质的网络服务和支持。本文将从校园网络的需求分析出发，详细介绍校园网络工程项目设计的需求分析。

一、业务需求

校园网络服务范围涵盖全校各个学院、部门和办公区域，网络服务类型包括网页浏览、在线视频、文件传输、邮件等常见服务。因此，校园网络需要满足以下业务需求：

高速宽带：为保证学生、教职工在校内能够流畅地进行在线学习、教学和工作，校园网络需要提供高速、稳定的宽带带宽。

安全保障：学校的网络安全是校园网络的重要组成部分。为保障网络的安全性，需要采取一系列的安全措施，如防火墙、流量控制、远程访问控制等。

带宽限制：为防止网络拥堵，需要对网络带宽进行限制和调节，确保网络资源合理分配和利用。

无线网络：为方便学生在校内移动学习和工作，校园网络需要提供高速、稳定的无线网络服务。

二、硬件需求

路由器：路由器是校园网络的核心设备，负责对网络数据进行路由和转发。为保证网络带宽和稳定性，需要选择性能高、稳定可靠的路由器设备。

交换机：交换机是校园网络的重要组成部分，负责在网络中传输数据和控制数据流。需要选择高性能、低延迟的交换机设备，以满足不同区域和用户的需求。

无线接入点：无线接入点是提供无线网络服务的重要设备。需要选择稳定性好、覆盖面积广的无线接入点，确保无线网络服务的可靠性和稳定性。

服务器：为保障校园网络的高效、稳定运行，需要采用高性能、高可靠性的服务器设备，支持多种服务和应用的部署，如文件共享、邮件服务、Web 服务器等。

三、软件需求

操作系统：需要选择稳定、安全、易管理的操作系统，如 Windows Server 和 Linux 等。

网络管理软件：需要选择专业、可靠的网络管理软件，如 Cisco Network Assistant、SolarWinds Network Performance Monitor 等，以对网络设备进行配置、监控和管理。

安全软件：需要采用可靠的防火墙软件、入侵检测系统等安全软件，以保障校园网络的安全。

应用软件：需要根据实际需求选择适当的应用软件，如文件共享软件、邮件服务软件、Web 服务器软件等，以满足用户的各种需求。

四、网络拓扑结构

根据校园网络的实际需求和规模，需要设计合理的网络拓扑结构。一般情况下，可以采用三层分布式网络结构，即核心层、汇聚层和接入层。其中，核心层主要承担数据中心和服务器之间的数据传输，需要选择高速路由器和交换机；汇聚层主要承担网络聚合和数据流控制，需要选择高性能、低延迟的交换机；接入层主要负责用户接入和数据传输，需要选择高性能、高可靠性的交换机和无线接入点。

五、服务质量要求

为保障校园网络的服务质量和用户体验，需要在设计和实施校园网络工程项目时，注重以下方面：

带宽：需要根据实际需求和用户数量，合理规划网络带宽，保证网络畅通和用户体验。

延迟：需要选择低延迟的网络设备和技术，尽可能降低数据传输的延迟，提高用户体验。

安全性：需要采用可靠的网络安全技术和软件，保障网络的安全性和数据的保密性。

可靠性：需要选择稳定、可靠的网络设备和技术，提高网络的可靠性和稳定性，减少网络故障和维护成本。

可扩展性：需要考虑未来校园网络的扩展和升级，选择具有良好可扩展性的网络设备和技术。

六、总体设计思路

根据以上需求分析，设计思路如下：

选择高性能、高可靠性的网络设备和技术，构建三层分布式网络结构，实现数据中心和用户接入的快速、稳定传输。

在数据中心层采用大型核心交换机，通过多路径（MPLS 或 VXLAN）构建虚拟网络，支持大规模服务器、存储设备和云计算等业务。

在汇聚层采用交换机进行汇聚，通过端口聚合（EtherChannel）技术，实现多个物理链路的汇聚，提高网络带宽和可靠性。同时，采用动态路由（OSPF）协议，实现多路径选择和快速收敛，提高网络的可用性。

在接入层采用交换机进行接入，通过 VLAN 与 TRUNK、VTP 等技术，实现不同用户和业务的隔离和优先级控制，保证网络的安全性和服务质量。同时，采用 NAT 技术，实现私网地址与公网地址的转换，支持 Internet 接入。

为了保证网络的安全性，需要采用 DHCP snooping 技术，防范恶意 DHCP 服务器和地址欺骗攻击，同时采用 STP 协议，防止网络环路产生，保证网络的稳定性和可靠性。

为了提高无线网络服务质量，需要在校园内部署多个无线接入点，并通过 WLAN 控制器进行集中管理，支持多种认证方式和安全机制，实现对用户接入的统一管理和控制。

七、实施方案

根据上述总体设计思路，具体实施方案如下：

数据中心网络：采用大型核心交换机进行汇聚，支持 MPLS 或 VXLAN 虚拟网络技术，实现多路径、高带宽、低延迟的数据中心网络。

汇聚层网络：采用高性能、低延迟的交换机设备，通过端口聚合（EtherChannel）技术，汇聚多个物理链路，提高网络带宽和可靠性。同时，采用动态路由（OSPF）协议，实现多路径选择和快速收敛，提高网络的可用性。

接入层网络：采用交换机进行接入，通过 VLAN 与 TRUNK、VTP 等技术，实现不同用户和业务的隔离和优先级控制，保证网络的安全性和服务质量。同时，采用 NAT 技术，实现私网地址与公网地址的转换，支持 Internet 接入。

安全性保障：采用 DHCP snooping 技术，防范恶意 DHCP 服务器和地址欺骗攻击，同时采用 STP 协议，防止网络环路产生，保证网络的稳定性和可靠性

3.2 设计原则

大学校园网络是支撑学校教学、科研和管理的重要基础设施，设计校园网络需要考虑到网络的可靠性、可扩展性、安全性、易管理性等多个方面。以下是本项目网络设计原则：

1. 分层设计：大学校园网络通常采用三层分布式网络结构，即核心层、汇聚层和接入层。核心层主要负责数据中心和汇聚层之间的高速数据传输，汇聚层负责连接核心层和接入层，而接入层则为用户提供网络接入。

2. 冗余设计：为了提高校园网络的可靠性和稳定性，需要采用冗余设计。例如，采用双机热备、双路冗余电源等技术，确保网络设备的故障不会影响网络的正常运行。

3. 安全设计：大学校园网络需要保护敏感信息和数据的安全性，采用各种安全技术和措施，例如网络防火墙、入侵检测系统、虚拟专用网络（VPN）等。

4. 可扩展设计：大学校园网络需要具备可扩展性，考虑未来的网络扩展和升级，需要选择具有良好可扩展性的网络设备和技术，例如虚拟化技术、软件定义网络（SDN）等。

5. 易管理设计：大学校园网络需要易于管理和维护，采用网络管理系统、自动化配置和运维、网络监控等技术，提高网络管理和运维的效率。

6. 多层次设计：大学校园网络需要考虑到不同用户的需求和安全等级，采用多层次设计，例如内部网络、教学网络、科研网络等，提供不同级别的网络接入和服务。

7. 性能设计：大学校园网络需要具备高性能和低延迟的特点，以满足学校的教学、科研和管理需求。需要选择高性能、低延迟的网络设备和技术，例如高速交换机、光纤网络等。

总之，大学校园网络设计需要考虑到多个方面的因素，以满足学校的需求和提高网络的可靠性、安全性和可扩展性。

3.3 Vlan 与子网划分

在大学校园网络设计中，VLAN 和子网划分都是非常重要的概念，它们可以帮助网络管理员更好地管理和优化网络。VLAN 和子网划分如下所示：

VLAN 1：默认 VLAN，不做任何设备或用户的归属。IP 地址范围：192.13.1.1/24。

VLAN 2：数据中心 VLAN，用于连接服务器和存储设备。IP 地址范围：192.13.2.1/24。

VLAN 10：办公区域 VLAN，用于连接校园工作人员的设备。IP 地址范围：192.13.10.1/24。

VLAN 11：教学区域 VLAN，用于连接教师和学生的设备。IP 地址范围：192.13.11.1/24。

VLAN 12：实验室 VLAN，用于连接实验室设备和学生设备。IP 地址范围：192.13.12.1/24。

VLAN 13：宿舍区域 VLAN，用于连接学生宿舍的设备。IP 地址范围：192.13.13.1/24。

VLAN 100：管理 VLAN，用于网络设备管理。IP 地址范围：192.13.100.1/24。

将交换机 S2960A、S2960B、S3560 配置为以下形式：

S2960A:

F0/1: 属于 VLAN 10, 连接到办公区域设备, 端口模式为 access。

F0/2-5: 属于 VLAN 10, 连接到办公区域设备, 端口模式为 access。

F0/6: 属于 VLAN 11, 连接到教学区域设备, 端口模式为 access。

F0/7-10: 属于 VLAN 11, 连接到教学区域设备, 端口模式为 access。

F0/11-15: 属于 VLAN 12, 连接到实验室设备, 端口模式为 access。

F0/16-22: 属于 VLAN 1, 未使用, 端口模式为 access。

F0/23-24: 不属于任何 VLAN, 连接到上级设备, 端口模式为 trunk。

S2960B:

F0/1、F0/3-5: 属于 VLAN 10, 连接到办公区域设备, 端口模式为 access。

F0/2: 属于 VLAN 10, 连接到办公区域设备, 端口模式为 access。

F0/6-10: 属于 VLAN 11, 连接到教学区域设备, 端口模式为 access。

F0/11: 属于 VLAN 12, 连接到实验室设备, 端口模式为 access。

F0/12-15: 属于 VLAN 12, 连接到实验

室设备, 端口模式为 access。

F0/16-22: 属于 VLAN 1, 连接到其他设备, 端口模式为 access。

F0/23-24: 属于 VLAN Trunk, 连接到其他交换机, 端口模式为 Trunk。

S3560:

F0/1-3: 未指定 VLAN, 可能为未使用端口。

F0/10-12: 属于 VLAN 100, 连接到服务器设备, 端口模式为 access。

F0/24: 属于 VLAN 2, 连接到其他交换机, 端口模式为 access。

Vlan1: 连接到路由器 R1, IP 地址为 192.13.1.2/24。

Vlan2: 连接到其他交换机, IP 地址为 192.13.2.2/24。

Vlan10: 连接到 S2960A 和 S2960B, IP 地址为 192.13.10.1。

Vlan11: 连接到 S2960B, IP 地址为 192.13.11.1。

Vlan12: 连接到 S2960B, IP 地址为 192.13.12.1。

Vlan100: 连接到服务器设备, IP 地址为 192.13.100.1。

R1:

F0/0: 连接到 S3560 的 Vlan1, IP 地址为 192.13.1.2/24。

S2/0: 连接到 R2 的 S2/0, IP 地址为 200.13.1.1/24。

R2:

F0/0: 连接到 S3560 的 Vlan10, IP 地址为 100.13.29.1/24。

S2/0: 连接到 R1 的 S2/0, IP 地址为 200.13.1.2/24。

以下为设计表:

S2960A

Port	Link	Vlan
F0/1	Up	10
F0/2-5	Down	10
F0/6	Up	11
F0/7-1	Down	11
F0/11-15	Down	12
F0/16-22	Down	1
F0/23-24	Up	--

S2960B

Port	Link	Vlan
F0/1、F0/3-5	Down	10
F0/2	Up	10
F0/6-10	Down	11
F0/11	Up	12

F0/12-15	Down	12
F0/16-22	Down	1
F0/23-24	Up	--

S3560

Port	Vlan	IP Address
F0/1-3	--	Net set
F0/10-12	100	Net set
F0/24	2	Net set
Vlan1	1	192.13.1.2/24
Vlan2	2	192.13.2.2/24
Vlan10	10	192.13.10.1
Vlan11	11	192.13.11.1
Vlan12	12	192.13.12.1
Vlan13	13	192.13.13.1
Vlan100	100	192.13.100.1

R1

Port	Link	IP Address
F0/0	Up	192.13.1.2/24
S2/0	Up	200.13.1.1/24

R2

Port	Link	IP Address
F0/0	Up	100.13.29.1/24
S2/0	Up	200.13.1.2/24

3.4 路由与安全设计

校园网络的路由与安全设计是保证校园网络高效稳定运行的关键。下面提供一个基于三层分布式网络的大学校园网络路由与安全设计方案：

一、网络架构设计

校园网络采用三层分布式网络架构，分为核心层、汇聚层和接入层。核心层主要承担数据交换和路由功能，汇聚层主要承担多种不同类型网络的汇聚和管理功能，接入层主要提供对终端设

备的接入和管理功能。核心层和汇聚层之间采用动态路由协议进行路由选择，汇聚层和接入层之间采用静态路由协议进行路由选择。

二、路由协议设计

校园网络采用 OSPF 作为核心层和汇聚层之间的路由协议，RIP 作为汇聚层和接入层之间的路由协议。OSPF 具有快速收敛、可扩展性好等特点，适合大型网络；RIP 具有简单易用、配置方便等特点，适合小型网络。同时，在实际应用中，也可以根据实际需要选择其他路由协议。

三、网络安全设计

防火墙安全设计

校园网络需要建立防火墙保护网络安全，防止网络攻击和未经授权的访问。可以将防火墙设置在核心层和汇聚层之间，对进出网络的数据进行检查过滤。防火墙可以根据需要对不同用户、不同网络进行访问控制和数据过滤，实现网络的安全管理。

VLAN 安全设计

VLAN 是校园网络中常用的安全隔离手段，可以将不同用户、不同网络划分为不同的 VLAN，实现彼此之间的安全隔离和控制。校园网络中可以将教学区、办公区、实验区等划分为不同的 VLAN，设置 VLAN 间访问控制列表，控制不同 VLAN 之间的通信。此外，也可以对不同 VLAN 的用户进行身份认证，实现网络安全管理。

VPN 安全设计

虚拟专用网络（VPN）可以为校园网络提供安全的远程访问服务，可以在公共网络上建立安全的私有网络，实现加密数据传输和身份认证等功能。校园网络中可以建立 VPN 服务器，为校内用户提供安全的远程访问服务，同时也可以控制访问权限，保证网络安全。

3.5 应用服务器设计

校园网应用服务器是支持校园网各种应用的核心设备之一，主要包括校园网门户网站、网络学习平台、图书馆管理系统、教务管理系统、学生信息管理系统、邮件服务器等。根据应用的不同需求，应用服务器的设计方案也会有所差异。下面是一些可能的设计方案：

校园网门户网站服务器设计方案

校园网门户网站是整个校园网的核心，是学生、教职工获取各种信息的主要途径，如学校公告、课表、成绩、校园新闻等。为确保校园网门户网站的稳定性和可靠性，需要采用高可靠性的服务器设备，支持负载均衡和容错处理技术，同时需要进行数据备份和恢复策略的设计。

网络学习平台服务器设计方案

网络学习平台是支持教师和学生进行在线学习和教学的核心设备，需要具备高并发性、高可靠性和高安全性。为保障网络学习平台的高效、稳定运行，需要采用高性能、高可靠性的服务器设备，支持负载均衡和容错处理技术，同时需要进行数据备份和恢复策略的设计，以及安全认证和访问控制等安全机制的实施。

图书馆管理系统服务器设计方案

图书馆管理系统是支持学生、教职工查询和借阅图书的核心设备，需要具备高并发性、高可靠性和高安全性。为保障图书馆管理系统的高效、稳定运行，需要采用高性能、高可靠性的服务器设备，支持负载均衡和容错处理技术，同时需要进行数据备份和恢复策略的设计，以及安全认证和访问控制等安全机制的实施。

教务管理系统服务器设计方案

教务管理系统是支持学校教务管理的核心设备，需要具备高并发性、高可靠性和高安全性。为保障教务管理系统的高效、稳定运行，需要采用高性能、高可靠性的服务器设备，支持负载均衡和容错处理技术，同时需要进行数据备份和恢复策略的设计，以及安全认证和访问控制等安全机制的实施。

学生信息管理系统服务器设计方案

学生信息管理系统是支持学生信息管理的核心设备，需要具备高并发性、高可靠性和高安全性。为保障学生信息管理系统的高效、稳定运行，需要采用高性能、高可靠性的服务器设备，支持负载均衡和容错处理技术，同时需要进行数据备份和恢复策略的设计，以及安全认证和访问控制等安全机制的实施。

具体的设计方案包括：

服务器硬件选择：选择高性能、高可靠性的服务器设备，例如品牌服务器，同时根据应用场景选择不同的服务器配置，如 CPU、内存、硬盘、网络接口等。

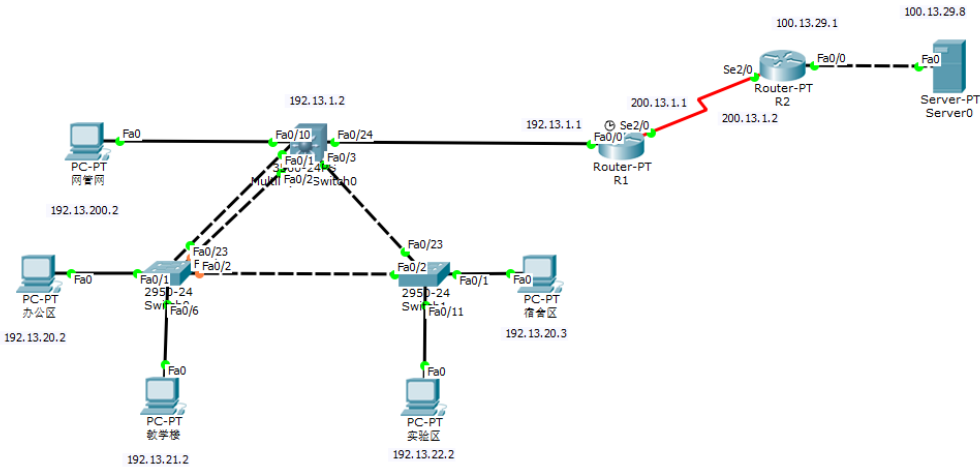
负载均衡技术的应用：通过负载均衡技术，将请求均衡地分配到多台服务器上，提高系统的可用性和并发性，避免单点故障导致的系统宕机。

容错处理技术的应用：通过容错处理技术，如冗余服务器、热备份、故障转移等方式，保障系统的高可用性，一旦服务器出现故障，立即切换到备份服务器，确保系统能够持续稳定地运行。

数据备份和恢复策略的设计：定期进行数据备份，保障数据的安全性和完整性，同时制定合理的数据恢复策略，确保数据能够快速、有效地恢复。

安全认证和访问控制等安全机制的实施：实施严格的安全认证机制，如密码策略、多因素认证、SSL/TLS 加密传输等，限制非授权访问。同时采用访问控制技术，对访问进行限制和审计，确保系统的安全性和完整性。

第 4 章 网络拓扑结构设计



上图即为该实验模拟该学校网络拓扑结构。在该学校网络接入层采用 S2960, 接入层交换机划分了办公网 VLAN 10、教师网 VLAN 11、学生网 VLAN 12 和网管网 VLAN 100。VLAN10 和、VLAN11 和 VLAN12 通过汇聚层交换机 S3650 与路由器 R1 相连,此外,在 S3560 上有一个 VLAN100 存放一台网管计算机。路由器 R1 与 R2 通过动态路由协议互联互通, 局域网内的主机均可以访问 R2 路

由器后的服务器 Server0。为了控制学生网内的主机访问重要的 Web Server，R1 路由器采用了访问控制列表技术作为控制手段。

第 5 章 校园网络工程项目实现

5.1 交换部分的实现过程

将 S2950A 上的 F0/1-5 加入 VLAN10； 将
S2950A 上的 F0/6-10 加入 VLAN11； 将
S2950B 上的 F0/11-15 加入 VLAN12； 将
S2950B 上的 F0/16-20 加入 VLAN13； 将
S3560 上的 F0/10-12 加入 VLAN100；
将 S3560 的 F0/1-2 和 S2960A 的 F0/23-24 相连接； 将
S3650 的 F0/3 和 S2960B 的 F0/24 相连接；
将 S2950A 上的 F0/21 和 S2950B 上的 F0/21 相连接。

5.2 路由部分的实现过程

设置 S2960A 的 VLAN 1 地址为 192.13.1.3；
S2960B 的 VLAN 1 地址为 192.10.1.4；
S3650 的 VLAN1 地址为 192.10.1.2；
S3560 通过 SV1 方式和 R1 互连。R1 和 R2 在全网运用 OSPF 动态路由协议，实现全网互通。

5.3 应用服务器部分的实现过程

通过访问列表控制所有人可以正常访问服务器，只有 VLAN 13 不可以访问 Server0 的 Web 和 FTP 服务，但可以 ping 通 Server0。

第 6 章 设备配置相关代码

相关设备的配置文件

(1) S3560 的配置文件

Building configuration...

Current configuration : 1839 bytes

!

version 12.2

no service timestamps log datetime msec no

service timestamps debug datetime msec no

service password-encryption

!

hostname S3560

!

!

!

enable secret 5 \$1\$mERr\$H7PDxl7VYMqaD3id4jVK/

!

!

!

!

!

!

!

!

!

!

```
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode rapid-pvst  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/1 switchport  
trunk encapsulation dot1q switchport mode  
trunk  
!  
interface FastEthernet0/2 switchport  
trunk encapsulation dot1q switchport mode  
trunk  
!  
interface FastEthernet0/3 switchport  
trunk encapsulation dot1q switchport mode  
trunk  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6
```

```
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
switchport access vlan 100  
!  
interface FastEthernet0/11  
switchport access vlan 100  
!  
interface FastEthernet0/12  
switchport access vlan 100  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20
```

```
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24 no  
switchport  
ip address 193.13.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.13.1.2 255.255.255.0  
!  
interface Vlan10  
ip address 192.13.10.1      255.255.255.0  
!  
  
interface Vlan11  
ip address 192.13.11.1      255.255.255.0  
!  
  
interface Vlan12  
ip address 192.13.12.1      255.255.255.0  
!  
  
interface Vlan13  
ip address 192.13.13.1      255.255.255.0
```

```
!  
interface Vlan100  
ip address 192.13.100.1 255.255.255.0  
!  
ip classless  
!  
ip flow-export version 9  
!  
!  
!  
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
password 123456  
login  
!  
!  
!  
end
```

S3560#conf t

Enter configuration commands, one per line. End with CNTL/Z.

S3560(config)#ip routing

S3560(config)#router ospf 1

```
S3560(config-router)#net      192.13.10.0    0.0.0.255  area 0
S3560(config-router)#net      192.13.11.0    0.0.0.255  area 0
S3560(config-router)#net      192.13.12.0    0.0.0.255  area 0
S3560(config-router)#net      192.13.13.0    0.0.0.255  area 0

S3560(config-router)#net 192.13.100.0 0.0.0.255 area 0
S3560(config-router)#net 192.13.1.0 0.0.0.255 area 0
S3560(config-router)#net 193.13.1.0 0.0.0.255 area 0
S3560(config-router)#
01:31:32: %OSPF-5-ADJCHG: Process 1, Nbr 200.13.1.1 on FastEthernet0/24 from LOADING to FULL,
Loading Done
```

S3560 con0 is now available

Press RETURN to get started.

S3560>

S3560>en

Password:

S3560#sh run

Building configuration...

Current configuration : 2156 bytes

!

version 12.2

no service timestamps log datetime msec no

service timestamps debug datetime msec no

service password-encryption

!

hostname S3560

!

!

!

enable secret 5 \$1\$mERr\$H7PDxI7VYMqaD3id4jJVK/

!

!

!

!

!


```
ip routing
!
!
!
!
!
!
!
!
!
!
!
!
!
spanning-tree mode rapid-pvst
!
!
!
!
!
!
interface FastEthernet0/1 switchport
trunk encapsulation dot1q switchport mode
trunk
!
interface FastEthernet0/2 switchport
trunk encapsulation dot1q switchport mode
trunk
!
interface FastEthernet0/3
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
!
```

```
interface FastEthernet0/4
```

```
!
```

```
interface FastEthernet0/5
```

```
!
```

```
interface FastEthernet0/6
```

```
!
```

```
interface FastEthernet0/7
```

```
!
```

```
interface FastEthernet0/8
```

```
!
```

```
interface FastEthernet0/9
```

```
!
```

```
interface FastEthernet0/10
```

```
switchport access vlan 100
```

```
!
```

```
interface FastEthernet0/11
```

```
switchport access vlan 100
```

```
!
```

```
interface FastEthernet0/12
```

```
switchport access vlan 100
```

```
!
```

```
interface FastEthernet0/13
```

```
!
```

```
interface FastEthernet0/14
```

```
!
```

```
interface FastEthernet0/15
```

```
!
```

```
interface FastEthernet0/16
```

```
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24 no  
switchport  
ip address 193.13.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.13.1.2 255.255.255.0  
!  
interface Vlan10  
ip address 192.13.10.1 255.255.255.0  
!
```

```
interface Vlan11
ip address 192.13.11.1      255.255.255.0
!
interface Vlan12
ip address 192.13.12.1      255.255.255.0
!
interface Vlan13
ip address 192.13.13.1      255.255.255.0
!
interface Vlan100
ip address 192.13.100.1 255.255.255.0
!
router ospf 1
log-adjacency-changes
network 192.13.10.0 0.0.0.255 area 0
network 192.13.11.0 0.0.0.255 area 0
network 192.13.12.0 0.0.0.255 area 0
network 192.13.13.0 0.0.0.255 area 0
network 192.13.100.0 0.0.0.255 area 0
network 192.13.1.0 0.0.0.255 area 0
network 193.13.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
```

```
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
password 123456  
login  
  
!  
!  
!  
  
end
```

S2960A 配置文件

Building configuration...

Current configuration : 1400 bytes

```
!  
version 12.1  
no service timestamps log datetime msec no  
service timestamps debug datetime msec no  
service password-encryption  
  
!  
hostname S2950A  
!  
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jVK/  
!  
!  
!  
spanning-tree mode rapid-pvst  
!
```

```
interface FastEthernet0/1
switchport access vlan 10
!
interface FastEthernet0/2
switchport access vlan 10
!
interface FastEthernet0/3
switchport access vlan 10
!
interface FastEthernet0/4
switchport access vlan 10
!
interface FastEthernet0/5
switchport access vlan 10
!
interface FastEthernet0/6
switchport access vlan 11
!
interface FastEthernet0/7
switchport access vlan 11
!
interface FastEthernet0/8
switchport access vlan 11
!
interface FastEthernet0/9
switchport access vlan 11
!
interface FastEthernet0/10
switchport access vlan 11
!
interface FastEthernet0/11
```

```
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
switchport mode trunk  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
switchport mode trunk  
!  
interface FastEthernet0/24  
switchport mode trunk  
!  
interface Vlan1
```

```
ip address 192.13.1.3 255.255.255.0
```

```
!
```

```
!
```

```
!
```

```
!
```

```
line con 0
```

```
!
```

```
line vty 0 4
```

```
password 123456
```

```
login
```

```
line vty 5 15 login
```

```
!
```

```
!
```

```
end
```

```
S2950A#
```

```
S2950A con0 is now available
```


Press RETURN to get started.

S2950A>

S2950A>en

S2950A>en

Password:

S2950A#sh run

Building configuration...

Current configuration : 1400 bytes

!

version 12.1

no service timestamps log datetime msec no

service timestamps debug datetime msec no

service password-encryption

!

hostname S2950A

```
!  
enable secret 5 $1$mERr$H7PDxI7VYMqaD3id4jJVK/  
!  
!  
!  
spanning-tree mode rapid-pvst  
!  
interface FastEthernet0/1  
switchport access vlan 10  
!  
interface FastEthernet0/2  
switchport access vlan 10  
!  
interface FastEthernet0/3  
switchport access vlan 10  
!  
interface FastEthernet0/4  
switchport access vlan 10  
!  
interface FastEthernet0/5  
switchport access vlan 10  
!  
interface FastEthernet0/6  
switchport access vlan 11  
!  
interface FastEthernet0/7  
switchport access vlan 11  
!  
interface FastEthernet0/8  
switchport access vlan 11  
!
```

```
interface FastEthernet0/9
switchport access vlan 11
!
interface FastEthernet0/10
switchport access vlan 11
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
switchport mode trunk
!
interface FastEthernet0/22
!
```

```
interface FastEthernet0/23
switchport mode trunk

!
interface FastEthernet0/24
switchport mode trunk

!
interface Vlan1
ip address 192.13.1.3 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
password 123456
login
line vty 5 15
login
!
!
end
```

S2960B 配置文件

Building configuration...

Current configuration : 1427 bytes

!

version 12.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

```
no service password-encryption
!  
hostname S2950B  
!  
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jVK/  
!  
!  
!  
spanning-tree mode rapid-pvst  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
switchport mode trunk  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
switchport access vlan 12
```

```
!  
interface FastEthernet0/11  
switchport access vlan 12  
!  
interface FastEthernet0/12  
switchport access vlan 12  
!  
interface FastEthernet0/13  
switchport access vlan 12  
!  
interface FastEthernet0/14  
switchport access vlan 12  
!  
interface FastEthernet0/15  
switchport access vlan 12  
!  
interface FastEthernet0/16  
switchport access vlan 13  
!  
interface FastEthernet0/17  
switchport access vlan 13  
!  
interface FastEthernet0/18  
switchport access vlan 13  
!  
interface FastEthernet0/19  
switchport access vlan 13  
!  
interface FastEthernet0/20  
switchport access vlan 13  
!
```

```
interface FastEthernet0/21
switchport mode trunk
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
switchport mode trunk
!
interface Vlan1
ip address 192.13.1.4 255.255.255.0
!
!
!
!
line con 0
!
line vty 0 4
password 123456
login
line vty 5 15
login
!
!
end
```

R1 配置文件

Building configuration...

Current configuration : 1100 bytes

```
!  
version 12.2  
no service timestamps log datetime msec no  
service timestamps debug datetime msec no  
service password-encryption  
  
!  
hostname R1  
!  
!  
!  
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jJVK/  
!  
!  
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!
```



```
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 193.13.1.2 255.255.255.0  
ip access-group 100 in ip  
access-group 100 out  
duplex auto  
  
speed auto  
!  
interface FastEthernet1/0 no  
ip address  
duplex auto  
speed auto  
shutdown  
  
!  
interface Serial2/0  
ip address 200.13.1.1 255.255.255.0  
clock rate 4000000  
!  
interface Serial3/0 no  
ip address shutdown  
  
!  
interface FastEthernet4/0 no  
ip address  
  
shutdown  
!
```

```
interface FastEthernet5/0 no
ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 193.13.1.0 0.0.0.255 area 0
network 200.13.1.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit tcp 192.13.13.0 0.0.0.255 host 100.13.29.2 eq www
access-list 100 permit tcp 192.13.13.0 0.0.0.255 host 100.13.29.2 eq ftp
access-list 100 deny tcp 192.13.0.0 0.0.255.255 host 100.13.29.2 eq www
access-list 100 deny tcp 192.13.0.0 0.0.255.255 host 100.13.29.2 eq ftp

!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
password 123456
login
```

```
!  
!  
!  
end
```

R2 配置文件

Building configuration...

Current configuration : 885 bytes

```
!  
version 12.2  
no service timestamps log datetime msec no  
service timestamps debug datetime msec no  
service password-encryption  
!  
hostname R2  
!  
!  
!  
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jVK/  
!  
!  
!  
!  
!  
!  
ip cef  
no ipv6 cef  
!  
!  
!
```

```
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 100.13.29.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface FastEthernet1/0 no  
ip address  
duplex auto  
speed auto  
shutdown  
!  
interface Serial2/0  
ip address 200.13.1.2 255.255.255.0  
!  
interface Serial3/0 no  
ip address
```

```
shutdown
!
interface FastEthernet4/0 no
ip address
shutdown
!
interface FastEthernet5/0 no
ip address

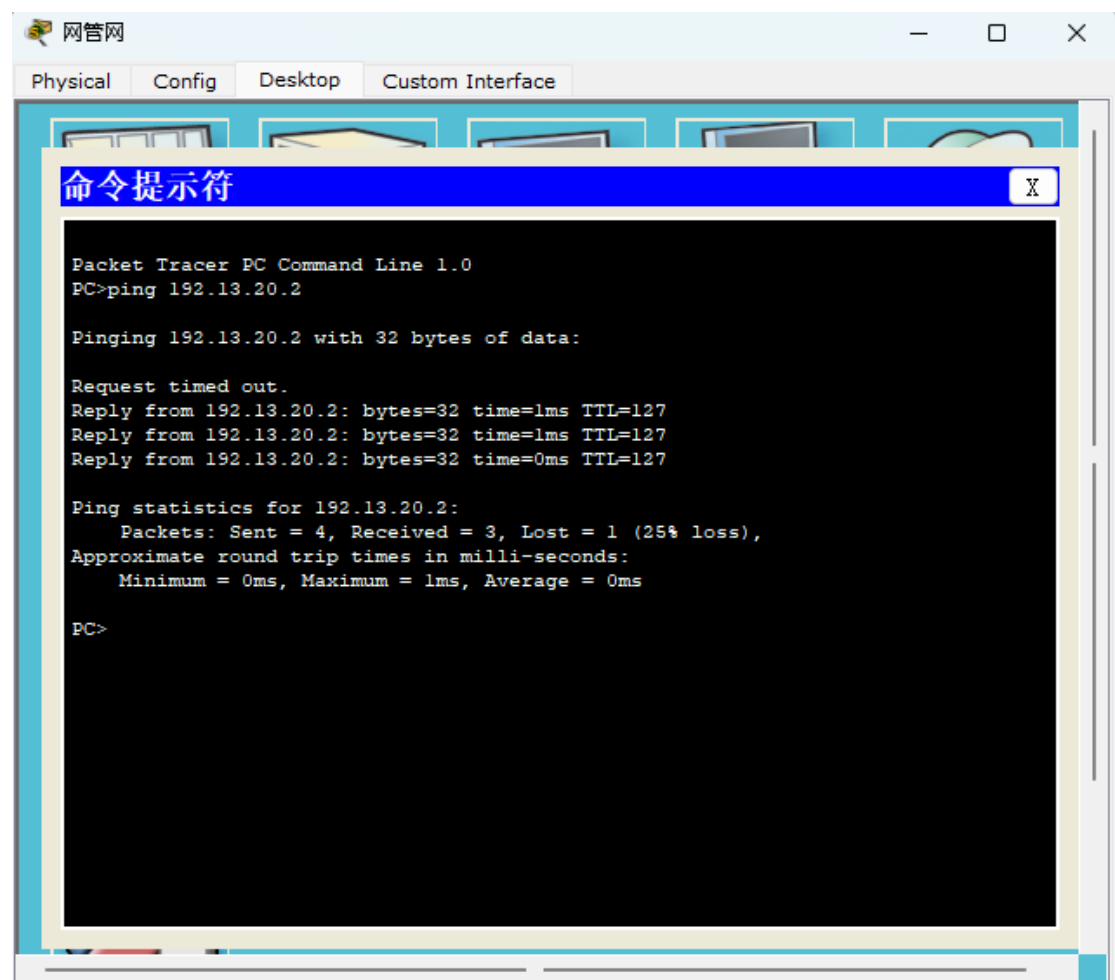
shutdown
!
router ospf 1
log-adjacency-changes
network 200.13.1.0 0.0.0.255 area 0
network 100.13.29.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
password 123456
```

```
login
!  
!  
!  
end
```

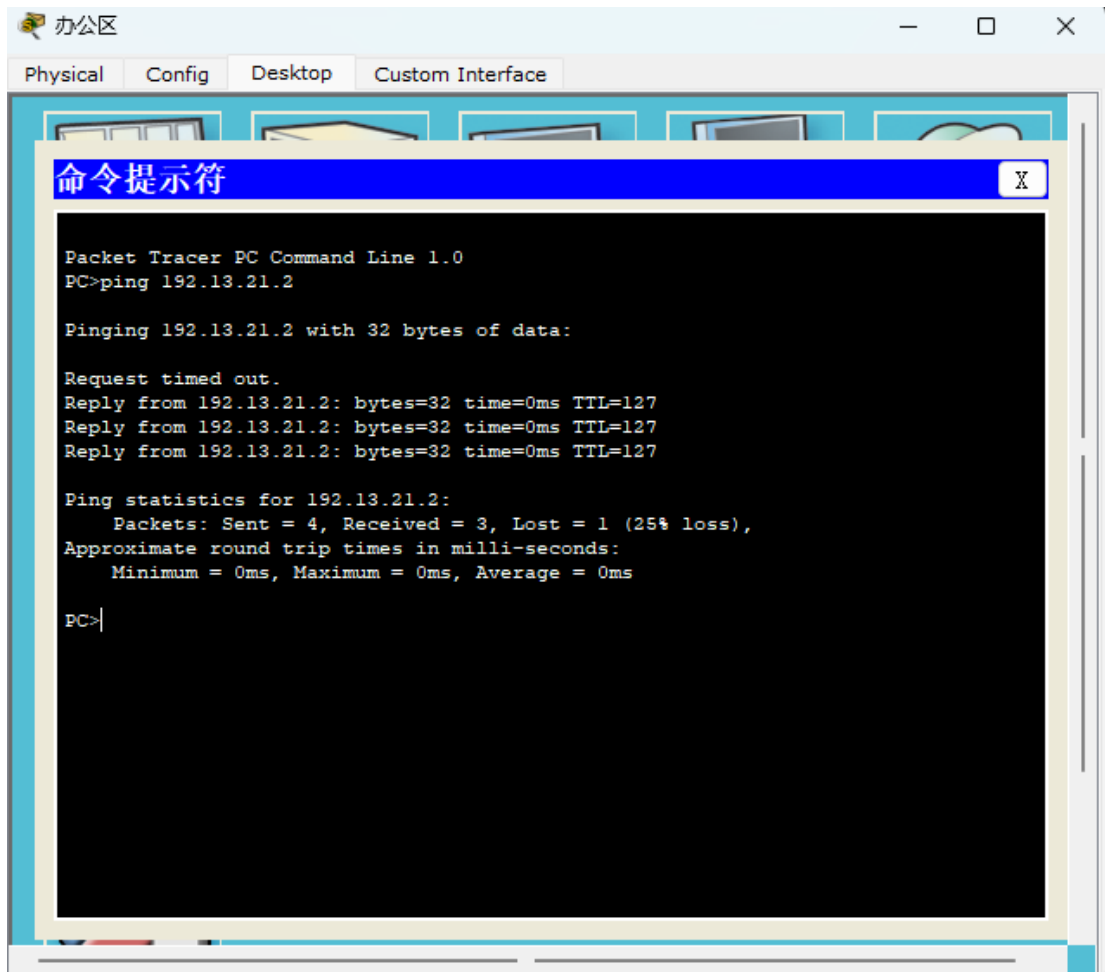
第 7 章网络工程项目测试

截图说明不同设备之间的连通性

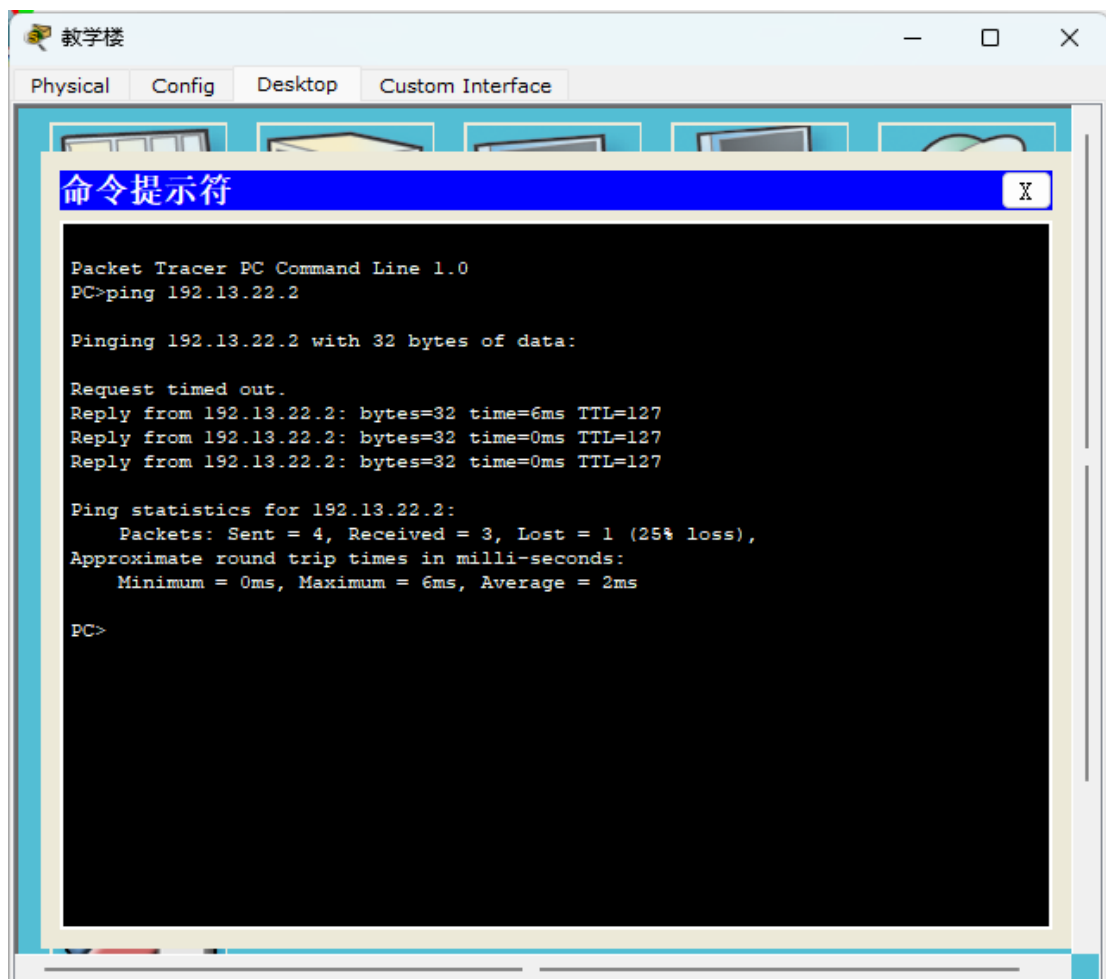
网管区-办公区



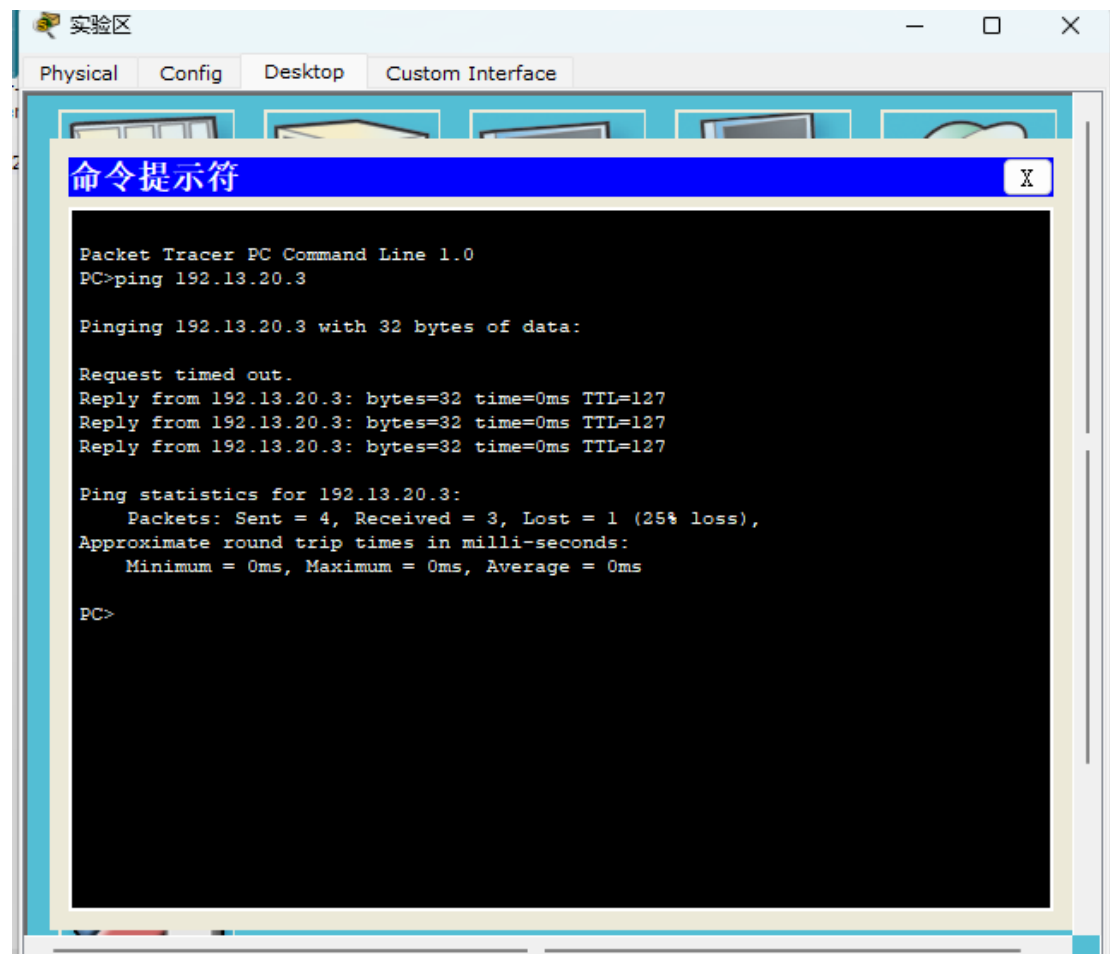
办公区-教学楼



教学楼-实验区



实验区-宿舍楼



访问服务器成功



第8章 项目总结与展望

本次校园网组网的设计方案，是我在网络知识掌握有限的情况下，通过不断的学习和实践完成的。在这个过程中，我发现了许多问题和不足之处，也积累了许多经验和收获。下面我将对这个项目进行总结，并展望未来的发展方向。

一、项目总结

设计方案的不足之处

由于网络知识掌握有限，本次组网的设计方案存在以下不足之处：

- （1）涉及的内容深度不够，一些细节的东西欠缺；
- （2）对网络安全方面考虑较少，尤其是局域网的安全性；
- （3）需要进一步完善和优化的地方还有很多，比如防火墙的配置和设置等。

学习和收获

在本次组网的过程中，我学到了很多新的知识和技能，其中包括：

- （1）对网络结构和组网技术有了更深入的了解；
- （2）熟练掌握了网络设备的基本配置和使用；
- （3）初步了解了网络安全方面的内容，如防火墙的配置和设置等；
- （4）通过实践，提高了解决问题的能力和应变能力。

二、展望未来

虽然本次校园网组网的设计方案存在一些不足之处，但是通过不断的学习和实践，我相信我会不断地完善和优化这个设计方案，并且在未来的工作中不断提高自己的水平和能力。以下是我未来的发展方向：

深入学习网络知识

为了更好地设计和实现网络，我需要深入学习网络知识，包括网络协议、网络安全等方面的内容，不断提高自己的专业水平和技能。

加强对网络安全的考虑

网络安全是网络建设中至关重要的一环，我需要加强对网络安全的学习和理解，并在实践中不断加强对网络安全的考虑和实现。

继续实践和完善

在未来的工作中，我将继续实践和完善网络设计方案，不断探索和尝试新的技术和方法，提高自己的实践经验和技能。

总之，本次校园网组网的设计方案虽然存在不足之处，但是我相信通过不断的学习和实践，我会不断地完善和改进它，让它更加完善和实用。在未来的工作中，我会注重提高自己的网络知识和技术，不断深入学习网络安全方面的知识，掌握更加先进的技术和方法，为企业的网络安全提供更加可靠的保障。

另外，我也会注重与同行业的专业人士交流和合作，借鉴他们的经验和思路，不断拓展自己的视野和能力。同时，我也会积极参加相关的技术交流和学习活动，提高自己的技能和水平，让自己成为一名更加优秀的网络设计师。

总之，通过本次校园网组网的实践和学习，我对网络设计有了更深入的认识和理解，也发现了自己在知识和技术方面的不足之处。在未来的工作中，我会不断地努力学习和实践，提高自己的实践经验和技能，成为一名更加出色的网络设计师。