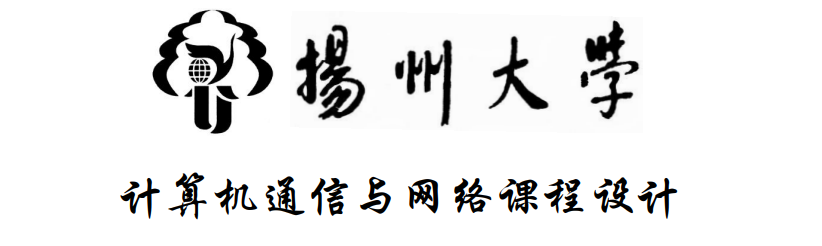
****

**课设题目：一个中小型企业网络的规划与设计**

**专 业： 计算机科学与技术**

**班 级： 计科2002**

**学 号： 202801108**

**姓 名： 李蔚**

**同组成员： 魏刘逸哲、卞睿、孙顺、吴煜明**

**指导老师： 刘萍**

**完成日期： 2023年2月26日**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项目名称 | 考核比重 | 得分 |
| 1 | 方案设计 | 10% |  |
| 2 | 网络搭建 | 50% |  |
| 3 | 设计验收 | 20% |  |
| 4 | 设计报告 | 20% |  |
| 5 | 总成绩 | 100% |  |

**《计算机通信与网络课程设计》任务书**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **课程编号** | 10130493 | **学分** | 1 | **周数** | 1周 |
| **专业** | 计算机科学与技术 | **学号** | 202801108 | | |
| **姓名** | 李蔚 | **班级** | 计科2002 | | |
| **组号** | 5 | **课程设计名称** | 一个中小型企业网络的规划与设计 | | |
| **目的与要求：**  本课程设计旨在通过对综合网络项目的设计与实现，使学生进一步理解并掌握计算机网络的原理，培养学生的协议分析与理解、网络设计、网络管理、网络故障排查等综合实践能力。 | | | | | |
| **主要任务及具体要求：**   1. **任务**   某公司有 800 台 PC；公司共有8个部门，不同部门的相互访问要求有限制，公司有2个跨省的分公司；公司有自己的内部网页与外部网站，公司能够提供匿名的FTP、E-mail、WWW服务，但FTP只对内部员工开放；公司有自己的 OA 系统；公司中的每台主机都能登录Internet，每个部门的办公室联合构成一个VLAN；核心技术采用VPN。  **2、具体要求**  ① 网络配置：综合布线、IP地址规划及子网划分、硬件设计② 网络拓扑：层次模型、拓扑结构、物理设备、物理介质和功能区域划分③ 物理设备选型④ 交换机配置信息⑤ 路由器配置信息⑥ 服务器配置信息⑦ 防火墙等配置信息⑧ 系统测试：网络连通性测试（LAN、VLAN）、邮件服务测试、Web服务测试、NAT测试、FTP服务测试⑨ 设计中的问题及其解决方案。  **3、软硬件要求**  （1）仿真软件：Cisco packet tracer  （2）硬件环境：cpu：i5 13500，内存：32G，操作系统：Windows 11   |  |  |  |  | | --- | --- | --- | --- | | **时间** | **内容** | **时间（天）** | **授课形式** | | 1 | 方案设计 | 2 | 讲练结合 | | 2 | 网络搭建 | 3 | 讲练结合 | | 3 | 设计验收及答辩 | 1 | 讲练结合 | | 4 | 撰写课设报告 | 1 | 讲练结合 |   **4、进程安排** | | | | | |

**《计算机通信与网络课程设计》答辩记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| **专业** | **计算机科学与技术** | **学号** | **202801108** |
| **姓名** | **李蔚** | **班级** | **计科2002** |
| **组号** | **5** | **题目** | **一个中小型企业网络的规划与设计** |
| **答辩记录：**  问题1：在本系统中你是如何选择路由协议的？为什么？  答：在公司内部网络的设计中，我们选择了RIP路由协议，因为它是一种基于距离向量的路由协议，适合于规模较小的内部网络。RIP协议的工作原理是通过跳数来判断链路的长度，因此可以根据网络拓扑图中的链路数来计算出最佳的路由路径。  在模拟外部网络中，我们选择了OSPF协议。OSPF是一种基于链路状态的路由协议，适用于规模较大、复杂的网络。OSPF协议能够通过链路的带宽、延迟等因素计算出最佳的路由路径，从而提高网络的传输效率。同时，OSPF协议还具有快速收敛、灵活配置等优点，能够更好地适应外部网络的需求。  除此之外，为了更好地适应网络的需求，我们在网络中还配置了一些静态路由。在网络中配置静态路由可以避免网络拓扑发生变化时带来的不必要的路由计算，从而提高网络的传输效率和稳定性  问题2：简要说明VPN的原理和作用。  答：VPN即虚拟专用网络，原理是通过在公共网络上建立加密隧道，将数据进行加密传输，使得远程用户可以通过公共网络接入公司内部网络，实现像在局域网中一样的通讯。  VPN的作用主要有以下几个方面：远程访问。数据加密传输。建立安全通讯渠道。网络扩容，VPN可以将不同地点、不同网络间的网络资源连接起来，扩展公司的网络覆盖范围。  问题3：实验中碰到了什么问题？如何解决的？  答：在进行课程设计中的VPN配置时，我遇到了一些问题，例如VPN隧道无法正常建立，不能对IP数据报进行加密封装，导致在外网上路由器无法在路由表中找到转发地址等问题。经过认真检查，我发现了问题所在，原来是我将VPN的加密映射配置到了错误的接口上。在进行VPN配置时，我们需要为加密隧道选择一个正确的接口，通常是路由器的外网接口。只有在正确的接口上配置加密映射，VPN才能正常工作。因为如果将加密映射配置到错误的接口上，路由器将无法识别加密隧道的出口地址，从而无法正确地转发加密数据包。在对各个端口的配置做出修改后，VPN恢复正常工作。  **答辩人：李蔚 日期：2023.3.8** | | | |

目录

[**第 1 章** **前言** 5](#_Toc129546069)

[1.1 背景分析 5](#_Toc129546070)

[1.2 采用的方法和原则 5](#_Toc129546071)

[**第 2 章** **用户需求性分析** 6](#_Toc129546072)

[2.1 功能性需求分析 6](#_Toc129546073)

[2.2 非功能性需求分析 7](#_Toc129546074)

[2.2.1拓扑结构需求分析 7](#_Toc129546075)

[2.2.2 综合布线需求分析 8](#_Toc129546076)

[**第 3 章** **网络拓扑结构设计** 9](#_Toc129546077)

[3.1拓扑结构 9](#_Toc129546078)

[3.2硬件结构 15](#_Toc129546079)

[3.3地址规划 16](#_Toc129546080)

[3.4网络设备配置 17](#_Toc129546081)

[**第 4 章** **网络物理设计** 25](#_Toc129546082)

[4.1 传输介质选择 25](#_Toc129546083)

[4.2 综合布线设计 27](#_Toc129546084)

[**第 5 章** **系统测试** 29](#_Toc129546085)

[5.1 服务器与各个 PC 机的连通性测试 29](#_Toc129546086)

[5.2 PCi与其它 PC 机的连通性测试 33](#_Toc129546087)

[5.3 测试及分析中的注意事项 36](#_Toc129546088)

[**第 6 章** **网络其他设计** 37](#_Toc129546089)

[6.1 性能设计 37](#_Toc129546090)

[6.2 安全性设计 40](#_Toc129546091)

[6.3 可靠性设计 45](#_Toc129546092)

[**第 7 章** **总结与体会** 46](#_Toc129546093)

[参考文献 48](#_Toc129546094)

1. **前言**
   1. **背景分析**

随着网络技术的发展，企业局域网已广泛应用于企业工作中，为企业正常运营带来便利，提高了企业效益。然而，传统的企业网络通常为有线局域网，虽满足了大部分的工作需求，但存在无法移动办公、布线繁琐等弊端，因此，企业若想在高效运营，应对企业网络进行详细规划，是企业网络具有先进性、实用性及可靠性。如今，已有越来越多的中小型企业**。**重视信息化平台的建设，深刻认识到了企业网络建设的必要性与紧迫性。[1]

企业网络是现代企业中必不可少的一部分，它承载着企业内部的信息交流、数据传输等重要任务。网络架构是企业网络建设的核心，传统的三层网络架构和扁平化网络架构分别具有自己的优点和缺点。本文结合文献和案例分析了企业网络建设需求，总结出了建设企业网络时需要考虑的几个关键点。在此基础上，本文提出了一些建设企业网络的建议，以帮助企业更好地建设自己的网络。

* 1. **采用的方法和原则**

在企业网络的设计中，需要采用一些基本的方法和原则，以确保网络能够满足不同业务对处理能力的要求，同时保证网络系统的可靠性、易管理性和易维护性。下面列举了我们参考的方法和原则：

（1）实用性原则：网络系统的性能指标应能够满足网络内各项业务对处理能力的要求。在网络设计时，需要考虑到整个系统的可靠性、易管理性和易维护性等方面。这需要网络管理员在网络的日常管理和维护中，不断地对网络进行监测和优化，确保网络系统能够稳定运行。

（2）可扩展性原则：随着企业用户业务的不断发展，网络系统必然随之不断扩大。因此，网络设计需要考虑到未来的扩充，留有足够的余地。在设计网络时，需要采用一些灵活的技术和方案，以适应不断变化的业务需求。例如，采用可扩展的硬件设备，实现动态扩容等。

（3）高安全性原则：在企业网络中，安全性是至关重要的。为了保护企业的机密信息和网络资源，需要采用一系列的安全措施。例如，增加防火墙等设备，用ACL、VLAN等对不同的用户进行隔离，采用VPN技术等保护机密信息的传输，以及采取多种技术从内部和外部同时控制用户对网络资源的访问。这些措施能够有效地提高网络的安全性，保障企业的信息安全。[2]

综上所述，企业网络的设计需要遵循实用性原则、可扩展性原则和高安全性原则等基本方法和原则，以确保网络系统的可靠性、易管理性和易维护性，同时保障企业的信息安全。

1. **用户需求性分析**
   1. **功能性需求分析**

项目概况：某公司有 800 台 PC；公司共有 8个部门，不同部门的相互访问要求有限制，公司有2个跨省的分公司；公司有自己的内部网站与外部网站，公司能够提供匿名的 FTP、E-mail、WWW 服务，但FTP只对内部员工开放；公司有自己的OA系统；公司中的每台主机都能登录Internet，每个部门的办公室联合构成一个VLAN；核心技术采用VPN。

这是一个关于某公司的信息描述，其中包含以下信息：

（1）公司拥有 800 台 PC。

（2）公司共有 8 个部门，不同部门之间有访问限制。

（3）公司有 2 个跨省分公司。

（4）公司拥有内部网站和外部网站。

（5）公司提供匿名的 FTP、E-mail、WWW 服务，但FTP只对内部员工开放。

（6）公司有自己的 OA 系统。

（7）公司中的每台主机都能登录 Internet。

（8）每个部门的办公室联合构成一个 VLAN。

（9）核心技术采用 VPN。

这些信息描述了公司的基本网络环境和网络服务。根据这些信息，我们可以了解到公司的基本网络结构和各种网络服务的提供情况，以及不同部门之间的访问限制。根据这些信息，我们可以对公司的网络进行初步分析和评估，以确定网络存在的问题和改进的方向。例如，可以评估公司网络的安全性和可靠性，了解各部门的网络需求和访问模式，以便优化网络架构和改进网络服务。

根据项目的相关概况进行分析，企业网络应分为内部网络和外部网络两个部分, 其中还包括在这两部分上的实际应用, 中小型企业在网络设计之初就应该充分考虑到自身的需求, 通过这些需求来具体设计适合自己需求的网络。[3]

通过ACL和VLAN划分，实现各部门之间的访问限制功能。基于MAC地址的VLAN划分方法即使主机移动了物理位置,接入了不同的交换机和不同的端口时,主机所属于的VLAN没有变化,不需要进行重新配置,方便公司日后对办公室内部进行装修、扩展。[4]

* 1. **非功能性需求分析**

2.2.1拓扑结构需求分析

对于中小型企业的网络拓扑结构需求分析，需要考虑多个方面，包括规模、安全性和成本等因素。

首先，中小型企业的网络规模通常较小，因此通常不需要过于复杂的拓扑结构。对于这类企业而言，一个简单的星型拓扑结构已经足够满足需求。这种结构具有简单易懂、易于维护等特点，能够满足企业基本的通信需求。

其次，网络安全是企业不容忽视的重要问题。中小型企业需要根据自身的安全需求来确定网络拓扑结构，例如使用虚拟专用网络（VPN）等技术，以确保数据的安全性。由于中小型企业一般会考虑经济承受能力，Cisco PIX 525防火墙通常被作为企业接入网络时过滤数据的选择，它可以将企业的内部网络和外部网络隔离开来，维护网络的边界安全。[5]

第三，成本问题是中小型企业需要考虑的另一个关键因素。由于中小型企业的预算相对有限，因此需要选择经济实惠的拓扑结构方案。简单的拓扑结构，如星型拓扑结构和总线型拓扑结构，通常是较为经济实惠的选择。

最后，可扩展性也是中小型企业需要考虑的问题。即使网络规模较小，但企业也需要有足够的扩展能力以满足未来的业务需求。因此，中小型企业需要选择一个具有一定可扩展性的网络拓扑结构。

综上所述，对于中小型企业而言，网络拓扑结构的选择需要综合考虑规模、安全性、成本和可扩展性等因素。尽管不同的企业在具体的拓扑结构选择上可能有所差异，但星型拓扑结构通常是一种现实和符合逻辑的选择。[6]

2.2.2 综合布线需求分析

在中小型企业中，网络的综合布线需求分析需要考虑以下几个方面：

办公环境： 中小型企业的办公环境可能相对简单，但是网络布线的难度和可行性却需要仔细考虑。在进行综合布线时，需要考虑建筑结构、电力供应和通信设备等因素，以确保网络布线的可靠性和稳定性。对于一些较为复杂的建筑结构，如多层楼建筑，可采用层间布线技术，以实现不同楼层之间的网络通信。此外，还需要考虑到布线对办公环境的影响，如美观性和安全性等。[7]

业务需求： 企业的业务需求也是进行综合布线的重要考虑因素。需要确定不同区域的网络使用频率和网络负载，以便选择合适的网络布线方式。在本项目中，需要考虑到总公司八个部门和分公司各个部门的布线方式，以及各部门与中央服务器之间的连接。为了满足这些需求，可以采用不同的布线方式和技术，如水平布线和垂直布线等，以确保网络的可扩展性和性能。

网络拓扑结构： 网络拓扑结构也是进行综合布线的重要因素之一。在进行综合布线时，应根据拓扑结构需求分析，以星型拓扑结构为基础进行拓展。星型拓扑结构具有简单、易于管理和可靠性高等优点，能够满足中小型企业的网络需求。[8]

设备选择： 在进行综合布线时，设备的选择和布置也是至关重要的。需要根据业务需求和网络拓扑结构来选择合适的交换机、路由器和其他网络设备，并且需要合理地布置这些设备，以实现网络的高性能和高可靠性。此外，还需要考虑到设备的兼容性和可维护性等因素，以确保网络的稳定运行。

综上，中小型企业的综合布线需求分析需要考虑多个因素。首先，办公环境、业务需求和网络拓扑结构都会影响网络布线的难度和可行性。其次，设备选择和布置也需要谨慎考虑，以确保网络的性能和可靠性。综合考虑这些因素后，中小型企业可以选择以星型拓扑结构为基础进行布线，以满足不同部门的网络使用频率和网络负载需求。在设备选择和布置方面，企业可以选择适合自己需求的交换机、路由器和其他网络设备，以提高网络的可靠性和性能。总之，综合布线需求分析需要全面、细致地考虑各个方面的因素，以确保网络的顺利运行。

1. **网络拓扑结构设计**

## 3.1拓扑结构

三层网络架构是目前企业网络建设中应用最广泛的网络架构之一。它由三个层级构成，包括核心层、汇聚层和接入层。其中，核心层是整个网络的中心，负责处理网络中的所有数据流量；汇聚层连接核心层和接入层，负责在不同的网络之间进行数据转发和过滤；接入层连接用户设备和网络，负责提供用户接入服务。针对该中小型企业的需求，我们设计了一个星型网络拓扑结构。星型拓扑结构包括至少一个核心设备，该设备通过直接连接各个设备来控制网络的流量和访问。在这个拓扑结构中，每个设备都直接连接到核心设备，而不与其他设备直接连接。

接入层：

接入层是企业网络中最底层的层次，主要负责将终端设备接入到网络中。接入层包含多个网络接入设备，如交换机。接入层交换机通过端口VLAN隔离不同用户的数据流，实现用户之间的互相隔离，同时还可以提供基本的安全策略，如802.1X认证和端口安全策略等。接入层还要提供足够的带宽支持终端设备，以确保数据传输的快速和可靠。

具体来说接入层是企业网络的边缘，主要负责接入终端设备，如PC、IP电话、打印机等，并提供对终端设备的接入、管理和安全控制。接入层交换机通常需要满足以下要求：

高密度接口：接入层交换机需要提供大量的接口，以满足企业大量终端设备的接入需求。因此，交换机需要具有高密度接口的特点，以支持大量的终端设备接入。

VLAN隔离：为了保证网络安全，接入层交换机需要支持VLAN隔离。通过配置VLAN，可以将不同的用户、设备或部门划分为不同的虚拟网络，从而避免不同用户之间的干扰和冲突。

安全控制：为了保证网络安全，接入层交换机需要支持安全控制功能，如MAC地址过滤、802.1X认证等，从而保障网络的安全性和合规性。

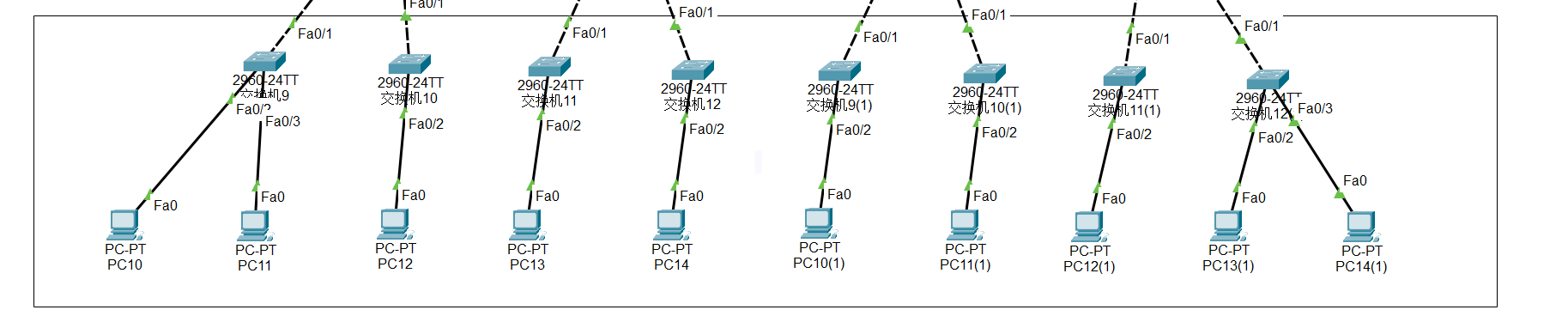


图3.1.1：总公司接入层

汇聚层：

汇聚层是连接接入层和核心层的中间层次，负责连接多个接入层交换机并将它们汇聚到核心层交换机中。汇聚层交换机通常拥有更高的端口密度和更强的性能，以满足多个接入层交换机的聚合需求。此外，汇聚层交换机还可以提供一些高级的安全和服务策略，如访问控制列表（ACL）等。

具体来说，汇聚层是企业网络的中间层，主要负责连接接入层和核心层，并实现不同VLAN之间的数据交换。汇聚层交换机通常需要满足以下要求：

高带宽：汇聚层交换机需要提供高带宽的特点，以支持大量数据的交换和传输。通常，汇聚层交换机需要提供千兆甚至万兆的带宽，以满足企业的需求。

VLAN管理：汇聚层交换机需要支持VLAN管理，以实现不同VLAN之间的数据交换。通过VLAN配置，可以将不同的用户、设备或部门划分为不同的虚拟网络，从而实现不同网络之间的数据隔离和安全控制。

聚合链路：为了提高带宽利用率和可靠性，汇聚层交换机需要支持聚合链路技术，即将多个物理链路绑定成一个逻辑链路。通过聚合链路技术，可以提高链路带宽和可靠性，并减少链路故障的影响范围。

多路径转发：汇聚层交换机需要支持多路径转发技术，以提高网络的可靠性和容错性。通过多路径转发技术，可以将数据流量分散到不同的链路上，从而减少链路故障的影响，提高网络的稳定性和可靠性。

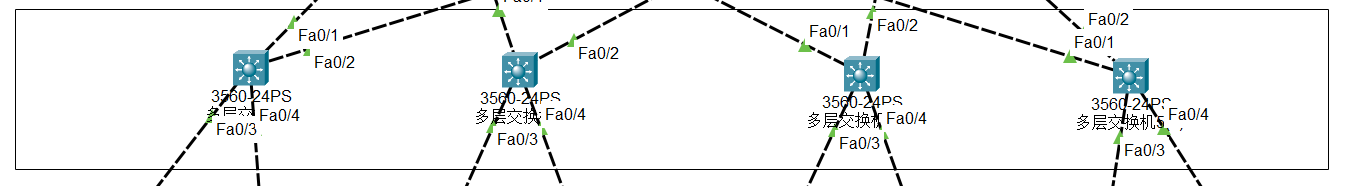


图3.1.2：总公司汇聚层

核心层：

核心层是企业网络的顶层层次，主要负责实现高速的数据转发和聚合，以满足企业网络中大量的数据流量需求。核心层交换机通常采用高速交换技术，如基于硬件的交换和多层交换等，以支持大量的流量。此外，核心层交换机还需要具备高可用性和冗余性，以保证企业网络的高可靠性和可用性。

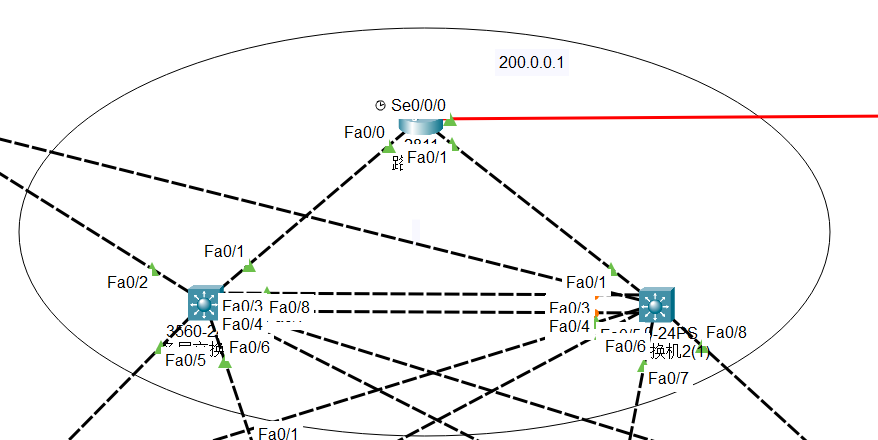


图3.1.3：总公司核心层

服务器集群：

服务器集群是指将多台服务器组成一个逻辑单元，通过软件和硬件的配合实现资源共享和负载均衡，从而提高服务器的可用性和性能。对于中小型企业来说，服务器集群的设计和部署需要考虑以下几个方面：首先是可靠性和可用性。还有是高可扩展性，随着企业的业务不断发展，服务器集群需要具备高可扩展性，能够根据业务需求动态扩展或缩减服务器数量，以满足企业的发展需求。因此，在设计服务器集群时，需要考虑到服务器的可扩展性，选用可扩展的硬件和软件架构。

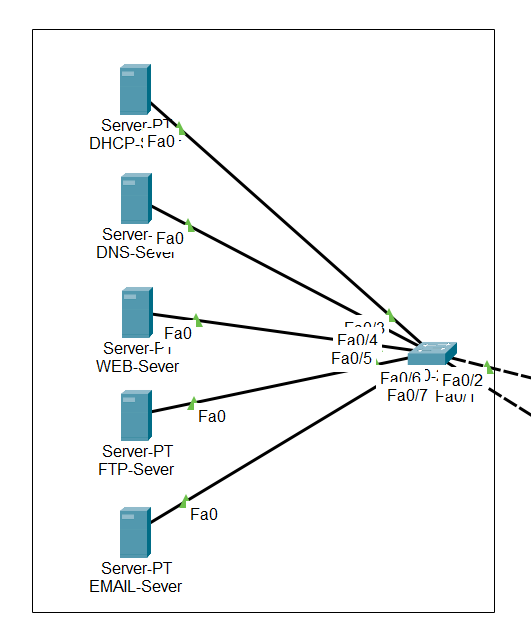


图3.1.4：总公司服务器集群

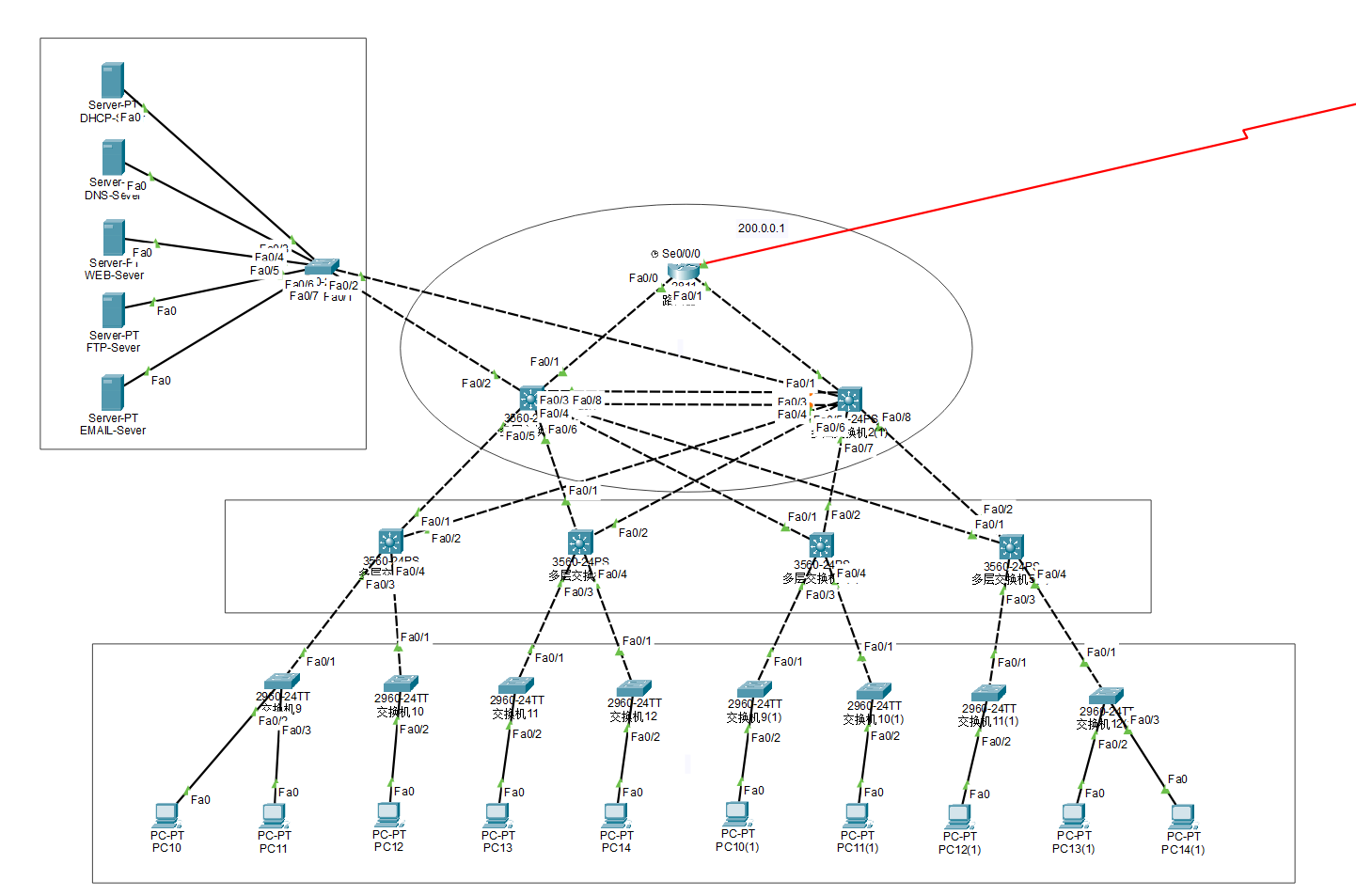


图3.1.5：总公司整体拓扑

分公司整体拓扑：

中小型企业的网络拓扑结构相对简单，一般采用星型或总线型结构，其中星型结构更为常见。由于分公司规模较小，往往只需要一台或几台服务器就能够满足企业的需求。此外，由于分公司的网络负载相对较小，因此网络带宽的要求也不高，一般1000Mbps的带宽就能够满足中分公司的需求。这么设计结构简单，也方便后期维护工作的进行，同时可以灵活地重新按需求进行配置。 [9]

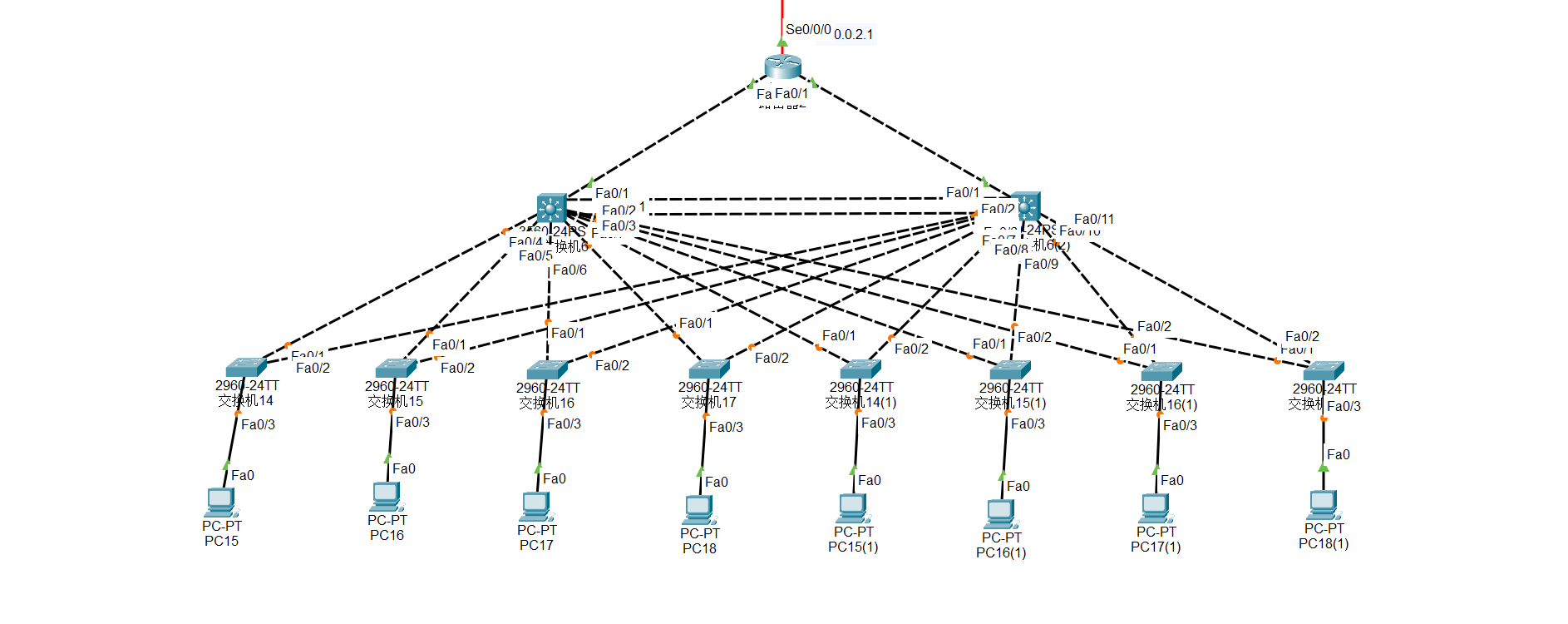


图3.1.6：分公司整体拓扑

模拟外部网络：

在模拟外部网络搭建的过程中，网络拓扑设计是非常重要的一步。网络拓扑设计涉及到各个设备之间的连接方式以及路由器之间的路由协议选择等。一般而言，网络拓扑设计应该考虑到网络的可靠性、可扩展性和安全性等方面。

在本次网络拓扑设计中，我们需要连接总公司、分公司1、分公司2以及外网服务器。首先，我们需要确定各个设备的IP地址。

我们需要将各个设备连接起来。由于总公司、分公司1和分公司2都连接到本地ISP路由器上，因此我们可以使用三条物理连接将它们连接到本地ISP路由器上。本地ISP路由器的WAN口连接互联网，因此不需要再连接到其他路由器上。另外，我们需要将外网服务器连接到本地ISP路由器的LAN口上。

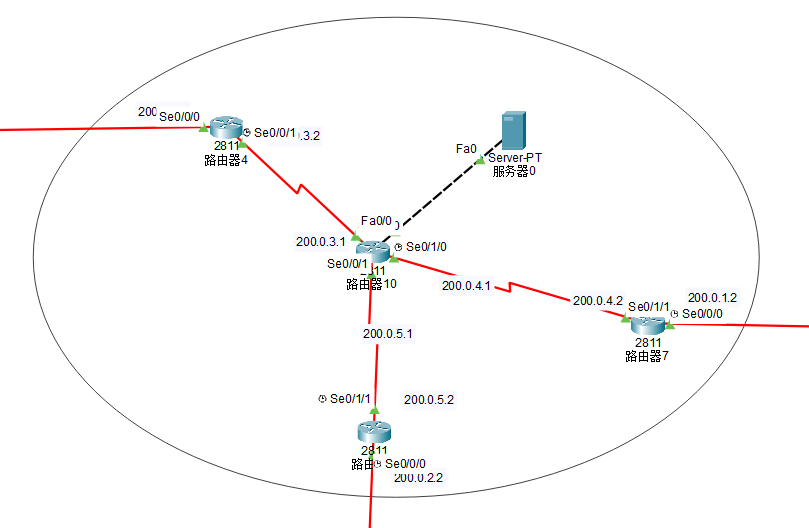


图3.1.7：模拟外部网络

整体拓扑结构：

总的来说，网络拓扑设计是一个非常重要的环节，需要考虑到多个方面。正确的网络拓扑设计可以保证网络的稳定性和可靠性，提高网络的性能和安全性。

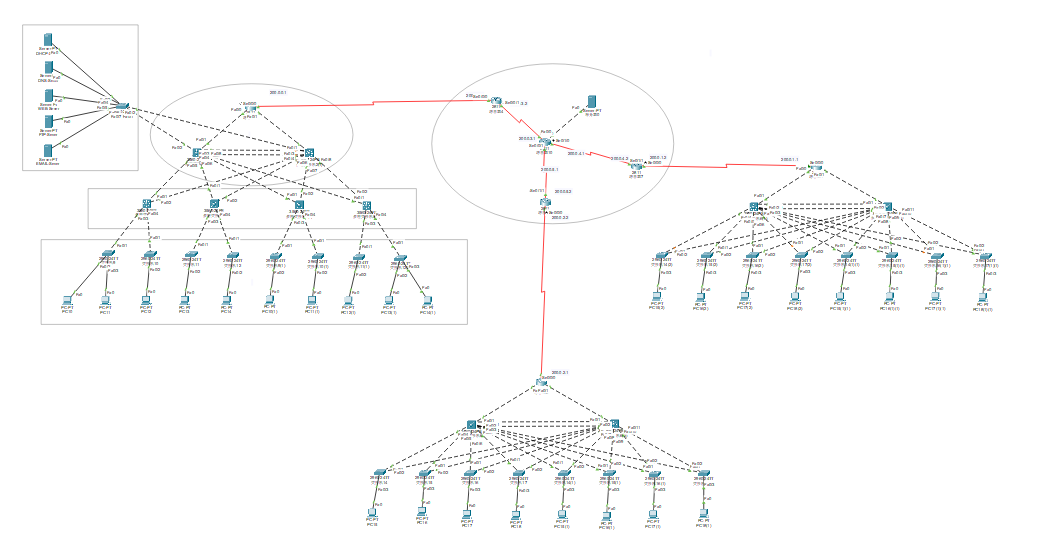


图3.1.8：整体拓扑结构

## 3.2硬件结构

在中小型企业中，网络硬件结构通常会包括PC、交换机、多层交换机、路由器以及服务器等设备。这些设备共同构成了企业的网络基础设施，支持企业的各种业务和应用。

首先，PC是企业中最基础的网络设备。它们通常用于员工的办公和生产活动，如办公文档处理、数据录入、客户管理等。在中小型企业中，PC通常会接入到交换机或多层交换机中，通过交换机来实现局域网内的数据通信。

交换机是一种用于局域网内数据交换的设备。它可以实现数据包的快速转发和广播等功能。在中小型企业中，交换机通常被用于连接PC和服务器等设备，以实现内部网络的快速通信。一般而言，中小型企业的交换机会采用快速以太网或千兆以太网技术，支持各种网络协议和QoS等功能。

多层交换机是一种更高级的交换机，它可以实现数据包的高效路由和分发等功能。在中小型企业中，多层交换机通常会被用于连接不同的子网，并实现不同子网之间的数据通信。多层交换机一般会支持更多的协议和功能，如VLAN、QoS、ACL等，从而为企业的网络提供更高的可靠性和安全性。

路由器是一种用于连接不同网络的设备，它可以实现数据包的路由和转发等功能。在中小型企业中，路由器通常会被用于连接内部网络和外部网络，如连接互联网或其他企业的网络。一般而言，中小型企业的路由器会支持各种路由协议和安全功能，如静态路由、动态路由、NAT等。

服务器是企业中最重要的网络设备之一，它可以提供各种应用和服务，如文件共享、数据库管理、Web服务器等。在中小型企业中，服务器通常会被用于存储和处理企业的关键数据和业务信息。服务器一般会采用专业的硬件和软件，如RAID、备份系统、虚拟化技术等，以提高可靠性和性能。

在中小型企业中，网络硬件结构的设计应该综合考虑企业的业务需求、网络规模、性能要求和安全要求等因素。例如，对于网络规模较小的企业，可以采用简单的交换机和路由器等设备，以实现基本的局域网和互联网连接。而对于网络规模较大或业务要求较高的企业，可以采用多层交换机、防火墙、VPN设备等设备，以实现更高的可靠性、性能和安全性。

另外，对于中小型企业的网络硬件结构设计还需要注意以下几点：

网络拓扑结构的选择。常见的网络拓扑结构有星型、环型、树型、网状等，每种结构都有其优缺点。设计人员应该根据企业的实际情况选择合适的网络拓扑结构。

网络带宽的设计。网络带宽的大小直接影响到企业的网络性能和用户体验。设计人员应该根据企业的网络需求和预算等因素，合理规划网络带宽的大小和分配方式。

网络安全的设计。网络安全是企业网络中最重要的问题之一。设计人员应该采用多种安全技术和措施，如防火墙、入侵检测系统、VPN等，以保障企业网络的安全性。

网络管理的设计。网络管理是企业网络中的重要组成部分，它涉及到网络设备的配置、监控、维护等工作。设计人员应该采用专业的网络管理工具和流程，以提高网络管理的效率和可靠性。

总之，中小型企业的网络硬件结构设计是一个复杂的问题，需要综合考虑多种因素。合理的设计可以提高网络的可靠性、性能和安全性，从而为企业的业务发展提供良好的支持。

## 3.3地址规划

IP地址规划是企业网络中非常重要的一环，它涉及到网络拓扑结构的设计、设备配置、路由设置、安全策略等多个方面。中小型企业的IP地址规划过程主要包括：

确定IP地址范围。根据企业网络规模和需求，确定IP地址范围，包括公网IP地址、私网IP地址、子网掩码等。

分配IP地址。根据网络拓扑结构和IP地址范围，对不同设备进行IP地址分配，如路由器、交换机、服务器、客户端等。通常建议为每个子网分配一个独立的IP地址段，以方便管理和维护。

测试和优化。在完成IP地址规划后，需要进行测试和优化，以确保网络的性能和可靠性。可以使用网络分析工具进行测试，如Ping、Tracert等。

需要注意的是，IP地址规划应该是一个动态的过程，随着企业网络的发展和扩展，IP地址范围和分配方式也需要不断调整和优化。因此，在进行IP地址规划时，应该考虑到网络的可扩展性和灵活性，以适应企业不断变化的需求。

下面给出具体的地址规划：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 部门名称 | 主机数 | IP地址范围 | 子网掩码 | VLAN |
| 总公司部门1 | <=200 | 192.168.11.1-192.168.11.253 | 255.255.255.0 | 11 |
| 总公司部门2 | <=200 | 192.168.12.1-192.168.12.253 | 255.255.255.0 | 12 |
| 总公司部门3 | <=200 | 192.168.13.1-192.168.13.253 | 255.255.255.0 | 13 |
| 总公司部门4 | <=200 | 192.168.14.1-192.168.14.253 | 255.255.255.0 | 14 |
| 总公司部门5 | <=200 | 192.168.15.1-192.168.15.253 | 255.255.255.0 | 15 |
| 总公司部门6 | <=200 | 192.168.16.1-192.168.16.253 | 255.255.255.0 | 16 |
| 总公司部门7 | <=200 | 192.168.17.1-192.168.17.253 | 255.255.255.0 | 17 |
| 总公司部门8 | <=200 | 192.168.18.1-192.168.18.253 | 255.255.255.0 | 18 |
| 总公司服务器集群 | 5 | 192.168.0.1-192.168.0.5 | 255.255.255.0 | 10 |
| 分公司1 | 每个部门<=200 | 192.168.32.0-192.168.47.255 | 255.255.240.0 | 21-28 |
| 分公司2 | 每个部门<=200 | 192.168.48.0-192.168.63.255 | 255.255.240.0 | 31-38 |

## 3.4网络设备配置

中小型企业网络硬件是一个典型的局域网环境，通常包括PC、交换机、多层交换机、路由器以及服务器等设备。为了保证网络正常运行，这些设备需要按照一定的配置进行设置和连接。下面将介绍中小型企业网络硬件的配置过程。

PC的配置：

PC是局域网的终端设备，需要配置IP地址、子网掩码、默认网关、DNS服务器等网络参数，以便正常连接到局域网和互联网。配置IP地址用的是DHCP协议，这样就不用手动输入IP地址、子网掩码、默认网关、DNS服务器等网络参数了。

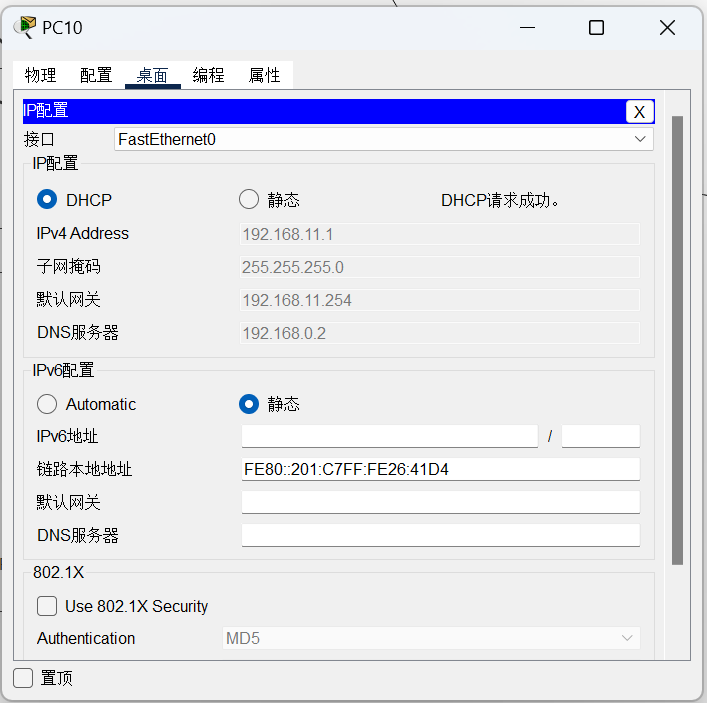


图3.4.1：PC的配置

交换机的配置：

交换机是局域网中连接多台PC的核心设备，需要配置VLAN、端口等参数，以便实现局域网内的通信和管理。配置VLAN：在交换机的Web管理界面中，选择“VLAN”菜单，点击“新增”按钮，设置VLAN的ID和名称，选择需要加入该VLAN的端口，保存并应用设置。配置端口：在交换机的管理界面中，选择选择需要配置的端口，设置端口的速率、双工模式、VLAN成员关系等参数，保存并应用设置。

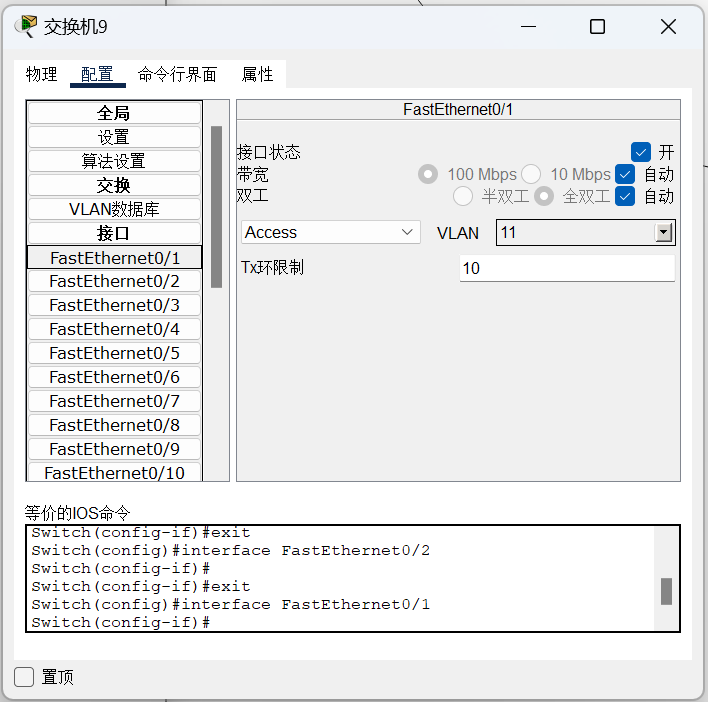


图3.4.2：交换机的配置

多层交换机的配置：

多层交换机是连接多个交换机的设备，需要配置IP地址、VLAN、端口、路由等参数，以便实现不同VLAN之间的通信和互联网的访问。在中小型企业网络中，核心交换机扮演着极其重要的角色，因此，在配置中心三层交换机时，需要考虑负载均衡和备份的问题。

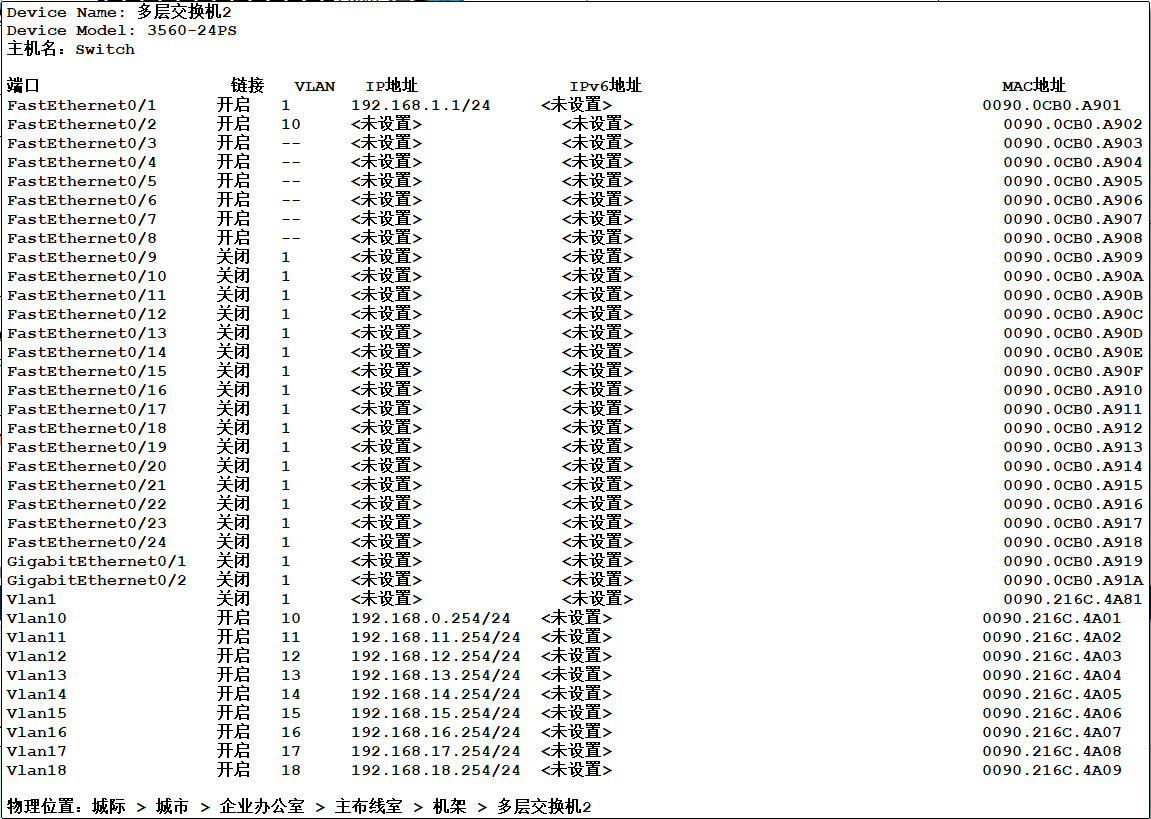


图3.4.3：多层交换机的配置

路由器的配置：

路由器是连接局域网和互联网的设备，需要配置IP地址、子网掩码、默认网关、静态和动态路由、端口转发等参数，以便实现互联网的访问和安全保护。



图3.4.4：路由器配置VPN



图3.4.5：路由器配置端口

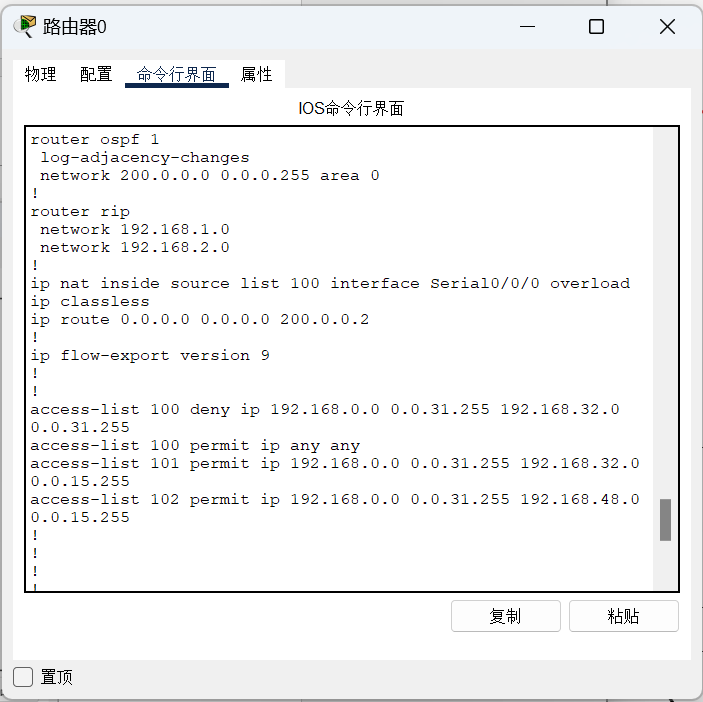


图3.4.6：路由器配置路由协议，NAT以及ACL

服务器的配置：

服务器是局域网中提供服务的设备，需要配置IP地址、子网掩码、默认网关、DNS服务器、防火墙等参数，以便实现服务的提供和安全保护。

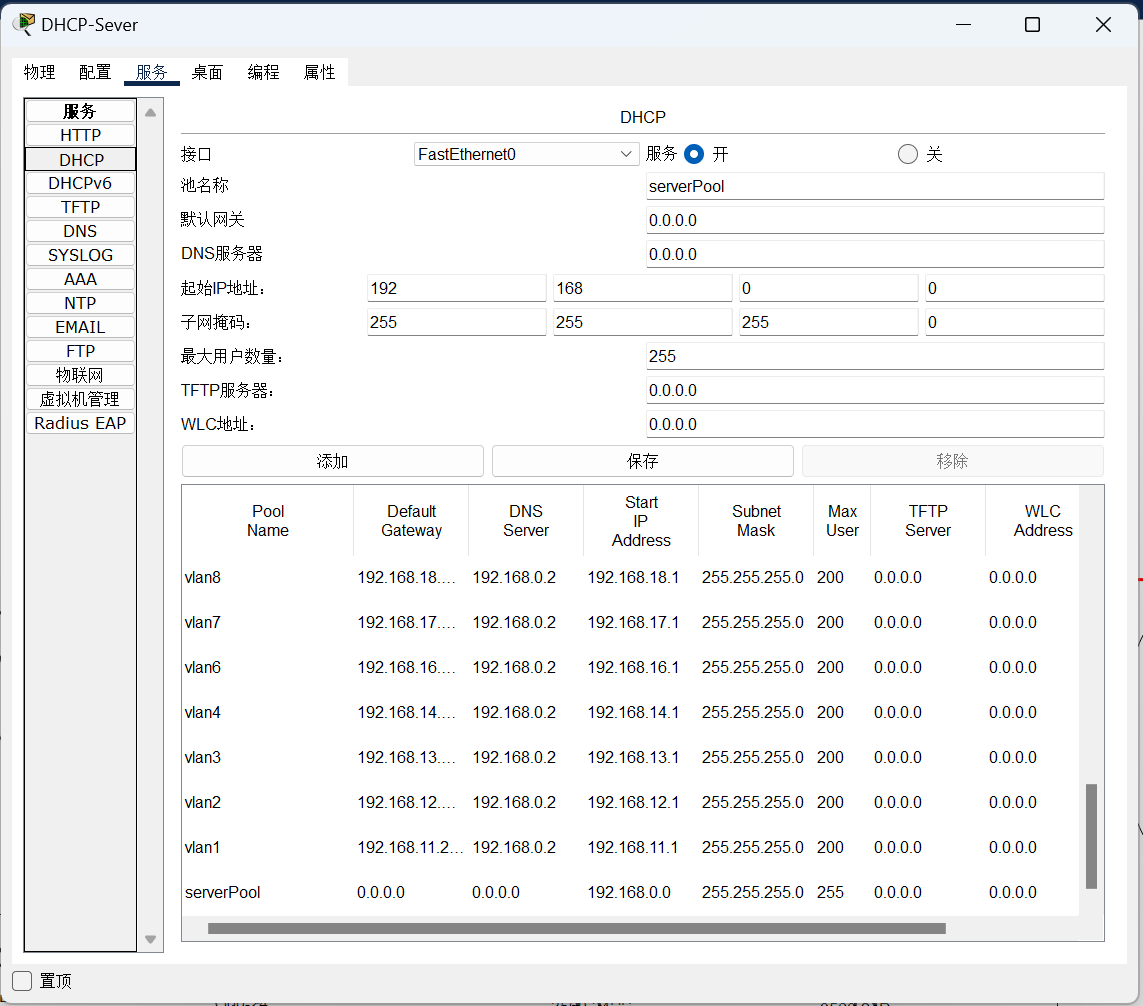


图3.4.7：DHCP服务器配置

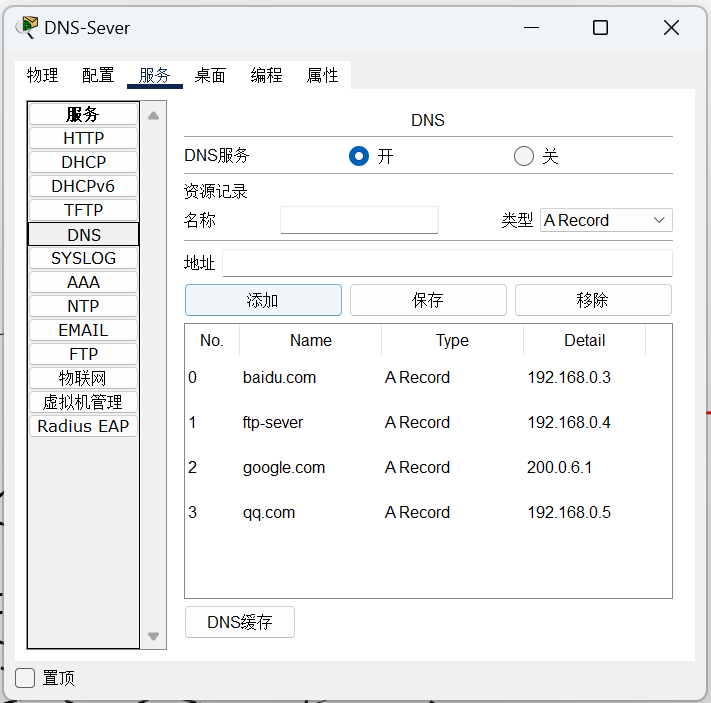


图3.4.8：DNS服务器配置

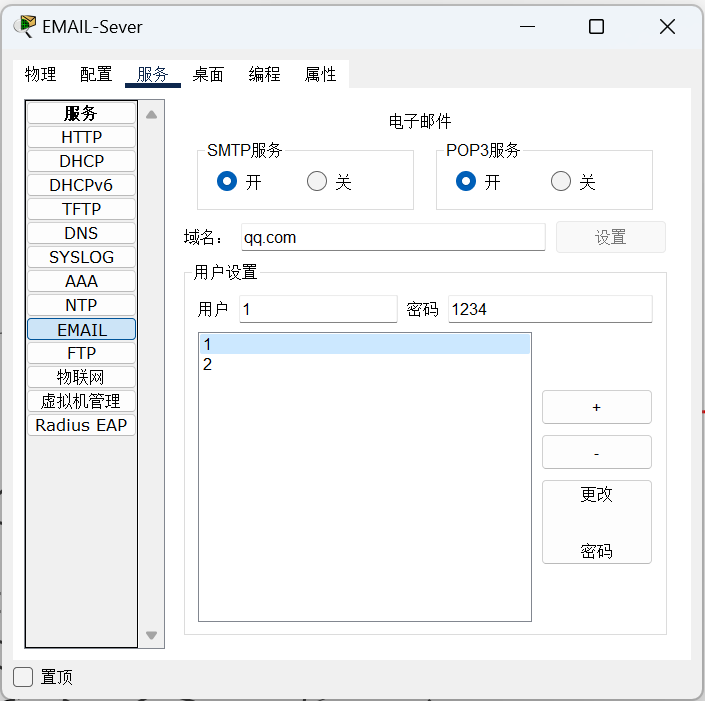


图3.4.9：EMAIL服务器配置

以上就是中小型企业网络硬件的大体配置过程，需要根据实际情况进行调整和优化。在配置过程中，需要注意网络安全、性能和可靠性等方面的问题，以保证网络的正常运行和管理。

下面给出各个设备分配的IP地址：

|  |  |  |  |
| --- | --- | --- | --- |
| 设备名称 | 接口 | IP地址划分 | 子网掩码 |
| 总公司核心多层交换机1 | F0/1 | 192.168.1.1 | 255.255.255.0 |
| 总公司核心多层交换机2 | F0/1 | 192.168.2.1 | 255.255.255.0 |
| 总公司核心路由器 | F0/0 | 192.168.2.1 | 255.255.255.0 |
| 总公司核心路由器 | F0/1 | 192.168.3.1 | 255.255.255.0 |
| 总公司核心路由器 | S0/0/0 | 200.0.0.1 | 255.255.255.0 |
| 分公司1多层交换机1 | F0/1 | 192.168.32.1 | 255.255.255.0 |
| 分公司1多层交换机2 | F0/1 | 192.168.33.1 | 255.255.255.0 |
| 分公司1核心路由器 | F0/0 | 192.168.32.2 | 255.255.255.0 |
| 分公司1核心路由器 | F0/1 | 192.168.33.2 | 255.255.255.0 |
| 分公司1核心路由器 | S0/0/0 | 200.0.1.1 | 255.255.255.0 |
| 分公司2多层交换机1 | F0/1 | 192.168.48.1 | 255.255.255.0 |
| 分公司2多层交换机2 | F0/1 | 192.168.49.1 | 255.255.255.0 |
| 分公司2核心路由器 | F0/0 | 192.168.48.2 | 255.255.255.0 |
| 分公司2核心路由器 | F0/1 | 192.168.49.2 | 255.255.255.0 |
| 分公司2核心路由器 | S0/0/0 | 200.0.2.1 | 255.255.255.0 |
| 总公司本地ISP路由器 | S0/0/0 | 200.0.0.2 | 255.255.255.0 |
| 总公司本地ISP路由器 | S0/0/1 | 200.0.3.2 | 255.255.255.0 |
| 分公司1本地ISP路由器 | S0/0/0 | 200.0.1.2 | 255.255.255.0 |
| 分公司1本地ISP路由器 | S0/0/1 | 200.0.4.2 | 255.255.255.0 |
| 分公司2本地ISP路由器 | S0/0/0 | 200.0.2.2 | 255.255.255.0 |
| 分公司2本地ISP路由器 | S0/0/1 | 200.0.5.2 | 255.255.255.0 |
| ISP路由器 | S0/0/0 | 200.0.3.1 | 255.255.255.0 |
| ISP路由器 | S0/0/1 | 200.0.5.1 | 255.255.255.0 |
| ISP路由器 | S0/1/0 | 200.0.4.1 | 255.255.255.0 |
| ISP路由器 | F0/0 | 200.0.6.254 | 255.255.255.0 |

以上各项配置完成之后, 验证是否配置成功, 可以用ping命令, 或者在PT模拟器中选择Simulation模式, 然后添加协议数据单元 (PDU) , 模拟各终端数据包传输路径, 看是否符合此实验设计的路由规则。[10]

1. **网络物理设计**

## 4.1 传输介质选择

传输介质是构建网络的基础，影响着网络的传输速率、距离和成本。针对中小型企业的网络物理设计，我们考虑以下几种传输介质的选择：

（三层）交换机与（三层）交换机之间、路由器与交换机之间都采用铜交叉线进行连接；

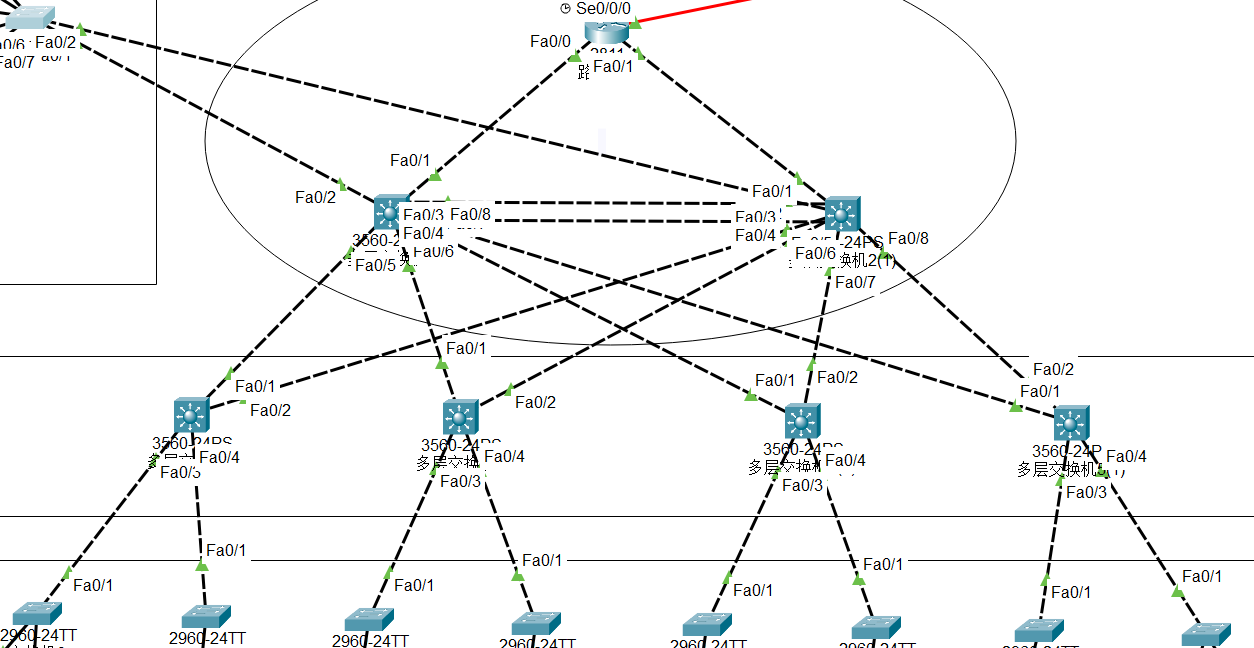


图4.1.1：铜交叉线

交换机与PC机，交换机与服务器之间用铜直通线进行连接。

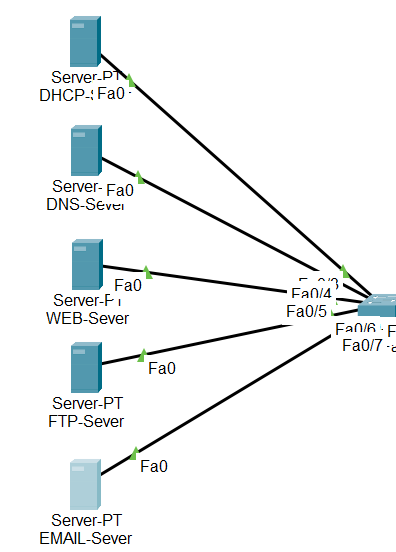


图4.1.2：铜直通线

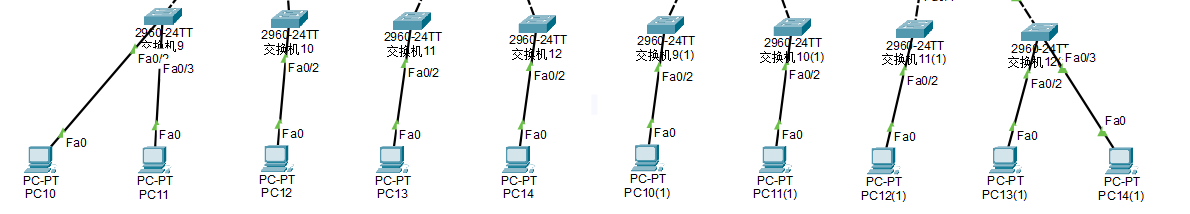


图4.1.3：铜直通线

ISP路由器间长距离通信用串行DCE，串行DTE进行连接。串行DCE(Data Communications Equipment)是指传输数据的设备，如调制解调器(Modem)、集线器(Hub)或网桥(Bridge)，它们提供的服务是将数据从一台计算机传输到另一台计算机或网络设备上，同时实现数据的编码、解码、错误检测和纠正等功能。DCE设备通常被连接到电话线或其他通信线路上，作为物理连接的一部分。串行DTE(Data Terminal Equipment)是指数据终端设备，如计算机、打印机、终端或路由器等，它们提供的服务是将数据传输到DCE设备或其他计算机上。DTE设备通常拥有串行接口(Serial Port)，可用于连接到DCE设备或其他DTE设备上，通过物理线路实现数据传输。在串行通信中，DTE设备与DCE设备之间需要通过物理线路建立连接，通过交换数据来实现通信。例如，一个计算机通过调制解调器将数据传输到远程计算机上，计算机是DTE设备，而调制解调器是DCE设备。

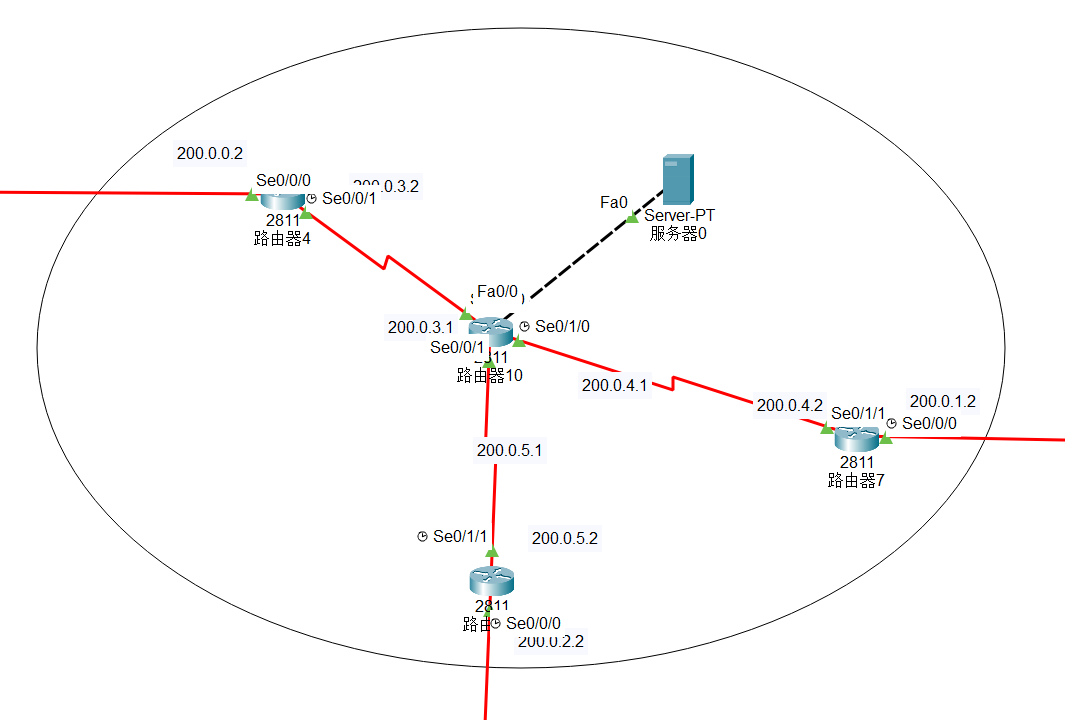


图4.1.4：串行DCE，串行DTE

## 4.2 综合布线设计

综合布线是指将各种传输介质、设备、端口连接在一起，形成网络的物理结构。综合布线设计的合理与否直接影响到网络的稳定性和可靠性。

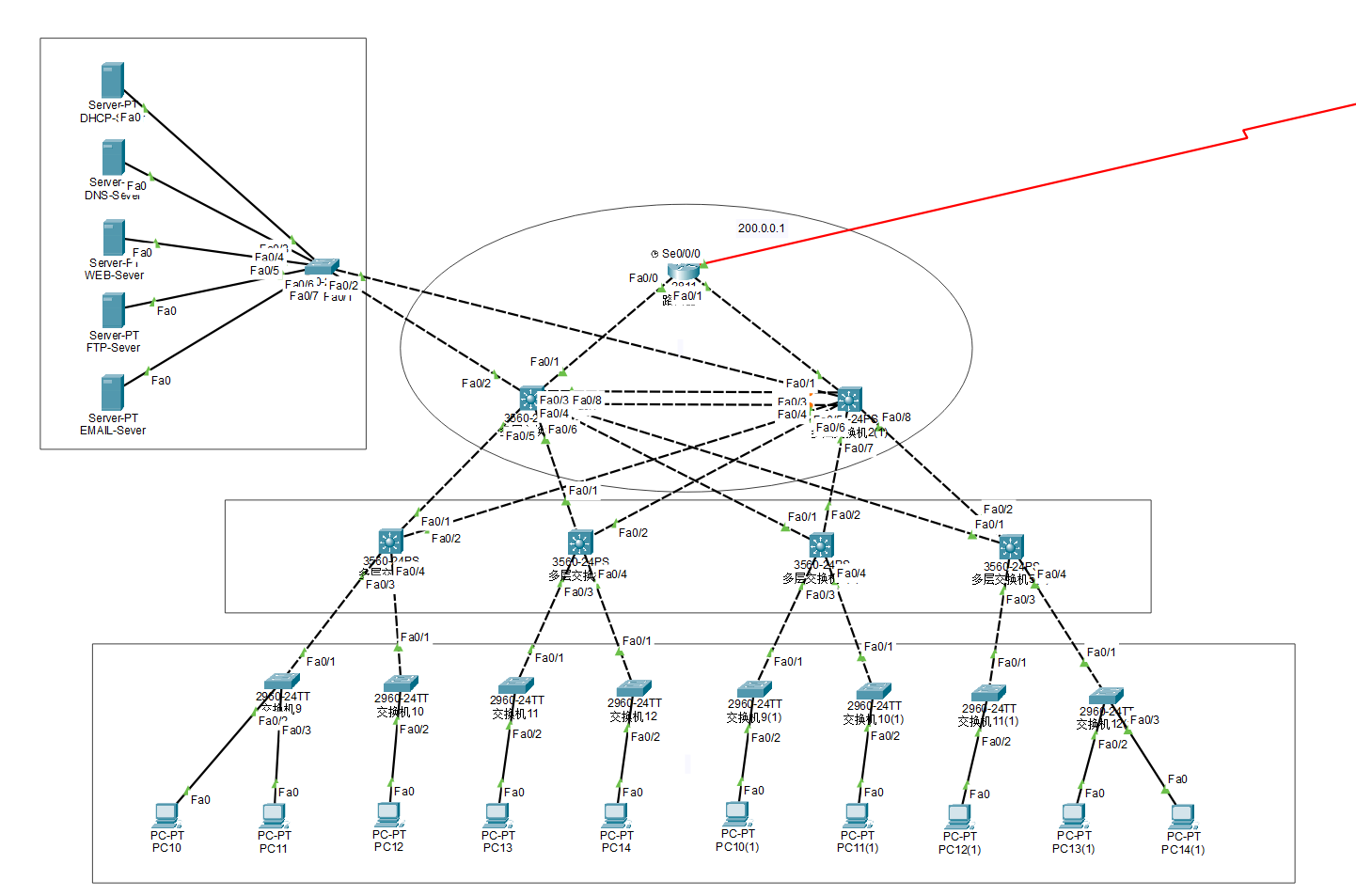


图4.2.1：总公司整体综合布线

针对本企业，采用星型布线结构。将所有的终端设备连接到交换机上，再将交换机连接到核心交换机，形成一个星型结构。这种布线结构的优点是易于维护和管理，当某一台设备发生故障时，只需更换故障设备，不会影响其他设备的正常工作。

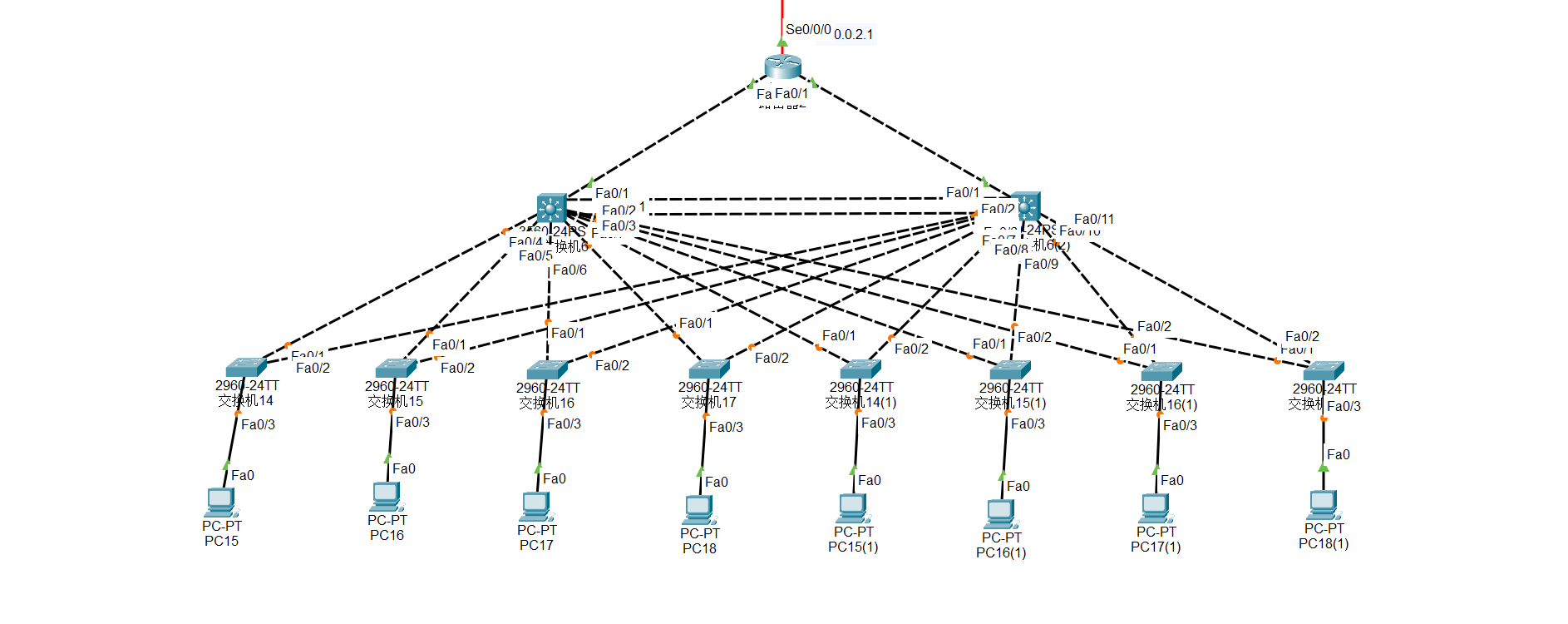


图4.2.2：分公司整综合布线

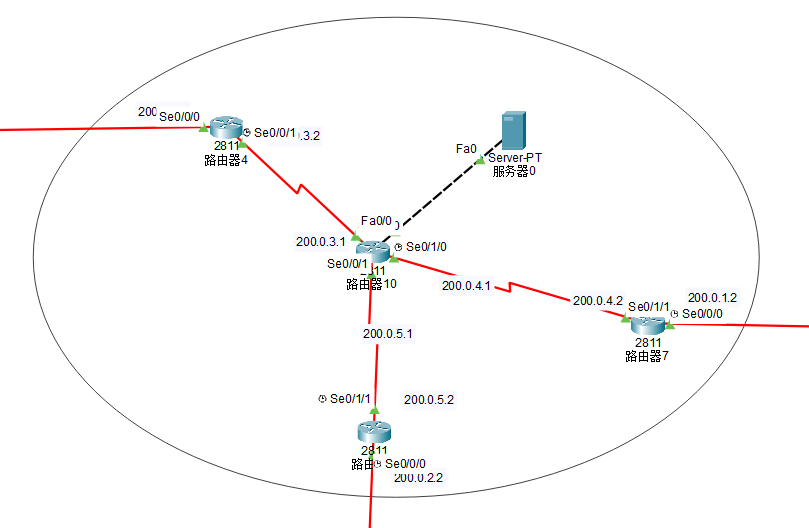


图4.2.3：模拟外部综合布线

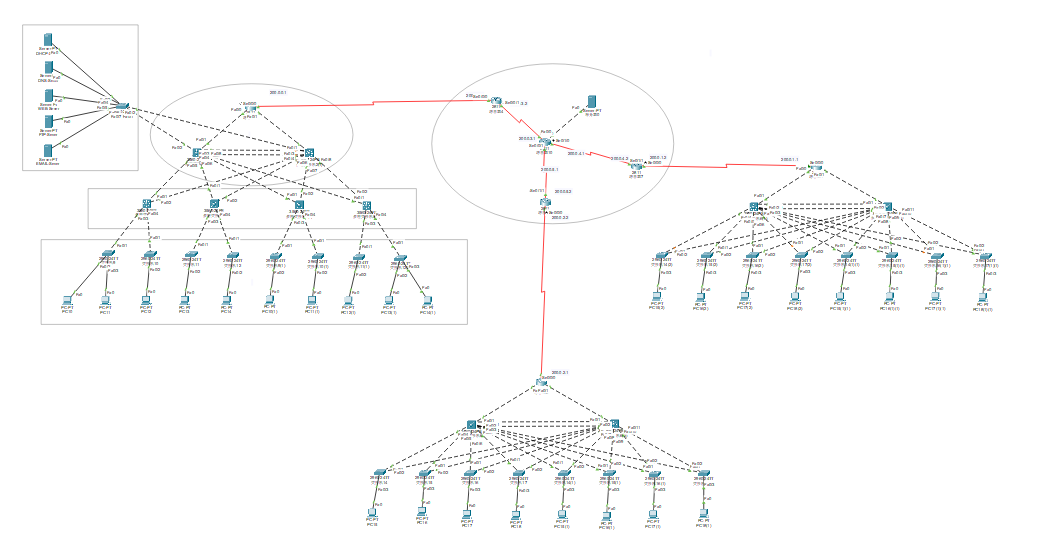


图4.2.4：系统整体综合布线

1. **系统测试**

**5.1 服务器与各个 PC 机的连通性测试**

DHCP服务测试：经过测试，总公司和分公司的PC机都可以通过DHCP的方式来动态获取IP地址。下面给出示例：

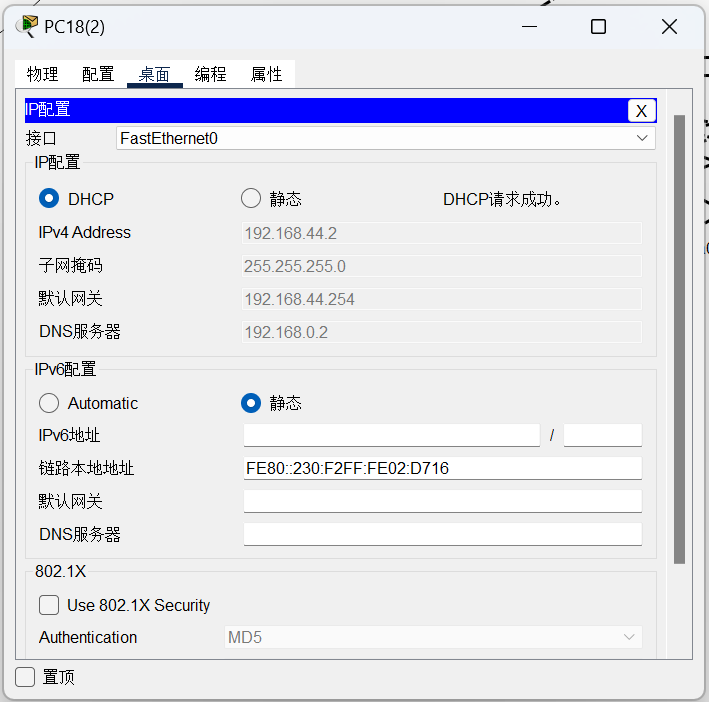


图5.1.1：DHCP服务测试

邮件服务测试：经过测试，总公司和分公司的PC机都可以连接电子邮件服务器，并通过电子邮件服务器来收发电子邮件。下面给出示例：



图5.1.2：邮件服务测试：发邮件

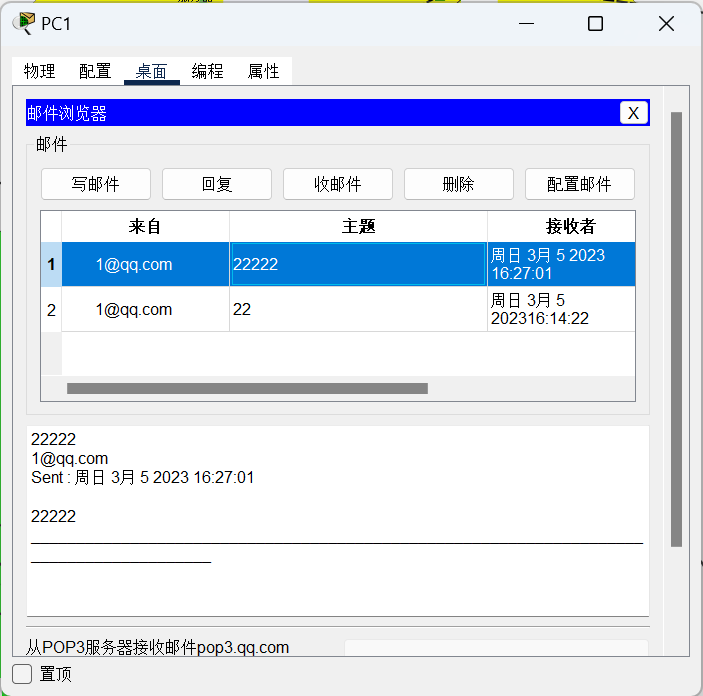


图5.1.3：邮件服务测试：收邮件

Web服务，DNS服务测试：经过测试，总公司和分公司的PC机不仅可以访问内网web服务器，还可以访问外网的Internet服务器。下面给出示例：

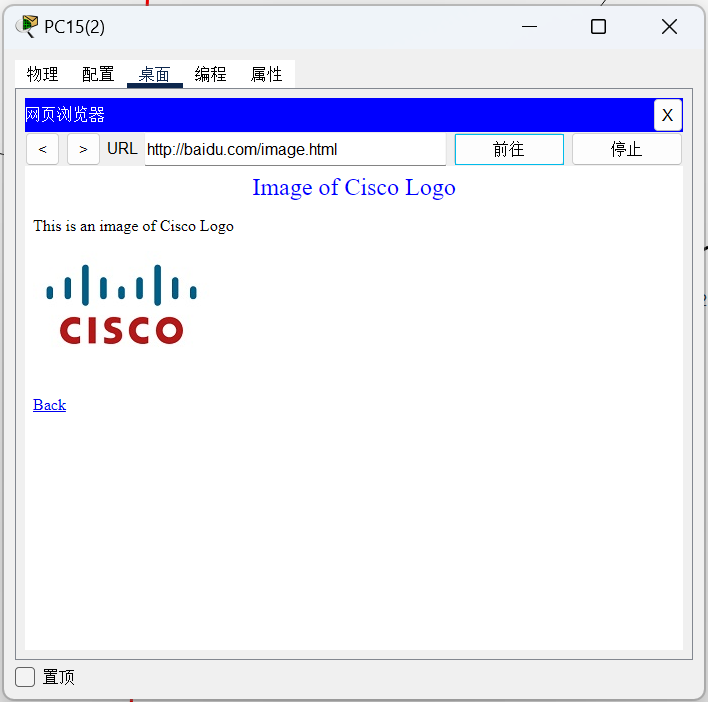


图5.1.4：访问内网web服务器成功，DNS工作正常

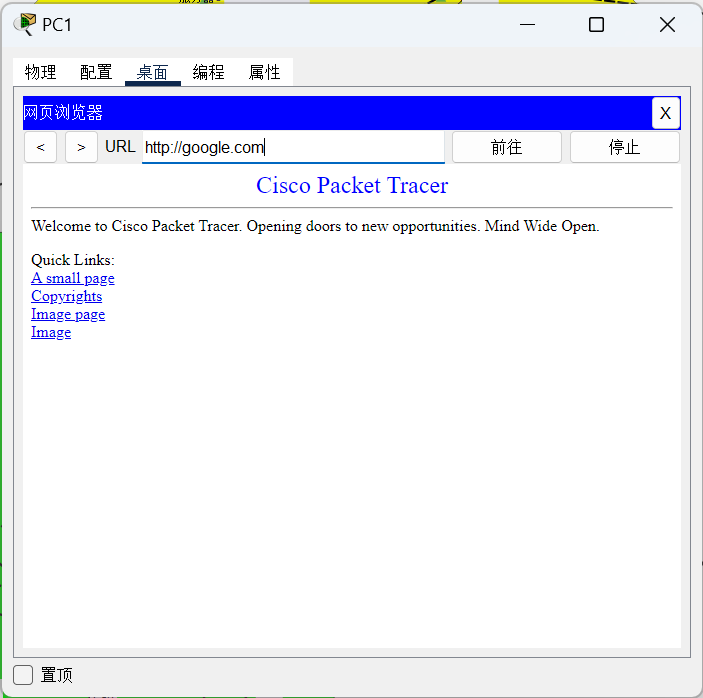


图5.1.5：访问外网web服务器成功，DNS工作正常

FTP服务测试：经过测试，总公司和分公司的PC机可以访问内网的FTP服务器，但是外网无法访问公司内部FTP服务。下面给出示例：

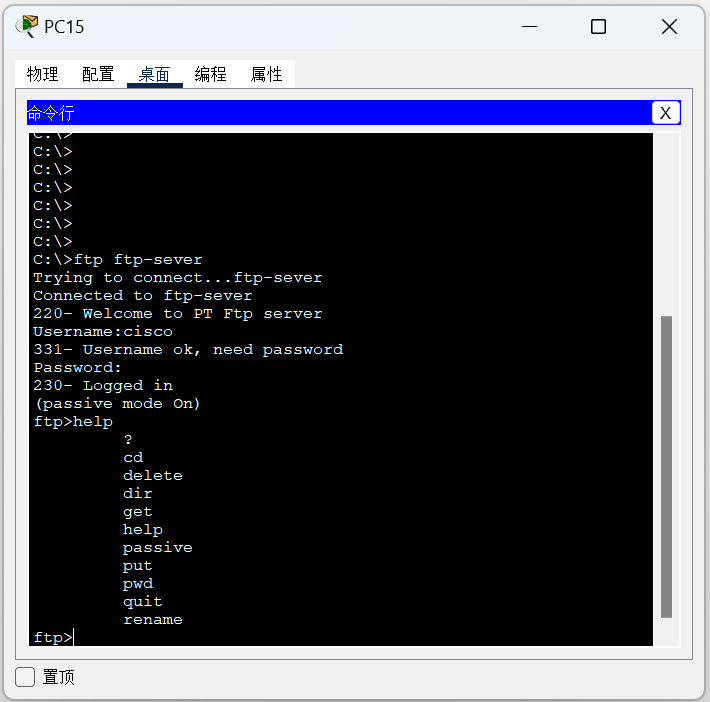


图5.1.5：公司内部可以连接FTP服务

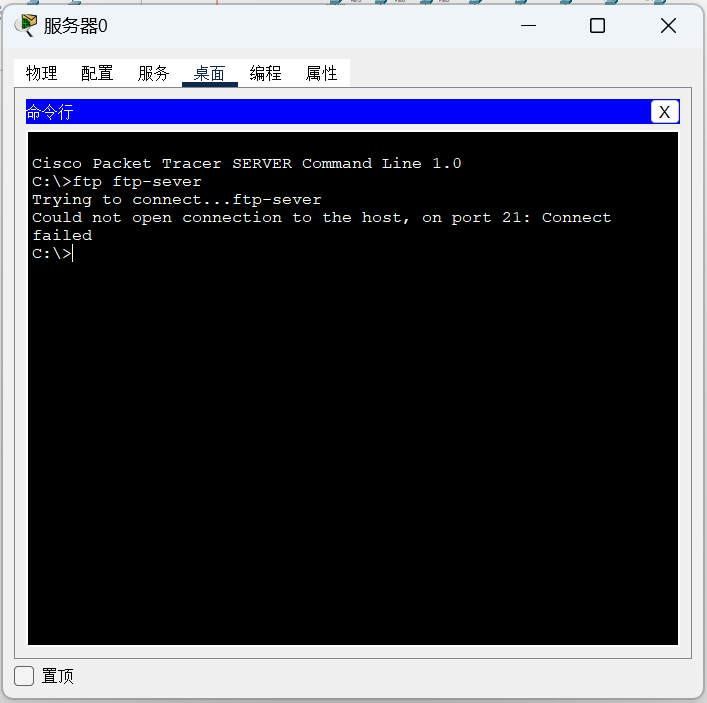


图5.1.5：外网无法访问公司内部FTP服务

## 5.2 PCi与其它 PC 机的连通性测试

Vlan内的通信测试：结果测试vlan内部可以正常通信，下面给出示例：

从192.168.11.1向192.168.11.2发送数据，可以正常通信：

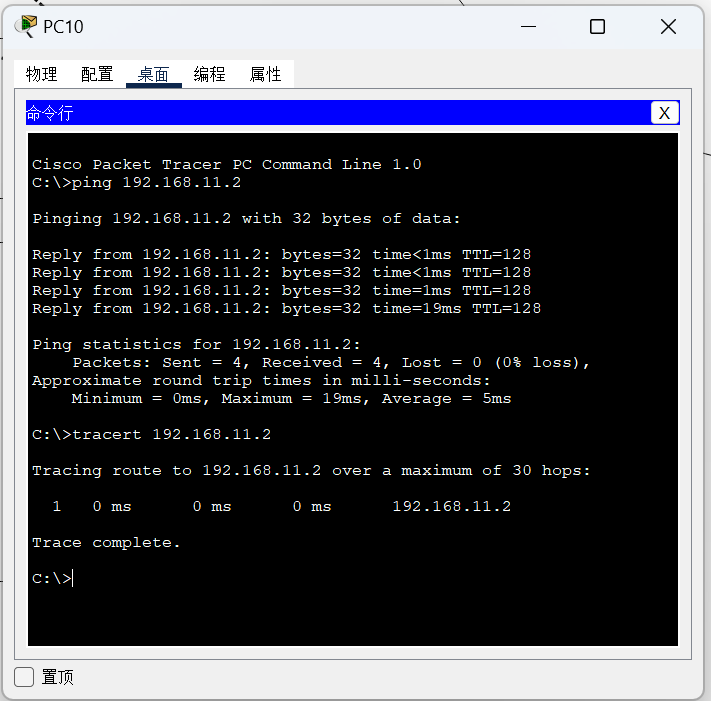


图5.2.1：Vlan内通信

跨Vlan的通信测试：结果测试跨vlan可以通过三层交换机正常通信，（当然，也可以通过ACL访问控制列表来限制vlan间数据的交互[11]）下面给出示例：

从192.168.11.2向192.168.18.1发送数据，可以正常通信：

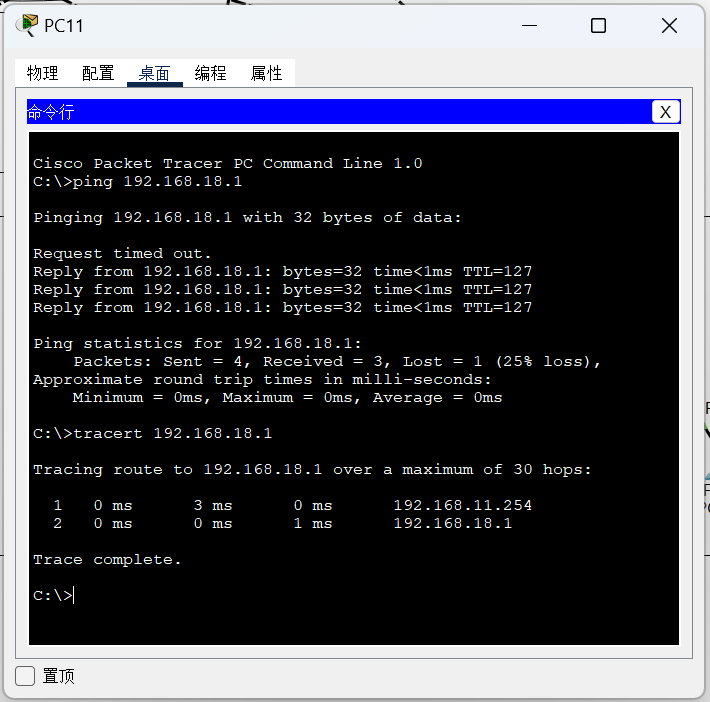


图5.2.2：跨vlan通信

总公司和分公司之间的通信测试：结果测总公司和分公司之间可以通过VPN正常通信，下面给出示例：

从192.168.12.1向192.168.41.1发送数据，可以正常通信：

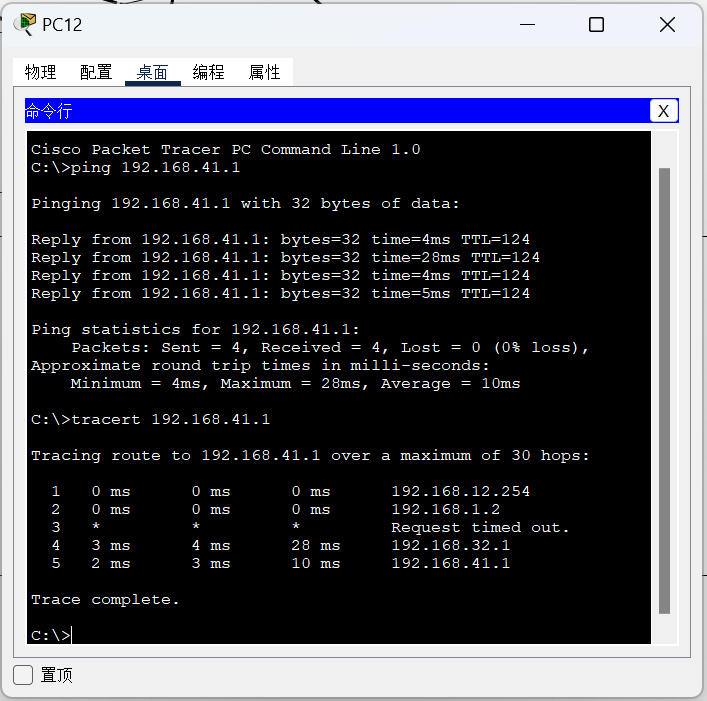


图5.2.3：总公司和分公司之间通过vpn来通信

总公司和分公司之间的通信测试：结果测分公司之间可以通过VPN正常通信，下面给出示例：

从192.168.41.1向192.168.51.1发送数据，可以正常通信：

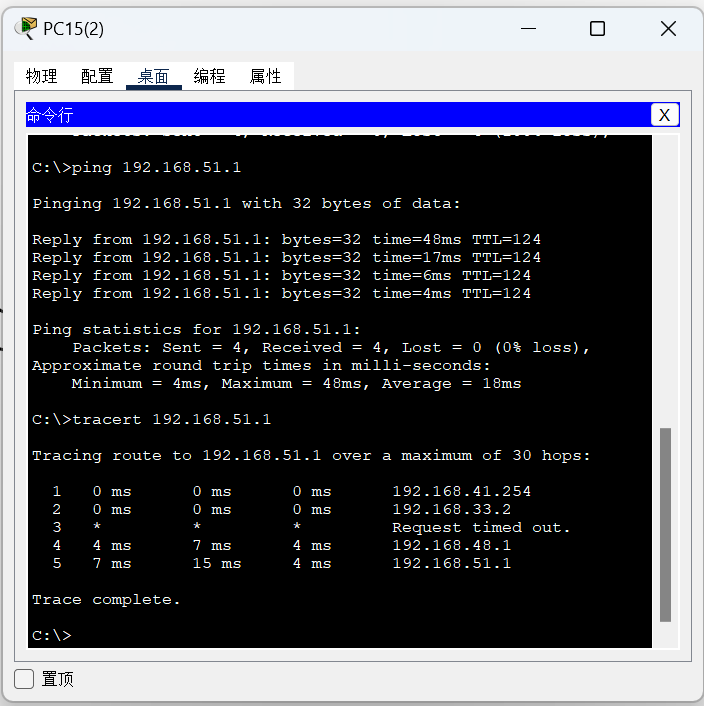


图5.2.4：分公司之间通过vpn来通信

## 5.3 测试及分析中的注意事项

系统测试是在软件开发或系统集成后进行的一种测试，目的是验证整个系统是否按照规格要求工作。对于中小型企业网络来说，系统测试的重要性不言而喻。

Ping和Tracert是两个常用的网络诊断命令，它们通常用于检查网络连接问题和确定数据包传输路径。Ping命令是一种网络诊断工具，用于测试与另一台计算机之间的连接。Ping命令通过发送一个ICMP回显请求数据包到目标计算机并等待它的响应，以确定与目标计算机的连接状态。Ping命令将返回有关目标计算机的一些基本信息，如响应时间、数据包传输成功率等。Ping命令也可以用于确定网络问题的根本原因，如路由器、交换机或网线的问题。Tracert命令也是一种网络诊断工具，用于确定数据包从本地计算机到目标计算机的传输路径。Tracert命令通过向目标计算机发送一系列的数据包，并在每个中间路由器的路径上绘制路径，从而确定数据包的传输路径。在命令行中输入"tracert"命令，后面跟随目标计算机的IP地址或主机名即可使用。Tracert命令将显示从本地计算机到目标计算机的路径，包括中间路由器和跃点。在确定数据包的传输路径方面，Tracert命令也可以用于排除网络问题，并确定需要优化或解决的问题。

总之，Ping和Tracert命令是非常有用的网络诊断工具，可以用于检查网络连接问题、确定数据包传输路径等。在网络管理和故障排除中，这两个命令是必不可少的。

在本系统的测试过程中，通过客户终端Ping命令，Tracert命令和客户端浏览器访问服务器网站的反馈,可以判断这次实验的成功性和可行性。此外，必须使用ip routing命令开启三层交换机的路由功能, 这是实现vlan间数据转发的关键. [12]

1. **网络其他设计**

## 6.1 性能设计

首先在网络拓扑结构方面，对于中小型企业网络，我们采用星型拓扑结构，其中所有的计算机都直接或间接地连接到一个核心交换机，交换机与路由器相连，连接到Internet。采用星型拓扑结构可以使网络更加稳定和可靠，同时也可以方便管理和维护。

其次在网络设备选择和配置方面，在选择网络设备时，需要考虑设备的性能和可靠性，包括处理器、内存、接口等方面。对于核心交换机和路由器，需要支持链路聚合和负载均衡等功能，以提高网络的性能和可靠性。

在网络带宽和传输介质方面，中小型企业网络采用千兆以太网作为传输介质，以满足网络的高速传输需求。对于带宽的设计，根据企业的实际需求进行合理的规划和分配，保证网络的稳定性和可靠性。

在网络搭建成本与性价比方面，本系统采用了NAT技术，NAT是一种常用的网络技术，其作用是将一个网络的IP地址转换为另一个网络的IP地址，从而实现两个网络之间的通信。在中小型企业网络中，NAT技术也被广泛应用，因为它可以有效地保护内部网络，同时实现与外部网络的连接和通信。

NAT的原理非常简单，就是将内部网络的IP地址转换为外部网络的IP地址，从而实现两个网络之间的通信。在NAT技术中，一般会使用一台NAT设备来完成转换操作。NAT设备一般会拥有两个网络接口，一个连接内部网络，一个连接外部网络。当内部网络的计算机需要访问外部网络时，它们会向NAT设备发送请求，然后NAT设备会将请求的IP地址进行转换，然后再将请求发送给外部网络。当外部网络的计算机需要访问内部网络时，NAT设备会将请求的IP地址进行转换，然后再将请求发送给内部网络。



图6.1.1：内网主机访问外网服务器时的NAT转换



图6.1.1：外网服务器响应内网主机时的NAT转换

在中小型企业网络中，使用路由器来实现NAT功能。在进行NAT配置之前，需要先配置内部网络。首先，需要将内部网络的IP地址设置为私有IP地址。其次，需要为内部网络设置网关地址，网关地址为路由器的内部IP地址。在配置NAT功能时，需要将路由器的外部接口和内部接口连接到对应的网络中。然后，需要启用NAT功能，并将内部网络的IP地址和外部网络的IP地址进行映射。一般来说，路由器都内置了NAT功能，只需要在路由器的配置界面中进行设置即可。

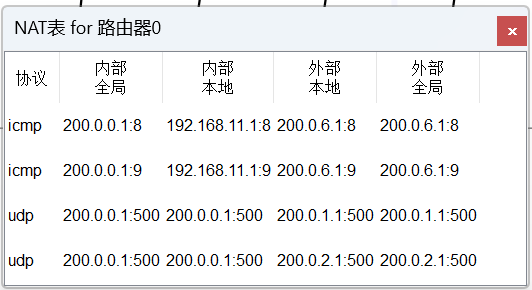


图6.1.3：路由器上的NAT表

NAT技术的主要作用是保护内部网络，同时实现与外部网络的连接和通信。具体来说，NAT技术可以实现以下几个方面的作用：

隐藏企业内部网络结构：NAT技术可以将企业内部的私有IP地址转换成公网IP地址，从而隐藏了企业内部网络的结构，防止攻击者直接针对企业内部网络进行攻击。减少公网IP地址的使用：中小型企业的公网IP地址数量有限，使用NAT技术可以将内部网络的私有IP地址转换成公网IP地址，从而减少了企业使用公网IP地址的数量。

方便网络管理：使用NAT技术可以将企业内部网络的IP地址空间和公网IP地址空间分离，方便网络管理员管理内部网络和外部网络之间的通信。

降低网络攻击的风险：使用NAT技术可以将内部网络的IP地址隐藏起来，减少攻击者对企业网络的攻击风险。

总之，NAT技术对于中小型企业网络的安全、可靠性和管理方面都具有非常重要的意义，是中小型企业网络设计中不可或缺的一部分。

## 6.2 安全性设计

为了实现总公司和两个异地分公司之间的通信，本系统采用了VPN技术。VPN（虚拟专用网）是一种通过公共网络建立安全通信的技术。在企业网络中，VPN常用于远程访问、跨地区联网、分支机构接入等应用场景。针对中小型企业网络需求，可以采用VPN技术实现总公司与两个分公司之间的通信，确保通信安全和稳定性。

VPN的原理是通过在公共网络上建立安全隧道，将通信数据进行加密，确保数据的机密性和完整性。VPN技术可以基于不同的协议和技术实现，包括PPTP（点对点隧道协议）、L2TP（第二层隧道协议）、IPSec（Internet协议安全）等等，本系统采用的是IPSec协议。



图6.2.1：进入VPN隧道，IP数据报加密并封装上一个新的IP首部



图6.2.2：出 VPN隧道，IP数据报解密还原

配置VPN时需要注意以下几个方面：VPN隧道的建立：需要定义VPN隧道的参数，包括隧道类型、隧道协议、本地和远程地址等。安全认证：需要选择合适的安全认证方式，如预共享密钥、数字证书等，以确保数据传输的安全性。数据加密：需要选择合适的加密算法和密钥长度，以确保数据传输的机密性。访问控制：需要对VPN用户进行身份验证，并根据需要限制用户访问的资源和服务。



图6.2.3：本系统VPN配置

VPN技术的作用主要有以下几个方面：数据安全性：VPN技术通过加密和认证确保通信数据的安全性，防止敏感数据被窃取或篡改。隐私保护：VPN技术可以隐藏通信数据的源地址和目的地址，保护用户隐私。跨地区联网：VPN技术可以通过公共网络连接不同地区的网络，方便企业间的跨地区协作和资源共享。  
远程访问：VPN技术可以实现用户在任何地点访问企业网络资源，提高员工工作效率。成本节约：VPN技术可以代替传统的专线连接，降低网络成本。

在企业网络中，VPN技术的重要性不言而喻。随着企业规模的扩大和办公场景的多样化，VPN技术已成为企业必备的通信工具。VPN在中小型企业网络中的作用非常重要，它可以提供安全、稳定、高效的远程连接服务，方便企业的远程办公和合作。同时，VPN还可以为企业的信息安全提供保障，避免敏感信息被黑客窃取。因此，在设计中小型企业网络时，VPN的重要性不可忽视。

ACL（访问控制列表）是一种网络安全机制，可用于控制网络流量并保护网络资源免受未授权访问。ACL是基于策略的安全机制，它通过允许或拒绝特定的流量，以实现对网络中的资源和设备的访问控制。通过ACL访问控制列表实现对外网非分公司的访问的拦截。[13]

ACL的原理是通过设置规则表，根据这些规则表来允许或拒绝流量。ACL规则可以根据源IP地址、目的IP地址、端口号、协议类型等多个因素来匹配网络流量，然后根据预先设置的操作（允许或拒绝）来决定是否允许这些流量通过。ACL可以部署在路由器、交换机、防火墙等网络设备上。

ACL的配置方法一般包括以下几个步骤：确定需要控制的网络流量类型，例如IP数据包、TCP数据包等。根据需要控制的流量类型，设置ACL规则，包括匹配条件和操作。部署ACL规则到相应的网络设备上，例如路由器、交换机、防火墙等。验证ACL规则是否正确地实现了网络安全策略。

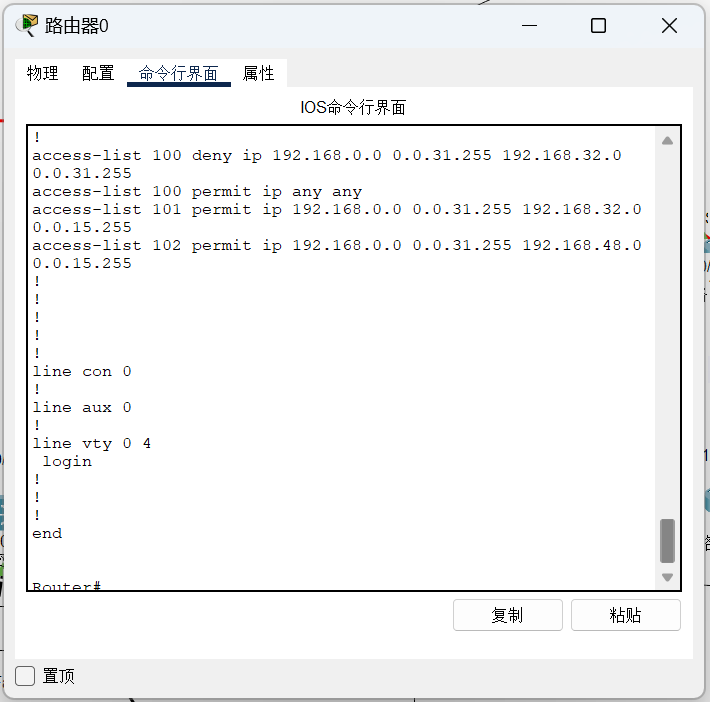


图6.2.4：本系统总公司路由器的ACL配置

ACL的作用包括：

控制网络访问：ACL可以控制特定IP地址、协议类型和端口号的网络流量的访问权限，从而保护网络资源免受未授权的访问和攻击。  
提高网络安全性：ACL可以限制来自恶意用户和攻击者的访问，从而提高网络的安全性。

改善网络性能：ACL可以防止不必要的流量进入网络，从而提高网络性能。ACL在网络安全中具有重要性，它可以帮助网络管理员实现对网络流量的细粒度控制，从而保护网络资源免受未授权访问和攻击。同时，ACL可以帮助企业提高网络性能和优化带宽使用，提高网络的可靠性和稳定性。因此，企业在设计和部署网络时，应该考虑使用ACL来加强网络安全和管理。

## 6.3 可靠性设计

链路聚合是一种将多个物理网络接口捆绑成一个逻辑接口的技术，从而提高网络吞吐量、可靠性和可扩展性。在一个链路聚合组中，多个物理端口会被视为一个逻辑端口来工作。链路聚合技术通过两种方式实现：静态链路聚合和动态链路聚合。在中小型企业网络中，链路聚合用于实现带宽聚合和故障转移。通过将多个物理端口捆绑成一个逻辑端口，链路聚合可以增加带宽并提供冗余，从而提高网络可靠性。如果其中一个物理端口发生故障，数据包可以通过其他可用的物理端口进行传输，从而保证了网络的可用性。另外，链路聚合还可以帮助网络管理员简化网络管理和配置。通过将多个物理端口捆绑成一个逻辑端口，网络管理员可以对整个逻辑端口进行管理和配置，而不需要对每个物理端口进行单独的管理和配置。

在进行链路聚合时，考虑以下几个因素：确定聚合组的大小：需要根据实际需求来确定聚合组中包含的物理端口数量。确定链路聚合控制协议。确定负载均衡算法：需要选择一种合适的负载均衡算法来平衡数据包在多个物理端口之间的分布。常见的负载均衡算法有基于源地址和目的地址的哈希算法、基于MAC地址的哈希算法、基于IP地址的哈希算法等。确定故障转移方式：需要选择一种合适的故障转移方式来保证链路聚合组的可靠性。常见的故障转移方式有主备模式和平衡轮询模式等。链路聚合是中小型企业网络中常用的技术之一，通过将多个物理端口捆绑成一个逻辑端口，可以提高网络带宽、可靠性和可扩展性。

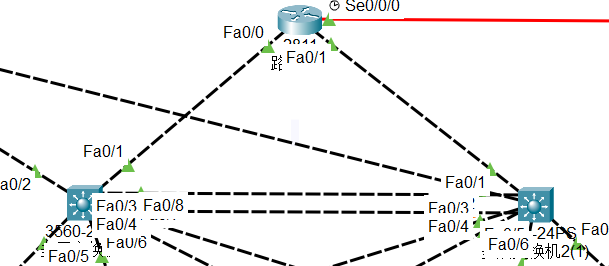


图6.2.4：本系统总公司核心层配置了两台三层交换机

本系统使用传统三层网络架构，通过四个三层交换机构成汇聚层，一个中央路由器和两个三层交换机构成核心层。整体结构简单，维护方便，拓扑结构可以比较轻松的修改。核心三层交的某一条链路断了,其他物理口也在工作,也不会影响传输数据,实现了冗余备份。[14]

1. **总结与体会**

经过本次课设，我对小型计算机网络系统的设计有了更加深入的理解。通过在cisco模拟器上进行相关操作，我深刻认识到了要想设计出高效、稳定的网络架构并不容易，需要深入了解网络拓扑结构、设备选择、IP地址划分、VLAN配置、路由协议、链路聚合、负载均衡、热备份、VPN、NAT、ACL等许许多多的协议和知识点。

在实际操作中，我发现IP地址划分是网络设计中非常重要的一步。只有对网络规模和结构进行准确的估算，才能在后续配置中避免出现冲突和安全隐患。VLAN的配置也是一个需要谨慎处理的环节，需要根据网络实际情况进行灵活配置，确保各部门之间的通讯安全可靠。[15]在交换机和路由器的配置方面，我深刻认识到了不同设备之间的区别和联系，需要根据不同的需求进行合理配置，才能实现网络的高效运转。

本次课程设计考察的知识点比较多，在实际操作中还是有不小难度的。我不断尝试、调试，才勉强将网络连通，并大致完成了课设要求的相关功能。这个过程让我深刻体会到了实践的重要性和挑战，也增强了我对网络设计的兴趣和热情。

当然，毕竟只是模拟设计，实质上依旧存在不少不足之处。例如我没有将所有部门之间的数据访问限制落实，这也是一个需要进一步完善的问题。在系统开发过程中，我们使用了DHCP协议来为每个部门的主机IP地址进行配置。此外，我们还在三层交换机上划分了八个VLAN，并为每个VLAN配置了DHCP、默认网关、通信网段和默认DNS。我们还在每台二层交换机上将对应接口划入相应的VLAN，同时开启另一个接口为trunk模式。此外，我们还发现交换机的路由功能默认关闭，需要用ip routing命令开启交换机的路由功能。在今后的学习和实践中，我会不断积累经验，进一步提升自己的技能水平，力求在网络设计领域取得更加出色的成绩。

通过本次课设，我们巩固了课堂学习到的知识，例如IP地址和子网掩码的划分以及设备间连接线的选取等。除此之外，我们还进行了补充学习，例如NAT技术、VPN技术和ACL技术的实现等。通过该课程设计，我们不仅仅理解了课堂中抽象的概念，还将所学知识具体地应用于生活场景中简单的网络连接中。这使得我们对于知识点的理解不仅仅局限于课堂上，而是实现于设计中的每一根线路的布局、每一台通信设备的选取、每一条控制命令的书写。我们掌握了路由的基本过程及其各阶段的基本原理，熟悉了拓扑图的各种结构与使用过程，了解了路由器与交换机及其相关的原理应用。此外，通过实践和同学一起探讨问题，我们在实验原理与作用上得到更多的体现，明白了控制命令在计算机中是如何执行和产生结果的。最终，我们构建了一个比较完整的网络通讯系统。

此次课程设计使我们深入了解了网络设计和实现的过程，掌握了一些实用的技术和知识，同时也让我们更加清楚地认识到网络设计和实现过程中存在的不足和需要改进的地方。通过实践，我们对所学知识有了更深刻的理解，更加熟练地掌握了一些技术和方法。同时，我们还能够将所学知识应用于实际生活中的网络连接中，更好地理解网络技术的应用和意义。在今后的学习和工作中，我们应该更加注重实践和应用，不断拓展自己的知识和技能，不断提高自己的能力和水平。同时，我们也应该注重团队合作和交流，通过与同学、同事和专业人士的交流和合作，不断学习和进步，共同推动网络技术的发展和应用。

# 参考文献

[1]陈昊阳.中小型企业网络规划设计与解决方案研究[J].长江信息通信,2021,34(11):86-88.

[2]吴国城,左文涛.浅析中小企业网络规划方案设计——以广州园心园林景观设计有限公司为例[J].电脑知识与技术,2020,16(08):282-283.

[3]祝晓明.中小型企业的网络规划与设计[J].大众科技,2009(06):200-201.

[4]张如花,屈正庚.中小型企业网络安全的规划与解决方案的研究[J].微型电脑应用,2020,36(02):1-4.

[5]于子甲.网络仿真模拟器在计算机网络实验课程教学中的应用[J].信息记录材料,2020,21(08):112-114.

[6]朱建帮,何军.基于Cisco模拟器的中小企业网络配置方案设计[J].无线互联科技,2022,19(20):102-105.

[7]孟丽.单臂路由及三层交换机实现VLAN通信的比较[J].电脑知识与技术,2016,12(06):23-25

[8]梅城. 中小企业网络设计研究与实现[D].南昌大学,2012.

[9]吴胜,瞿惠琴.基于思科模拟器的中小企业网络设计[J].电子测试,2021,No.459(06):79-81

[10]李剑辉.计算机网络配置课程中模拟器的应用探索[J].电脑知识与技术,2017,13(14):33-34

[11]刘燕.基于思科模拟器三层交换机实现VLAN间路由实验的设计与实现[J].价值工程,2016,35(14):219-221

[12]冯焕华,任翔,吕尉.基于思科模拟器实现VLAN之间跨设备通信的方案研究[J].云南大学学报(自然科学版),2017,39(S1):36-40.

[13]贾春旺,李旺,岳磊,舒昊.中小型企业网络规划与部署[J].现代经济信息,2019,(05):149-150.

[14]朱玉祥.探讨中小型企业网络的组建[J].信息与电脑(理论版),2015,(16):95-96.

[15]张泉海,黄育雁.基于Packet Tracer构建计算机网络教学实验平台[J].电脑知识与技术,2013,9(17):3960-3962.