广州市乐顺服装有限公司网络设计与规划

摘要: 今广州市乐顺服装有限公司目前所处的时代，正是处于经济全球化的当代时代背景下，全球化已经成为当今世界体系中一颗耀眼的新星。对此，无论是处于全球哪一地理位置的人民来说，都受到其巨大的影响。无论是日常生活习惯，经济商品贸易，还是信息科技技术都亦是如此。本公司多年来线下的销售不断积累了大量的客户资源，不仅在逐渐开拓自己的市场，而且随着现代社会的科技技术的革新和发展，原有的基础的经济的结构发生了重大的改变，为了追随时代的变化并且紧跟跟上时代的步伐，所以公司将目光注重逐渐放在线上批发销售。而线上的批发销售，促进了网络营销的发展，网络上的营销是带给公司或企业另外一个竞争的机会，就算是一个刚刚成立的的企业或者公司也是如此。利用网络科技开展自己线上的销售，一来得到了更多的机会，二来可以提高自己的知名度，服装产品的品牌的知名度。公司所面向业务众多，随着企业对自身定位的不断发展，需要增加的投入管理的，提高办公服务质量的水平的要求不断的增加，并随着客户数量的增加，需要的网络业务的能力也不断提高。为了获取更多的潜在客户，公司将工作的重心从线下的零售销售转变成线上的批发销售。随着公司的不断扩大，各部分之间的分化也显得越来越细致，所以各部门之间需要用 VLAN 来划分。

目前公司的建设正处于疫情阶段，各个方面的资金都普遍欠缺，为了维持企业的正常运转，公司高层管理人员决定在满足企业运行所需的基本情况下，尽量减少开销支出。
在完成公司有限的资金下进行网络规划的同时，尽最大限度来满足公司各方面的最基本网络需求。完成有线网络以及无线网络的融合组网，能够实现公司总部与分企之间的通过 VPN 专用的通道来传输。

关键字：VLAN，网络规划，无线，VPN

Guangzhou leshun clothing co., LTD. Network design and planning

Abstract: At present, guangzhou leshun clothing co., ltd. is in the era of economic globalization, which has become a shining star in the current world system. This has a huge impact on people in all geographic locations around the world. Whether it is daily life habits, economic goods trade, or information technology technology is the same. The company over the years offline sales to accumulate a large amount of customer resources, not only in the gradually develop their own market, and with the innovation and development of the technology of modern society, the basis of the original economic structure significant changes have taken place in, in order to follow the change of The Times and follow closely keep up with the pace of The Times, so the company to focus the attention gradually online wholesale sales. And online wholesale sales, promote the development of network marketing, the network marketing is to give a company or enterprise another opportunity to compete, even if a newly established enterprise or company is also so. The use of network technology to carry out their own online sales, on one hand to get more opportunities, and on the other hand to improve their own visibility, brand awareness of clothing products. The company is facing a large number of businesses, with the continuous development of the enterprise's own positioning, the need to increase the input management, improve the level of office service quality requirements continue to increase, and with the increase in the number of customers, the need for network business capacity is also constantly improved. To reach more potential customers, the company shifted its focus from offline retail sales to online wholesale sales. With the expansion of the company, the differentiation between the parts is becoming more and more detailed, so the divisions need to be divided by VLAN.

At present, the construction of the company is in the epidemic stage, and there is a general shortage of funds in all aspects. In order to maintain the normal operation of the enterprise, the senior management of the company decides to reduce the expenditure as much as possible while meeting the basic requirements of the enterprise.

Keywords： VLAN · Network planning · wireless · VPN

目　录

1 绪　论

1.1 论文研究背景

广州市乐顺服装有限公司面向业务非常只多，在企业的不断发展下，市场规模的逐步扩大，导致国内业务不断的扩大，需要投入更多的管理，并且同时要求提高办公服务质量的水平能够不断增强，并随着客户数量的增加，需要的网络业务的能力也不断提高。网络科学技术的存在和发展不仅可以帮助公司能够找到，查询，捕获到更多的目标客户，并且也能够发现并获取更多的潜在客户，有了这个业务目标，企业才会有目标和策略。如果企业无法获取到到更多有需求的客户，那么公司的业务能力再高，也不挖掘不到客户，更无法获取客户信息。因为广州市乐顺服装有限公司多年来主要业务是服装的设计和国内市场的销售，所以积累了大量的用户及客户资源，逐渐开拓自己的市场，在目前现代社会的科技技术的革新和发展，原有的经济的结构发生了重大的改变，导致公司为了追随时代的变化能跟上时代的步伐，所以公司将所有迦目光注重逐渐放在线下的服务和线上的营销策略。所以，为了更进一步发展公司，发展公司的市场，公司高层将决定把企业更多的经理和投资放在线上的销售中。虚拟专用（VPN）是一种新发展开来的技术，它不仅可以帮助企业减少的网络日常的升级和维护工作，也可以使 Internet 网上公共网络的资源能够得到非常有效的利用，减少资源的浪费。VPN 技术，就可以让总公司和其他分企之间利用现有的公共网络资源去建立私有专用网络，数据使用安全的加密然后在公共网络中进行信息的传递。使用了 VPN 能够节省成本、进行远程的访问、并且扩展的能力强、方便于以后的管理和实现企业全面上的控制，是为现在目前所处，和未来企业网络发展的趋势。而作为 VPN 技术中有非常重要的 MPLS VPN 技术虽然是目前还是被认为最安全的，但是因为 MPLS VPN 是应用在网络服务商的，但是就目前公司所处的阶段分析，分部公司只是作为未来规划的一部分而已，所以决定采用常用的 GRE VPN，如果以后公司达到了其需要的规模，再使用。

1.2 课题意义

首先是能够保证总公司与分企之间进行数据的有效传输，保障总公司内部网络中各个部门的合理性，能互相隔离有可以进行之间的通信的情况下，满足现中

小型企业的对于网络的需求，在保障目前网络的通信的质量在未来能够进行网络的扩展和部门之间的升级，为公司节省所有的开销成本，在原有的网络上重新设计新的结构，其中分公司为设想阶段。

1.3 研究主要内容

对于目前主要研究的部分和内容，主要是处于针对在一个中小型企业而言，完成其交代的必须完成的工作内容，既完成基本的对于一个企业内部网络的搭建和设备上的选择。根据传统的设计思路，结合实际，从实际中出发，分析搭建一个符合企业需求的拓扑，再根据拓扑和其他应用的需求，实现其要求的功能。例如，在实现基本内网的通信之后，其内部企业的用户主机去访问外网了，为了整个企业内部网络的安全性，防火墙该进行如何处理去实现其要求的功能，并且为其后来网络的扩展需求，去分析 GRE VPN 等技术在未来分企和总部之间的一个数据通信，并且也初步分析 MPLS VPN 技术在众多 VPN 的优越性，和未来的应用。

2 企业网络的需求分析

企业内部一共有 5 个大部门和一个总经理的办公室。其中，总经理室作为其他 5 个部门之首，是公司总部的主要核心，所以可以当成独立的一个部门。其他的部门分别为：行政部，业务部，财务部，咨询部，市场部。公司总部位于广州市增城新塘镇。总经理室与其他所有部门都在同一楼，都属于一个平面层，不存在其他的分楼层段，总公司平面结构如图 2-1 所示：

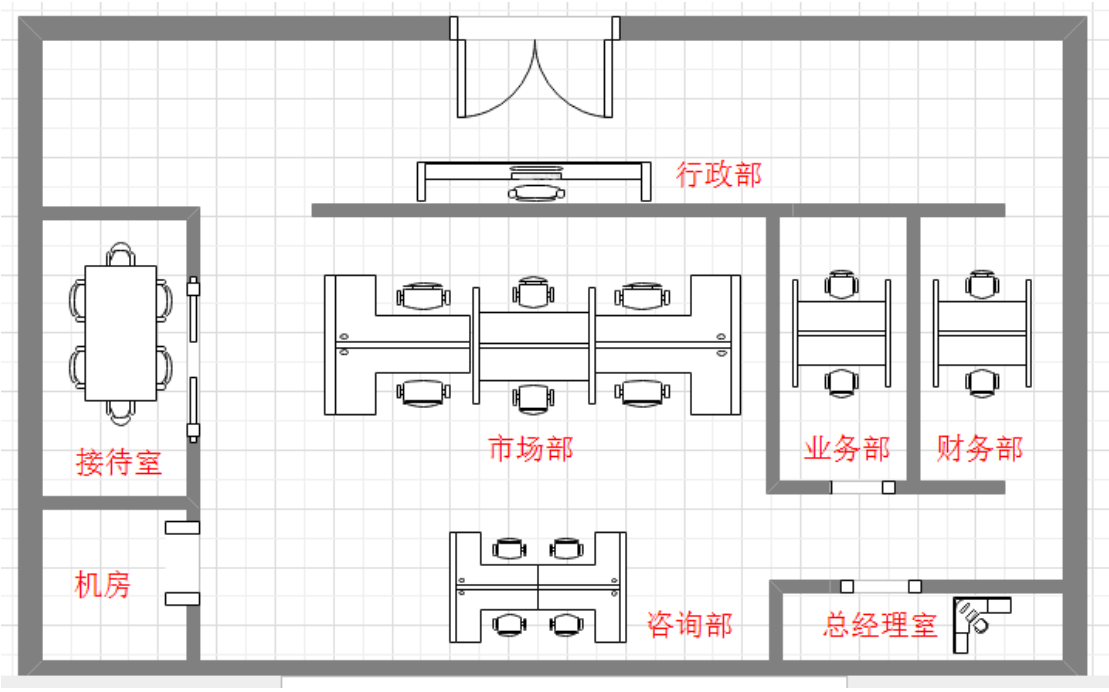


图 2-1 总公司平面结构图

未来规划的分部公司一共分为三个部门，为分公司经理部，运营部及推广部，市场二部，分公司平面结构如图 2-2 所示：

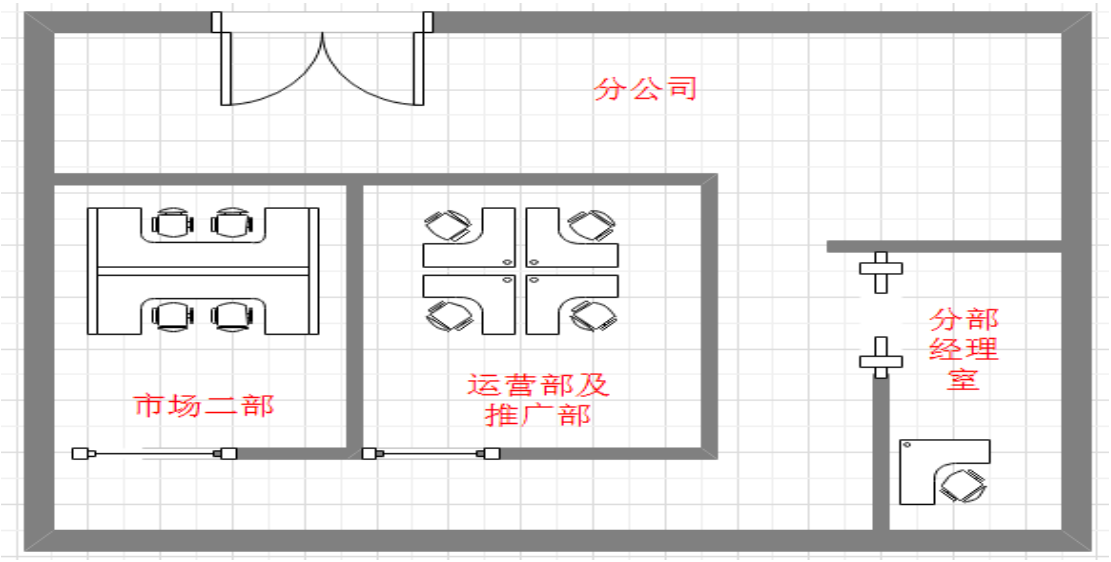


图 2-2 分公司平面结构图

2.1 网络结构分析

因为公司目前的阶段是较小型的公司，所以真正对于公司的实际网络中，决定采用树型拓扑结构，为了节省交换机的端口，并且也是考虑到市场部和行政部的主机需要的比较多的端口，所以市场部和行政部的主机通过集线器再连接到接入层的交换机端口，以节省资源，拓扑结构如下，分公司目前所处阶段只为设想，主要为了配合与总公司总经理部之间的 VPN，所以分公司内部结构进行简化，公司内部网络如图 2-3 所示：

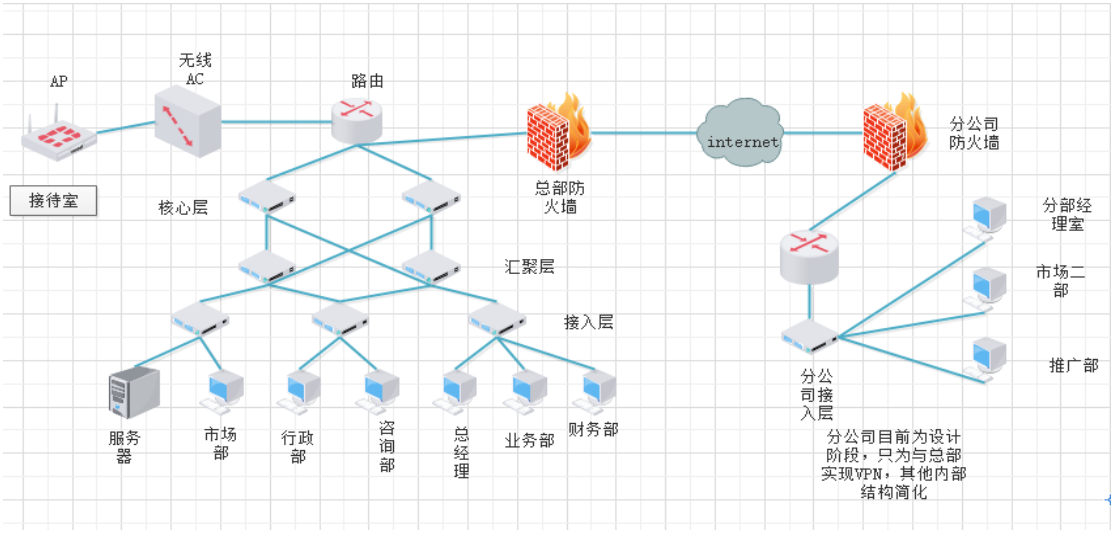


图 2-3 公司内部网络

2.2 网络链路带宽性能分析

企业的内网使用 fast 以太网，传输速率为 100Mbit/s。使用屏蔽超 5 类双绞线。子接入层分别使用二层的交换机，汇聚，核心层采用三层交换机。主干的网络使用常规的光纤接入到外网。

目前条件下，现代的企业网络被要求应该有更高的带宽，具有更强的性能，才能够满足企业业务疯狂增长的基本的通信要求。现在是互联网的天下，所以各种的网络的应用需求普遍增加，今天企业网络的网络已经是成为一个具承载了各种各样信息和业务的平台。不单单是被要求必须完成最基本的企业的办公，包括应用查找一些数据业务，还要去运营和处理公司里面包含的各种业务的数据，所以对于带宽和延时普遍要求都比较高，并且一些企业会要求如疫情期间需要使用网络上的视频会议，网络办公等，这无疑加大了对企业内部网路的需求。因此，流量也必将成倍的增加，尤其会对核心网路会甚至是达到前所未有的要求。

无可厚非，现在企业网路的要求是非常全面的，并且要求企业的网络一定要给办公的员工提供一个非常稳定的网络环境，这样一来，才是对企业员工网络办公的一个最基本的保障，没有这个保障会给客户带来非常差的体验感，会让客户对办公人员产生厌烦，是企业内部的员工无法得到在客户面前好好表现的机会，错失良机。就像最近的现在视屏会议，视频办公，需要一个稳定良好的网络环境，所以现在的企业的稳定性要求必须着重考虑。

2.3 网络安全需求分析

企业内部的网络同时也被要求有更加安全的保障，用来防止网络上不法分子的恶意攻击，渗透，骚扰等，避免企业遭受无端的损失。对此，企业使用常规的操作，在接入外网的路由器上设置了防火墙，防火墙的应用，再加上防火墙上的安全策略，使内网的用户在业务之时，根据需要访问外网 Internet，而外部网络是绝对不允许访问公司的内网。并且财务部的网络不被允许登录外网，一来可以防止下载了恶意的软件或者浏览了什么恶意的网站，使公司的财务遭受损失，二来可以防止爬虫等对财务业务的扒取。避免了公司的遭受不必要的风险，大大的减少了内部网的用户遭受攻击的风险。

本企业是较小型的规模，与其他的普通企业需求差别大，企业内部的网络主要用于对客户的一些个人资料的浏览和保存一些客户的有利用价值的个人信息，和对市场部去挖掘潜在的客户和对市场的一些调查，并且能够与其他的部门之间的进行一些信息的交互。能够支持一些必要的和实时性比较强的如微信，QQ 等一些应用;能够给客户的咨询，和访问提供一个相对来说比较良好的，比较愉悦的环境。

2.4 技术可行性分析

由于公司的所处的地理位置为一个平面，不分楼层，所有的部门都共处一个平面内，所以将决定使用传统的结构，及三层结构，包括接入层，汇聚层和核心层。核心层千兆网应用，然后再将百兆网络接入到桌面来。接入层的信息是二层交换机来接入的，然后再使用 VLAN 划分不同的部门，分隔各个部门，并且在核心层的路由器使用单臂路由，让企业内部的用户不同的部门对应不同的 vlan 之间可以互相访问，对于不同的 VLAN 就使用不同的 IP 地址网段方便日后的管理，使用了 NAT 技术，把内网的私有的 IP 地址映射成公网的 IP 地址，公网的两个地址分别是 210.1.1.3 和 210.1.1.4 另外还用 STP 生成树算法，使用 OSPF 动态路由协议接入到外网。

3 网络逻辑设计

3.1 总公司及分公司拓扑图

总部网络拓扑如图 3-1 所示：

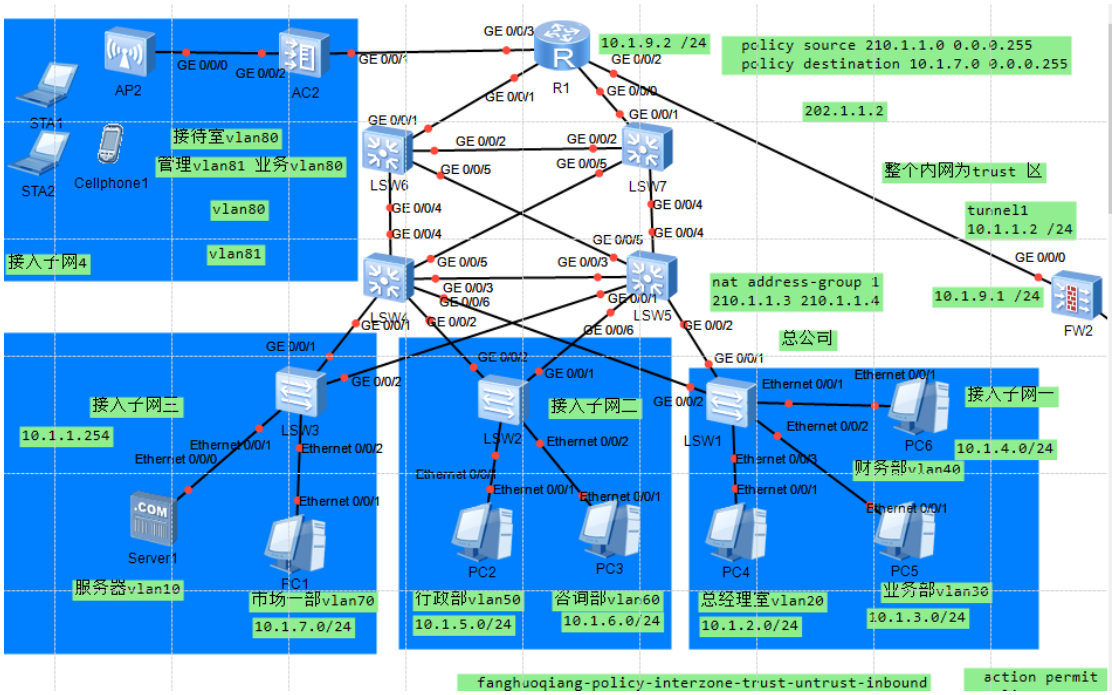


图 3-1 总部网络拓扑图

分公司拓扑图如图 3-2 所示：

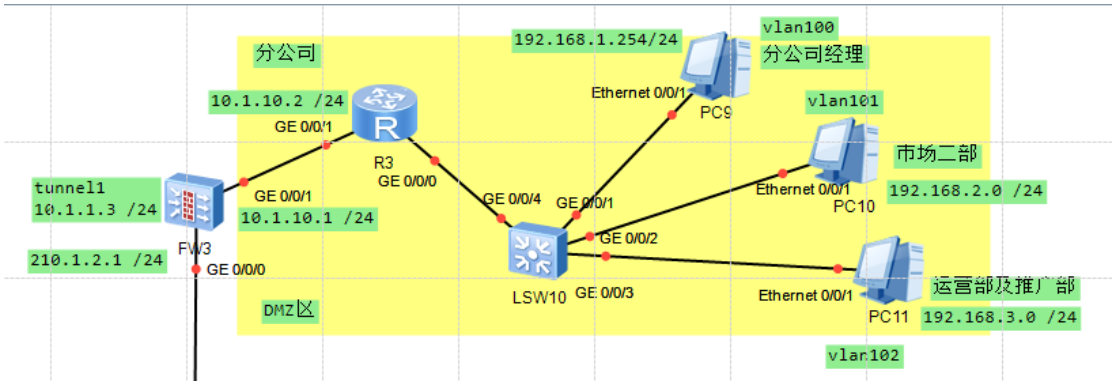


图 3-2 分公司拓扑图

使用路由器模拟接入外网，拓扑如图 3-3 所示:

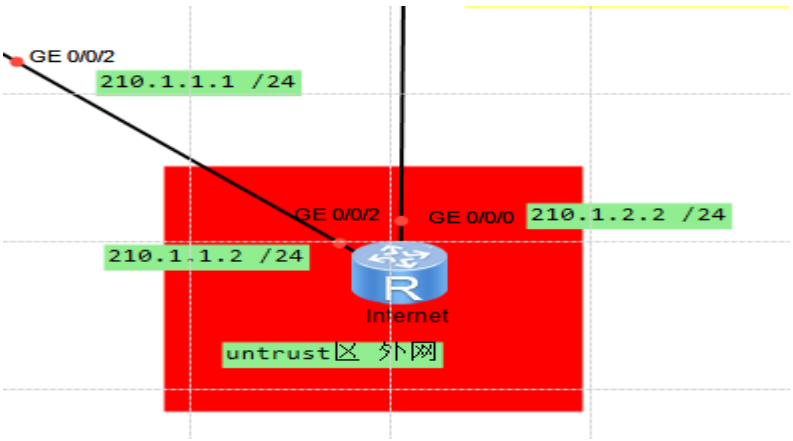


图 3-3 路由器模拟外网

3.2 设备选择

接入层的六个部门（总经理室、业务部、财务部、市场部、行政部、咨询部，接待室，服务器）分别划入八个不同的虚拟局域网 VLAN，子网一为总经理室，业务部和财务部三个部门，咨询部和行政部两个部门归属于子网二。子网三为机房的服务器，市场一部，对于子网三中的市场部共需要 100 台主机左右的网络规模，在分配给服务器和接待室之后（分别为 21 个接入端口）之后，剩下的接入端口提供给市场部使用，市场部对于交换机端口不足的问题使用集线器汇聚之后再接入交换机的端口。在网络的搭建中一共需要 7 台交换机和 1 台路由器接入到外网，实现小型企业网络的搭建，实现高性价比的目标，符合小型企业的需求和节省经济支出的目标。

1. 交换机选择。核心层与汇聚层采用 4 台华为的三层交换机 S5700-48TP-SI-AC9（实物图）:

图 3-9 华为 S5700-48TP-SI-AC9 交换机

参数如表 3-1 所示：

表 3-1 华为 S5700-48TP-SI-AC9 交换机参数

类型	千兆以太网交换机
层级	三层
传输速率	1000Mbps
交换方式	存储转发
背板带宽	256Gbps
包转发率	72MppS
MAC 地址表	16K
端口结构	非模块化
端口数量	52 个
端口描述	48 个 10/100/100Base-T端口，4 个 100/1000Base-x 千兆端口 Combo 口
扩展模块	1 个堆叠扩展插槽
传输模式	全双工

接入层为 3 台华为 S1720-52GWR-4P 交换机（实物图），如图 3-10 所示，参数如表 3-2 所示。

:

图 3-10 华为 S1720-52GWR-4P 交换机

表 3-2 华为 S1720-52GWR-4P 交换机参数

产品类型	网管交换机
传输速率	10/100/1000Mbps

MAC 地址表	16K
端口数量	52 个
端口描述	48 个 10/100/1000Base-T 以太网端口
网络标准	支持 EEE 能效以太网
VLAN	支持
电源电压	100v-240v AC,50-60Hz
电源功率	47.3W
产品尺寸	442×220×43.6mm
扩展模块	1 个堆叠扩展插槽
传输模式	全双工

2.路由器及服务器的选择。接入 Internet 的外网的主干网络使用的路由器华为 AR3260-S 路由器和华为 2288H V5 服务器。接入外网的主干网络采用华为 AR3260-S 路由器 （实图）如图 3-11 所示，参数如表 3-3 所示。

图 3-11 华为 AR3260-S 路由器

表 3-3 华为为 AR3260-S 路由器参数

路由器类型	企业级路由器
端口结构	模块化
其它端口	3×GE(2×Combo)/4×GE Combo+ 2×10GE
扩展模块	4 个 SIC 插槽+2/4 个 WSIC 插槽+4/6 个 XISC 插槽

端口描述	48 个 10/100/1000Base-T 以太网端口
包转发率	6Mpps-40Mpps
产品内存	8GB
产品重量	11kg（不含电源及插卡）
电源电压	100v-240v AC,50-60Hz
电源功率	700W（双电源）
产尺寸	130.5×442×470mm
传输模式	全双工

服务器采用华为 2288H V5 服务器（实图），如图 3-12 所示，参数如表 3-4 所示。

图 3-12 华为 2288H V5 服务器

表 3-4 华为 2288H V5 服务器参数

产品类型	企业级
产品类别	机架式
产品结构	2U
处理器	
CPU 类型	Intel 至强铜牌
CPU 类型	Xeon Bronze 3106
CPU 频率	1.7Ghz
标配 CPU 数量	1 颗
最大 CPU 数量	2 颗

CPU 线程数	八线程
CPU 核心数	八核

3.3 公司网路的设计原则

以满足目前的基本需求为前提，减少不必要的资源的铺张和浪费。将公司的服务器的和路由器交换机等一同放在机房里面，唯一的一台服务器配置将用于DNS，DHCP，以及 FTP 业务等。在服务器中的数据库中存放的客户的资料，可以使用另外的新的硬盘进行备份。

为了方便企业的管理，完成各个部门之间有效的隔离，让每一个部门与总经理室划分不同的 VLAN，可以隔离各个部门之间的相互影响，在核心层的路由器中配置单臂路由，让企业内部不同部门之间的通讯不需要配置动态路由，就可以完成不同 vlan 之间的通信。使用安全策略使内部网络的用户可以访问外网，但是，外网却无法访问内网。这增加内网的安全性，再使用了 nat，所有内部网络的私网地址的主机都被映射成了两个固定的公网 IP 地址,节省了 IP 地址的资源。总经理室的化分 vlan2，ip 地址块 10.1.2.0/24，业务部划分 VLAN3，IP 地址为 10.1.3.0/24，财务部划分 VLAN4，IP 地址为 10.1.4.0/24，行政部划分 VLAN5，IP 地址为 10.1.5.0 /24，咨询部划分 vlan6，IP 地址为 10.1.6.0/24，市场部划分为vlan7,IP地址为 10.1.7.0/24。接待室使用vlan80,IP地址为10.1.8.0/24，服务器固定 IP 地址为 10.1.1.254/24 并且划入 vlan10，内网主干路由器使用 10,1.9.0/24 与防火墙互相连接，防护墙与外网相互连接，其中与防火墙的 untrust 区互相的路由是模拟 Internet 的外网。

根据基础的需求，对应的完成了企业的网络设计。在设计上遵守实用，标准、安全，经济、等原则要求；在设计的方案中给出的设计结构是中使用树形拓扑架构，并且根据经济的可行性选出搭载网络需要的设备，完成设计的总任务和工作；公司网络一共分为 4 个不同的工作子网，每个子网包含不同的所管理的不同的几个部门，保障了企业内部网络的方便管理，为以后网络的日常维护提高了效率，其中各 VLAN 地址划分如表 3-5 所示。

表 3-5 各 VLAN 地址划分

部门	vlan	Ip 地址	网关
总经理室	Vlan20	10.1.2.0/24	10.1.2.1
业务部	vlan30	10.1.3.0/24	10.1.3.1
财务部	vlan40	10.1.4.0/24	10.1.4.1
行政部	vlan50	10.1.5.0/24	10.1.5.1
咨询部	vlan60	10.1.6.0/24	10.1.6.1
市场部	vlan70	10.1.7.0/24	10.1.7.1
接待室	vlan80	10.1.8.0/24	10.1.8.1
机房服务器	Vlan10	10.1.1.254/24	10.1.1.1
接入防火墙的路由		10.1.9.0/24	
接入外网的防火墙		210.1.1.0/24	

4 技术分析与实施

4.1 基本内容配置

服务器配置静态的 IP 地址，固定为 10.1.1.254，配置网关地址为 10.1.1.1 。为接入防火墙的路由器配置接口的 IP 地址：10.1.9.2/24，放火墙的接口的内网网段配置地址：10.1.9.1/24，连接外网路由网段的接口配置为 210.1.1.1/24。其中使用一个路由器模拟外部网络，与总公司相连的网段为：210.1.1.0/24 接口为 210.1.1.2/24，与分公司网段相连的网段是 210.1.2.0/24 ，接口为 210.1.2.2 /24

4.2 虚拟局域网 VLAN

最早的局域网基本上都是使用了总线型的，就是整个拓扑结构由一根单独网络电缆构成的，所有的用户都是通过单独的线接入到这一根总线的。这种拓扑结构虽然简易，但是会暴露出很多的问题，暴露出很多的问题，因为所有用户的主机都是处于同一个冲突域的，如果同一个时间内多台主机同时发送信息，就无法正常进行通信。

为了不让这一情况发生，并且解决这一个问题，能够让多台主机一时间进行通信。所以采用了 vlan，这样一来，处于同一 vlan 中的主机就是同一个冲突域了，其他主机接入在其他的 vlan 中，彼此之间就是隔离冲突域，也可以隔离了广播域。虚拟局域网的是根据 4 个方面去划分的：一是端口，二是 MAC 地址，三是根据网络层，四是 IP 组播。它的出现，解决了广播域的问题，也提高了内网的安全性，不同的 vlan 之间的用户几乎不受其他的影响。

使用了这个技术，大大的提高了网络的安全，因为隔开来之后，互相之间的影响就相对就小。提高了稳定的能力，同时也提高了网络的利用率，也同时保证了网络的保密性和安全性。因为人们通常在使用 vlan 传送一些很保密的数据。需要保密的数据被保证了安全。让一个网络段分成了 n 个不同的广播组，不被允许的用户不可以去访问其他 vlan 中的应用程序。甚至在交换端可以使用基于应用的类型，和访问的特权来为其分组,各部门 VLAN 划分及分布如图 4-1 所示。

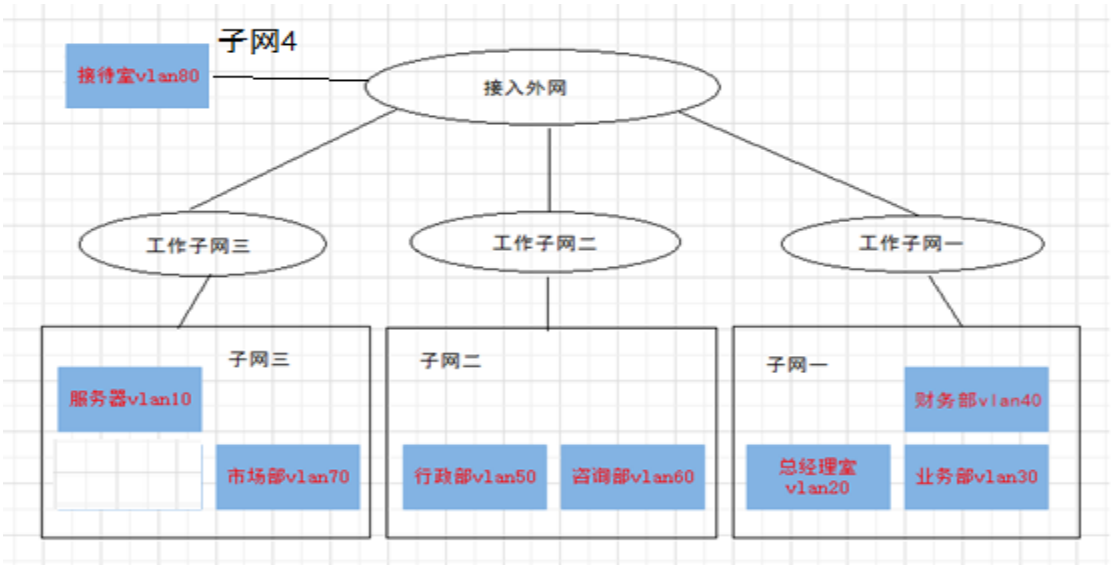


图 4-1 各部门 VLAN 划分及分布图

在接入层的接入子网一中的交换机 LSW1 上，首先在 LSW1 上创建总经理室 vlan20，业务部 vlan30，财务部 vlan40，然后再将不同的 vlan 分别化入对应不同的 ACESS 接口配置如下：

[LSW1]vlan batch 20 30 40

在接口 Ethernet0/0/3 上配置总经理 vlan20 的接口 ACESS 并同时加入相应的 vlan 中。进入后配置如下：

[LSW1]port link-type access

[LSW1]port default vlan 20

同理，财务部 vlan40 和 vlan30 分别加入对应的接口 Ethernet0/0/1 和 Ethernet0/0/2，结果如图 4-2 所示：

```
interface Ethernet0/0/1
 port link-type access
 port default vlan 40
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 30
#
interface Ethernet0/0/3
 port link-type access
 port default vlan 20
```

图 4-2 Access 配置

分别在接入子网二，接入子网三的接入层交换机配置 vlan 并且配置 ACCESS 接口，LSW2（子网二）上的配置如图 4-3 所示：

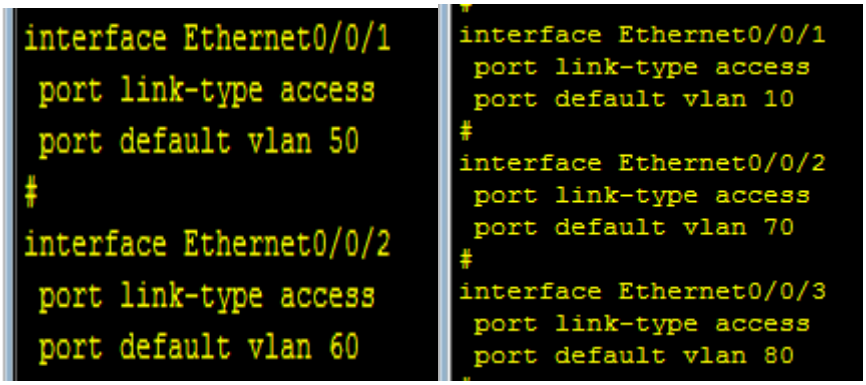


图 4-3 子网二与子网三 ACCESS 接口配置

并为所有汇聚层与核心层的交换机创建 vlan 10—80，配置如下：

[Huawei]vlan batch 10 20 30 40 50 60 70 80

4.3 干道链路 Trunk

原理概述：在 LAN 中，可以使用划分了 vlan 来保证每一个不同部门之间的隔离性，也加强了整一个网络的安全。以太网包含了多很多的主机和交换机，为了让其数据能够穿越多台交换机，所以就在交换机之间必须配置干道链路。干道链路是为了让在不同类型的设备中间，比如说再交换机连到交换机，或是到了路由器上。因为他们的干道之间拥有了多个不同类型的 vlan 中的数据，为了让其能全部过通过，必须要让干路能够流通所有的在 vlan 中的数据。在每一台交换机与交换机之间,或交换机与路由之间的接口上配置命令,在 LSW1 与汇聚层 LSW4 的接口 g0/0/2 上配置，允许所有 vlan 通过。

ink-type trunk

[LSW1-GigabitEthernet0/0/2] port trunk allow-pass vlan all

结果查看 Trunk 接口如图 4-4 所示。

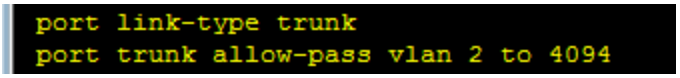


图 4-4 Trunk 接口

4.4 单臂路由

在如上的配置过程中，已经把所有的各个网段划分到了对应的不同的 vlan 中了，这样一来，在同一 vlan 间的主机用户是可以互相通信的，但是不同的却不被允许，为了让他们虽然所处不同，但是互相之间可以信息的往来，决定使用单臂路由。

在常规中，会使用 VLAN 来隔离来分割了二层网络中的广播域来消除其带来的广播的影响，而且还能加强了网络中的安全与可易管理。但是与此带了一个非常严重的后果，就是他隔了所有的不同部门之间的二层网络中的流量，所以分别属于不同的部门中的用户不可以互相信息来往，但是在真实的情况中，往往是不同的的用户之间需要互相之间信息的往来，也就是数据流量的互通，使用单臂路由，是实现跨越不同 vlan 之间实现互通的一种办法。

单臂路由的原理非常的简单，就是通过使用一台路由器为不同的所属不同的部门之间使用路由进行三层转发。通过去使用同一接口中的不同子接口作为其 VLAN 的网关，节省了物理端口的数量。当不同的用户之间互相访问时，就把需要转发的数据包转发到路由的子接口的网关，在处理后转发到目的地。在汇聚层的路由器 R1 的接口 GigabitEthernet0/0/1 中，配置如下：

[R1]interface g0/0/1.2　//进入子接口 1.2

[R1-GigabitEthernet0/0/1.2]ip address 10.1.2.1 24　//配置网关地址

使用 dot1q termination vid 命令配置子接口对一层 tag 报文的终结功能。既配置该命令后，路由器子接口在接受带有 VLAN tag 的报文时，将剥掉 tag 进行三层转发，在发送报文时，会将与接口无法对应 VLAN 的 VLAN tag 添加到报文中。[R1-GigabitEthernet0/0/1.2]dot1q termination vid 20

开启子接口的 ARP 广播功能。如果不配置该命令，将会导致该子接口无法主动发送 ARP 广播报文，以及向外转发 IP 报文。

[R1-GigabitEthernet0/0/1.2]arp broadcast enable　// 开启 ARP 广播功能。同理，所有的 VLAN 都在 R1-GigabitEthernet0/0/1 的子接口中依次如上述配置，最后所有的子接口完成后，在路由器 R1 上查看接口状态如图 4-5 所示。

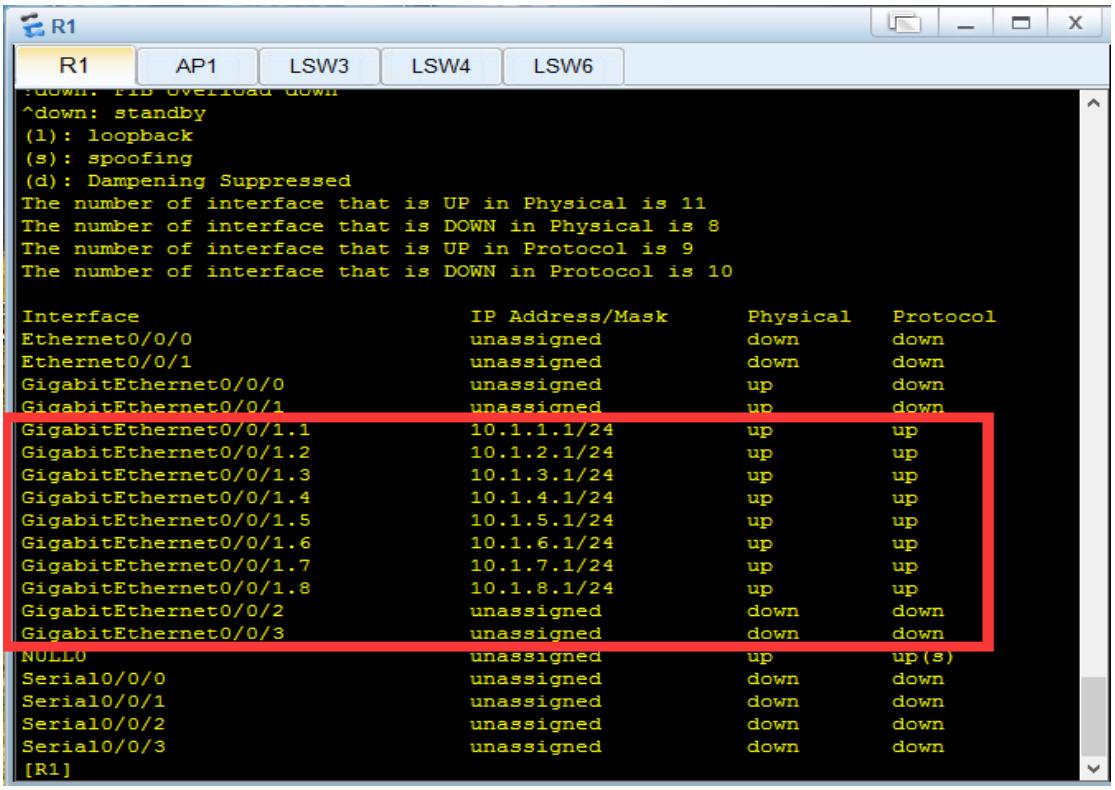


图 4-5 单臂路由接口状态

4.5 动态 IP 地址分配 DHCP

DHCP 就是动态主机配置协议，它是使用 UDP 协议进行工作的的，常用于对内部网络中的主机分配 IP 地址，也可以是企业内部网管对内网主机一个中心控制的方式。DHCP 的使用，可以节省了企业网管静态的去给所有的用户划分并且配置 IP 地址的时间精力。它能够动态的去分配，让那个客户机获得一个 IP 地址，而且也可以去大大简化客户的 TCP/ip 运行。其模式是 C/S 模式。它拥有了三种机制去分配 IP 地址。

基于上一节配置单臂路由之后，为了简易方便配置，鉴于路由器的性能较高，决定使用基于接口地址池的 DHCP 配置。目前企业的虽然是比较小型的，但是，内网的员工的规模也是达到了上百人，面对于这样的一个规模，为了减少企业网管的工作压力，决定使用 DHCP。也是初步得考虑到以后员工人事的更改可能会影响到主机的地理位置，及其日后主机数量的增加，不好配置静态的 IP 地址。DHCP 使用 C/S 进行工作，DHCP 内部企业的用户员工向 DHCP 的服务去请求动态地

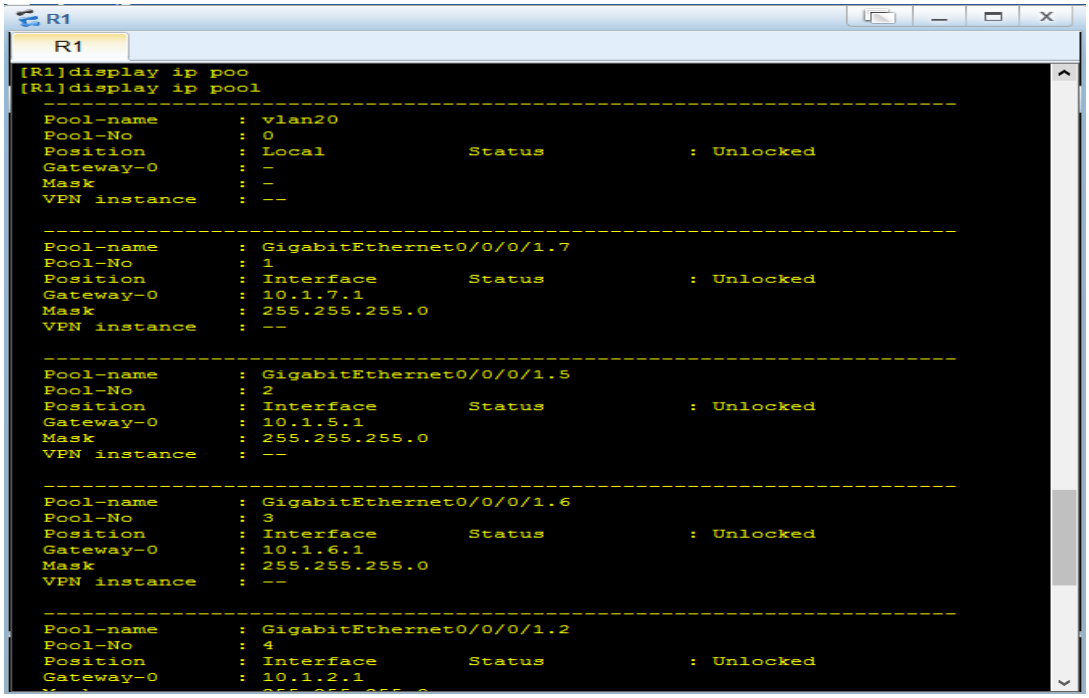
去分配地址，DHCP 服务器 再根据请求返回相应的地址信息等。（如 IP 地址等）。

接口地池的分配如表 4-1 所示。

表 4-1 Nat 接口地址池

vlan	接口地址池	网关	部门
vlan20	10.1.2.2-10.1.2.254	10.1.2.1	总经理室
vlan30	10.1.3.2-10.1.3.254	10.1.3.1	业务部
vlan40	10.1.4.2-10.1.4.254	10.1.4.1	财务部
vlan50	10.1.5.2-10.1.5.254	10.1.5.1	行政部
vlan60	10.1.6.2-10.1.6.254	10.1.6.1	咨询部
Vlan70	10.1.7.2-10.1.7.254	10.1.7.1	市场部
Vlan80	10.1.8.2-10.1.8.254	10.1.8.1	接待室

以总经理办公室（即 vlan20）为例子，直接在接入层的交换机上配置 DHCP 接口地址池：使用命令 dhcp enable// 在 R1 上开启 DHCP 功能，同理，为所有需要 DHCP 的 VLAN 在其对应的子接口如上所配置，完成之后在 R1 上使用 display ip pool 命令查看 DHCP 地址池中的地址分配情况，结果如图 4-6 所示。



4-6 DHCP 配置结果

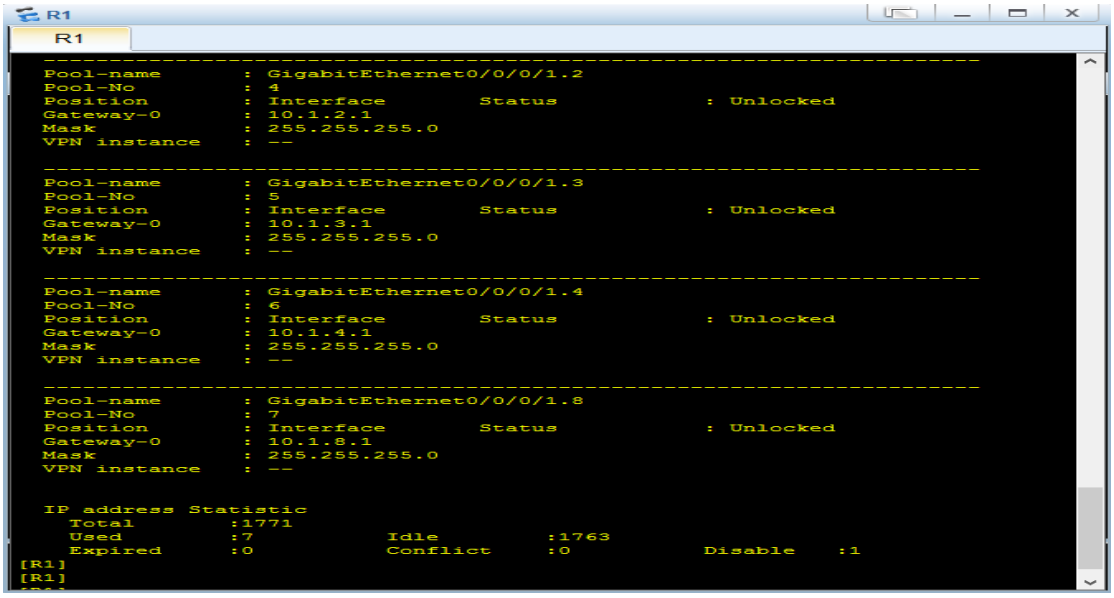


图 4-7 DHCP 配置结果

通过上面的命令，为每一个不同的部门配置分配不同的网段，搭建 DHCP 服务，为每个 vlan 分配一个地址池，为该网段的所有设备动态分配 ip 地址。

4.6 动态路由协议 OSPF

动态路由协议是根据路由表的中的信息，如果发现了网络中的拓扑出现了改变的时候，可以去动态的去维护更改路由表和其表项，然后就根据开销等其他的方式去分析然后选择一个条综合起来开销最小的路径，能够根据链路中的节点出现了异常去自动的改变，选中一个最优的路径，它与这个静态路由是一个相对的概念，是因为它可以去自动得去更新而不需要人为的去指定，所以常用于实际中，这样一来可以节省企业网管的精力和时间。在内网中配置动态路由协议，可以方便的为内网的所有客户端提供网络服务，确保网络的联通性，保证网络的联通。首先使用 ospf 命令创建并运行 ospf，1 代表的是进程号。然后在 [R1]ospf 1 中用 area 0 命令创建区域并进入 OSPF 区域视图，由于是是单区域，所以使用骨干区域，既区域 0 即可。最后再使用 network 命令来指定运行的 OSPF 协议的接口和接口所属的区域。将路由器的接口 10.1.9.0 的网段通告出去：

[R1-ospf-1-area-0.0.0.0] network 10.1.9.0 0.0.0.255

将市场部的的网段 10.1.7.0 通告出去：

[R1-ospf-1-area-0.0.0.0]network 10.1.7.0 0.0.0.255

同理，将内部网络的所有网段通告出去。其中，财务部的网络不允许访问外网，也不允许外网对其的访问，所以不配置动态路由协议，只允许内部的主机对其访问），路由器上的 OSPF 如图 4-8 所示。

```
[R1-ospf-1-area-0.0.0.0]dis this
#
 area 0.0.0.0
  network 10.1.9.0 0.0.0.255
  network 10.1.7.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
  network 10.1.5.0 0.0.0.255
  network 10.1.6.0 0.0.0.255
  network 10.1.8.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
```

图 4-8 上述路由器所有 OSPF 配置

下述为防火墙的 OSPF 配置，也同为区域 0，配置如图 4-9 所示：

```
ospf 1
 area 0.0.0.0
  network 10.1.9.0 0.0.0.255
  network 210.1.1.0 0.0.0.255
```

图 4-9 防火墙 OSPF 配置

4.7 网络地址转换协议 NAT

NAT 是网络地址转换协议，它是一个 IETF(Internet Engineering TaskForce，Internet 工程任务组)标准，它可以让企业内部的用户使用私网的地址，然后将其映射成公网的地址，一来可以节省现在 IP 地址的枯竭，二来是将内部网络的 IP 地址给隐藏了起来。保护了内部企业中的主机。避免了受到网络外部恶意的攻击。使用 NAT 中的 NAPT 转换方式，NAPT 既是网络地址和端口进行转换，既同时对 IP 地址和端口进行转换。首先，配置 NAT 的地址池，包含两个 IP 地址：

[fanghuoqiang]nat address-group 1 210.1.1.3 210.1.1.4

以市场部为例配置 NAT 策略，NAT 策略如图 4-10 所示。