题 目：基于集群技术的网络系统规划与设计

摘要　　现阶段，我国的经济发展飞速，伴随着信息化时代的到来，信息化技术不断地深入各行各业，影响着各个领域的发展。与此同时，我们的用户也会随着网络这个大环境的变化和信息技术的革新对网络提出更多的需求和更高的要求。通俗点说，用户除了要求能够登录互联网获取信息外，并且网络环境的安全性也受到了广泛的关注。特别是

针对对网络比较敏感的特殊用户，他们对于网络的安全程度和稳定程度相较其他用户也会更高。本论文主要以企业网络为背景，基于集群技术对北方实验室（沈阳）股份有限公司网络进行规划设计。该企业总部在沈阳，分公司设在广州。在保证数据的安全性的基础上，总部服务器资源可以被分公司内部用户进行连接，总部和分公司内部用户都可以连上外网。总部由好几个部门组成，但是不能让所有的部门之间都能够互相连通，一次有必要设定一些重要的部门不能随便被访问。

设计由典型的接入层和核心层架构模式并通过实现华为 ensp 模拟器进行仿真。接入层与服务器、用户终端 PC 及打印机等相连接；核心层交换机上配置总部内部用户网关，两台核心交换机连接在一起，并通过集群技术虚拟化成一台，核心层主备交换机分别上联出口路由器，基于接口配置 OSPF 动态路由协议，实现核心交换机跟出口路由器之间路由的同步学习。由于分公司现规模较小，所以再设计网络的时候采用大二层结构，接入层跟汇聚层合并成一层，下面是公司电脑，打印机等终端设备，双上联核心层，增加链路的冗余备份。总部和分公司之间有必要建立 VPN，这是因为在 Internet 公网中，总部与分公司之间的相互访问是由设置 IPsec VPN 技术来达到目的的。在此设计中，通过对实验进行测试，并由相应的配置测试网络的连通性来实现用户的用网需求。关键词：iStack；网络规划；IPsec VPN

1 绪论

1.1 背景

本课题以北方实验室（沈阳）股份有限公司网络搭建为背景，专门对企业的网络进行一次模拟与规划。此公司总部在沈阳，主要部门有人事部、营销部、监理部、监理部、商务部等。随着公司的业务不断发展壮大，开始在广州设立了一个分公司，分公司有商务部、监理部和营销部。总公司跟分公司开始搭建网络，为了减少在公司后续出现网络故障的时候排错时间和实现不同部门之间相互隔离。所以我将公司各个部门规划分配不同的 VLAN，而这些不同的 VLAN 也有着不一样的 IP 地址段，从而达到部门之间是互相隔离的状态。由于大部分的应用服务器都部署在总公司，所以分公司需要对总部的资源进行访问。通过配置相关的安全技术，实现分公司跟总公司相互访问，保证数据的安全性。

1.2 发展趋势

随着时代的发展，经济的增长，信息技术的改进和网络的普及，我们的日常生活与网络的关系越来越紧密。网络已经成为很平常很普遍的事物，如移动数据网络，有线网络，WIFI、视频监控以及电子眼等是我们生活中最常见的几种网络。网络不仅便利了我们的生活，而且还保障了我们的人身安全。就如同有了电子眼的存在，我们的交通安全得到了极大的保障，让不遵守交通规则的人无处遁形，从而减少交通事故的发生保障我们的生命安全。首先，无线网络，通过它，人们摆脱了传统的有线网络的束缚，无论何时何地通过手机等智能移动设备来刷新闻、发邮件、追剧、聊天，让工作娱乐两不误[1]。其次现在的监控设备和电子眼都是与大数据网络相连接，在高速上、在城市中，因有监控设备的存在很大程度上保障了人们的出行安全和人身安全。在网络普及发展过程中在看到优势的同时也会发现其缺陷，无线网络在使用过程中的安全性、在使用时网络信号出现不稳定等等问题。相信无线网络的发展和完善会在我国社会稳定发展的趋势下，网络的使用、安全等方面问题都将随着时间迎刃而解[2]。

1.3 意义

现代人的生活已经跟网络密不可分，网络在生活中的占的比重性越来越大。伴随着计算机网络的发展，现有企业用户的需求与传统的网络架构模式越来越不匹配。网络的发展不仅便利了我们的生活和工作，一个好的网络环境可以大大提升我们的办公效率，也使得我们的业余娱乐活动越来越丰富多彩，同时，飞速发展的网络也进一步推动着社会经济的发展。 2 项目需求分析

2.1 项目概述

北方实验室（沈阳）股份有限公司，成立于 2003 年，公司涉猎的业务范围十分广泛。随着业务的发展，后来在广州成立了分公司。公司的主要数据都存放在沈阳的总部，随着数据的不断增多，数据的存放就存在一个难题，传统的网络架构也不能满足现在的发展需要。公司开始致力于建设一个服务器的集群。在提高网络的性能的同时也对数据进行数据备份。防止数据出现丢失，造成不可挽回的经济损失。公司早期由于资金原因，在网络的建设上投入的成本不是很大，所以早期公司的网络架构存在很多的单点故障。核心设备只有一台，运行着公司所有的业务。当这一台设备出现故障时，公司的业务就可能会受到不可以挽回的损失。随着公司的业务不断发展。公司开始越来越重视公司网络的稳定性可靠性。所以加大网络建设的投资。部署两台核心设备通过堆叠技术做到设备的冗余备份。总部有两栋办公楼，主要有人事部、营销部、监理部、测试部、商务部等，另外还有一个数据服务器集群区域用于存放公司的数据信息。总部人事部、营销部、监理部都设在一楼。人事部门有 4 人左右，营销部、监理部约 40 人，共 45 台 PC。测试部、商务部设在 2 层楼上，共 60 人，需要 PC60 台。分公司部门包括商务部、监理部和营销部。分公司一楼部署核心机房，小型机房设在二楼。

2.2 功能需求

（1）公司的业务不断发展，数据也越来也多，数据的存放就存在一个问题。公司由原来的几台服务器，开始发展为有几百台服务器。为了提高数据的安全性，可靠性。公司开始建立服务器集群。致力于完善公司的数据完整性。

（2）公司早期的网络架构在主要的节点都只有一台设备，为了提高公司网络的稳定性，可靠性。公司开始对网络架构进行改造。在主要的节点，部署备份网络设备，提高网络的稳定性。

2.3 用户需求分析

（1）企业总部和分部有多个部门，每一个部门我们在规划的时候划分不同的 VLAN，定义不同的 VLAN-ID。VLAN-ID 最好是跟网段的第三位保持一致。方便以后运维人员的维护。

（2）企业总部部门之间要求能够共同分享内部资源，还需要能够互相访问网络资源和资料。

（3）核心设备 HA 部署，内部重要业务系统集群部署。

（4）尽可能避免不必要的攻击，以保障总部内部服务器的资源的安全性。

（5）在成本方面， ISP 网络运营商为企业总部提供了 200.200.200.0/29 网段地址，但是公网地址比较少，只有 6 个。基于端口转换可以转换为企业出口设备出接口地址。只有通过网络地址转换才能实现内部用户对外网的连接。 （6）企业总部和分支机构之间需要相互访问，因此，有必要在总部和分支机构间建立 IPsec VPN，这样不仅能减少浪费，最重要的还是能保证网络数据安全地传输。

（7）总公司分人事部、营销部、监理部、测试部、商务部。划分不同部门为不同 VLAN，实现网络间的互通。 分公司商务部、监理部、营销部，实现网络间的互通

2.4 技术需求分析

（1）部署 WEB 服务器：每个企业都需要搭建自己的官方网站，一方面是可以方便企业对网络的日常需要，另一方面是可以对外做到一线宣传，增加本企业的特色和活动以更好的形象呈现出来。企业内部用户和外网用户对网络资源进行访问和浏览都在 WEB 服务器中完成。此外，外网用户能登录访问的另一种方式就是在 WEB 服务器中做静态地址转换[3]。

（2）FTP 文件传输服务器：足够大容量的磁盘和存储空间对 FTP 服务器来说非常重要，企业内部用户保存和查阅网络资源都是在 FTP 服务器中进行。对于一些比较重要的文件夹可以进行权限配置，具体到具体用户或者组，来配置读写权限，从而提高资料的安全性。可以设置固定的登录用户名和密码，来验证 FTP 用户登录。

（3）DHCP 服务器：考虑到不是所有人都可以对 DHCP 服务器有了解，而企业内部用户数肯定不少，为了减少工作量，DHCP 经常用于为用户动态分配 IP 地址。DHCP 服务器可以用专门的服务器配置 DHCP Server，也可以配置三层的交换机和路由器等网络设备上。部署动态 DHCP 服务器可以避免用户配置 IP 地址冲突的问题，而且还能也减少了网络管理员的工作量[4]。

（4）DNS 域名服务器：允许用户通过配置域名和 IP 地址映射的方式更便捷地对网站进行访问。通过配置域名与 IP 地址对应映射，在浏览器里面输入相应的域名，查找对应的 IP 地址之后再进行访问，就很容易。与之相反的是，一般用户对于 IP 地址的存储记忆有限，如果 IP 地址较多，这时候就不容易识别或记住。再加上现在的网站类型多种多样，如果需要记住所有 IP 地址的话是一项非常庞大的工程。

2.5 功能需求分析

（1）防止外部的 IP 地址欺骗

（2）阻断外网用户入侵公司内部网络，同时还要控制内部网的非法 IP 地址连接外网 。IP 由公司内部特别规划使用，只有进行地址转换协议才能连接外部网。

（3）对内部网资源主机的访问控制 （4）防止外部的 ICMP 重定向欺骗

（5）防止外部的资源路由选择欺骗

（6）内部网络流量的控制

2.6 网络设备需求分析

由于信息技术的不断更迭替换，越来越多的网络设备厂商也随着产生。尤其在产品性能和价格等方面，每个设备厂商之间都有竞争性的差别。总的来说，在价格上，Cisco 的网络设备没有竞争优势，因为它比常见的竞争对手 h3c 和华为等设备高出很多。但在稳定性和性能上，h3c 和华为都较 Cisco 薄弱。因此，企业在进行网络设备的选择时，以下几方面都应该综合进行考量才能得出性价比比较高的理想设备[5]。

（1）性能方面：在网络中，数据包的转发能力快慢是由网络设备的转发性能决定的，从而决定了网络的稳定性与用户体验，所以一般就是转发性越高越好。

（2）安全方面：现在网络安全在网路设计中是至关重要的一个环节，甚至现在网络安全工程师都是比较吃香的，一个设备能支持的基本安全协议有哪些将是重点考虑的对象。那么，只有特定的安全设备和相应的平台才能更好地保护网络的安全性。一般是看品牌或者售后能力[6]。

（3）管理性方面：为满足网络管理员配置网络设备和便于远程管理，网络设备应该要能支持一些最基本的、常用的协议，其中包括 telnet、SSH、SNMP 等。

（4）可靠性方面：用户需求实现链路冗余和用户网关备份，在汇聚层交换机选型最好可以支持常用的 STP、
HSRP 及 VRRP 网关备份冗余协议，如果可以与时俱进支持一些新技术都是可以考虑的，保证用户网络的可靠性。

2.7 信息点需求分析

在统计企业信息点时，不只是单纯对 PC 数量进行统计，而是根据不同部门人员数量和 PC 的数量来进行统计的。统计结果如表 2-1 所示。

楼层	部门	信息点
1F	人事部	4
1F	营销部	20
1F	监理部	20
2F	测试部	35
2F	商务部	25

表 2-1 信息点统计 3 项目功能规划与设计

3.1 网络设计原则

3.1.1 先进性

现在设备的更新换代越来越快，新的技术不断地出现，新设备出现的周期也随之变短，与此同时信息化技术飞速发展和很多的网络厂商自己的产品越来越趋近于成熟。那些落后的产品就会更加跟不上步伐，所以，在进行设备挑选的时候我们要更全面的关注设备的更新能力，不只是可以满足当下的需求，更应该考虑到后续的发展。在硬件挑选的时候，目光要放长远一点，有一定的预见能力，选择软件的时候也要关注其开发性，实用性和软件优势等。还有，网络设计有时也要考虑到通信稳定的需求[7]。

3.1.2 可靠性

对于一些影响比较大的地方如学校、企业，网络运维的可靠性使非常重要的，他们是绝对不允许出现比较夸张的故障的。所以，在设计网络的时候我们要重点考虑网络的可靠性，努力完善，从而使系统可以在较长的时间里能够可靠的稳定的运行，也要保证其系统的安全性，禁止未认证用户的访问，系统也不是说不允许出现故障，故障使无法避免的，一个成熟的网络要做到的是即使出现设备故障问题，也需要有相应的备份可以用于数据恢复[8]。

3.1.3 实用性

系统的设计需要满足现有用户的需求，能够实现用户对网络的使用，能够满足企业内部用户的体验，网络的设计不用太复杂，要从实际情况出发，要实现用户一些基本的要求，如用户能够访问外网、内部用户之间实现资源共享等。

3.1.4 安全性

要想维护网络的安全性，就必须要有效预防非法攻击和操作。因此，网络的安全性在实际运用中和在网络设计中都至关重要。因此，在此网络设计中，一个不可忽略的问题就是网络的安全性。网络设备的权限可以自己设置，防火墙位于服务器区域中。在安装网络设备时或在安装网络设备的位置，仅允许专业人员进入计算机室[9]。

3.2 主要技术

3.2.1 iStack

简单来说，几台具备堆叠性质的设备组在一起就是堆叠技术。堆叠技术是一种虚拟化技术，通过对多台设备的硬件资源和软件资源组合在一起，从而使这些设备能够协同工作、统一管理和维护。如下图 3-1 所示，进行必要的配置后，即虚拟化成了一台设备。

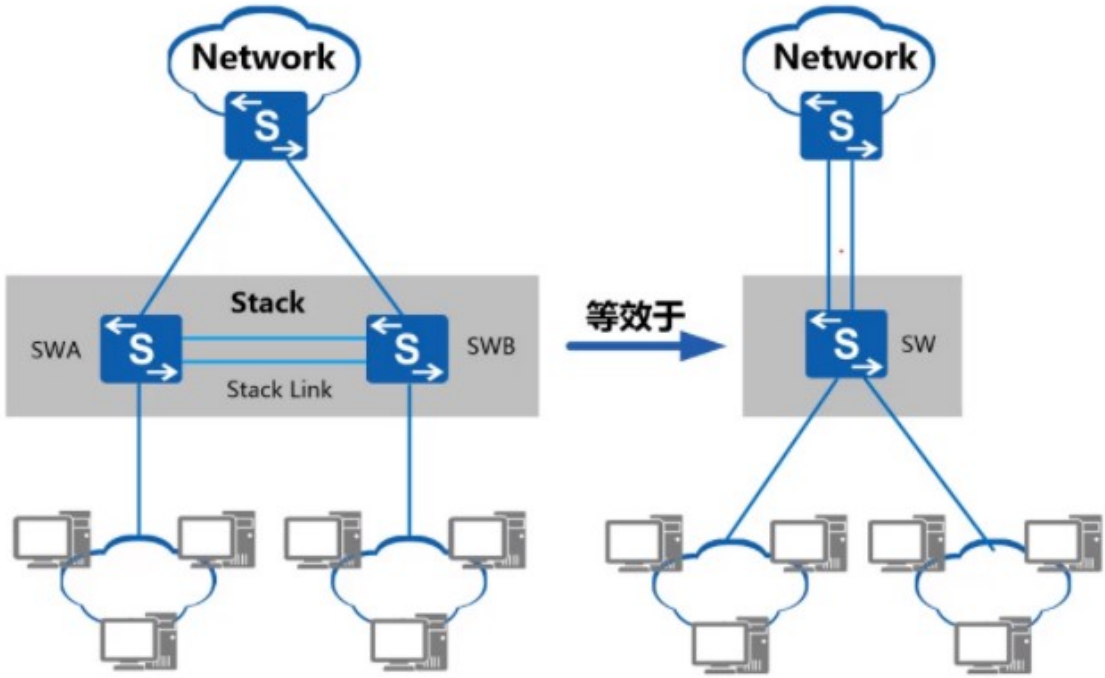

图 3-1 iStack 堆叠逻辑图 iStack 的优点[10]见下表 3-1：

优点	说明
简化管理	堆叠形成之后，用户通过任意成员设备的任意端口都可以登录 iStack 系统，对 iStack 内所有成员设备进行统一管理
1:N 备份的设备就	几台具备堆叠性质的设备组在一起就是 iStack。在这些设备中，担任 iStack 运行、管理及维护 是主设备。为保障业务的连续性，万一主干设备有问题了，系统会自动产生出适合的设备替代问题设备。相应地，其他从属设备在作为备份设备也可以同时处理业务。这就是设备的 1:N 备份。跨成员 iStack 和上、下层设备之间的物理链路支持聚合功能，并且不同成员设备上的物理链路可以聚合成一个

设备的逻辑链路，多条物理链路之间可以互为备份也可以进行负载分担，当某个成员设备离开 iStack，其它成链路聚员设备上的链路仍能收发报文，从而提高了聚合链路的可靠性合强大的通过增加成员设备，可以轻松自如的扩展 iStack 的端口数、带宽。因为各成员设备都有 CPU，能够独立处网络扩理协议报文、进行报文转发，所以 iStack 还能轻松自如的扩展处理能力
展能力
表 3-1
4 项目的详细设计
4.1 网络架构
4.1.1 总部网络架构规划
总部网络在稳定性和安全性上有相应的需求，接入层到汇聚层避免出现线路单点故障，同时要求用户网关设备实现主备。实现总部内部用户访问外网，实现总部与分公司相互访问。总部网络规划设计思路如下：
1 、核心层（汇聚层）
核心层是一个网络的心脏，是最重要的一层，作为网络三层架构的核心部分，是不可缺少的。所有该网络的用户的流量都需要经过核心交换机进行转发和数据备份，这次网络的设计中就考虑的是资金充足的情况下，核心层有两台三层交换机，负责转发总部内部用户的流量，并起到了内部用户网关的作用，不同网段用户的连通性都是在核心上实现的。两台核心交换机间部署 HA，通过集群虚拟化成一台设备，实现负载均衡；核心交换机之间还运行了 HSRP 协议，实现网关备份，万一其中一台核心设备发生故障或死机等突发现象，另外一台核心交换机还能正常转发流量，保证网络不中断，从而保障了网络的可靠性。在出口路由器和核心层之间都配置了动态路由协议，通过配置
OSPF 动态协议保证网络了可扩展性和连通性[11]。
2 、接入层
一般地，接入层设备直连终端设备。企业内部人数较多，根据部门划分不同 VLAN，交换机设备上创建 vlan id，连接终端设备的接口模式配置为 access 模式，基于端口的划分将接口划分到对应 vlan。上联交换机设备的接口，接口模式配置为中继端口，vlan 裁剪，透传特定 vlan 通过[12]。
3 、服务系统
企业总部部署办公系统和业务系统，服务器区域通过一台高性能交换机连接服务器，接口千兆，保证接口带
宽。搭建常用办公应用系统，如 FTP Server、DNS Server 和 DHCP Server，模拟器自带 FTP 服务器和 DNS 服务器，
DHCP Server 配置在核心设备。业务系统部署多台服务器，部署集群技术保证业务系统稳定性[13]。
4.1.2 分公司网络架构规划
分公司的网络架构相对于总部来说比较简单，分公司用一台核心交换机作为用户的网关，出口的话还是部署一台路由器，接入层部署几台二层交换机。网络的稳定性和安全性没有总部的考虑周到，因为分公司较小，资金问题考虑比较周到。但是实现用户访问外网和访问总部资源都是可以的。
1 、核心层
核心层是一个网络的心脏，是最重要的一层，作为网络三层架构的核心部分，是不可缺少的。所有该网络的用户的流量都需要经过核心交换机进行转发和数据备份，这次网络的设计中就考虑的是资金充足的情况下，核心层有两台三层交换机，负责转发总部内部用户的流量，并起到了内部用户网关的作用，不同网段用户的连通性都是在核心上实现的。两台核心交换机间部署 HA，通过集群虚拟化成一台设备，实现负载均衡；核心交换机之间还运行了 HSRP 协议，实现网关备份，万一其中一台核心设备发生故障或死机等突发现象，另外一台核心交换机还能正常转发流量，保证网络不中断，从而

保障了网络的可靠性。在出口路由器和核心层之间都配置了动态路由协议，还是通过配置 OSPF 动态协议保证网络的可扩展性和连通性[14]。

2 、接入层

在接入交换机上，连接用户终端的端口设置为 access，规划到到相对应的不同 VLAN 中，上联汇聚交换机的端口

设置为 trunk 口，使 VLAN 通过。。

分公司分为三个部门，因此需要规划和创建多个不同的 VLAN。相应的 VLAN 由不同部门的接入层交换机与终端相连接的端口来划分，上联汇聚层交换机的端口设置为 trunk 口，配置相应的 VLAN 能够通过。

4.2 网络拓扑

4.2.1 网络描叙

该企业总部位于沈阳，分公司在广州。为实现总部与分公司能够共享网络资源，以及保证数据的安全性，总部和分公司间之间有必要部署 VPN，在 internet 公共网络基础上通过配置 IPsec VPN 实现总部与分公司之间的相互访问。总部由多个部门组成，设定一些重要的部门不能随便被访问，并限制一些部门之间的连通性。网络拓扑设计采用用经典的三层架构（接入层、汇聚层、核心层）设计。局域网接入层设备主要连接用户终端，上联汇聚交换机；汇聚层设备上联核心设备和下联接入设备；核心层设备连接企业内部多个区域，实现数据快速转发，核心设备相当重要，考虑可靠性部署 2 台设备，2 台设备主备。IGP 内部网关规划 OSPF，实现内部互通。

在本次实验设计中，华为 ensp 模拟器用于完成网络设计和模拟仿真。通过网络设备二层交换机、三层交换机、路由器、PC 和服务器的添加来进行组网连接。网络的连通性和相关测试由相关配置来实现和满足用户的需求。　　由于模拟器无法模拟 iStack 集群技术，所以仿真设计采用 VRRP 与 MSTP 技术的双重结合保证网络可靠性[15]。

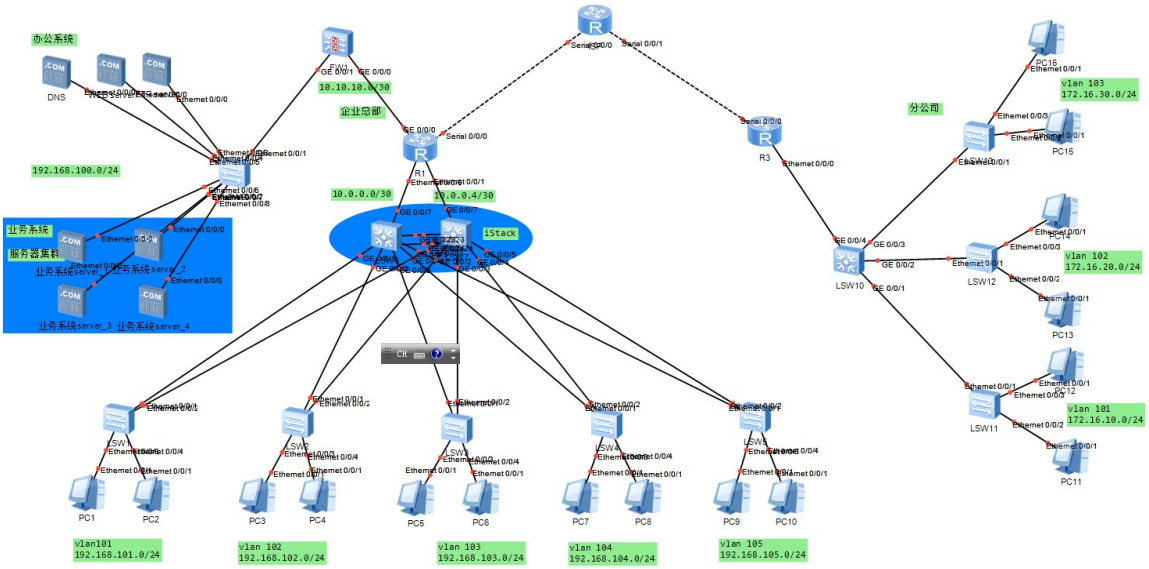

图 4-1 网络拓扑图

4.3 IP 地址规划和 VLAN 划分

由于公司存在很多的部门，不同的部门都有不同的职能，比如说，公司的财务部门对公司的财务管理尤为重要，为了提高网络的安全性。所以通常财务部门不能够访问外网。如果将所有的部门都同意规划在一个 VLAN 内，不利于对网络的进行有效控制。

划分 VLAN 的优点[16]见表 4-1：

优点	说明
限制广播域	广播域备限制在一个 VLAN 内，节省带宽，提高网络处理能力
增强局域网的安全性	不同 VLAN 内不能够进行通信，二层之间相互隔离
灵活构建虚拟工作组	用 VLAN 可以划分不同的用户到不同的用户组，同意用户组的用户也不用所限于地理位置的影响。网络构建更加方便灵活

表 4-1 VLAN 优点 4.3.1 VLAN 划分如表 4-2

VLAN	VLAN 描述	备注
VLAN 101	人事部	总部
VLAN 102	营销部	总部
VLAN 103	监理部	总部
VLAN 104	测试部	总部
VLAN 105	商务部	总部
VLAN 101	商务部	分支机构
VLAN 102	监理部	分支机构
VLAN 103	营销部	分支机构

表 4-2 VLAN 划分 4.3.2 IP 地址规划

随着网络规模的日趋壮大，以及不断增长的用户数量和不同需求对网络的要求也越来越高，管理起来也并非易事。为有效提高网络管理的灵活性和安全性，IP 的划分规范有必要按照合理性、完整性、科学性的代码分类原则进行，这样可以保证信息交换的稳定性和速度问题。同时，IP 地址规划不但要确保技术的先进性，同时也要贴合实际保证工程的可实施性。

IP 地址规划的原则[17]如下表 4-3：

原则	说明
唯一性	一个 IP 网络中不能存在两个相同 IP 地址的主机
简单性	IP 地址的分配应简单易于管理，降低网络扩展的复杂性，简化路由表
连续性	连续的 IP 地址规划，在后期网络中易于路由表的聚合，减少路由条目

表 4-3 IP 地址规划原则

IP 地址规划如表 4-4 所示：

VLAN	VLAN 描述	IP 地址	子网掩码	网关	备注		
VLAN 101	人事部	192.168.101.0	255.255.255.0	192.168.101.254	总部		
VLAN 102	营销部	192.168.102.0	255.255.255.0	192.168.102.254	总部		
VLAN 103	监理部	192.168.103.0	255.255.255.0	192.168.103.254	总部		
VLAN 104	测试部	192.168.104.0	255.255.255.0	192.168.104.254	总部		
VLAN 105	商务部	192.168.105.0	255.255.255.0	192.168.105.254	总部		
VLAN 101	商务部	172.16.10.0	255.255.255.0	172.16.10.254	分支机构		
VLAN 102	监理部	172.16.20.0	255.255.255.0	172.16.20.254	分支机构		
VLAN 103	营销部	172.16.30.0	255.255.255.0	172.16.30.254	分支机构		

表 4-4 IP 地址规划

4.4

网络实施

4.4.1接入层实施

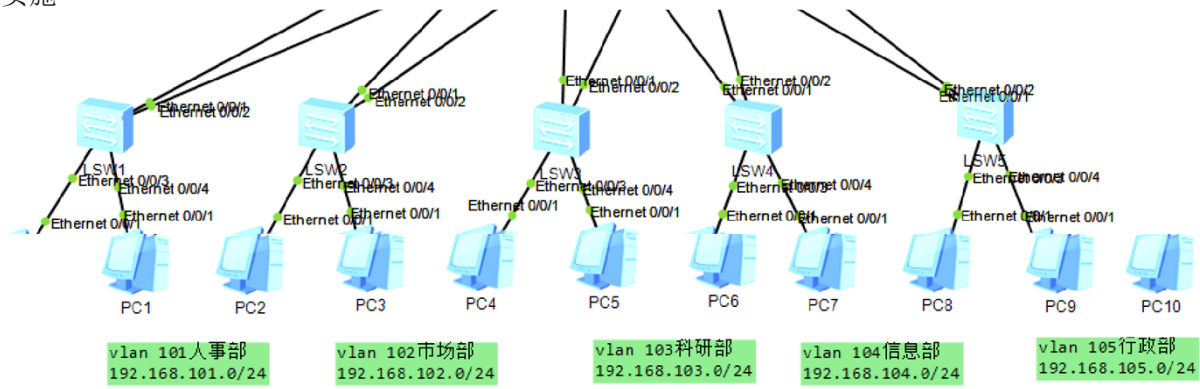

图 4-2 接入层实施图

以人事部接入层交换机为例，对应的用户 VLAN 在接入层交换机上配置，设置连接终端设备和用户接口为 access，并设置交换机互联的接口为 trunk。

```
[Huawei]vlan 100
[Huawei-vlan100]vlan 101
[Huawei-vlan101]vlan 102
[Huawei-vlan102]vlan 103
[Huawei-vlan103]vlan 104
[Huawei-vlan104]vlan 105
[Huawei-vlan105]#
[Huawei-vlan105]interface eth0/0/1
[Huawei-Ethernet0/0/1] port link-type trunk
[Huawei-Ethernet0/0/1] port trunk allow-pass vlan 2 to 4094
[Huawei-Ethernet0/0/1]#
[Huawei-Ethernet0/0/1]interface eth0/0/2
[Huawei-Ethernet0/0/2] port link-type trunk
[Huawei-Ethernet0/0/2] port trunk allow-pass vlan 2 to 4094
[Huawei-Ethernet0/0/2]#
[Huawei-Ethernet0/0/2]stp region-configuration
[Huawei-mst-region] region-name huawei
[Huawei-mst-region] instance 1 vlan 100 to 105
[Huawei-mst-region] active region-configuration
Info: This operation may take a few seconds. Please wait for a moment...done.
[Huawei-mst-region]#
[Huawei-mst-region]interface Ethernet0/0/3
[Huawei-Ethernet0/0/3] port link-type access
[Huawei-Ethernet0/0/3] port default vlan 101
[Huawei-Ethernet0/0/3]#
```

图 4-3 配置截图 4.4.2 核心层实施对应的用户 VLAN 在核心层交换机上配置，并设置与交换机互联的接口为 trunk。

```
[Huawei]sysname Core-SW-1
[Core-SW-1]#
[Core-SW-1]vlan 100
[Core-SW-1-vlan100]vlan 101
[Core-SW-1-vlan101]vlan 102
[Core-SW-1-vlan102]vlan 103
[Core-SW-1-vlan103]vlan 104
[Core-SW-1-vlan104]vlan 105
[Core-SW-1-vlan105]vlan 2
```

图 4-4 配置截图

```
[Core-SW-1]interface GigabitEthernet0/0/1
[Core-SW-1-GigabitEthernet0/0/1] port link-type trunk
[Core-SW-1-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 4094
[Core-SW-1-GigabitEthernet0/0/1]#
[Core-SW-1-GigabitEthernet0/0/1]interface GigabitEthernet0/0/2
[Core-SW-1-GigabitEthernet0/0/2] port link-type trunk
[Core-SW-1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 4094
[Core-SW-1-GigabitEthernet0/0/2]#
[Core-SW-1-GigabitEthernet0/0/2]interface GigabitEthernet0/0/3
[Core-SW-1-GigabitEthernet0/0/3] port link-type trunk
[Core-SW-1-GigabitEthernet0/0/3] port trunk allow-pass vlan 2 to 4094
[Core-SW-1-GigabitEthernet0/0/3]#
[Core-SW-1-GigabitEthernet0/0/3]interface GigabitEthernet0/0/4
[Core-SW-1-GigabitEthernet0/0/4] port link-type trunk
[Core-SW-1-GigabitEthernet0/0/4] port trunk allow-pass vlan 2 to 4094
[Core-SW-1-GigabitEthernet0/0/4]#
[Core-SW-1-GigabitEthernet0/0/4]interface GigabitEthernet0/0/5
[Core-SW-1-GigabitEthernet0/0/5] port link-type trunk
[Core-SW-1-GigabitEthernet0/0/5] port trunk allow-pass vlan 2 to 4094
```

图 4-5 配置截图通过 VRRP 和 MSTP 协议，在核心层交换机之间配置端口聚合和用户网关，实现用户网关主备和链路冗余。

```
[Core-SW-1]interface Eth-Trunk0
[Core-SW-1-Eth-Trunk0] port link-type trunk
[Core-SW-1-Eth-Trunk0] port trunk allow-pass vlan 2 to 4094
[Core-SW-1-Eth-Trunk0]#
[Core-SW-1-Eth-Trunk0]interface GigabitEthernet0/0/23
[Core-SW-1-GigabitEthernet0/0/23] eth-trunk 0
Info: This operation may take a few seconds. Please wait for a moment...done.
[Core-SW-1-GigabitEthernet0/0/23]#
[Core-SW-1-GigabitEthernet0/0/23]interface GigabitEthernet0/0/24
[Core-SW-1-GigabitEthernet0/0/24] eth-trunk 0
```

图 4-6 配置截图

```
[Core-SW-1]stp region-configuration
[Core-SW-1-mst-region] region-name huawei
[Core-SW-1-mst-region] instance 1 vlan 100 to 105
[Core-SW-1-mst-region] active region-configuration
Info: This operation may take a few seconds. Please wait for a moment...done.
[Core-SW-1-mst-region]#
[Core-SW-1-mst-region]stp instance 1 root primary
```

图 4-7 配置截图

```
[Core-SW-1]interface Vlanif100
[Core-SW-1-Vlanif100] ip address 192.168.100.252 255.255.255.0
[Core-SW-1-Vlanif100] vrrp vrid 100 virtual-ip 192.168.100.254
[Core-SW-1-Vlanif100] vrrp vrid 100 priority 120
```

图 4-8 配置截图

OSPF 动态路由协议在核心层交换机上开启，在核心层交换机与路由器之间运行，宣告用户网段和路由器互联的接口地址

```
[Core-SW-1]ospf 100
[Core-SW-1-ospf-100]area 0
[Core-SW-1-ospf-100-area-0.0.0.0]network 192.168.101.0 0.0.0.255
```

图 4-9 配置截图

内部用户网段能够自动获取 IP 地址，DHCP servr 服务器配置在核心交换机上，动态为用户分配 IP 地址，避免用户手动配置 IP 地址出现地址冲突。

```
[Core-SW-1]ip pool vlan101
Info:It's successful to create an IP address pool.
[Core-SW-1-ip-pool-vlan101] gateway-list 192.168.101.254
[Core-SW-1-ip-pool-vlan101] network 192.168.101.0 mask 255.255.255.0
[Core-SW-1-ip-pool-vlan101] dns-list 192.168.100.3
```

图 4-10 配置截图 4.4.3 出口路由器实施

对应的静态路由、默认路由、接口地址以及 NAT 网络地址转换都统一在出口路由器上配置

```
<Huawei>system
Enter system view, return user view with Ctrl+Z.
[Huawei]#
[Huawei]sysname R1
[R1]#
[R1]interface se0/0/0
[R1-Serial0/0/0] ip address 200.200.200.1 29
[R1-Serial0/0/0]#
[R1-Serial0/0/0]interface Ethernet0/0/0
[R1-Ethernet0/0/0] ip address 10.0.0.2 30
[R1-Ethernet0/0/0]#
[R1-Ethernet0/0/0]interface Ethernet0/0/1
[R1-Ethernet0/0/1] ip address 10.0.0.6 30
[R1-Ethernet0/0/1]#
[R1-Ethernet0/0/1]ip route-static 0.0.0.0 0.0.0.0 200.200.200.6
[R1]#
[R1]ospf 100
[R1-ospf-100] area 0.0.0.0
[R1-ospf-100-area-0.0.0.0] net 10.0.0.0 0.0.0.3
[R1-ospf-100-area-0.0.0.0] net 10.0.0.4 0.0.0.3
[R1-ospf-100-area-0.0.0.0] default-route-advertise always
[R1-ospf-100]#
[R1-ospf-100]acl 2000
[R1-acl-basic-2000] rule permit source 192.168.0.0 0.0.255.255
```

图 4-11 配置截图为实现总部与分公司能够共享网络资源，以及保证数据的安全性，总部和分公司间之间有必要部署 VPN。

```
[R1]acl number 3000
[R1-acl-adv-3000] rule  permit ip source 200.200.200.1 0 destination 100.100.100
.1 0
[R1-acl-adv-3000]#
[R1-acl-adv-3000]ipsec proposal vpn
[R1-ipsec-proposal-vpn] esp authentication-algorithm sha1
[R1-ipsec-proposal-vpn] esp encryption-algorithm aes-192
[R1-ipsec-proposal-vpn]#
[R1-ipsec-proposal-vpn]ike proposal 10
[R1-ike-proposal-10]#
[R1-ike-proposal-10]ike peer R3 v1
[R1-ike-peer-R3] pre-shared-key cipher huawei
[R1-ike-peer-R3] ike-proposal 10
[R1-ike-peer-R3] remote-address 100.100.100.1
[R1-ike-peer-R3]#
[R1-ike-peer-R3]ipsec policy map1 10 isakmp
[R1-ipsec-policy-isakmp-map1-10] security acl 3000
[R1-ipsec-policy-isakmp-map1-10] ike-peer R3
[R1-ipsec-policy-isakmp-map1-10] proposal vpn
[R1-ipsec-policy-isakmp-map1-10]#
[R1-ipsec-policy-isakmp-map1-10]interface se0/0/0
[R1-Serial0/0/0] ipsec policy map1
```

图 4-12 配置截图 4.5 设备选型

品牌	设备型号	设备类型	数量	备注
Huawei	S3700-26C-HI	接入层交换机	6	总部
Huawei	S5700-28C-HI	核心层交换机	2	总部
Huawei	AR1220-S	出口路由器	1	总部
Huawei	USG5500	防火墙	1	总部
Huawei	S3700-26C-HI	接入层交换机	3	分公司
Huawei	S5700-28C-HI	汇聚层交换机	1	分公司
Huawei	AR1220-S	出口路由器	1	分公司

表 4-5 设备清单 5 项目的配置与实现

5.1 网络仿真配置

5.1.1 接入交换机配置

在接入层，不同的 VLAN 被划分到不同部门，目的在于隔离广播域，防止广播风暴。LAN 在接入层交换机上创建，然后基于端口的划分将用户加入到对应的 VLAN 中。接入层交换机与上联交换机互联端口配置为中继端口，使 VLAN 都能通过。

```
[ Huawei]vlan 100 //创建相应的 VLAN
[ Huawei]interface eth0/0/1 //进入接口将接口配置为中继端口
[Huawei-Ethernet0/0/1] port link-type trunk
    [Huawei-Ethernet0/0/1] port trunk allow-pass vlan 2 to 4094
[ Huawei]interface Ethernet0/0/3 //将接口划分到 VLAN 101
[Huawei-Ethernet0/0/3]port link-type access
[ Huawei-Ethernet0/0/3] port default vlan  101
```

5.1.2 核心交换机配置

用户网关配置在核心交换机上，并设置对应的 VLAN，与交换机互联的端口配置为中继。IP 地址配置在路由器互联的接口上，路由协议配置 ospf 动态路由协议实现全网互通。

```
[ Core-SW-1]vlan 100 //创建相应的 VLAN
在接入交换机命令行的全局配置模式下创建用户 vlan106
[Core-SW-1]vlan 101
在接入交换机命令行的全局配置模式下创建用户 vlan101
[ Core-SW-1]vlan  102
在接入交换机命令行的全局配置模式下创建用户 vlan102
[ Core-SW-1]vlan  103
在接入交换机命令行的全局配置模式下创建用户 vlan103
[ Core-SW-1]vlan  104
在接入交换机命令行的全局配置模式下创建用户 vlan104
[ Core-SW-1]vlan  105
在接入交换机命令行的全局配置模式下创建用户 vlan105
[ Core-SW-1]interface Ethernet0/0/ 1
[ Core-SW-1-Ethernet0/0/1] port link-type trunk
    [Core-SW-1-Ethernet0/0/1] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/1]#
[ Core-SW-1-Ethernet0/0/1]interface Ethernet0/0/ 2
[ Core-SW-1-Ethernet0/0/2] port link-type trunk
```

```
    [Core-SW-1-Ethernet0/0/2] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/2]#
[ Core-SW-1-Ethernet0/0/2]interface Ethernet0/0/ 3
[ Core-SW-1-Ethernet0/0/3] port link-type trunk
    [Core-SW-1-Ethernet0/0/3] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/3]#
[ Core-SW-1-Ethernet0/0/3]interface Ethernet0/0/ 4
[ Core-SW-1-Ethernet0/0/4] port link-type trunk
    [Core-SW-1-Ethernet0/0/4] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/4]interface Ethernet0/0/ 5
[ Core-SW-1-Ethernet0/0/5] port link-type trunk
    [Core-SW-1-Ethernet0/0/5] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/5]#
[ Core-SW-1-Ethernet0/0/5]interface Ethernet0/0/ 6
[ Core-SW-1-Ethernet0/0/6] port link-type trunk
    [Core-SW-1-Ethernet0/0/6] port trunk allow-pass vlan 2 to 4094
[ Core-SW-1-Ethernet0/0/6]#
```

将接口 Ethernet0/0/1 -6 配置为中继端口

```
[Core-SW-1]interface Eth-Trunk0
[ Core-SW-1-Eth-Trunk0] port link-type trunk
    [Core-SW-1-Eth-Trunk0] port trunk allow-pass vlan 2 to 4094
    [Core-SW-1-Eth-Trunk0]interface GigabitEthernet0/0/23
[ Core-SW-1-GigabitEthernet0/0/23] eth-trunk  0
    [Core-SW-1-GigabitEthernet0/0/23]interface GigabitEthernet0/0/24
[ Core-SW-1-GigabitEthernet0/0/24] eth-trunk  0
```

配置端口聚合，增加链路带宽

```
[ Core-SW-1]mstp mode mstp
[Core-SW-1]stp region-configuration
[ Core-SW-1-mst-region] region-name Core-SW -1
[Core-SW-1-mst-region] instance 1 vlan 100 to 105
[ Core-SW-1-mst-region] active region-configuration
```

配置 stp 生成树协议模式为多生成树协议

```
[Core-SW-1]interface Vlanif101
    [Core-SW-1-Vlanif101] ip address 192.168.101.252 255.255.255.0
    [Core-SW-1-Vlanif101] vrrp vrid 101 virtual-ip 192.168.101.254
[ Core-SW-1-Vlanif101] vrrp vrid 101 priority  120
[ Core-SW-1-Vlanif101]interface Vlanif 102
    [Core-SW-1-Vlanif102] ip address 192.168.102.252 255.255.255.0
    [Core-SW-1-Vlanif102] vrrp vrid 102 virtual-ip 192.168.102.254
[ Core-SW-1-Vlanif102] vrrp vrid 102 priority  120
[ Core-SW-1-Vlanif102]interface Vlanif 103
    [Core-SW-1-Vlanif103] ip address 192.168.103.252 255.255.255.0

[Core-SW-1-Ethernet0/0/4]#
```