得帆信息技术有限公司的网络优化与升级

# 摘要

当今是信息化世纪，信息网络化、办公自动化是必不可少的条件。因此想要提高自身的发展必须加强在网络方面的竞争力才能促进自身的强大。目前网络全世界都已经触手可及了，几乎覆盖到了全世界，这使得网络建设变得困难了起来，尤其是要对网络进行更加周密的设计，并对企业的网络完成安全的设计保障。各部门进行划分VLAN，对OSPF协议的使用，ACL访

问列表的配置，NAT/NAT server地址转换，DHCP的配置和设置MPLS VPN等安全操作能最大

的处理这些问题。在完成的拓扑结构中，有关设备技术的应用，并在其原有的基础上进行新的设计和升级，使企业能够在更高效和安全的基础上进行数据传输和打包传送，从而达到优化企业网络的目标。

关键词：网络优化；相关配置优化，MPLS VPN；简洁高效

1绪论

1.1论文研究的背景及意义

1.2企业网现状

1.3优化设计方法

2，优化方案

2.1企业网设计需求

2.2使用运营商网络进行搭建

2.3降低部门关联度

3优化关键技术分析

3.1路由协议简介

路由协议是一种指定数据包转送方式的网上协议,工作在网络层。路由器是网络的主要节点设备，路由表被使用在路由器转发数据。其路由信息在相邻的路由器之间传递，以此来获得其他路由器的路径，并且路由表的建立描述了网络状态。路由协议和路由器并行数据转发功能。

3.2VLAN简介

VLAN技术是一种逻辑网络，通常在网络的物理拓扑上通过路由和交换设备运行。VLAN是一种虚拟局域网，不受地理位置影响。它工作在OSI参考模型的第二层和第三层，传递信息主要靠在第三层的路由器。VLAN技术比传统局域网更加灵活；减少了对网络设备的开销更改，由于划分不同的VLAN使网络更加安全。

3.3IP协议简介

IP协议是网络层协议，属于TCP/IP体系。其主要目的是为了实现计算机互联互通，解决网络问题。并且它是互联网必须遵守的规则。

3.4ACL简介

ACL是一种基于包过滤的访问控制技术，在三层交换机和路由器上被广泛使用，它可以确保网络设备不被入侵和非法使用，是保护网络安全的主要策略。并且它还是

3.5BFD简介

3.6MPLS VPN简介

3.7NAT

4网络安全设计

4.1vlan技术

4.2防火墙技术

4.3VPN技术

4.4安装杀毒软件

在这个信息技术时代，家家户户都有了自己的计算机，个人计算机的信息显得尤为重要，尤其是在网络安全方面，对于系统的病毒入侵和检测显得尤为重要。对此建议安装一些杀毒软件，如火绒，瑞星杀毒，360和金山毒霸等来提高自己计算机的安全能力。

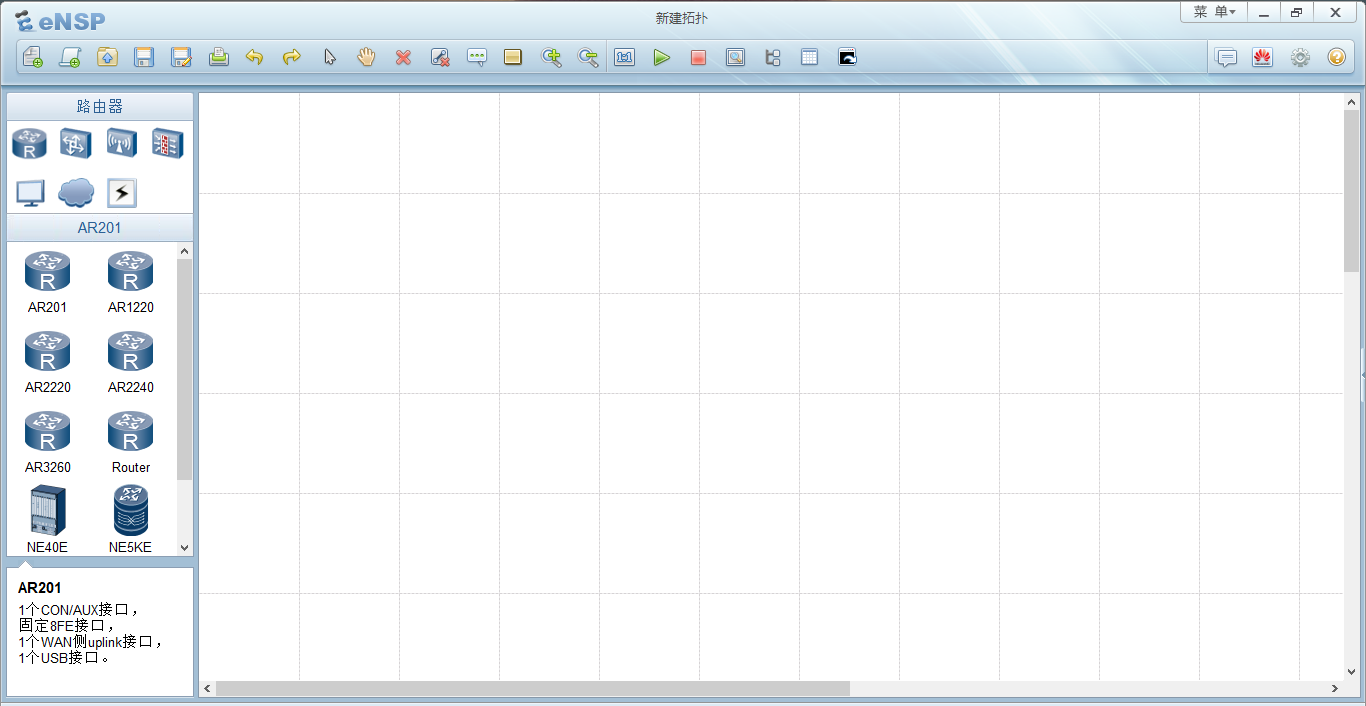
4.5其他措施

出于对财力的节省，服务器上不同的功能尽量在不同的主机上，可能有时候会将多种应用系统在一台主机上运行承担。例如：一台同时拥有HTTP服务和数据库服务的服务器考虑合并时，要对其处理能力和承受能力经行考虑，并且还要考虑各种安全级别的服务。比如操作系统：不同权限的授予可以有效提高安全级别。系统管理员也要重视并养成良好的习惯，比如定期检查漏洞，设置一些不易猜测和没有规律的密码来确保安全问题。

5网络模拟实现

5.1模拟器介绍

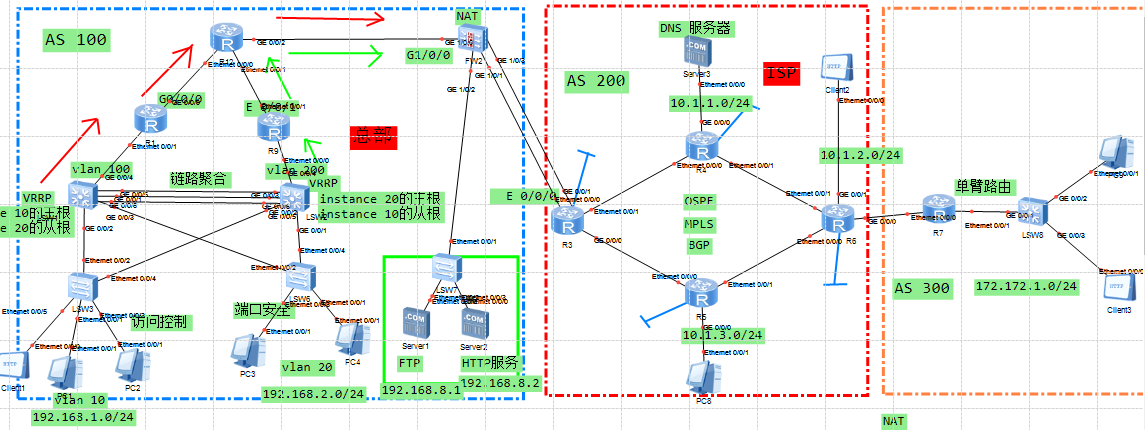
### eNSP(Enterprise Network Simulation Platform)是一款图形化网络仿真平台，里面具有免费的、可扩展的、图形化操作，都是由华为提供的。主要对企业网路由器、交换机进行软件仿真，帮助广大从事华为数通的人员快速熟悉该系列产品，了解并掌握其操作和配置，提升对企业网络的建设及规划，直观的体现真实设备情景。使广大从业者和客户在没有实体设备的时候可以学习并演练其网络技术。



5.2模拟环境拓扑图

由于公司规模较大，本次只能针对重要区域进行模拟配置。

网络拓扑如图：



5.3需求和配置

该公司该企业由于发展迅速，拓展了人员规模，急需扩大网络规模，交换机接入人员增加为原来的一倍，为避免出现流量拥塞请给出相应的解决方案；提高安全性，防止网络瘫痪，为避免新增的人员造成流量拥塞需增加带宽，在不造成经济浪费的情况下尽量节约成本；为防止核心由器出现突发性状况，可以实现数据流量迁移转发；为提高网络安全性，取消使用Internet公网，使用运营商网络进行搭建；为减少对公网地址的占用

需求：

1、再LSW1及LSW2上配置vrrp，为1.0和2.0网段实现网关备份

2、LSW1和LSW2上要求配置DHCP服务，基于接口地址池为所有PC分配IP地址。

3、LSW1和LSW2之间做链路聚合，工作模式为手工负载分担模式。

4、两台交换机都与上行路由器之间建立BFD会话并且与VRRP联动，当BFD会话Down掉后，自动降低优先级，进行主备切换

5、要求在PC3上开始端口安全功能，MAC学习地址上限为1，一旦介入非法用户，要求能够自动Down掉该接口

6、要求在AR1上进行访问控制，PC2不允许访问外网

7、在服务器区域，部署HTTP服务器和FTP服务器，要求内外网用户均能访问，需要在防火墙处配置NAT Sever，HTTP服务器对应的公网IP为13.2.2.100，域名为www.123.com，FTP对应的公网IP为13.2.2.101

8、防火墙上根据需求，配置相应的安全策略

9、分部处配置单臂路由实现不同vlan之间的互访

10、要求在在必要的接口配置边缘端口

11、在公网行存在DNS服务器，该服务器为所有公网用户访问总部的HTT服务器提供域名解析功能

配置：

防火墙内部属于AS100，运营商网络属于AS200，分部为AS300。

AS100内，IGP运行OSPF，进程为100

其公司内部网络属于trust区域，服务器是dmz区域，防火墙外部是untrust。

S1和S2是核心交换机，S3,S4是接入层交换机，R3是核心层路由器。

为防止重要电脑PC2出现不安全情况，在R1上进行访问控制PC2不允许访问外网。

要求在PC3上开启端口安全功能，MAC地址学习上限为1，一旦介入非法用户，要求能自动Down掉该接口。

该企业拓扑规划如上图所示，其中S1和S2是核心交换机，其上配置DHCP，方便用户的接入；配置MSTP和VRRP（vrrp是为了实现分担冗余，mstp可以阻塞多余的冗余链路，达到消除环路的目的），为实现分担冗余并消除环路达到优化网络目的；为实现

5.4

6测试

7总结

8致谢