《网络工程》

实验任务书

国防科学技术大学计算机学院

2024 年 11 月

目录

实验 1 VPN 配置

1. 实验目的

理解 VPN 的应用场景；
掌握 在路由器上VPN实例配置。

2. 实验设备

- 台式机
- 交换机
- 路由器
- 网线
- 配置线

3. 实验原理

3.1VPN介绍

随着社会的发展，IT 技术越来越多地影响现代企业的业务流程，如企业资源规划、基于 IP 网络的语音、会议和教学活动等，为企业的自动化办公和信息的获取提供了构架。随着网络经济的发展，越来越多的企业的分布范围日益扩大，合作伙伴日益增多，公司员工的移动性也不断增加。这使得企业迫切需要借助电信运营商网络连接企业总部和分支机构，组成自己的企业网，同时使移动办公人员能在企业以外的地方方便地接入企业内部网络。

最初，电信运营商是以租赁专线（Leased Line）的方式为企业提供二层链路，这种方式的主要缺点是：

- 建设时间长
- 价格昂贵
- 难于管理

传统专网难以满足企业对网络的灵活性、安全性、经济性、扩展性等方面的要求。这促使了一种新的替代方案的产生——在现有 IP 网络上模拟传统专网；这种新的解决方案就是虚拟专用网 VPN。VPN 通过骨干网建立专用数据传输通道，并利用隧道技术把 VPN 报文封装在此通道中，从而实现报文的透明传输。

VPN 具有以下两个基本特征：

- 专用（Private）：对于 VPN 用户，使用 VPN 与使用传统专网没有区别。VPN 与底层承载网络之间保持资源独立，即 VPN 资源不被网络中非该 VPN 的用户所使用；且 VPN 能够提供足够的安全保证，确保 VPN 内部信息不受外部侵扰。
- 虚拟（Virtual）：VPN 用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非 VPN 用户使用，VPN 用户获得的只是一个逻辑意义上的专网。这个公共网络称为 VPN 骨干网（VPN Backbone）。

利用 VPN 的专用和虚拟的特征，可以把现有的 IP 网络分解成逻辑上隔离的网络。这种逻辑隔离的网络应用丰富：可以用在解决企业内部的互连、相同或不同办事部门的互连；也可以用来提供新的业务，如为 IP 电话业务专门开辟一个 VPN，以此解决 IP 网络地址不足、QoS 保证、以及开展新的增值服务等问题。
从客户角度看，VPN 和传统专网相比具有如下优势：

- 安全：在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的连接，保证数据传输的安全性。这对于实现电子商务或金融网络与通讯网络的融合特别重要。
- 廉价：利用公共网络进行信息通讯，企业可以用更低的成本连接远程办事机构、出差人员和业务伙伴。
- 支持移动业务：支持驻外 VPN 用户在任何时间、任何地点的移动接入，能够满足不断增长的移动业务需求。
- 服务质量保证：构建具有服务质量保证的 VPN（如 MPLS VPN），可为 VPN 用户提供不同等级的服务质量保证。

从运营商角度看，VPN 具有如下优势：

- 可运营：提高网络资源利用率，有助于增加 ISP 的收益。
- 灵活：通过软件配置就可以增加、删除 VPN 用户，无需改动硬件设施。在应用上具有很大灵活性。
- 多业务：SP 在提供 VPN 互连的基础上，可以承揽网络外包、业务外包、客户化专业服务的多业务经营。

VPN 以其独具特色的优势赢得了越来越多的企业的青睐，使企业可以较少地关注网络的运行与维护，从而更多地致力于企业的商业目标的实现。另外，运营商可以只管理、运行一个网络，并在一个网络上同时提供多种服务，如 Best-effort IP 服务、VPN、流量工程、差分服务(Diffserv)，从而减少运营商的建设、维护和运行费用。

VPN 在保证网络的安全性、可靠性、可管理性的同时提供更强的扩展性和灵活性。在全球任何一个角落，只要能够接入到 Internet，即可使用 VPN。

3.2 VPN应用场景

根据业务用途不同，VPN 可以分为：

- 企业内部虚拟专网 Intranet VPN
  - Intranet VPN 通过公用网络进行企业内部的互联，是传统专网或其它企业网的扩展或替代形式。
  - 使用 Intranet VPN，企事业机构的总部、分支机构、办事处或移动办公人员可以通过公有网络组成企业内部网络。VPN 也用来构建银行、政府等机构的 Intranet。
  - 典型的 Intranet 例子就是连锁超市、仓储物流公司、加油站等具有连锁性质的机构。
- 扩展的企业内部虚拟专网 Extranet VPN
  - Extranet 利用 VPN 将企业网延伸至供应商、合作伙伴与客户处，在具有共同利益的不同企业间通过公网构筑 VPN，使部分资源能够在不同 VPN 用户间共享。
  - 在传统专线构建方式下，Extranet 需要维护网络管理与访问控制，甚至还需要在用户侧安装兼容的网络设备。虽然可以通过拨号方式构建 Extranet，但此时需要为不同的 Extranet 用户进行设置，同样降低不了复杂度。因合作伙伴与客户的分布广泛，拨号方式的 Extranet 需要昂贵的建设与维护费用。因此，企业常常放弃构建 Extranet，使得企业间的商业交易程序复杂化，商业效率被迫降低。
  - Extranet VPN 以其易于构建和管理为以上问题提供了有效的解决方案，其实现技术与 Intranet VPN 相同。目前，企业间通常使用 VPN 来构建 Extranet。为了保证 QoS，企业外部通讯一般不直接使用 Intranet。并且，企业间的通讯数据通常是敏感的，而 Extranet 的安全性比 Intranet 强。各 Extranet 用户访问 Extranet VPN 的权限可以通过防火墙等手段来设置与管理。
- 远程访问虚拟专网 Access VPN
  - Access VPN 使出差流动员工、家庭办公人员和远程小办公室可以通过廉价的拨号介质接入企业内部服务器，与企业的 Intranet 和 Extranet 建立私有网络连接。Access VPN 有两种类型：一种是用户发起（Client-initiated）的 VPN 连接，另一种是接入服务器发起（NAS-initiated）的 VPN 连接。

4. 实验任务

本实验模拟企业网络场景。利用VPN实例技术实现公司内员工所用电脑 client1 不可访问管理client4和client2；公司内管理员所用电脑client2 不可访问管理client3和client1。

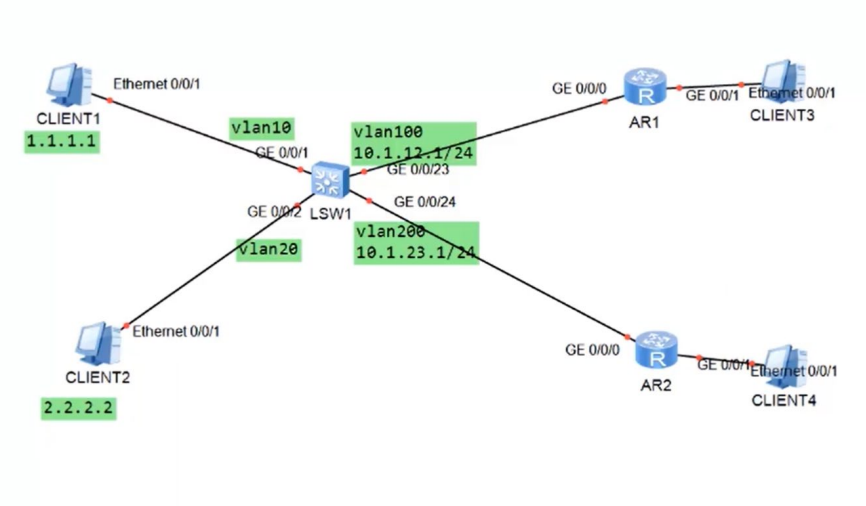


图1-1 VPN实例基本配置拓扑

5. 实验步骤

1) 规划并设计各设备IP地址并完成下表：

表 IP地址表

设备名	接口	IP地址	子网掩码	网关
Client1				
Client2				
Client3				
Client4				
LSW1				N/A
				N/A
				N/A
				N/A
AR1				N/A
				N/A
AR2				N/A
				N/A

2) 据图1-1完成网络连接并配置端口和VLAN的IP地址。
3) 在LSW1的根实例和AR1、AR2上建立路由，检查互通情况
4) 在LSW1上建立VPN实例，将vlan20和vlan200接口加入VPN实例
5) 在VPN实例上加入路由配置
6) 检查互通情况

6. 实验评测

对比第三步和第六步的互通结果。

实验 2 DHCP 配置

1. 实验目的

- 掌握DHCP Server配置方法；
- 掌握基于全局地址池的DHCP Server配置方法；
- 掌握配置 DHCP 租期/网关地址/不参与自动分配地址方法。

2. 实验设备

- 台式机
- 交换机
- 网线
- 配置线

3. 实验原理

基于接口地址池的DHCP服务器，连接这个接口网段的用户都从该接口地址池中获取IP地址等配置信息，由于地址池绑定在特定的接口上，可以限制用户的使用条件，因此在保障了安全性的同时也存在一定局限性。当用户从不同接口接入DHCP服务器且需要从同一个地址池里获取IP地址时，就需要配置基于全局地址池的DHCP。

配置基于全局地址池的DHCP服务器，从所有接口上连接的用户都可以选择该地址池中的地址，也就是说全局地址池是一个公共地址池。在DHCP服务器上创建地址池并配置相关属性（包括地址范围、地址租期、不参与自动分配的IP地址等），再配置接口工作在全局地址池模式。路由器支持工作在全局地址池模式的接口有三层接口及其子接口、三层Ethernet接口及其子接口、三层Eth-Trunk接口及其子接口和VLANIF接口。

表 DHCP 配置部分命令说明

操 作	命 令
使能DHCP 服务	DHCP { enable | disable }
配置DHCP 地址池中不参与自动分配的IP 地址范围	dhcp server forbidden-ip
创建DHCP 地址池并进入DHCP 地址池视图	dhcp server ip-pool
在地址池视图下配置DHCP 客户端使用	Network

的出口网关路由器的IP 地址	
在地址池视图下配置动态分配的IP 地址范围	stp root primary

4. 实验内容

本实验将路由器 R1 模拟成公司 DHCP Server，配置全局地址池，该公司市场部和财务部下的 PC 通过 DHCP 的方式自动配置 IP 地址。

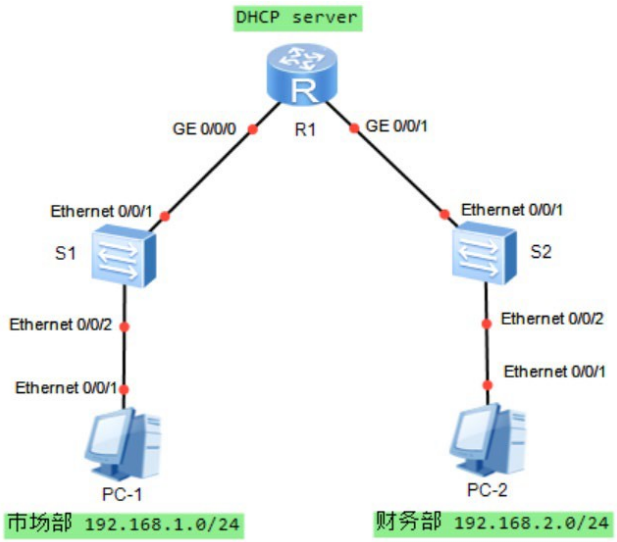


图 3 DHCP 拓扑图

5. 实验步骤

1) 根据图2-1完成网络连接及IP地址配置。
2) 配置基于全局地址池的DHCP Server。在R1上开启DHCP功能。
3) 使用ip pool命令创建一个全局地址池，地址池名称为huawei。
4) 使用network命令配置全局地址池huawei可分配的网段192.168.1.0。
5) 使用lease day命令配置DHCP全局地址池下的地址租期为2天。
6) 配置DHCP客户端的出口网关地址。
7) 配置地址池中192.168.1.250到192.168.1.253这些地址不参与自动分配。
8) 配置DNS服务器地址为8.8.8.8。
9) 开启接口的DHCP功能。使用该命令配置设备指定接口采用全局地址池为客户端分配IP地址。
10) 为财务部配置的全局地址池名称为huawei2，IP网段为192.168.2.0，网关地址为

192.168.2.254，DNS服务器地址为8.8.8.8。配置完成后在GE0/0/1接口下启用全局地址池的DHCP服务器模式。

6. 实验评测

使用 disp ip pool 查看 IP 地址池信息。
在台式机上使用 DHCP 获取 IP，查看获取到的 IP 地址，测试网络连通性。
释放获取到的 IP 地址，再次获取 IP 地址，是否有变化。

7. 思考题

1) DHCP服务器在分配地址时是从该网段中最小的地址还是最大地址进行分配？这样做的好处是什么？
2) 由于在IP地址动态获取的过程中，客户端采用广播方式发送请求报文，而广播报文不能跨网段传送，因此DHCP只适用于DHCP客户端和服务器处于同一个网段内的情况。当多个网段都需要进行动态IP地址分配时，就需要在所有网段上都设置一个DHCP服务器，这种情况下该如何配置？

实验 3　ACL 配置

1. 实验目的

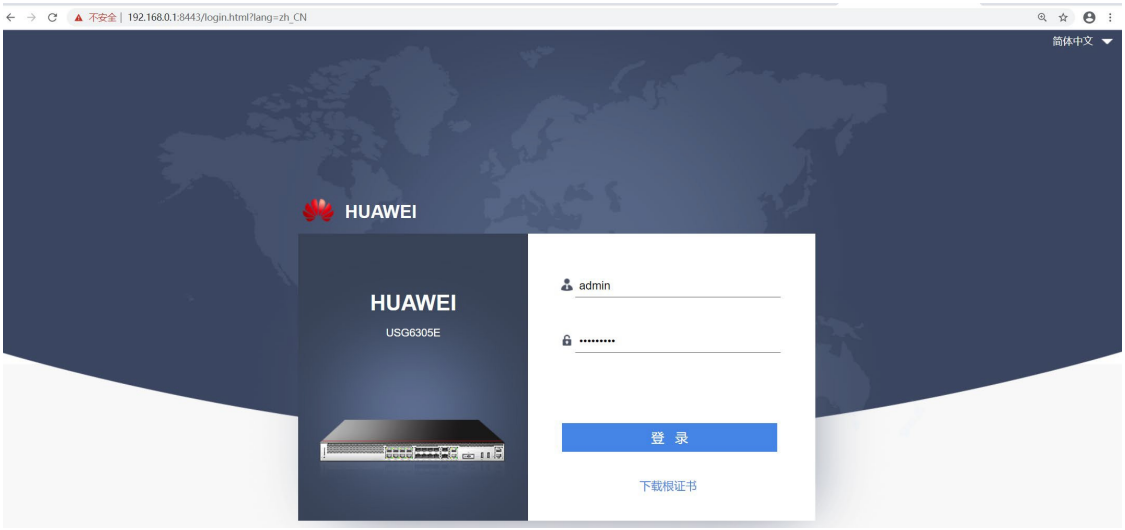
- 理解访问控制的应用场景
- 掌握配置防火墙访问控制的方法
- 了解访问控制原理。

2. 实验设备

- 台式机
- 防火墙
- 网线

3. 实验原理

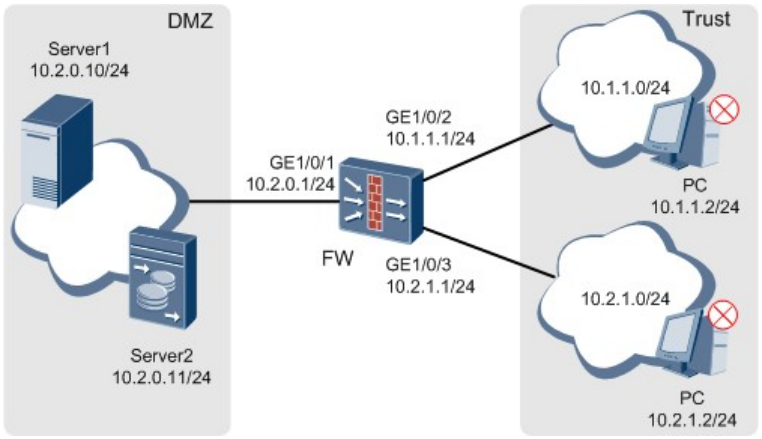
华为防火墙登陆说明：设置本机 IP 为 192.168.0.XX，使用浏览器访问防火墙 URL：https://192.168.0.1:8443。账号：admin，密码：admin@123（请勿修改密码）。



企业网络中的设备进行通信时，需要保障数据传输的安全可靠和网络的性能稳定。访问控制列表 ACL（Access Control List）可以定义一系列不同的规则，设备根据这些规则对数据包进行分类，并针对不同类型的报文进行不同的处理，从而可以实现对网络访问行为的控制、限制网络流量、提高网络性能、防止网络攻击等等。

4. 实验内容

如下图所示，某企业部署两台业务服务器，其中 Server1 通过 TCP 8888 端口对外提供服务，Server2 通过 UDP 69 端口对外提供服务。需要通过 FW 进行访问控制，8：00～17：00 的上班时间段内禁止 IP 地址为 10.1.1.2、10.2.1.2 的两台 PC 使用这两台服务器对外提供的服务。其他 PC 在任何时间都可以使用这两台服务器对外提供的服务。



5. 实验原理

1) 配置各接口基本参数。
2) 配置名称为 server_deny 的地址集，将几个不允许访问服务器的 IP 地址加入地址集。
3) 配置名称为 time_deny 的时间段，指定 PC 不允许访问服务器的时间。
4) 分别为 Server1 和 Server2 配置自定义服务集 server1_port 和 server2_port，将服务器的非知名端口加入服务集。
5) 配置安全策略，引用之前配置的地址集、时间段及服务集。

注意：系统默认存在一条缺省安全策略（条件均为 any，动作默认为禁止）。如果需要控制只有某些 IP 可以访问服务器，则需要保持缺省安全策略的禁止动作，然后配置允许哪些 IP 访问服务器的安全策略。另外安全策略是按照配置顺序匹配的，注意先配置细化的后配置宽泛的策略。例如需要控制在 10.1.1.0/24 网段中，除了某几个 IP 不能访问服务器外，其他的 IP 都可以访问。此时需要先配置拒绝特殊 IP 通过的安全策略，然后再配置允许整个网段通过的安全策略。

6. 实验评测

在 08:00 到 17:00 时间段内，IP 地址为 10.1.1.2、10.2.1.2 的两台 PC 无法使用这两台服务器对外提供的服务，在其他时间段可以使用。其他 PC 在任何时间都可以使用这两台服务器对外提供的服务。。

7. 思考题

（1） 在某防火墙安全规则配置时，已经允许从主机 A 到主机 B 通过 ICMP 协议，但使用 ping 测试时发现从 A 到 B 还是不通，请问是什么原因？

（2） 什么是 DMZ，设置 DMZ 有何意义？

实验 4 防火墙安全策略配置实验

1. 实验目的

- 理解地址转换的应用场景和原理
- 掌握配置防火墙地址转换的方法
- 了解基于源地址转换的 NAT。

2. 实验设备

- 台式机
- 防火墙
- 网线

3. 实验原理

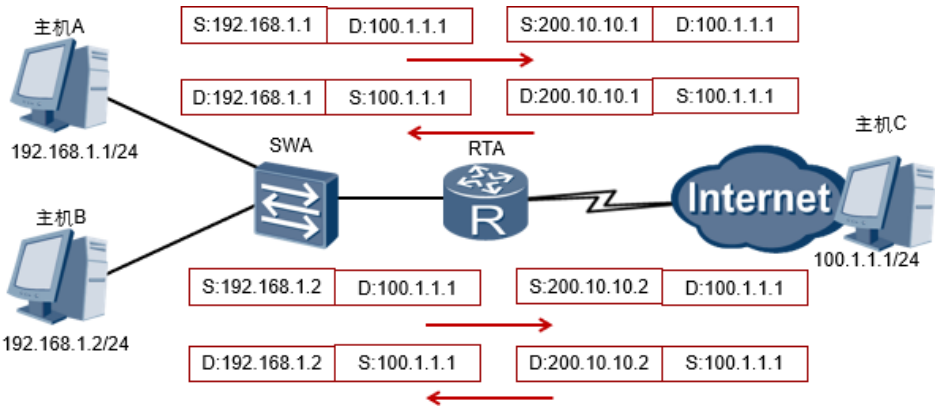
随着网络设备的数量不断增长，对 IPv4 地址的需求也不断增加，导致可用 IPv4 地址空间逐渐耗尽。解决 IPv4 地址枯竭问题的权宜之计是分配可重复使用的各类私网地址段给企业内部或家庭使用。但是，私有地址不能在公网中路由，即私网主机不能与公网通信，也不能通过公网与另外一个私网通信。

NAT 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程，主要用于实现内部网络（私有 IP 地址）访问外部网络（公有 IP 地址）的功能。NAT 一般部署在连接内网和外网的网关设备上。当收到的报文源地址为私网地址、目的地址为公网地址时，NAT 可以将源私网地址转换成一个公网地址。这样公网目的地就能够收到报文，并做出响应。此外，网关上还会创建一个 NAT 映射表，以便判断从公网收到的报文应该发往的私网目的地址。

NAT 的实现方式有多种，适用于不同的场景。

静态 NAT 实现了私有地址和公有地址的一对一映射。如果希望一台主机优先使用某个关联地址，或者想要外部网络使用一个指定的公网地址访问内部服务器时， 可以使用静态 NAT。但是在大型网络中，这种一对一的 IP 地址映射无法缓解公用地址短缺的问题。

如下图所示，源地址为 192.168.1.1 的报文需要发往公网地址 100.1.1.1。在网关 RTA 上配置了一个私网地址 192.168.1.1 到公网地址 200.10.10.1 的映射。当网关收到主机 A 发送的数据包后，会先将报文中的源地址 192.168.1.1 转换为 200.10.10.1 ，然后转发报文到目的设备。目的设备回复的报文目的地址是 200.10.10.1。当网关收到回复报文后，也会执行静态地址转换，将 200.10.10.1 转换成 192.168.1.1，然后转发报文到主机 A。和主机 A 在同一个网络中其他主机，如主机 B，访问公网的过程也需要网关 RTA 做静态 NAT 转换。



动态 NAT 通过使用地址池来实现。动态 NAT 地址池中的地址用尽以后，只能等待被占用的公用 IP 被释放后，其他主机才能使用它来访问公网。

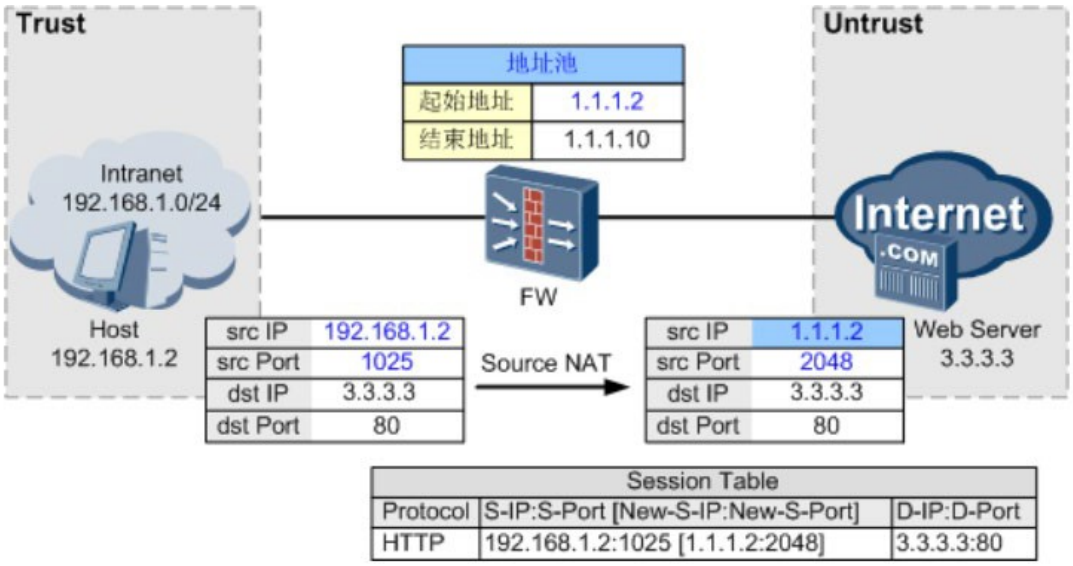
网络地址端口转换 NAPT（Network Address Port Translation）允许多个内部地址映射到同一个公有地址的不同端口。当 Host 访问 Web Server 时，FW 的处理过程如下：

FW 收到 Host 发送的报文后，根据目的 IP 地址判断报文需要在 Trust 区域和 Untrust 区域之间流动，通过安全策略检查后继而查找 NAT 策略，发现需要对报文进行地址转换。

FW 从 NAT 地址池中选择一个公网 IP 地址，替换报文的源 IP 地址，同时使用新的端口号替换报文的源端口号，并建立会话表，然后将报文发送至 Internet。

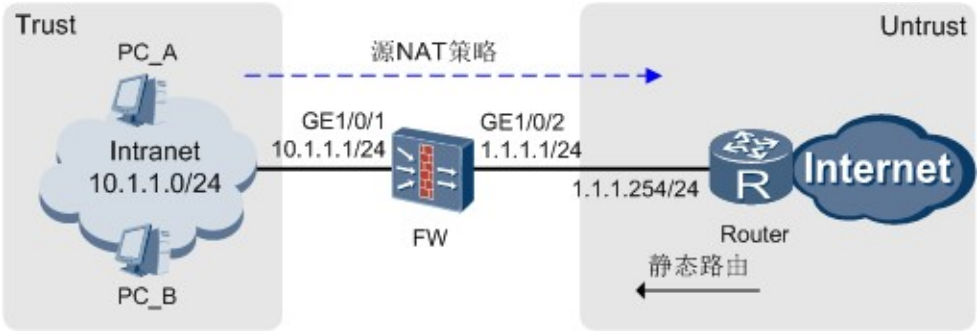
FW 收到 Web Server 响应 Host 的报文后，通过查找会话表匹配到步骤 2 中建立的表项，将报文的目的地址替换为 Host 的 IP 地址，将报文的目的端口号替换为原始的端口号，然后将报文发送至 Intranet。

此方式下，由于地址转换的同时还进行端口的转换，可以实现多个私网用户共同使用一个公网 IP 地址上网，FW 根据端口区分不同用户，所以可以支持同时上网的用户数量更多。



4. 实验内容

某公司在网络边界处部署了 FW 作为安全网关。为了使私网中 10.1.1.0/24 网段的用户可以正常访问 Internet，需要在 FW 上配置源 NAT 策略。除了公网接口的 IP 地址外，公司还向 ISP 申请了 6 个 IP 地址（1.1.1.10～1.1.1.15）作为私网地址转换后的公网地址。网络环境如下图所示，其中 Router 是 ISP 提供的接入网关。



5. 实验步骤

1) 配置接口 IP 地址和安全区域，完成网络基本参数配置。
2) 配置安全策略，允许私网指定网段与 Internet 进行报文交互。
3) 配置 NAT 地址池，配置时开启允许端口转换，以实现公网地址复用。
4) 配置源 NAT 策略，实现私网指定网段访问 Internet 时自动进行源地址转换。
5) 在 FW 上配置缺省路由，使私网流量可以正常转发至 ISP 的路由器。
6) 在私网主机上配置缺省网关，使私网主机访问 Internet 时，将流量发往 FW。
7) 在 Router 上配置静态路由，使从 Internet 返回的流量可以被正常转发至 FW。

6. 实验评测

内网主机能够访问路由器接口，且日志中有记录。

实验 5 异构网络综合设计实验（场景 1）

1. 实验目的

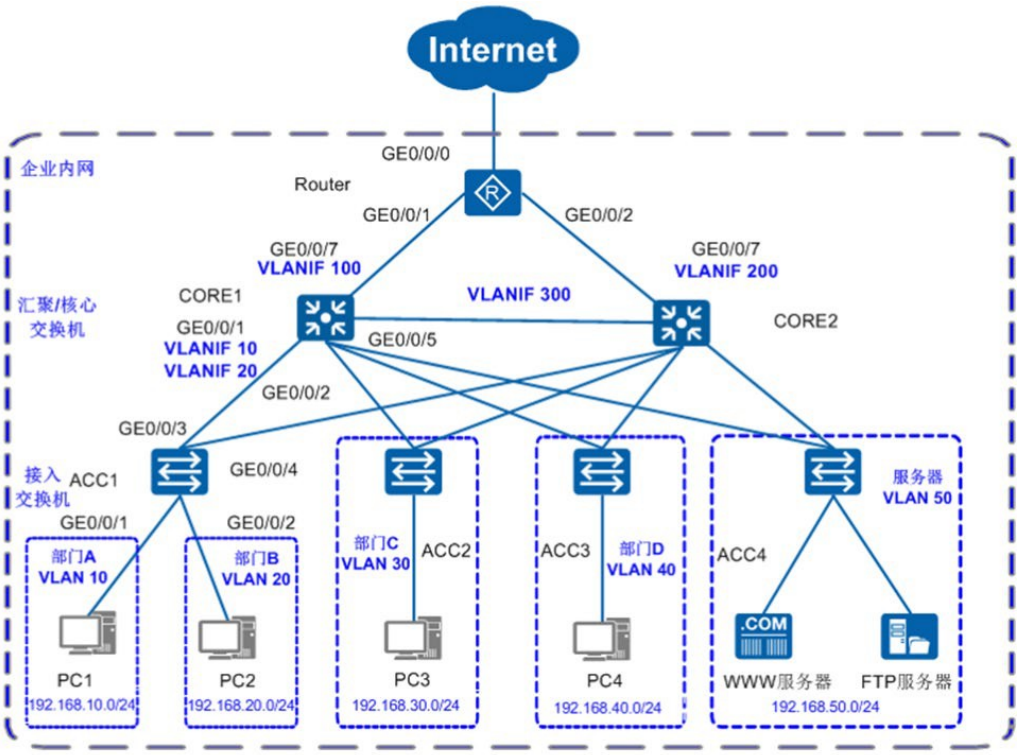
- 规划和设计中小型局域网，掌握常见网络应用的设置。

2. 实验设备

- 台式机
- 防火墙
- 交换机
- 路由器
- 网线

4. 实验内容

下图为中小园区常用配置。



要求：

核心交换机配置 VRRP 保证网络可靠性，配置负载分担有效利用资源。

每个部门业务划分到一个 VLAN 中，部门间的业务在 CORE 上通过 VLANIF

三层互通。

核心交换机作为 DHCPServer，为园区用户分配 IP 地址。

接入交换机上配置 DHCPSnooping 功能，防止内网用户私接小路由器分配 IP 地址；同时配置 IP 报文检查功能，防止内网用户私自更改 IP 地址。

5. 实验步骤

操作	准备项	数据	说明
配置管理IP和Telnet	管理口IP地址	10.10.1.1/24	管理IP用于登录交换机。
	管理VLAN	VLAN 5	框式交换机管理口是Ethernet0/0/0。 盒式交换机管理口是MEth0/0/1。 对于没有管理口的交换机建议使用VLANIF接口进行带内管理。
配置接口和VLAN	端口类型	连接交换机的端口建议设置为trunk，连接PC的端口设置为access。	trunk 类型端口一般用于连接交换机。 access 类型端口一般用户连接PC。 hybrid类型端口是通用端口，既可以用来连接交换机，也可用来以连接PC。
	VLAN ID	ACC1：VLAN 10 20 CORE1： VLAN 10、20、30、40、50、100、300	交换机有缺省VLAN1。 为二层隔离部门A和部门B，将部门A划分到VLAN 10中，部门B划分到VLAN 20中。 CORE1通过VLANIF100连接出口路由器。
配置DHCP	DHCP Server	CORE1、CORE2	在CORE1、CORE2上部署DHCP Server。
	地址池	VLAN 10：ip pool 10 VLAN 20：ip pool 20	部门A的终端从ip pool 10中获取IP地址。 部门B的终端从ip pool 20中获取IP地址。
	地址分配方式	基于全局地址池	无
配置核心交换机	IP地址	CORE1: VLANIF100 172.16.1.1/24 VLANIF300 172.16.3.1/24 VLANIF10 192.168.10.1/24 VLANIF20 192.168.20.1/24	VLANIF100用于CORE1与园区出口路由器对接。VLANIF300用于CORE1与CORE2对接。 CORE1上需要配置一条主用路由，下一跳指向出口路由器；一条备用路由，下一跳指向CORE2。 在CORE1上配置VLANIF10、VLANIF20的IP地址后，部门A与部门B之间可以通过CORE1互访。
	链路聚合	—	Eth-Trunk链路聚合有手工负载分担和静态LACP两种工作模式。

操作	准备项	数据	说明
配置出口路由器	公网接口IP地址	GE0/0/0：1.1.1.2/30	GE0/0/0用于出口路由器连接Internet的接口，一般称为公网接口。
	公网网关	1.1.1.1/30	该地址是与出口路由器对接的运营商设备的IP地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至Internet。
	DNS地址	8.8.8.8	DNS服务器用于将域名解析成IP地址。
	内网接口IP地址	GE0/0/1：172.16.1.2/24 GE0/0/2：172.16.2.2/24	GE0/0/1、GE0/0/2为出口路由器连接内网的接口，GE0/0/1连接主设备，GE0/0/2连接备设备。
配置DHCP Snooping和IPSG	信任接口	GE0/0/3 GE0/0/4	配置信任接口后，用户只会接收从信任接口进入的DHCP报文，防止内网私接小路由器为主机分配IP地址。
配置内网服务器	FTP服务器 WWW服务器	FTP服务器：192.168.50.10 WWW服务器：192.168.50.20	1、出口路由器会通过NAT实现服务器公网地址和私网地址之间的映射。 2、外网用户可以通过访问公网地址访问服务器。

1) 配置管理 IP 和 Telnet（可选）
2) 配置网络互联互通。
3) 配置 DHCP
4) 配置 OSPF
5) 配置可靠性和负载均衡
6) 配置链路聚合
7) 配置限速（可选）
8) 配置映射内网服务器和公网多出口

6. 实验评测

部门内部选两台 PC 进行 ping 测试，验证部门内部二层互通是否正常。

从两个部门内各选一台 PC 进行 ping 测试，验证部门之间通过 VLANIF 实现三层互通是否正常。

每个部门各选一台PC 进行ping 公网地址测试，验证公司内网用户访问Internet是否正常。

实验 6 异构网络综合设计实验（场景 2）

1. 实验目的

- 规划和设计中小型局域网，掌握常见服务器的设置。

2. 实验设备

- 台式机
- 防火墙
- 交换机
- 路由器
- 网线

3. 实验原理

园区网出口一般位于企业网内部网络与外部网络的连接处，是内部网络与外部网络之间数据流的唯一出入口。对于中小型企业来说，考虑到企业网络建设的初期投资与长期运维成本，一般希望将多种业务部署在同一设备上。企业网络用户一般同时需要访问 Internet 和私网 VPN，而对于中小型企业来说考虑到建设及维护成本问题，一般租用运营商 Internet 网络组建私网 VPN。对于部分可靠性要求较高的园区网络，一般考虑部署两台出口路由器做冗余备份实现设备级可靠性，同时应用链路聚合、VRRP、主备路由等技术保证园区出口的可靠性。

园区出口设备需要具备 NAT Outbound 及 NAT Server 的功能，实现私网地址和公网地址之间的转换，以满足用户访问 Internet 或者 Internet 用户访问内网服务器的需求。

园区出口设备需要具备通过 Internet 构建私网 VPN 的功能，以满足企业用户各个机构之间私网 VPN 互通的需求。

园区出口设备需要具备数据加密传输的功能，以保证数据的完整性和机密性，保障用户业务传输的安全。

中小型园区出口需要具备可靠性、安全性、低成本、易维护等特点。

4. 实验内容

某企业总部和分支分别位于不同的城市，地域跨度较远，总部存在 A、B 两个不同的部门，分支只有一个部门。现在需要建设跨地域的企业园区网络，需要实现的需求如下：

总部和分支都需要实现用户访问 Internet 的需求。总部划分为 A、B 两个部门，其中 A 部门的用户可以访问 Internet，但是 B 部门的用户不能访问 Internet；分支所

有用户都可以访问 Internet。

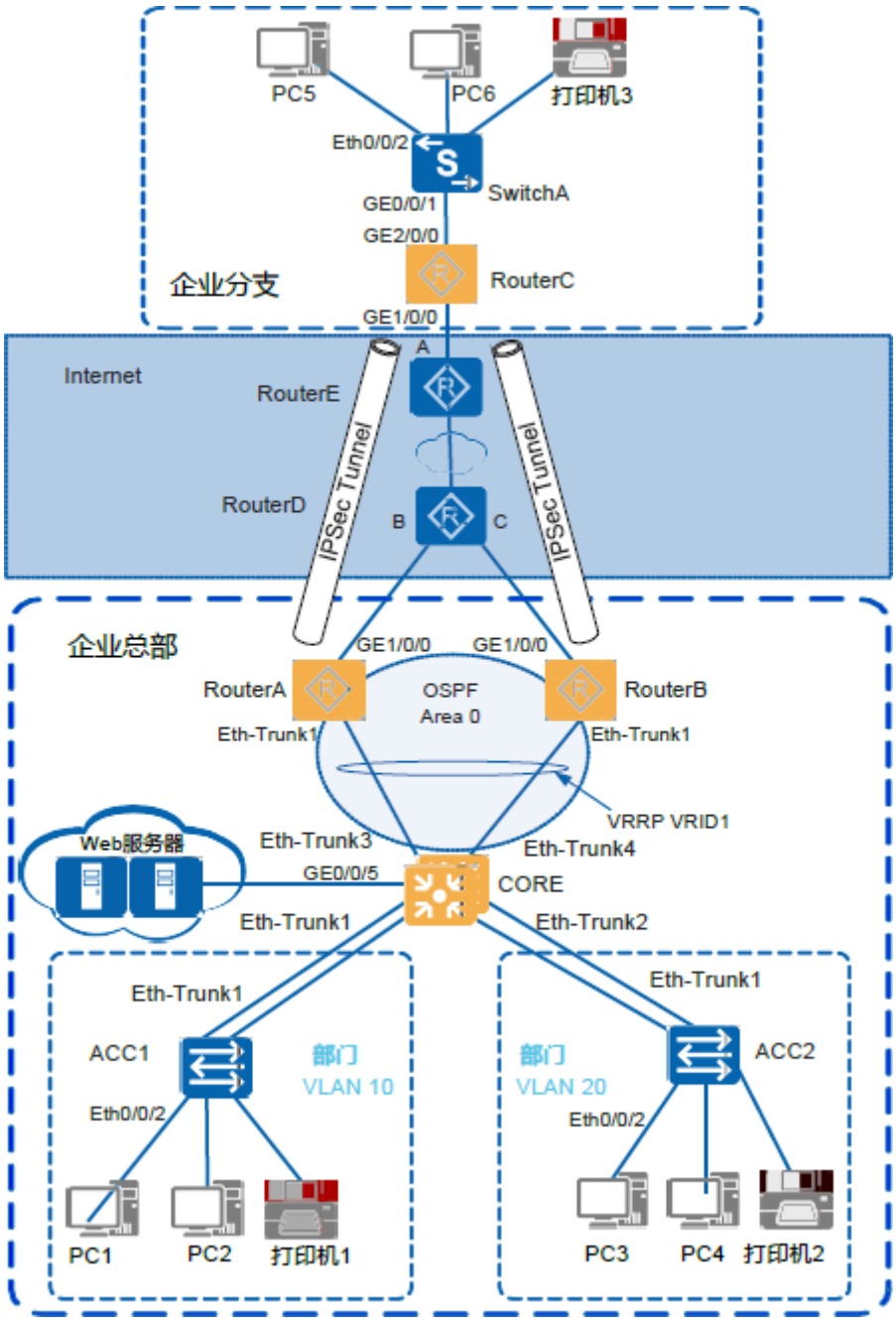
总部有 Web 服务器，对外提供 WWW 服务，外网用户可以访问内网服务器。

总部和分支之间需要通过 Internet 进行私网 VPN 互通，通信内容需要有安全保护。

总部园区出口可靠性要求较高，需要考虑链路级的可靠性和设备级的可靠性。

分支可以适当降低可靠性要求。

根据用户需求，可以给出如下图所示的综合配置解决方案，该方案具备层次化、模块化、冗余性、安全性的特点，适用于中小型企业/分支的园区网络部署。



要求：

接入交换机与核心交换机通过 Eth-Trunk 组网保证可靠性。

每个部门业务划分到一个 VLAN 中，部门间的业务在 CORE 上通过 VLANIF 三层互通。

核心交换机作为 DHCPServer，为园区用户分配 IP 地址。

接入交换机上配置 DHCPSnooping 功能，防止内网用户私接小路由器分配 IP 地址；同时配置 IPSG 功能，防止内网用户私自更改 IP 地址。

5. 实验步骤

1) 部署总部及分支园区内网

总部：部署堆叠、链路聚合，配置各 VLAN 及 IP 地址、部署 DHCP Server，实现园区内网互通。部门内部通过接入层交换机进行二层互通，部门间通过核心交换机 CORE 上的 VLANIF 进行三层互通。分支：配置接入层交换机及出口路由器的各接口 VLAN 及 IP 地址，部署 DHCPServer，实现分支园区内网互通。

2) 部署 VRRP

为了保证总部核心交换机与两个出口路由器之间的可靠性，在两个出口路由器之间部署 VRRP，VRRP 的心跳报文经过核心交换机进行交互。RouterA 为 Master 设备，RouterB 为 Backup 设备。为了防止总部 RouterA 上行链路故障的时候业务断流，将 VRRP 状态与 RouterA 的上行口进行联动，保证上行链路故障时 VRRP 进行快速倒换。

3) 部署路由

为了引导各设备的上行流量，在总部核心交换机上配置一条缺省路由，下一跳指向 VRRP 的虚地址，在总部及分支的出口路由器上各配置一条缺省路由，下一跳指向运营商网络设备的对接地址（公网网关）。为了引导总部两个出口路由器的回程流量，在两个出口路由器和核心交换机之间部署 OSPF，核心交换机上将所有用户网段发布到 OSPF 里面，通告给两个出口路由器。为了引导外网用户访问 Web 服务器的流量，需要在总部的运营商路由器上配置两条目的地址为服务器公网地址的静态路由，下一跳分别指向两个出口路由器的上行口 IP 地址。并且为了保证路由和 VRRP 同步切换，设置下一跳为 RouterA 的这条路由优先，当这条路由失效的时候下一跳指向 RouterB 的路由生效。

4) 部署 NAT Outbound

为了使内网用户访问 Internet，在两台出口路由器的上行口配置 NAT，实现私网地址和公网地址之间的转换。通过 ACL 匹配 A 部门的源 IP 地址，从而实现 A 部门的用户可以访问 Internet，而 B 部门的用户不能访问 Internet。

5) NAT Server

为了实现外网用户访问内网 Web 服务器，在两个出口路由器的上行口上配置 NAT Server，实现服务器公网地址和私网地址之间的映射。

6) 部署 IPSec VPN

为了实现总部和分支之间进行私网 VPN 互通，在总部出口路由器和分支出口路由器之间部署 IPSec VPN，通过 Internet 构建IPSec VPN，实现总部和分支之间的安全通信。

6. 实验评测

PC1 和 PC5、PC3 和 PC5 之间都是可以互通的，公司总部和分支之间可以通过运营商网络组建的私网 VPN 进行互通。部门 A（PC1）的用户可以访问公网，部门 B（PC3）的用户不能访问公网。

实验 7 异构网络综合设计实验（场景 3）

一个完整的组网工程包括需求分析、方案设计、设备选型与采购、硬件安装与配置、软件安装与配置、系统测试与联调、工程验收等若干个环节，其中硬件与应用系统安装、配置工作量大，技术含量高，是信息系统集成或网络工程的关键环节， 其中既涉及到技术上的问题，也涉及到工程组织、协调配合上的问题，一个网络工程师只有通过多次工程的实际锻炼，不断积累经验、吸取教训才能提高自己的水平。

1. 实验目的

通过对常用的组网设备（包括交换机、路由器、防火墙）、常见的网络服务系统（Web 服务、Smtp & Pop3 服务等）的安装与配置与调试实验，加深对上述设备和系统工作原理的理解，初步掌握其安装配置方法，为将来从事网络工程建设打下基础。

2. 实验设备

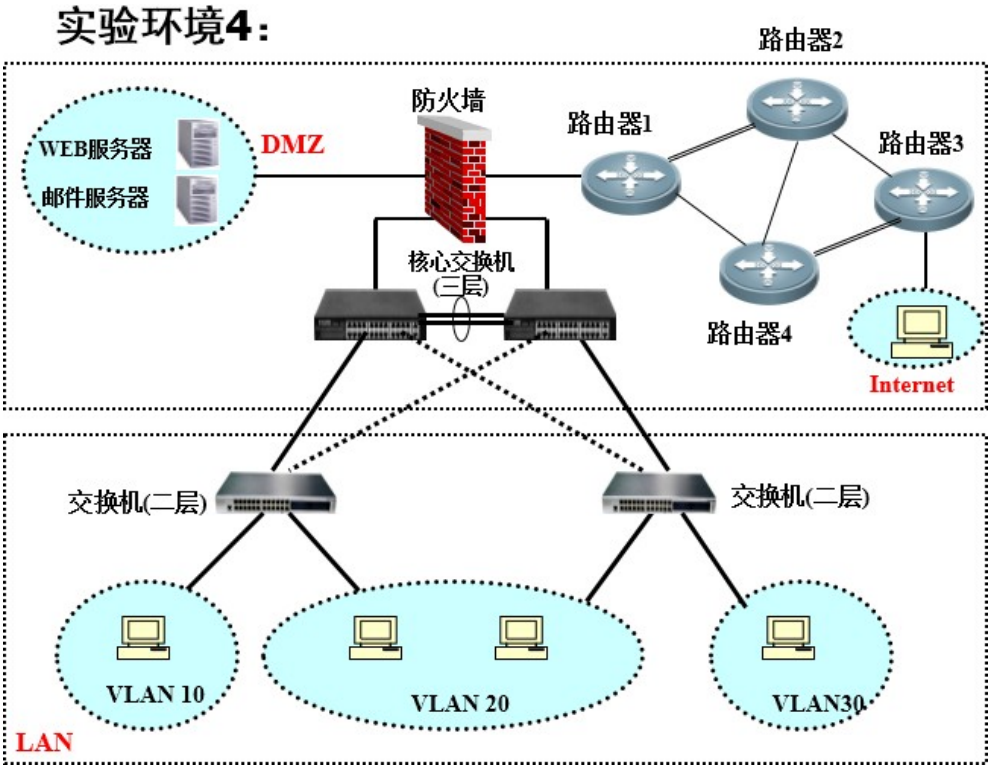
- 台式机
- 防火墙
- 交换机
- 路由器
- 网线

3. 实验内容

设计并构建一个中小型的校园网络平台，并在该平台上构建 INTERNET 服务平台，该网络工程建成后，将具有以下服务功能（如下所示）：

① 具有内部 Web 服务功能；
② 具有外部 Web 服务代理功能 ；
③ 具有邮件收发功能；
④ 具有对内部核心子网安全保护功能；
⑤ 具有简单的内外网有限制访问功能。

可参考下图的拓扑结构，也可以基于下图进行改进。



4. 实验步骤

4.1 WEB 服务

- 建立一个内部 WEB 服务网站： www.test.com ， 设计测试网页；
- 在外部网站上提供 3 个虚拟主机服务： www.test1.com, www.test2.com, www.test3.com ， 并设计相应的测试网页。

4.2 邮件服务

（1） SMTP 服务器安装与配置

- 安装 SMTP 服务器：在 Linux 环境下，使用 sendmail 8.13 源代码，进行编译、安装和基本配置，构建 2 个 SMTP 服务器 smtp.nudt.com ， smtp.test.com；
- 建立邮件测试帐号：abc@nudt.com, xyz@nudt.com, test@test.com ；
- 向所在邮件服务器上的帐号发送邮件：使用帐号 abc@nudt.com，在 PC 机上通过命令行 telnet smtp.nudt.com 25 和 outlook 向 smtp.nudt.com 服务器上的用户 xyz@nudt.com 发送测试邮件；
- 向其它邮件服务器上的帐号发送邮件：使用帐号 abc@nudt.com ，在 PC 机上通过命令行 telnet smtp.nudt.com 25 和 outlook 向 smtp.test.com 服务器的用户 test@test.com 发送测试邮件；

（2） SMTP 服务器安装与配置

- 安装 POP3 邮件服务器：在 Linux 环境下，对 Qpopper 4.05 源代码进行编译、

安装和基本配置，构建 2 个 POP3 服务器 pop3.nudt.com , pop3.test.com；

- 使用 POP3 接收邮件：分别使用上述三个邮件帐号： abc@nudt.com , xyz@nudt.com，test@test.com，通过 telnet pop3.nudt.com 110 和 outlook 从两个 POP3 服务器上接收前面发送的测试邮件。

4.3 交换机和路由器

对交换机和路由器进行配置，具体内容包括：

- VLAN 划分与配置
- 链路聚合协议配置
- RSTP 生成树协议配置
- VRRP 协议配置
- 动态路由协议配置

4.4 防火墙

在防火墙上，通过 GUI 界面，按下面安全策略的要求对包过滤规则进行配置：

- 允许 LAN 上任何设备访问通过 80 端口访问 DMZ 中的 Web Server;
- 允许 LAN 上任何设备访问通过 25 和 110 端口访问 DMZ 中的 Mail ;
- 允许 LAN 上任何设备访问通过 ICMP 协议访问 DMZ 中的任何设备;
- 允许 LAN 上任何设备访问 Internet;
- 允许 Internet 上的任何设备通过 80 端口访问 DMZ 中的 Web Server;
- 允许 Internet 上的任何设备通过 25 和 110 端口访问 DMZ 中的 Mail;
- 拒绝 Internet 上的任何设备通过任何端口访问 LAN；
- 拒绝 Internet 上的任何设备通过其它任何端口访问 DMZ；
- 拒绝 DMZ 上的任何设备通过任何其它端口访问 LAN 和 Internet。在

防火墙上，通过 GUI 界面，按下面安全策略的要求对 NAT 进行配置：

- 允许 LAN 上任何设备通过公共的地址池 202.198.31.200—202.198.31.254 动态地访问 Internet 上的 任何设备。
- 允许 Internet 上的任何设备通过 IP 为 202.198.31.100，端口为 80 访问 DMZ 中的 Web Server;
- 允许 Internet 上的任何设备通过 IP 为 202.198.31.101，端口为 25 和 110 端口访问 DMZ 中的 Mail Server。

5. 实验评测

根据实验要求，针对每一个实验内容，自行设计评测方法进行验证。

附：设备清空配置

交换机清空配置:

用备份文件覆盖当前配置

```
copy backup.zip vrpcfg.zip
```

注意后面的问题，三个 Y。

```
reboot
```

注意后第一个 N，第二个 Y。如下图所示。

```
<SW3>copy backup.zip vrpcfg.zip
Copy flash:/backup.zip to flash:/vrpcfg.zip?[Y/N]:Y
The file flash:/vrpcfg.zip exists. Overwrite it?[Y/N]:Y
Warning: The file flash:/vrpcfg.zip is a system resource file that is in use, ov
erwrite it?[Y/N]:Y
100%  complete.
Info: Copied file flash:/backup.zip to flash:/vrpcfg.zip...Done.
<SW3>reboot
Info: The system is now comparing the configuration, please wait.............
..
Warning: The configuration has been modified, and it will be saved to the next s
tartup saved-configuration file flash:/vrpcfg.zip. Continue? [Y/N]:N
Info: If want to reboot with saving diagnostic information, input 'N' and then e
xecute 'reboot save diagnostic-information'.
System will reboot! Continue?[Y/N]:Y_
```

路由器清空配置:

```
startup saved-configuration backup.zip
reboot fast
Y
```

重启后会让重新配置密码，请输入 **admin@123**

```
  Press any key to get started

Please configure the login password (<8-128>)
Enter password:
Confirm password:
```