**《计算机网络》实验指导书**

**实验四：组网设计与配置实验**

重庆大学计算机学院专业实验室

二零二二年十一月

**目录**

[1. 综合实验 组网设计与配置 1](#_Toc120969373)

[1.1. 实验目标 1](#_Toc120969374)

[1.2. 实验内容 1](#_Toc120969375)

[1.2.1. 实验组网图 1](#_Toc120969376)

[1.2.2. 实验内容 1](#_Toc120969377)

[1.2.3. 实验要求 2](#_Toc120969378)

[1.2.4. 实验步骤 3](#_Toc120969379)

[1.2.5. 实验报告提交结果 5](#_Toc120969380)

[2. 补充知识点1 三层交换机配置 5](#_Toc120969381)

[2.1. 实验目标 5](#_Toc120969382)

[2.2. 三层交换机 5](#_Toc120969383)

[2.3. 实验内容 6](#_Toc120969384)

[2.3.1. 实验组网图 6](#_Toc120969385)

[2.3.2. 实验内容 7](#_Toc120969386)

[3. 补充知识点2 路由协议混合组网 8](#_Toc120969387)

[3.1. 实验目标 8](#_Toc120969388)

[3.2. 实验内容 9](#_Toc120969389)

[4. 补充知识点3 简单防火墙配置 11](#_Toc120969390)

[4.1. 实验目标 11](#_Toc120969391)

[4.2. 实验内容 11](#_Toc120969392)

[4.2.1. 实验组网图 11](#_Toc120969393)

[4.2.2. 实验内容 11](#_Toc120969394)

[**文档版本** 14](#_Toc120969395)

# 综合实验 组网设计与配置

## 实验目标

* 掌握三层交换机VLAN配置、混合路由协议组网及简单防火墙配置。
* 通过组网设计，加深对小型网络的组建及网络设备配置的掌握，初步具备小型网络建网的能力。
* 能综合利用所学知识，实现小型网络的互连互通。
* 具备对小型网络系统进行分析的能力。

## 实验内容

### 实验组网图

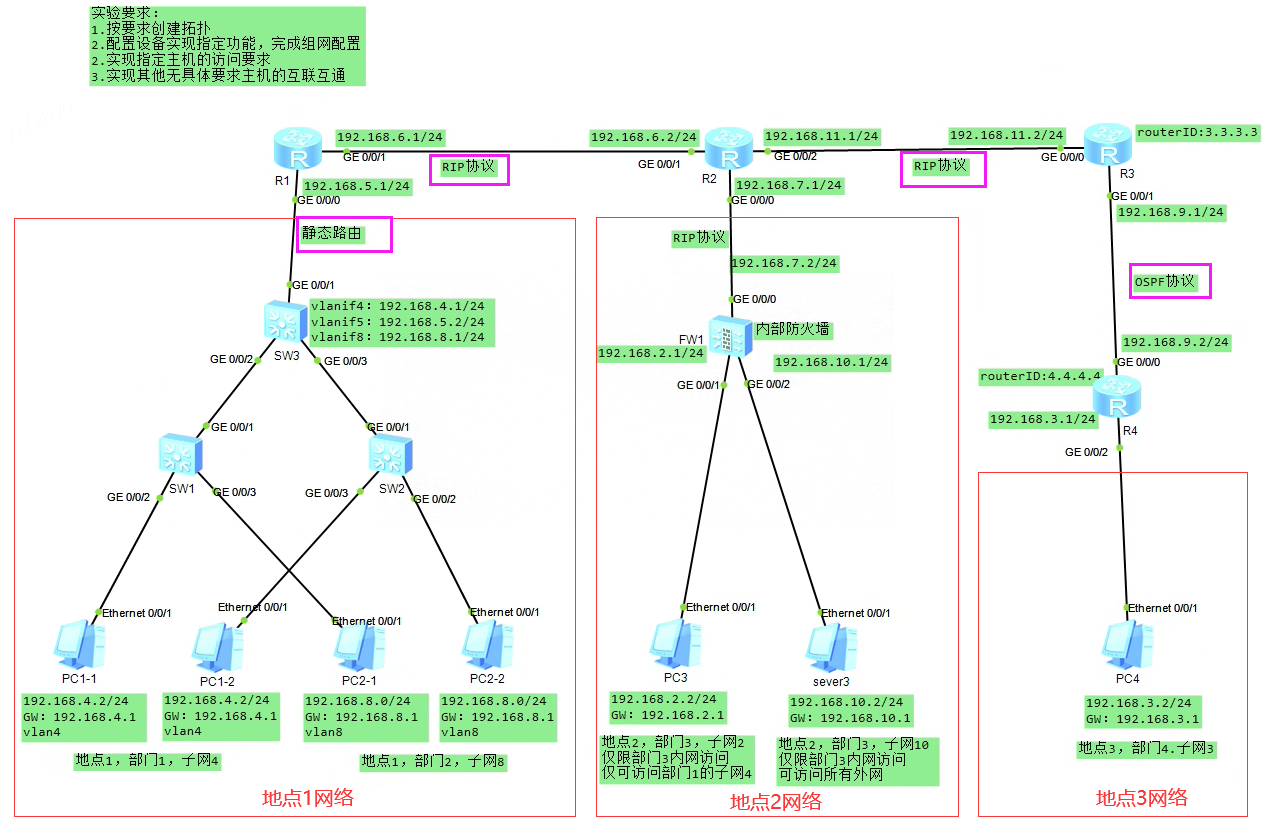


图 1 组网拓扑

### 实验内容

假设某公司在三地设立了办公点，其详细网络拓扑如图 1所示，各地点之间通过路由器（三层交换机可作为路由器使用）相互连接进行通信，各部门子网需按照以下需求实现通信：

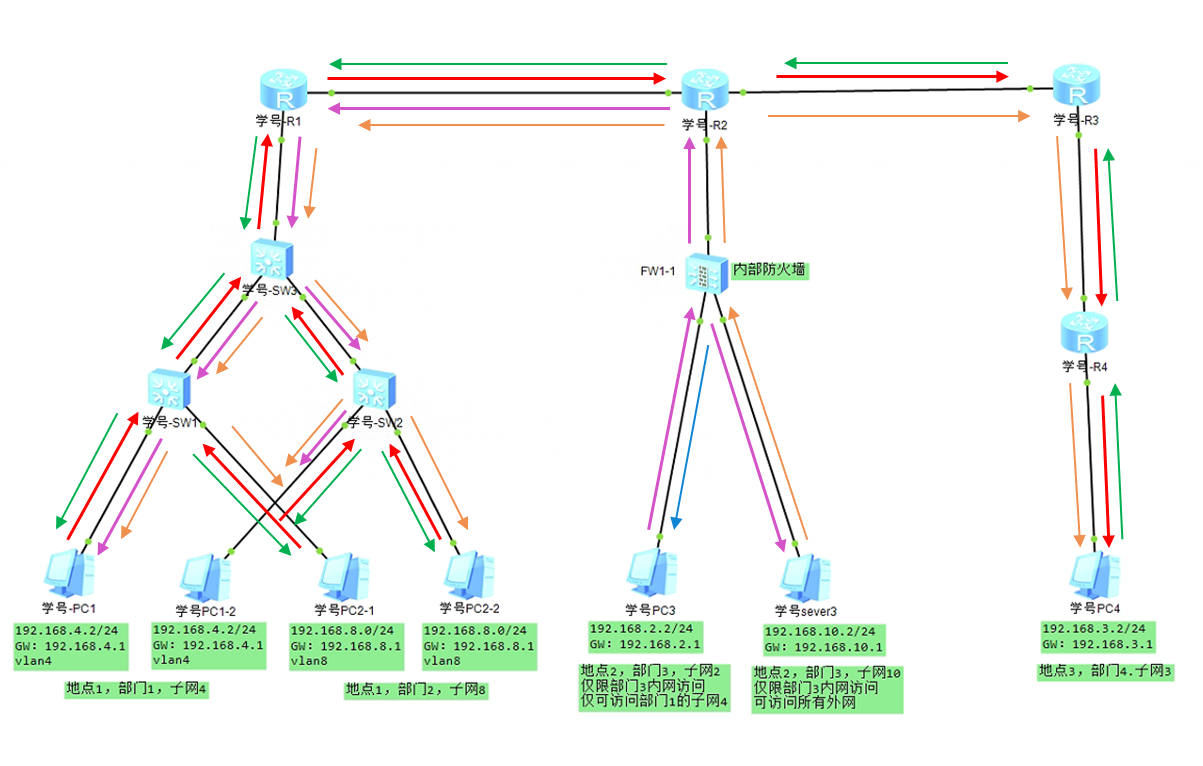
1. 三地通过路由器连接实现通信，其中，地点1与地点2为直连路由（R1-R2），路由协议采用**RIPv1**；地点2与地点3之间通过三台路由器直连（R2-R3-R4），R2-R3路由协议采用**RIPv1**，R3-R4路由协议采用**OSPF**。地点1中三层交换机SW3与路由器R1间采用**静态路由**实现跨网端通信，地点2中防火墙FW1与R2间采用路由协议**RIPv1**。
2. 地点1中的2个部门分属2个子网，分别处于不同VLAN下：**子网4处于VLAN4，子网8处于VLAN8**，2个子网通过三台交换机（SW1、SW2、SW3）实现二者间的通信。
3. 地点2中仅有1个重要部门，包含子网2与子网10。因业务要求需进行防火墙配置，实现部门3中的网络设备仅限其内部子网可访问，子网2中设备可访问外网中部门1的子网4，子网10中服务器可访问外网所有子网。
4. 地点3中的1个部门包含子网3。
5. 通过路由配置，地点1中网络设备可与地点3中网络设备互联互通，二者不能访问地点2中网络设备，地点2中设备按照3）实现外网访问。

### 实验要求

根据上文描述，请完成本次实验的具体要求：

1. 根据图 1创建网络拓扑图。
2. 正确网络设备IP信息（IP信息与图 1保持一致，修改设备名称含学号信息）。
3. 按照1.2.2实验内容的需求描述，配置交换机、路由器及防火墙。
4. 实现地点1和地点3中的5台设备能两两ping通。
5. 实现地点1与地点3中设备不能ping通地点2中设备。
6. 实现地点2中设备可以两两ping通。
7. 实现子网2中设备可以ping通子网4中设备，子网10中设备可以ping通外网所有设备。

设备可连通详情如下图：



设备连通情况如下表：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | PC1-1 | PC1-2 | PC2-1 | PC2-2 | PC3 | sever3 | PC4 |
| PC1-1 | **-** | **√** | **√** | **√** | **×** | **×** | **√** |
| PC1-2 | **√** | **-** | **√** | **√** | **×** | **×** | **√** |
| PC2-1 | **√** | **√** | **-** | **√** | **×** | **×** | **√** |
| PC2-2 | **√** | **√** | **√** | **-** | **×** | **×** | **√** |
| PC3 | **√** | **√** | **×** | **×** | **-** | **√** | **×** |
| sever3 | **√** | **√** | **√** | **√** | **√** | **-** | **√** |
| PC4 | **√** | **√** | **√** | **√** | **×** | **×** | **-** |

说明：

1. 表格纵向标题表示源地址，横向标题表示目的地址。

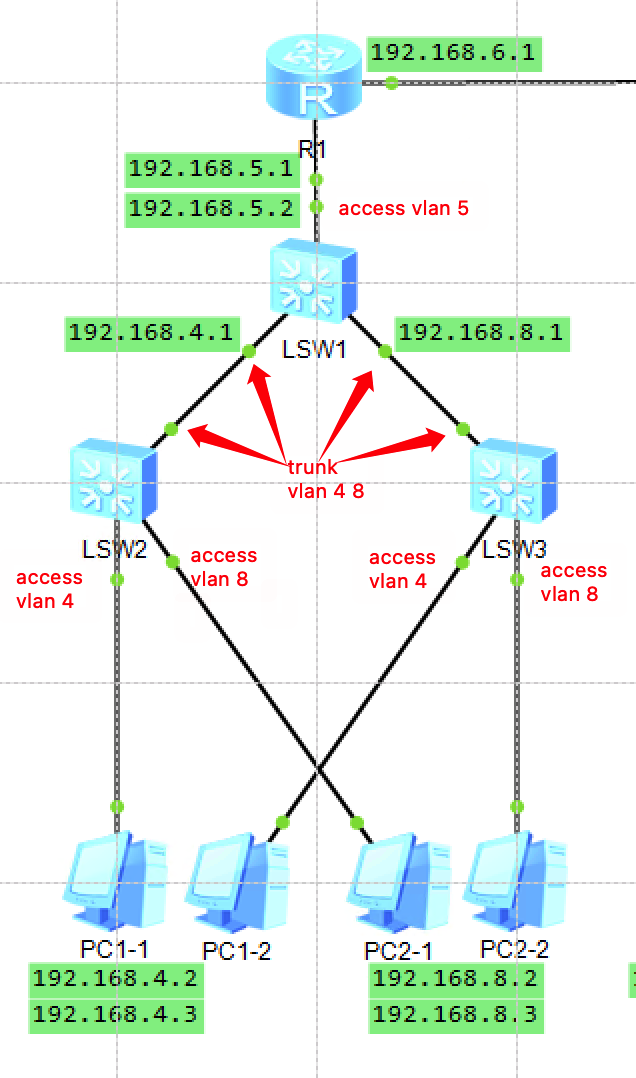
2. √表示可连通，×表示不可连通。

### 实验步骤

#### 搭建拓扑，设置PC和sever的IP及网关。

#### 配置网地点1网络

1. SW1和SW2：创建VLAN，添加端口到对应VLAN，配置access、trunk链路类型。
2. SW3：创建VLAN，设置链路类型，配置Vlanif。
3. **PC1-1、PC1-2、PC1-3、PC1-4可两两互通。**



#### 配置路由

1. SW3：添加默认路由（或静态路由）。
2. R1：配置端口，添加静态路由，配置RIP。（涉及import-route xxx，详见补充知识点2）
3. R2：配置端口，配置RIP。
4. R3：配置端口，配置RIP，配置OSPF。（涉及import-route xxx，详见补充知识点2）
5. R4：配置端口，配置OSPF。
6. **PC4与PC1-1、PC1-2、PC1-3、PC1-4可两两互通。**
7. FW1：配置端口，设置防火墙安全的区域，配置防火墙区域间包过滤。（详见补充知识点3，提示：policy需创建2条）
8. PC3可ping 通sever3、PC1-1、PC1-2。
9. **sever3可ping 通PC3、PC1-1、PC1-2、PC1-3、PC1-4。**

### 实验报告提交结果

1. SW3、R1、R2、R3、R4、FW1的路由表，截图及分析。
2. 所有PC、server间的连通情况，使用tracert（路由追踪），截图及分析。
3. 截图需要体现出个人学号。

# 补充知识点1 三层交换机配置

## 实验目标

* 掌握交换机Vlanif的配置。
* 利用三层交换机实现跨网段通信。

## 三层交换机

三层交换机可利用Vlanif实现跨网段的主机通信。Vlanif 接口是在三层交换机上虚拟出来三层口，用来充当不同VLAN下主机的网关**，**从而实现不同VLAN之间的通信。

三层交换 = 二层交换+三层转发，三层交换机通过硬件来交换和路由选择数据包。三层交换机的**工作原理**如下**：**

1. 当一个数据包进入三层交换机以后，会查看路由表，即“**一次路由**”，查找出接口和下一跳，之后会找到下一跳的MAC地址，进行二层封装的变换，这和三层设备即路由器的本质是一样的，完成一次“路由器“的工作。（三层的本质：是把一个子网的MAC迁移到另外一个子网，不同子网的MAC不可能会出现在同一个包的源目MAC上，把原有的二层封装去掉，封装上新的MAC地址，源是出接口的MAC地址，目的是下一跳的MAC地址，此时新的二层封装形成，数据包转发出设备）。

2. 如果找不到下一跳的MAC地址，进行ARP洪范，再找不到就丢弃。在做二层封装的时候，因为有目标MAC的存在，所以也可以说是三层的目标IP最后会映射到目标MAC上，此时会形成一个目标IP和封装目标MAC的映射，而三层交换机具有二层交换机的功能，则此时就形成了三层到二层的一个映射，转发一定是要找到接口，通过IP找到MAC，通过MAC找到对应出接口，这就相当于形成了一个IP的MAC表，那么三层IP进来以后就直接会找到对应的出接口，数据包就不需要再查看数据表，只需要变换一次二层封装就可以了。

简化工作过程描述即为：**数据包进入交换机 🡪 查看路由表 🡪 更换二层封装 🡪 数据包导出。**

注意：三层交换机是无法替代路由器的，因为路由器的主要功能是查询路由表、计算最优路由、转发数据，而三层交换机是做不到这点的，所以，一个成熟的网络架构，是不能没有路由器的。

## 实验内容

利用Vlanif实现交换机下跨网段的主机通信。

### 实验组网图

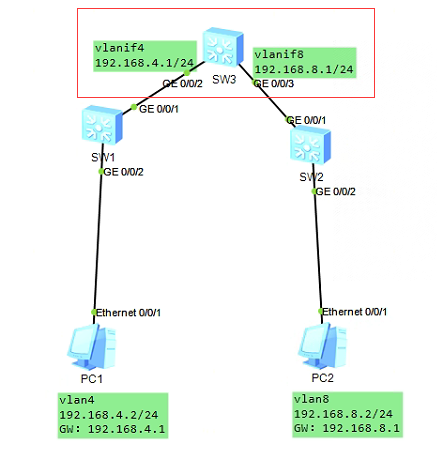


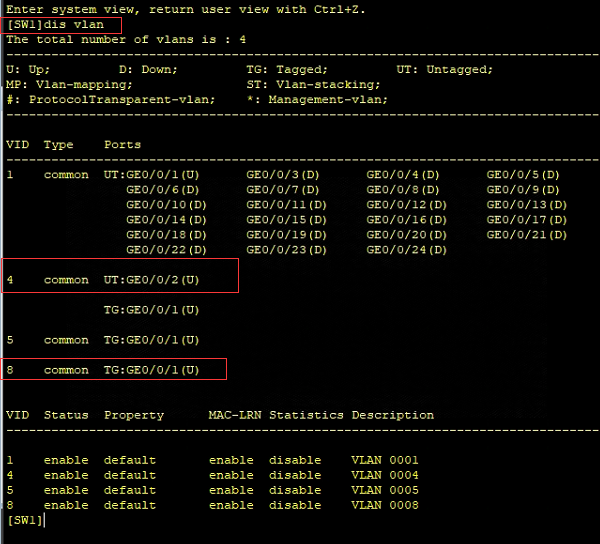
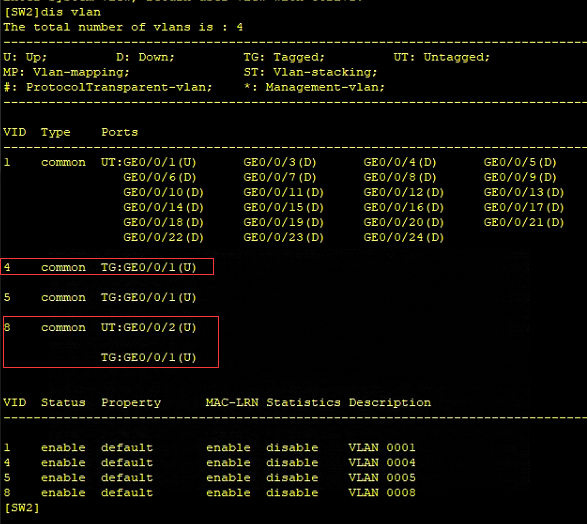
图 2 VLAN通信拓扑

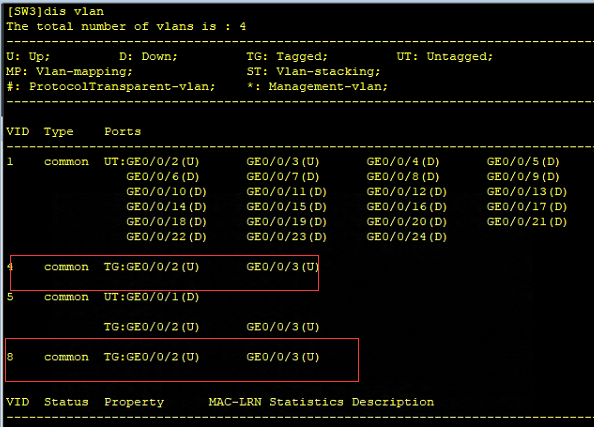
### 实验内容

本实验内容为**深入学习三层交换机的VLAN配置，实现图 2中不同VLAN下的主机可以跨网段通信**。

实验步骤：

1. 按照图 2创建网络拓扑，配置主机和服务器IP。
2. 在SW1、SW2、SW3创建VLAN4和VLAN8，添加端口到VLAN，配置链路类型等（步骤同实验2，此处不再说明）。



1. 配置SW3交换机的Vlanif4和Vlanif8端口信息：

[SW3]**interface vlan 4**或者**interface Vlanif 4**

[SW3-Vlanif4]**ip add 192.168.4.1 24**

[SW3]**interface Vlanif 8**

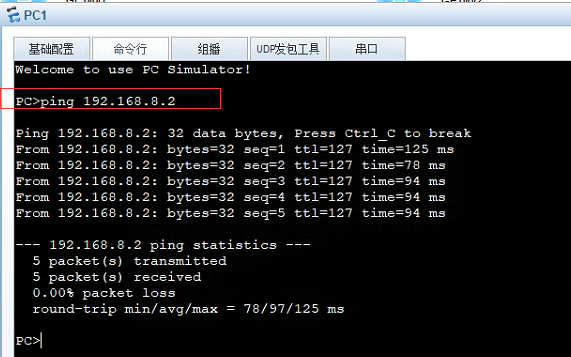
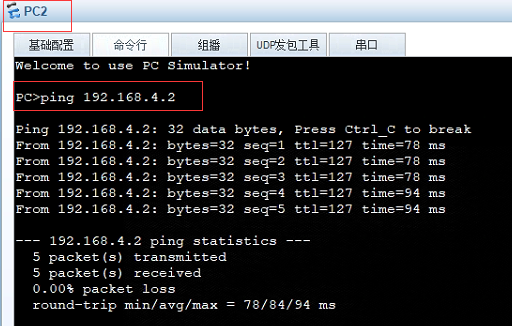
[SW3-Vlanif8]**ip add 192.168.8.1 24**



1. 实验结果：

PC1和PC2可以互相ping通。

# 补充知识点2 路由协议混合组网

## 实验目标

* 掌握同一个路由器使用多种路由协议时的配置方法。

## 实验内容

若同一台路由器使用了多种路由协议，则可在路由器配置采用以下命令，完成多种路由算法在同一台交换机同时工作：

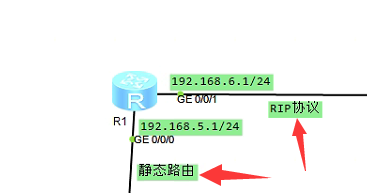
import-route direct （导入直连路由，一般没必要）

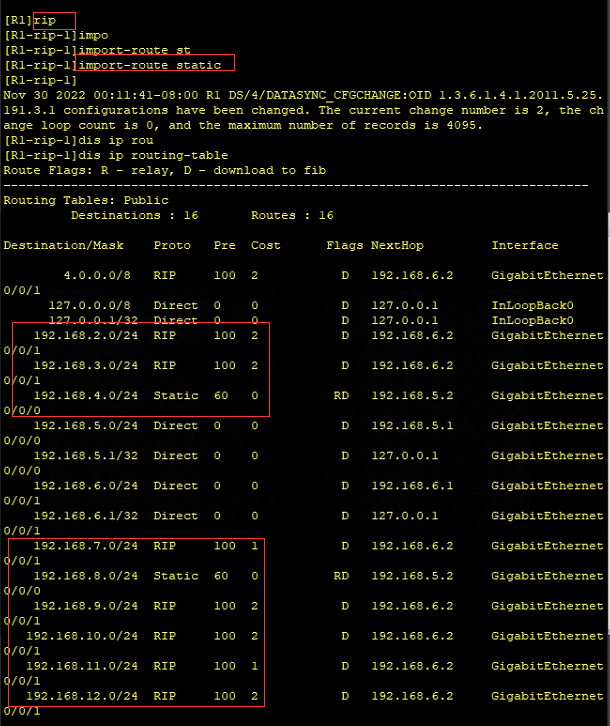
import-route static （导入静态路由）

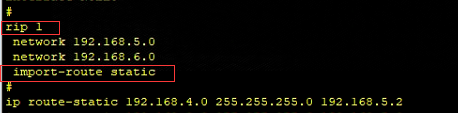
import-route rip （导入RIP）

import-route ospf （导入OSPF）

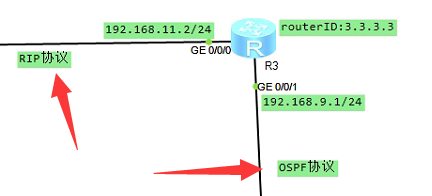
例1，下图路由器R1同时使用了静态路由和RIP，则可进行如下命令，将静态路由导入RIP：

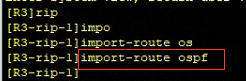
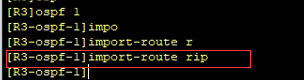


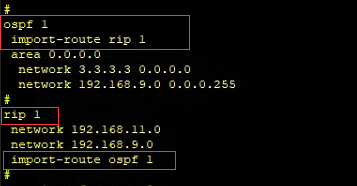


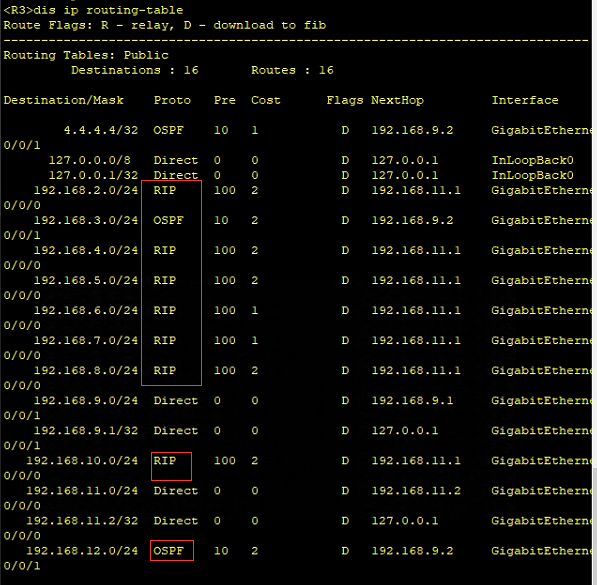


例2，下图路由器R3同时使用了OSPF，则可进行如下命令，将R3的RIP导入OSPF，将OSPF导入RIP：







# 补充知识点3 简单防火墙配置

## 实验目标

* 掌握简单防火墙的配置，实现指定网络的访问控制

## 实验内容

* 掌握简单防火墙的配置，实现指定网络的访问控制

### 实验组网图

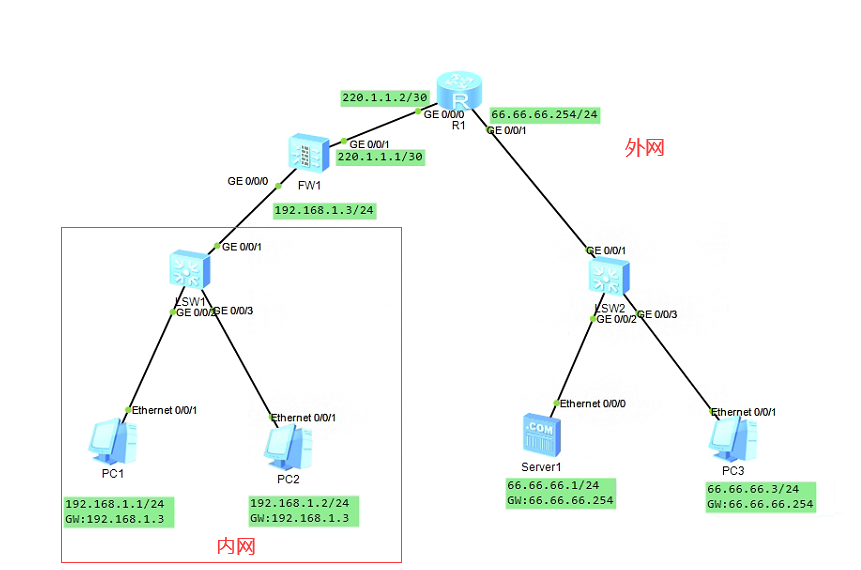


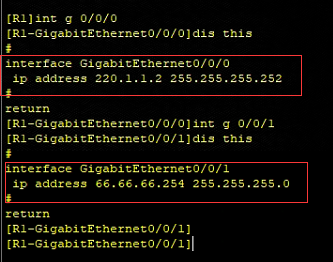
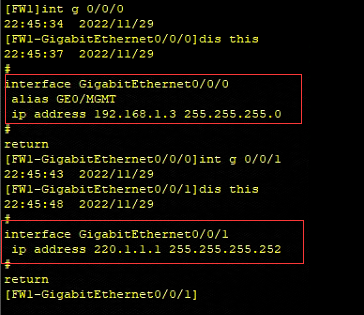
图 3 防火墙测试拓扑

### 实验内容

本实验内容为**学习防火墙配置，实现图 3中内网设备可以访问外网，外网设备不能访问内网**。

实验步骤：

1. 按照图 2创建网络拓扑，配置主机和服务器IP。
2. 配置路由器端口信息、防火墙端口信息（命令同路由器）。

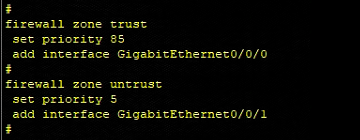
1. 设置防火墙安全的区域，即将内网加入到可信区域，外网加入到不可信区域，配置如下：

[FW1]**firewall zone trus**t （进入可信区域）

[FW1-zone-trust]**add int g 0/0/0** （添加内网端口到可信区域）

[FW1]**firewall zone untrust** （进入不可信区域）

[FW1-zone-untrust]**add int g 0/0/1** （添加内网端口到不可信区域）



1. 配置防火墙区域间包过滤：

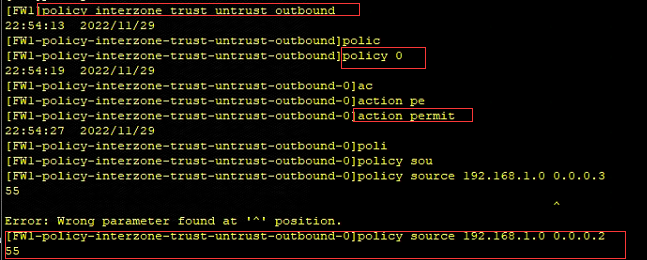
[FW1]**policy interzone trust untrust outbound**

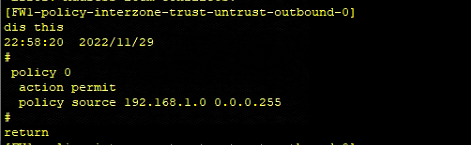
[FW1-policy-interzone-trust-untrust-outbound]**policy 0 （创建规则命名为0，若不止一条规则，则可创建1、2、3……）**

[FW1-policy-interzone-trust-untrust-outbound-0]**action permit**

[FW1-policy-interzone-trust-untrust-outbound-0]**policy source 192.168.1.0 0.0.0.255**（指定可访问外网的内网网段，0.0.0.255为反掩码）

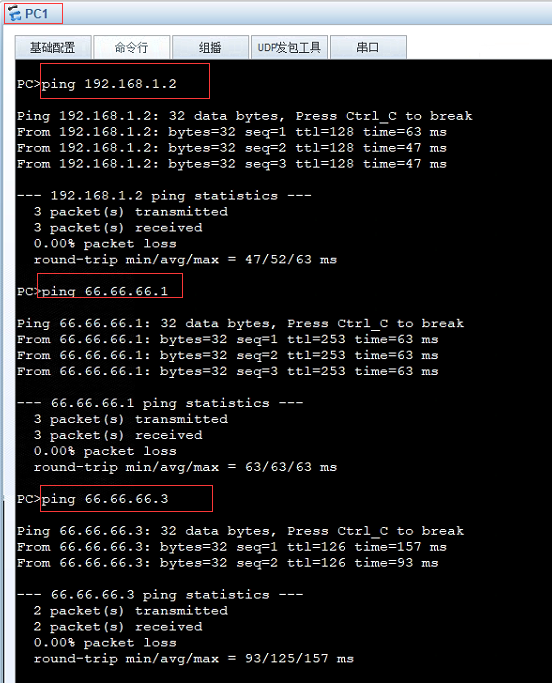
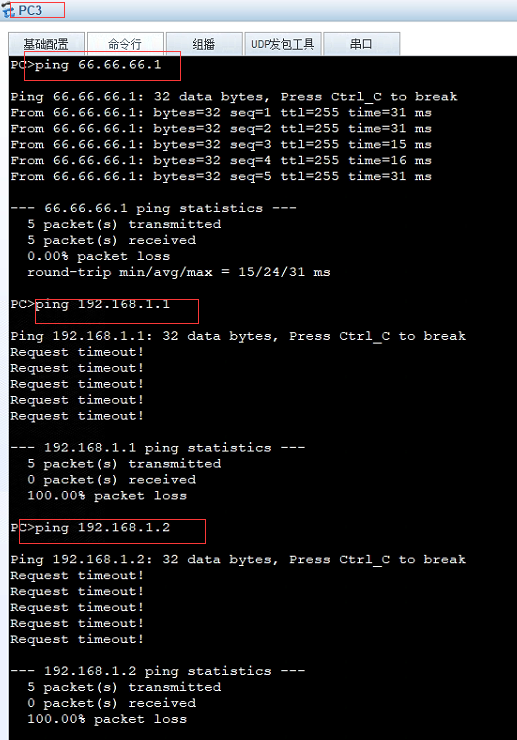
注：上述配置表述指定网段可以访问外网任意网段，若要指定某一网段，则使用添加命令policy destination 可访问外网IP 反掩码。





1. 实验结果：

PC1、PC2可访问server1、PC3；server1、PC3不可访问PC1、PC2。

**补充说明：**

若需要创建另一条规则，**要求内网中ip1网段只能访问外网中ip2网段，**命令如下：

[FW1-policy-interzone-trust-untrust-outbound]**policy 1**

[FW1-policy-interzone-trust-untrust-outbound-0]**policy source ip1 反掩码**（指定可访问外网的内网网段为ip1）

[FW1-policy-interzone-trust-untrust-outbound-0]**policy destination ip2 反掩码**（指定可访问的外网网段为ip2）

**文档版本**

|  |  |  |
| --- | --- | --- |
| **日期** | **版本** | **描述** |
| 2022.11 | 1.0 | 撰写内容 |