东北大学软件学院学生实训阶段总结报告

2018 年 7 月 4 日

学　号	20155362	姓　名	薛旗	班　级	软信-1503
阶段总结成绩（百分制）			批阅人		
实训单位	天津市大学软件学院				
前一阶段工作总结	第一部分：渗透测试部分（Web 安全及数据库安全高级渗透防护技术） 通过第一部分学习，复习了 HTML 语言的相关知识，熟练掌握了 JavaScript 和 php 脚本语言，知道了 php 会话控制的两种方式；熟知了数据库查询语句，并对 SQL 注入有了深刻的理解，知道了 SQL 注入的原理及主要方法；知道了 XSS 漏洞及文件上传漏洞；学会使用了 BurpSuite 工具，并知道如何通过一句话木马和中国菜刀来获取磁盘文件。在实践过程中，能够熟练运用 Nmap 工具对 web 应用进行漏洞扫描，然后使用 sql 注入或 xss 进行渗透，提权。 第二部分：网络安全部分 1.计算机网络基础安全加固技术：通过第一小节的学习，复习了计算机网络的基础知识，学会了 Cisco 模拟器的基础配置，知道了路由器原理与静态、默认路由基本配置，浮动路由及策略路由原理及配置，ACL 访问控制列表和 NAT 原理与配置；了解了动态路由与 RIP 路由协议，ospf 路由协议原理、单区域配置、多区域配置，完成了 NAT、静态路由组网、RIP 路由组网、ospf 路由组网的综合实训。 2.网络基础技术：通过第二小节的学习，知道了 Vlan 技术与配置，Trunk 协议与配置，VTP 协议与配置，单臂路由配置及 DHCP 中继，三层交换技术与配置，完成了运用 vlan/trunk/vtp 等技术构建二层交换网络实验，单臂路由实验和 vlan 间网络互通实验。 3.安全设备技术：通过第三小节的学习，了解了网络安全框架，认识了防火墙设备，知道了防火墙的安全策略及安全区域的配置；能够利用华为 eNSP 模拟器完成相关的配置工作，掌握了 NAT 技术，并能够知道防火墙在企业网络中的应用和实现。				
存在主要问题	在实训过程中，主要问题是理论知识与实践过程的对接。 在第一部分的实践过程中，知道了 SQL 注入原理，但是在实践过程中，需要通过不断的测试，使用不同的方法来挖掘漏洞，并使用不同的技巧来提高挖掘效率，这就需要有丰富的漏洞发掘经验。 在第二部分的实践过程中，主要问题是对配置命令及含义的记忆与理解。不同的模拟器，不同的设备有不同的配置方法，在配置综合实验的时候，需要综合利用学到的知识，对需求进行整体布局，完成对一个系统的网络配置，这样才能保证系统无差错运行，符合要求。				

第一部分：渗透测试重点知识总结

一、数据库基本操作：

连接数据库：mysql -hlocalhost -uroot -proot

显示数据库：show databases;

创建数据库：create database student character set utf8;

使用数据库：use student;

查看所有表：show tables;

创建表：create table users(xxx);

删除数据库：drop database temp;

查看表信息：desc users;

添加列：alter table users add headimg varchar(30);

修改列名：alter table users change headimg headpic varchar(30);

修改列类型：alter table users modify headpic varchar(50);

重命名表名(as 可省略)：alter table users rename as members;

查询所有数据：select * from users;

查询指定数据：select * from users where id = 1;

查询指定列名：select username,password from users;

修改数据：update users set score = score+1 where id = 8;

删除全部数据：delete from members;

删除指定数据：delete from members where id = 8;

聚合函数：sum,max,min,sum,count

统计部门成绩大于 80 的人数：

select dept,count(username) from users where score > 80 group by dept;

统计部门成绩大于 80 的人数并且部门人数大于 1：

(1)select dept,count(username) as deptcount from users where score > 80 group by dept having deptcount > 1;

(2)select dept,count(username) from users where score > 80 group by dept having count(username) > 1;

联合查询：使用 union 关键字；列数要对应

(1)select username,dept from users union select 1,2;

(2)select username,dept from users union select score,sex from users;

二、SQL 注入分类及利用

根据数据类型

1.整形注入 and 1=1 and 1=2

2.字符型注入 ‘ and 1=1 -- - ‘and 1=2 -- +

根据注入语法

1. UNION query SQL injection（可联合查询注入）

2. Stacked queries SQL injection（可多语句查询注入）

3.Error-based SQL injection（报错型注入）

4.Boolean-based blind SQL injection（布尔型注入）

5.Time-based blind SQL injection（基于时间延迟注入）

三、SQL 注入挖掘以及防御

1.and 1=1 / and 1=2 回显页面不同（整形判断）

‘and 1=1 -- -/ ‘and 1=2 -- -回显页面不同（字符型判断）

2.单引号判断 ‘ 显示数据库错误信息或者页面回显不同（整形，字符串类型判断）

3.\ (转义符)

4.-1/+1 回显下一个或上一个页面（整型判断, 只对整形注入有效）

5.and sleep(5) (判断页面返回时间)

6.and 2>1 （布尔型注入）

四、MYSQL 中的 3 种注释风格

1.#

2.--

3./* …*/

4./*!...*/ 内联注视

五、MySQL 函数利用

system_user() 系统用户名

user() 用户名

current_user() 当前用户名

session_user()连接数据库的用户名

database() 数据库名

version() MYSQL 数据库版本

@@datadir 读取数据库路径

@@basedir MYSQL 安装路径

@@version_compile_os 操作系统

load_file() MYSQL 读取本地文件的函数

六、报错注入：database(),version()

1.编码绕过

2.大小写绕过

3.%0a 换行

七、XSS 漏洞挖掘

1.XSS 手动挖掘

- 看 URL 参数输出的位置
- 看输入框输出位置

2.输出点位置

a 输出在标签外

需要可以构造标签，如果不能构造标签就不存在 XSS 漏洞。

b.输出到标签内

如果输出在"双引号或者'单引号内部，需要能够闭合引号，如果不能闭合引号，就需要看能否在当前的标签属性中执行 js 代码，如果不能，就不存在 XSS 漏洞。如果没有输出在"双引号或者'单引号内部，可以构造一个新的属性，使用新的属性的值来执行 JS 代码，比如事件属性。

c.输出到 Script 标签中

如果输出在"双引号或者'单引号内部，需要能够闭合引号，如果不能 闭合引号(引号内部可以使用 unicode 编码)，需要看当前变量能不能 innerHTML，插入到网页中，如果可以就可以构造 XSS，如果没有，就 不存在 XSS

如果输出"双引号或者'单引号内部，需要能够闭合引号，如果可以闭合引号，就可以直接传递进去 js 代码，使用注释符号，注释掉后面的 js 代码就可以构造 XSS

第二部分：网络安全实践

一、VLAN 工作原理

交换机

1.进入全局配置模式：configure terminal

2.配置VLAN：vlan 10,20

3.重命名：vlan 10
　　name student

4.退出特权模式：end

5.show vlan-switch brief

6.configure terminal

7.进入接口：interface fastEthernet 1/0

8.switchport mode access

9.switchport access vlan 10

...

10.exit

上线新加入的交换机（重启）

->end

->show ip interface brief

->conf t

->interface range fa1/2 -3

->shutdown

->no shutdown

分配流量

->int fa 1/3

->switchport mode access

->switchport mode access vlan 10

PC

配置ip：ip 192.168.10.1/24

Trunk

int fa 1/2

no switchport access vlan 20

do show run int fa 1/2　//do不需要在特权模式

switchport trunk encapsulation dot1q
switchport mode trunk
show interfaces trunk

show interfaces fa 1/2 switchport　//接口详细信息

int fa 1/2
switchport trunk allowed vlan remove 20
show interfaces trunk

链路捆绑

->conf t

配置trunk

.....

->int range fa 1/2 -3
->channel-group 1 mode on
->show interfaces port-channel 1

二、VTP 及单臂路由

VTP

1.
->conf t
->vtp domain simp

2.
->int fa 1/0 //(int ran fa 1/0 -1)
->switchport trunk encapsulation dot1q
->switchport mode trunk

3.
->vtp password simp.com

4.(依次)
->vtp mode server
->vtp mode transparent
->vtp mode client

5.
->end
->show vtp status

->vlan 10
->exit
->vlan 20
->exit

->show vtp status
->show run | in vlan
->show vlan-s brief
->show interfaces trunk

6.测试修剪，需加入主机（还是交换机配置信息）
->int fa 1/1
->shutdown
->no shutdown
->switchport mode access
->switchport access vlan 10
->end
->vtp pruning

单臂路由

1.配置ESW1
->conf t
->vlan 10,20
->exit
->int fa 1/1
->switchport mode access
->switchport access vlan 10
->int fa 1/2
->switchport mode access
->switchport access vlan 20
->exit
->int fa 1/0
->switchport trunk encapsulation dot1q
->switchport mode trunk
->end
->show vlan-s brief
2.配置R1
->conf t
->int fa 0/0
->shutdown
->no shutdown
->exit
->int fa 0/0.?
->int fa 0/0.10
->encapsulation dot1Q 10
->ip add 192.168.10.254 255.255.255.0
->int fa 0/0.20
->encapsulation dot1Q 20
->ip add 192.168.20.254 255.255.255.0
->end
->show ip int brief
->show ip route
3.PC1
->ip 192.168.10.1/24 192.168.10.254
4.PC2
->ip 192.168.20.1/24 192.168.20.254
5.ping
ping 192.168.20.1
6.抓包

三、三层交换技术

三层交换（接第六章实验）

其实没有R1，需要关闭

两个交换机，其中一个只充当线

1.ESW1
->conf t
关闭1/0接口
->int fa 1/0
->shutdown
->exit
-> int vlan 10
->ip add 192.168.10.254 255.255.255.0
->no shutdown
-> int vlan 20
->ip add 192.168.20.254 255.255.255.0
->no shutdown
->end
->show ip int brief
->show ip route
开启路由功能
->conf t
->ip routing
->end
->show ip route

->sho int fa 0/0.10
->sho int vlan 10

ESW1:
->conf t
->vlan 10,20
->exit
->int fa 1/1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->int fa 1/0
->switchport mode access
->switchport access vlan 10
->int vlan 10
->ip add 192.168.10.254 255.255.255.0
->int vlan 20
->ip add 192.168.20.254 255.255.255.0
->no shutdown
->exit
->ip routing
->end
->show vlan-switch brief
->show ip interface brief
->show ip route

ESM2:
->conf t
->vlan 20
->exit
->int fa 1/1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->int fa 1/0
->switchport mode access
->switchport access vlan 20
->no shutdown
->exit
->ip routing
->end
->show vlan-switch brief
->show ip interface brief
->show ip route

PC1:
->ip 192.168.10.1/24 192.168.10.254

PC2:
->ip 192.168.20.1/24 192.168.20.254

ping:
->ping 192.168.10.1
->ping 192.168.20.1

四、STP 服务

需求：所有交换机同步 vlan10,设置 sw1 为根桥，实现 sw2 的 fa1/3 和 sw4 的 fa1/5 端口被 block 掉，其他接口保持 forwarding

解答方案：

1.ESW1(ESW2,ESW3,ESW4同理)配置trunk

```
->conf t
->int range fa1/0 -1   //或 int range fa1/0 , fa1/1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->end
```

2.ESW1配置域和VLAN，其他几个会自动学习

```
->conf t
->vtp domain simp
->end

->conf t
->vlan 10
```

3.配置STP

```
->conf t
->spanning-tree vlan 10 root primary   //设置根网桥 或者直接配置桥优先级
                                       spanning-tree vlan 10 priority ?(一般是8192)
->int fa 1/3
->spanning-tree vlan 10 port-priority ?   //配置优先级
->spanning-tree vlan 10 cost ?            //配置路径成本
```

4.各种show

```
->show interfaces trunk
->show vtp status
->show vlan-switch brief
->show spanning-tree vlan 10 brief
->show spanning-tree int fa 1/0   查看端口ID
```

五、路由原理与静态路由

Ⅰ.基础路由

->show ip route (static)
->show ip route 0.0.0.0
->show ip cef 192.168.3.0
->show run | in ip route

配置环回地址
-> int loopback 0

traceroute
->traceroute 3.3.3.3

默认路由，目标前缀和目标掩码均为0.0.0.0
在末端设置(如R1)
->ip route 0.0.0.0 0.0.0.0 12.1.1.2

R1:
->conf t
->ip fa 0/0
->ip add 12.1.1.1 255.255.255.0
->no shutdown
->exit
->ip route 23.1.1.0 255.255.255.0 12.1.1.2
->ip route 3.3.3.3 255.255.255.255 12.1.1.2
……..
->ping 3.3.3.3

R2:
->conf t
->ip fa 0/0
->ip add 12.1.1.2 255.255.255.0
->no shutdown
->ip fa 1/0
->ip add 23.1.1.2 255.255.255.0
->no shutdown
->ip route 3.3.3.3 255.255.255.255 23.1.1.3

R3
->conf t
->int fa0/0
->ip add 23.1.1.3 255.255.255.0
->no shutdown
->int loopback 0
->ip add 3.3.3.3 255.255.255
->exit
->ip route 12.1.1.0 255.255.255.0 23.1.1.2

Ⅱ.配置默认路由

R1:
->conf t
->no ip route 3.3.3.3 255.255.255.255 12.1.1.2
->no ip route 23.1.1.0 255.255.255.0 12.1.1.2
->ip route 0.0.0.0 0.0.0.0 12.1.1.2

R2:
->conf t
->no ip route 12.1.1.0 255.255.255.0 23.1.1.2
->ip route 0.0.0.0 0.0.0.0 23.1.1.2

Ⅲ.浮动静态路由(接Ⅱ)

R1:
->conf t
->int fa 1/0
->ip add 122.1.1.1 255.255.255.0
->no shutdown
->no ip route 0.0.0.0 0.0.0.0 12.1.1.2//删除Ⅱ原来的路由

配置缺省
->ip route 0.0.0.0 0.0.0.0 12.1.1.2 10 //10为管理距离值
->ip route 0.0.0.0 0.0.0.0 122.1.1.2 20
//默认路由为管理距离值小的，若链路故障，则启用其他路由

R2:
->conf t
->int fa 2/0
->ip add 122.1.1.2 255.255.255.0
->no shutdown

负载均衡 按如下方式配置 流量比为1:1
->ip route 0.0.0.0 0.0.0.0 12.1.1.2 20
->ip route 0.0.0.0 0.0.0.0 122.1.1.2 20

Ⅳ.汇总路由：相同位保留，不同位置零

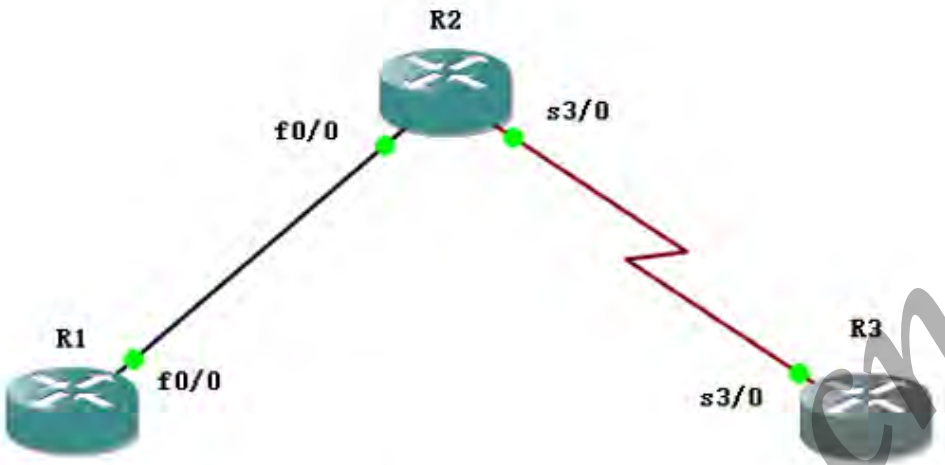
R1:配置默认路由（见Ⅲ）
R2:配置汇总路由
->conf t
->ip route 192.168.0.0 255.255.248.0 23.1.1.3
->end
R3:
->conf t
->int lo 1
->ip add 192.168.3.1 255.255.255.0
->ip add 192.168.4.1 255.255.255.0 se
->ip add 192.168.5.1 255.255.255.0 se
->ip add 192.168.6.1 255.255.255.0 se
->ip add 192.168.7.1 255.255.255.0 secondary
//secondary：给接口配置多个IP

Ⅴ.递归路由

R1:
->conf t
(->no ip route 0.0.0.0 0.0.0.0) //清空实验IV配置的默认路由
->ip route 192.168.3.0 255.255.255.0 23.1.1.3
->ip route 192.168.4.0 255.255.255.0 23.1.1.3
->ip route 192.168.5.0 255.255.255.0 23.1.1.3
->ip route 192.168.6.0 255.255.255.0 23.1.1.3
->ip route 192.168.7.0 255.255.255.0 23.1.1.3

->ip route 23.1.1.0 255.255.255.0 12.1.1.2
->ip route 23.1.1.0 255.255.255.0 122.1.1.2
->end
->ping 192.168.3.1
->ping 192.168.4.1
……
R2:实验IV配置
R3:实验IV配置

六、动态路由 ospf



R1:
->conf t
->int fa 0/0
->ip add 12.1.1.1 255.255.255.0
->no shutdown
->int lo 0
->ip add 11.1.1.1 255.255.255.255
->end
->conf t

->router ospf 1	//指定进程号
->router-id 1.1.1.1	//指定ID
->network 12.1.1.0 0.0.0.255 area 0	//宣告

->network 11.1.1.1 0.0.0.0 a 0
//反掩码，0精确匹配

R2:
->conf t
->int fa 0/0
->ip add 12.1.1.2 255.255.255.0
->no shutdown
->int lo 0
->ip add 22.1.1.1 255.255.255.255
->int s 3/0
->ip add 23.1.1.2 255.255.255.0
->no shutdown
->exit
->router ospf 10
->network 12.1.0.0 0.0.255.255 a 0
->network 22.1.1.0 0.0.0.255 a 0

->conf t
->router ospf 10
->network 23.1.1.0 0.0.0.255 a 0

R3:
->conf t
->int s 3/0
->ip add 23.1.1.3 255.255.255.0
->no shutdown
->int lo0
->ip add 33.1.1.1 255.255.255.255
->router ospf 1

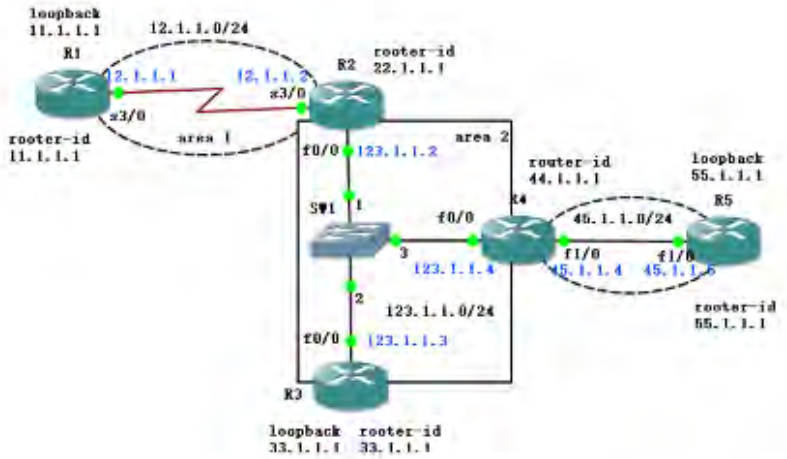
->network 0.0.0.0 0.0.0.0 a 0	//所有接口启用ospf

->end

->show ip protocols
->sho ip ospf neighbor
->show ip ospf int fa 0/0
->show ip ospf database
->show int s 3/0
->debug ip ospf events
->debug ip ospf adj
->undebug all
->clear ip ospf process

->ip ospf priority 0	//更改优先级
->ip ospf network point-to-point	//网络类型改为点到点

七、LSA



R1:
R1#conf t
R1(config)#int s 3/0
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo 0
R1(config-if)#ip add 11.1.1.1 255.255.255.255
R1(config-if)#router ospf 1
R1(config-router)#router-id 11.1.1.1
R1(config-router)#network 0.0.0.0 0.0.0.0 a 1
R1(config-router)#end
R1#show ip ospf database

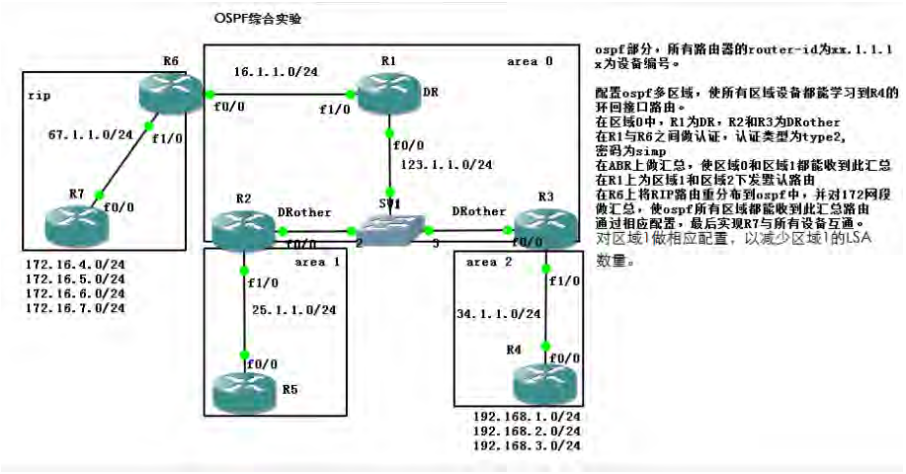
R2:
R2#conf t
R2(config)#int s 3/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#int fa 0/0
R2(config-if)#ip add 123.1.1.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#router ospf 1
R2(config-router)#router-id 22.1.1.1
R2(config-router)#network 12.1.1.0 0.0.0.255 a 1
R2(config-router)#network 123.1.1.0 0.0.0.255 a 0
R2(config-router)#end
R2#show ip ospf neighbor

R3:
R3#show ip ospf database router
R3#sho ip ospf database external

R4:
R4(config)#router rip
R4(config-router)#ver 2
R4(config-router)#no au
R4(config-router)#network 45.0.0.0
R4(config-router)#exit
R4(config)#router ospf 1
R4(config-router)#redistribute rip subnets
R4(config-router)#end

R5:
R5(config)#int fa 1/0
R5(config-if)#ip add 45.1.1.5 255.255.255.0
R5(config-if)#no shutdown
R5(config-if)#int lo 0
R5(config-if)#ip add 55.1.1.1 255.255.255.255
R5(config-if)#router rip
R5(config-router)#ver 2
R5(config-router)#no au
R5(config-router)#netwo
R5(config-router)#network 0.0.0.0
R5(config-router)#end

八、ospf综合实验



R1:
->conf t
->int fa 1/0
->ip add 16.1.1.1 255.255.255.0
->no shu
->int fa 0/0
->ip add 123.1.1.1 255.255.255.0
->no shu
->exit
->router ospf 1
->router-id 11.1.1.1
->network 16.1.1.0 0.0.0.255 a 0
->network 123.1.1.0 0.0.0.255 a 0
//开启认证
->exit
->int fa 1/0
->ip ospf authentication message-digest
->ip ospf message-digest-dey 1 md5 simp
->end
->sho ip ospf border-routers

//在R1上为区域1和区域2下发默认路由
->conf t
->router ospf 1
->default-information originate always
->end
R2:
->conf t
->int fa 0/0
->ip add 123.1.1.2 255.255.255.0
->no shu
->int fa 1/0
->ip add 25.1.1.2 255.255.255.0
->no shu
->router ospf 1
->router-id 22.1.1.1
->network 123.1.1.0 0.0.0.255 a 0
->network 25.1.1.0 0.0.0.255 a 1
->end
->sho ip ospf neighbor
//设置为DRother
->conf t
->int fa 0/0
->ip ospf priority 0
//减少区域1的LSA数量
->conf t
->int fa 0/0
->ip ospf priority 0
->router ospf 1
->area 1 stub no-summary

R3:
->conf t
->int fa 0/0
->ip add 123.1.1.3 255.255.255.0
->no shu
->int fa 1/0
->ip add 34.1.1.3 255.255.255.0
->no shu
->router ospf 1
->router-id 33.1.1.1
->network 123.1.1.0 0.0.0.255 a 0
->network 34.1.1.0 0.0.0.255 a 2
//设置为DRother
->int fa 0/0
->ip ospf priority 0
->end
->sho ip ospf neighbor
//在ABR上做汇总
->conf t
->router ospf 1
->area 2 range 192.168.0.0 255.255.252.0
R4:
->conf t
->int fa 0/0
->ip add 34.1.1.4 255.255.255.0
->no shu
->int lo 0
->ip add 192.168.1.1 255.255.255.0
->ip add 192.168.2.1 255.255.255.0 se
->ip add 192.168.3.1 255.255.255.0 se
->router ospf 1
->router-id 44.1.1.1
->network 34.1.1.0 0.0.0.255 a 2
->network 192.168.0.0 0.0.255.255 a 2
->end
//R1下发完默认路由，查看一下
->sho ip ro ospf
R5:
->conf t
->int fa 0/0
->ip add 25.1.1.5 255.255.255.0
->no shu
->router ospf 1
->router-id 55.1.1.1
->network 25.1.1.0 0.0.0.255 a 1
->end
->sho ip ospf neighbor
->sho ip ro ospf
//R3做完汇总，查看一下
->sho ip ro ospf

R5:

//R1下发完默认路由，查看一下

->sho ip ro ospf

//R6将RIP路由分布到ospf中后，查看一下

->sho ip ospf database

//R6对172网段进行汇总后，查看一下

->sho ip ospf database
->sho ip ro ospf

//减少区域1的LSA数量

->conf t
->router ospf 1
->area 1 stub
->end
->sho ip ro ospf
->sho ip ospf database

R6:

->conf t
->int fa 0/0
->ip add 16.1.1.6 255.255.255.0
->no shu
->int fa 1/0
->ip add 67.1.1.6 255.255.255.0
->no shu
->router ospf 1
->router-id 66.1.1.1
->network 16.1.1.0 0.0.0.255 a 0
->end
->sho ip ro ospf

//开启认证

->conf t
->int fa 0/0
->ip ospf authentication message-digest
->ip ospf message-digest-dey 1 md5 simp
->end

//做完汇总，查看一下

->sho ip ro ospf

//配置RIP

->conf t
->router rip
->ver 2
->no au
->network 67.0.0.0
->end
->sho ip ro rip

R6:

//R6将RIP路由重分布到ospf中

->conf t
->router ospf 1
->redistribute rip subnets
->end

//对172网段进行汇总

->conf t
->router ospf 1
->summary-address 172.16.4.0 255.255.252.0

//配置实现R7与所有设备互通

->router rip
->default-information originate
->end
->sho ip ro

R7:

->conf t
->int fa 0/0
->ip add 67.1.1.7 255.255.255.0
->no shu
->int lo 0
->ip add 172.16.4.1 255.255.255.0
->ip add 172.16.5.1 255.255.255.0 se
->ip add 172.16.6.1 255.255.255.0 se
->ip add 172.16.7.1 255.255.255.0 se
->end

//查看路由表，未配置时R7不能与所有设备想通

->sho ip ro

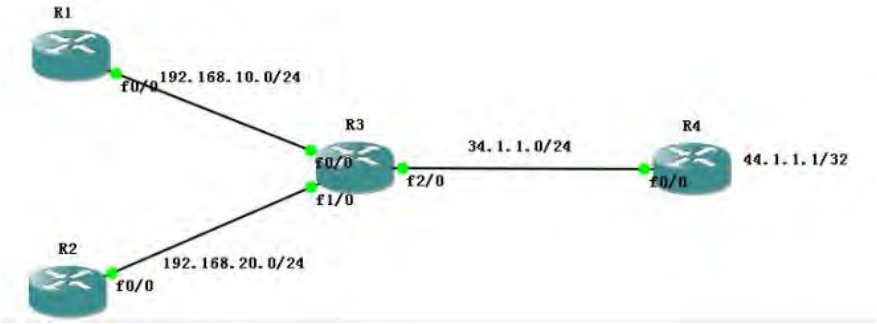
//配置完成，查看一下，实现了

->sho ip ro rip
->ping 192.168.1.1

//配置RIP

->router rip
->ver 2
->no au
->network 67.0.0.0
->network 172.16.0.0

九、ACL



//正常配置网段及ospf，把路由打通

//R4配置一个环回接口

//router ospf 1
//router-id 11.1.1.1
//network 0.0.0.0 0.0.0.0 a 0

//配置标准ACL

R4:
->conf t
->access-list 10 permit 192.168.10.0 0.0.0.255
->access-list 10 deny 192.168.20.0 0.0.0.255
->access-list 10 permit any
->do sho ip access
->int fa 0/0
->ip access-group 10 in

//配置远程管理

->no ip access-group 10 in
->line vty 0 4
->password simp
->login
->exit
->line vty 0 4
->access-class 10 in

//其他主机连接

->telnet 44.1.1.1

//释放

->no access-class 10 in

//配置扩展ACL

R3:
->conf t
->access-list 100 permit icmp 192.168.10.0 0.0.0.255 host 44.1.1.1 echo

//不允许telnet（23端口）

->access-list 100 deny tcp 192.168.10.0 0.0.0.255 host 44.1.1.1 eq 23
->access-list 100 permit tcp 192.168.20.0 0.0.0.255 host 44.1.1.1 eq 23
->access-list 100 deny icmp 192.168.20.0 0.0.0.255 host 44.1.1.1 echo
->access-list 100 permit ospf any any
->end
->conf t
->int fa 2/0
->ip access-group 100 out

//释放

->no ip access-group 100 out

//配置命名ACL

R4:
->ip access-list extended permit_http
->5 permit tcp 192.168.10.0 0.0.0.255 host 44.1.1.1.1 eq 80
->10 deny icmp 192.168.10.0 0.0.0.255 host 44.1.1.1 echo
->ip http server
->ip access-list ex permit_http
->permit ospf any any
->int fa 0/0
->ip access-group permit_http in

//释放

->no access-class 10 in

//基于时间因素的ACL

R4:
->sho clock
->conf t
->ip access-list extended permit_http
->no 10
->10 permit icmp 192.168.10.0 0.0.0.255 host 44.1.1.1 echo
->no 5
->exit
->time-range worktime
->periodic weekdays 9:00 to 12:00
->periodic weekdays 14:00 to 18:00
->do sho time-range
->exit
->ip access-list extended permit_http
->5 permit tcp 192.168.10.0 0.0.0.255 host 44.1.1.1 eq www time-range worktime
->end

//测试

->telnet 44.1.1.1 80
->clock set 15:00:00 27 june 2018
->sho time-range

十、路由策略与策略路由

Ⅰ.distribute-list

R1:
```
->conf t
->int fa 0/0
->ip add 12.1.1.1 255.255.255.0
->no shu
->int lo 0
->ip add 192.168.1.1  255.255.255.0
->ip add 192.168.2.1  255.255.255.0  se
->ip add 192.168.3.1  255.255.255.0  se
->router rip
->ver 2
->no au
->network 12.0.0.0
->network 192.168.1.0
->network 192.168.2.0
->network 192.168.3.0
->access-list 10 deny 192.168.3.0  0.0.0.255
->access-list 10 permit any
->do sho ip access
```
//在出方向进行过滤
```
->router rip
->distribute-list 10 out fa 0/0
```
//R2将ospf重分布到rip后
```
->sho ip r
->clear ip ro *
```
//过滤之后重新查看
```
->sho ip ro rip
```
R2:
```
->conf t
->int fa 0/0
->ip add 12.1.1.2 255.255.255.0
->no shu
->int fa 1/0
->ip add 23.1.1.2 255.255.255.0
->no shu
->router rip
->ver 2
->no au
->network 12.0.0.0
->do sho ip ro rip
->router ospf
->router-id 22.1.1.1
->network 23.1.1.0 0.0.0.255  a 0
->do sho ip ro  rip
->end
->clear ip route *   //清除路由表
->sho ip ro rip
->conf t
->access-list 10 deny 192.168.8.0  0.0.0.255
->access-list 10 permit any
->router ospf 1
->distribute-list 10 in fa 1/0
->end
->sho ip route ospf
```
//rip重分布到ospf
```
->conf t
->router ospf 1
->redistribute rip subnets
->end
->sho ip route rip
```
//过滤
```
->conf t
->acess-list 20 permit 192.168.1.0 0.0.0.255
->sho ip access-list
->conf t
->router ospf 1
->distribute-list 20 out rip
```
//ospf重分布到rip
```
->router rip
->sedistribute ospf 1 metric 5
```
//过滤
```
->access-list 30 permit  192.168.8.0  0.0.3.255
->router rip
->distribute-list 30 out ospf 1   ///从ospf出方向匹配过滤30
```
R3:
```
->conf t
->int fa 1/0
->ip add 23.1.1.3 255.255.255.0
->no shu
->int lo 0
->ip add 192.168.8.1  255.255.255.0
->ip add 192.168.9.1  255.255.255.0  se
->ip add 192.168.10.1  255.255.255.0  se
->ip add 192.168.11.1  255.255.255.0  se
->ip ospf network point-to-point
->router ospf 1
->router-id 33.1.1.1
->network 23.1.1.0 0.0.0.255  a 0
->network 192.168.0.0.0  0.0.255.255  a 0
```
//R2将rip重分布到ospf后
```
->sho ip ro ospf
```
//过滤之后
```
->sho ip ro ospf
```

Ⅳ.路由策略防环(双向重分布过滤)

1.构建环，配置R3到R1走4-5-2-1线路，然而3-1为最优。此时R3次优

R2:
```
->conf t
->router ospf 1
->redistribute rip subnets
//->router rip
//->redistribute ospf 1 metric 1
```

R3:使流量从4-5-2-1走
```
->conf t
->router rip
->offset-list 10 in 4 fa 0/0
->exit
->access-list 10 permit 11.1.1.1 0.0.0.0
->end
```

R4:
```
->conf t
->router rip
->redistribute ospf 1 metric 1
//->router ospf 1
//->redistribute rip subnets
```

2.解决方案

R2:
```
->conf t
->access-list 10 permit 11.1.1.1 0.0.0.0
->route-map r2o permit 10
->match ip address 10
->set tag 100
->route-map o2r deny 10
->match tag 200
->end
->sho route-map

->conf t
->route-map r2o permit 20
->exit
->route-map o2r permit 20
->end
```

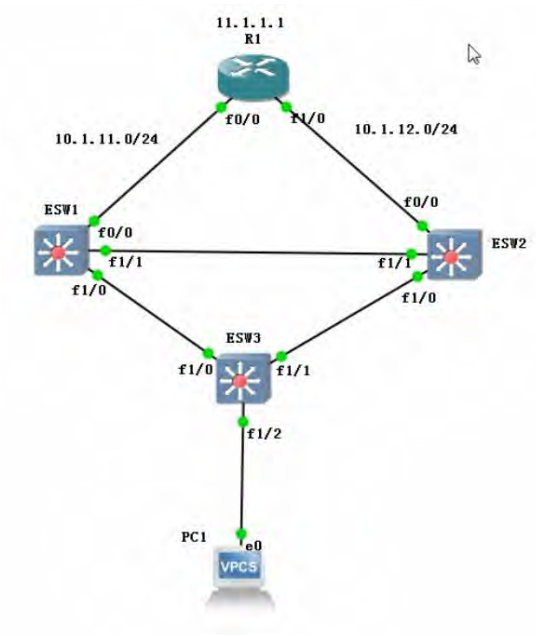
//调用
```
->conf t
->router ospf 1
->redistribute rip subnets route-map r2o
->router rip
->redistribute ospf 1 metric 1 route-map o2r

->conf t
->router rip
->distance 109 12.1.1.1 0.0.0.0 10
->traceroute 11.1.1.1
```
R4:
```
-> conf t
->route-map o2r deny 10
->match tag 100
->exit
->access-list 10 permit 11.1.1.1 0.0.0.0
->route-map r2o permit 10
->match ip address 10
->set tag 200
->end
->sho route-map
->conf t
->route-map o2r permit 20
->exit
->route-map r2o permit 20
->end
->sho route-map

->conf t
->router rip
->redistribute ospf 1 metric 1 route-map o2r
->exit
->router ospf 1
->redistribute rip subnets route-map r2o
->end
->conf t
->router rip
->distance 109 34.1.1.3 0.0.0.0 10
->end
->sho ip ro rip

->traceroute 11.1.1.1
```

十一、HSRP/VRRP 协议



ESW1:
->conf t
->int ran fa1/0 -1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->exit
->vtp domain simp
->vlan 10
->exit
->int vlan 10
->ip add 192.168.10.1 255.255.255.0
->no shu
->exit
->spanning-tree vlan 10 root primary
->int vlan 10
->standby 1 ip 192.168.10.254
->standby 1 priority 200 优先级200
->standby 1 preempt
->end
->sho standby brief
->conf t
->int fa 0/0
->ip add 10.1.11.2 255.255.255.0
->no shu
->ip routing
->router ospf 1
->router-id 1.1.1.1
->network 0.0.0.0 0.0.0.0 a 0
->passive-interface vlan 10
//模拟ESW1网关挂掉
->conf t
->int vlan 10
->shu
->no shu
//模拟ESW1上行电路故障
->int fa 0/0
->shutdown
->int vlan 10
->standby 1 track fa 0/0 51 监控fa 0/0状态，出现故障优先级降低51
->end
->sho standby brief
->sho standby
->sho track
//故障恢复
->conf t
->int fa 0/0
->no shutdown
//配置回切时延
->int vlan 10
->standby 1 preempt delay minimum 60
->end
->sho standby

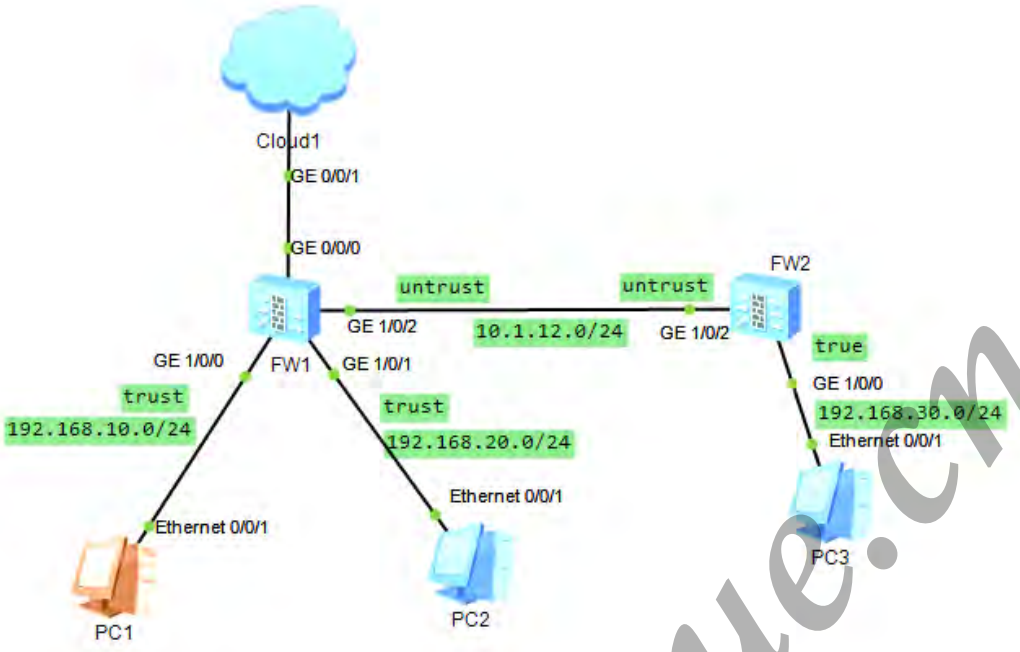
ESW2:
->conf t
->int ran fa1/0 -1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->do sho vtp status
->int vlan 10
->ip add 192.168.10.2 255.255.255.0
->no shu
->exit
->spanning-tree vlan 10 root secondary
->int vlan 10
->standby 1 ip 192.168.10.254
->standby 1 priority 150
->standby 1 preempt
->int fa 0/0
->ip add 10.1.12.2 255.255.255.0
->no shu
->ip routing
->router ospf 1
->router-id 2.2.2.2
->network 0.0.0.0 0.0.0.0 a 0
->passive-interface vlan 10

ESW3:
->conf t
->int ran fa1/0 -1
->switchport trunk encapsulation dot1q
->switchport mode trunk
->end
->sho vlan-s brief
->conf t
->int fa 1/2
->switchport mode access
->switchport access vlan 10
->end
->sho mac-address-table

PC1:
->ip 192.168.10.10/24 192.168.10.254
->ping 192.168.10.254
->ping 11.1.1.1 -c 4
->ping 11.1.1.1 -t
//vlan 10关闭（模拟ESW1网关挂掉）
//再次开启vlan 10
//ESW1上行流量故障，则目标主机不可达
//ESW1降低优先级后再次ping通
//ESW1上行电路切换修复，线路切换会有丢包

R1:
->conf t
->int fa 0/0
->ip add 10.1.11.1 255.255.255.0
->no shu
->int fa 1/0
->ip add 10.1.12.1 255.255.255.0
->no shu
->int lo 0
->ip add 11.1.1.1 255.255.255.255
->router ospf 1
->router-id 11.1.1.1
->network 0.0.0.0 0.0.0.0 a 0
->end
->sho ip ospf int brief

十二、防火墙基础



SW1:

```
[USG6000V1]sy
[USG6000V1]sysname sw1
[sw1]
[sw1]int g 1/0/0
[sw1-GigabitEthernet1/0/0]ip add 192.168.10.254  24
[sw1-GigabitEthernet1/0/0]int g 1/0/1
[sw1-GigabitEthernet1/0/1]ip add 192.168.20.254 24
[sw1-GigabitEthernet1/0/1]int g 1/0/2
[sw1-GigabitEthernet1/0/2]ip add 10.1.12.1 24
[sw1-GigabitEthernet1/0/2]q
[sw1]dis ip int brief
[sw1]firewall zone trust
[sw1-zone-trust]add int g 1/0/0
[sw1-zone-trust]add int g 1/0/1
[sw1-zone-trust]add int g 1/0/1
[sw1-zone-trust]q
[sw1]firewall zone untrust
[sw1-zone-untrust]add int g 1/0/2
[sw1-zone-untrust]q
[sw1]ip address-set 10 type object
[sw1-object-address-set-10]address 192.168.10.0 mask 24
[sw1-object-address-set-10]ip address-set 20 type object
[sw1-object-address-set-20]address 192.168.20.0 mask 20
[sw1-object-address-set-20]q
[sw1]dis ip address-set all
[sw1]ip route-static 192.168.30.0  24 10.1.12.2
[sw1]security-policy
[sw1-policy-security]rule name permit_pc1_pc3
[sw1-policy-security-rule-permit_pc1_pc3]source-zone trust
[sw1-policy-security-rule-permit_pc1_pc3]destination-zone untrust
[sw1-policy-security-rule-permit_pc1_pc3]source-address address-set 10
[sw1-policy-security-rule-permit_pc1_pc3]service icmp
[sw1-policy-security-rule-permit_pc1_pc3]action permit
[sw1-policy-security-rule-permit_pc1_pc3]q
[sw1-policy-security]rule name permit_pc2_pc3
[sw1-policy-security-rule-permit_pc2_pc3]source-zone  trust
[sw1-policy-security-rule-permit_pc2_pc3]destination-zone untrust
[sw1-policy-security-rule-permit_pc2_pc3]source-address address-set 20
[sw1-policy-security-rule-permit_pc2_pc3]service icmp
[sw1-policy-security-rule-permit_pc2_pc3]action permit
```

SW2:

```
<USG6000V1>sy
[USG6000V1]sysname sw2
[sw2]int g 1/0/0
[sw2-GigabitEthernet1/0/0]ip add 192.168.30.254  24
[sw2-GigabitEthernet1/0/0]int g 1/0/2
[sw2-GigabitEthernet1/0/2]ip add 10.1.12.2 24
[sw2-GigabitEthernet1/0/2]q
[sw2]firewall zone trust
[sw2-zone-trust]add int g 1/0/0
[sw2-zone-trust]firewall zone untrust
[sw2-zone-untrust]add int g 1/0/2
[sw2-zone-untrust]q
[sw2]ip address-set 30 type object
[sw2-object-address-set-30]address 192.168.30.0 mask 24
[sw2-object-address-set-30]q
[sw2]ip route-static 192.168.10.0  24 10.1.12.1
[sw2]ip route-static 192.168.20.0  24 10.1.12.1
[sw2]security-policy
[sw2-policy-security]rule name permit_to_pc3
[sw2-policy-security-rule-permit_to_pc3]source-zone untrust
[sw2-policy-security-rule-permit_to_pc3]destination-zone trust
[sw2-policy-security-rule-permit_to_pc3]destination-address address-set 30
[sw2-policy-security-rule-permit_to_pc3]service icmp
[sw2-policy-security-rule-permit_to_pc3]action permit
```

十三、会话表

R1:

```
->sy r1
->int g 0/0/0
->ip add 192.168.10.254 24
->int g 0/0/1
->ip add 192.168.20.254 24
->int g 1/0/0
->ip add 10.1.122.254 24
->int g 0/0/2
->ip add 10.1.12.254 24
->display ip int brief
//配置策略路由
->acl 3000
->rule 5 permit icmp source 192.168.20.1 0
  destination 192.168.10.1 0 icmp-type echo-reply
->q
//定义流量类型
->traffic classifier permit_echo
->if-match acl 3000
->q
//定义流量行为
->traffic behavior to_fw1
->redirect ip-nexthop 10.1.122.1
->q
//定义策略路由，将流量类型与流量行为进行关联
->traffic policy pbr
->classifier permit_echo behavior to_fw1
//将配制好的策略路由调用至接口的入方向
->int g 0/0/1
->traffic-policy pbr inbound
```

FW:

```
->sy fw1
->int g 1/0/0
->ip add 10.1.12.1 24
->int g 1/0/1
->ip add 10.1.122.1 24
->q
->firewall zone trust
->add int g 1/0/0
->firewall zone untrust
->add int g 1/0/1
->q
->ip route-static 0.0.0.0 0.0.0.0 12.1.12.254
->security-policy
->rule name permit_icmp_echo_reply
->source-zone untrust
->destination-zone trust
->service icmp
->action permit
->q
->int g 1/0/1
->service-manage ping permit
->dis firewall statistic system discard

//关闭防火墙的状态检测机制，PC5pingPC6可ping通
->undo firewall session link-state check
```

十四、安全策略-aspf

FTP服务建立过程模拟：

FW1:

```
->sy
->sy fw1
->int g 1/0/0
->ip add 192.168.10.254  24
->int g 1/0/1
->ip add 192.168.20.254  24
->q
->firewall zone trust
->add int g 1/0/0
->firewall zone untrust
->add int g 1/0/1
->undo firewall detect ftp
->security-policy
->rule name permit_ftp
->source-zone trust
->destination-zone untrust
->service ftp
->ac permit
```

//开启aspf功能

```
->firewall detect ftp
->dis firewall server-map
->dis firewall session table ver
```