实验：路由控制

HCIP 分解实验 - 路由控制

臧家林制作

路由控制实验 1：访问控制列表
路由控制实验 2：路由策略

==========

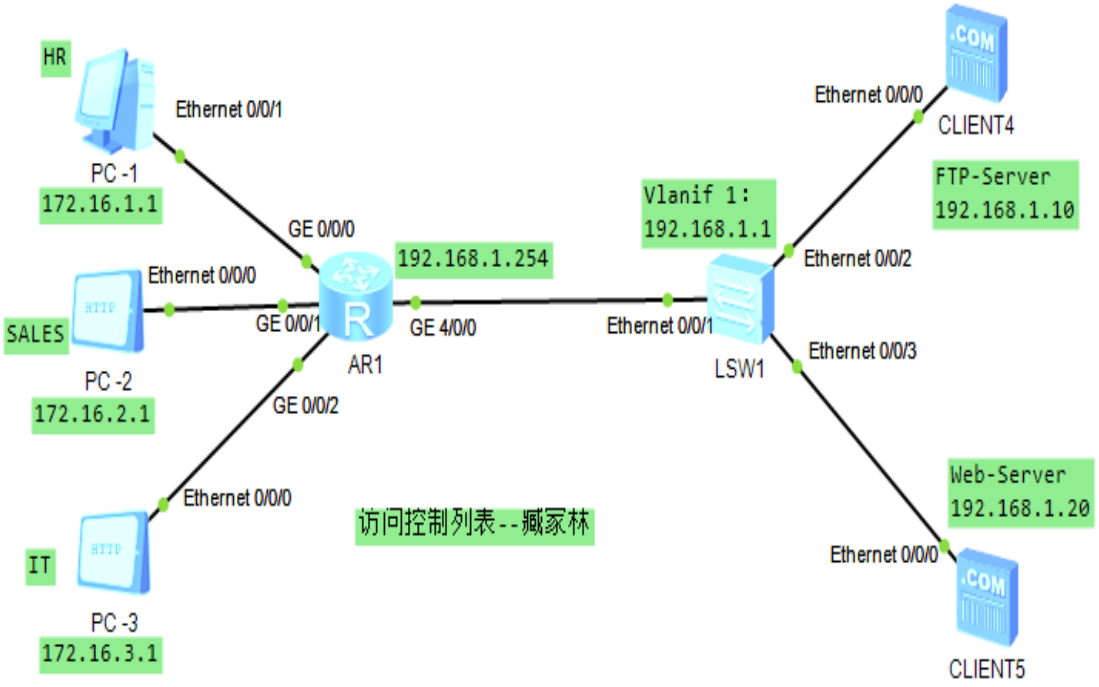
路由控制实验 1：访问控制列表

访问控制列表（ACL： Access Control List）是一种常用的网络技术，它的基本功能是对经过网络设备的报文进行过滤处理。

ACL 是由 permit 和 deny 语句组成的一个有序规则的集合。它首先通过报文匹配过程来实现对报文的分类识别，然后根据报文的分类信息和相关的执行动作来判断哪些报文可以放行，哪些报文不能放行，从而实现对特定报文的过滤处理。除此之外，ACL 还有其他一些功能，这些功能常常被 route-policy 、QOS 、IPSec、Firewall 等技术结合来使用。

ACL 的常用类型：基本 ACL，高级 ACL，二层 ACL，用户自定义 ACL 等，其中应用最为广泛的是基本 ACL 和高级 ACL。基本 ACL 可以根据源 IP 地址、报文分片标记和时间段信息来定义规则。高级 ACL 可以根据源/目的 IP 地址、TCP 源/目的端口号、UDP 源/目的端口号、协议号、报文优先级、报文大小、时间段等信息来定义规。高级 ACL 可以比基本 ACL 定义出精细度更高的规则。

基本 ACL　:2000-2999
高级 ACL　:3000-3999



1.基本配置

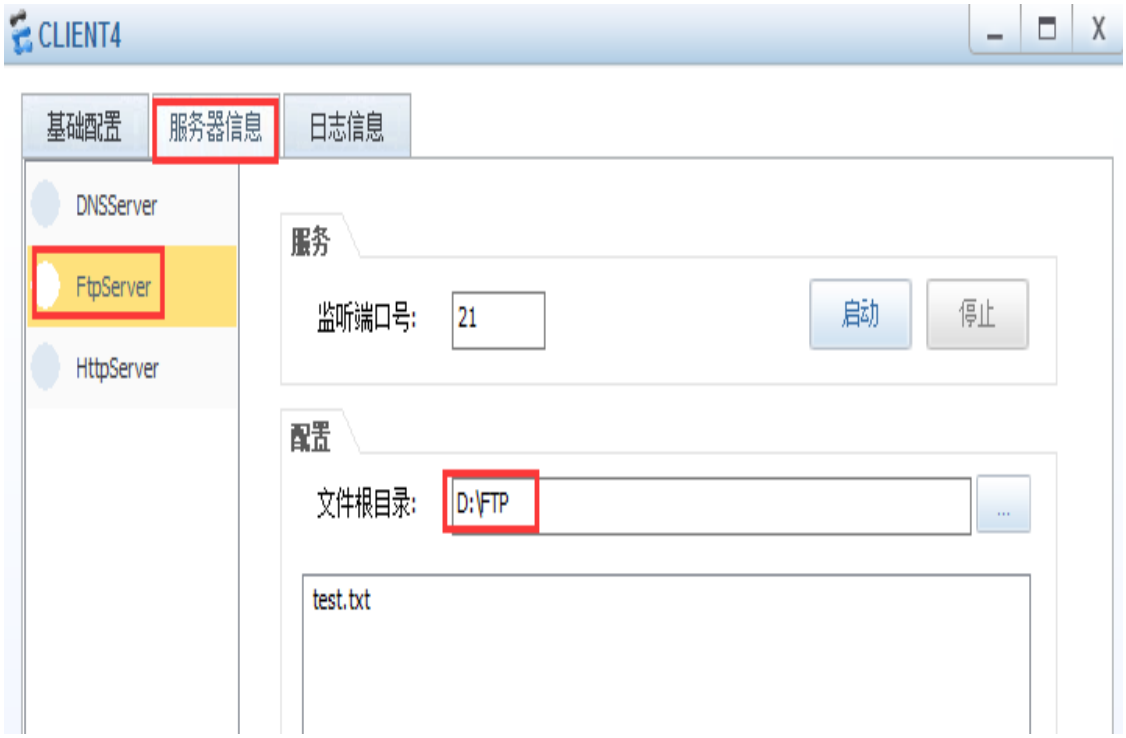
R1:
un ter mo
sys
sysname R1
int g0/0/0

ip add 172.16.1.254 24
int g0/0/1
ip add 172.16.2.254 24
int g0/0/2
ip add 172.16.3.254 24
int g4/0/0
ip add 192.168.1.254 24
q

SW1:
un ter mo
sys
sysname SW1
int vlanif 1
ip add 192.168.1.1 24
q

设置 FTP 服务器

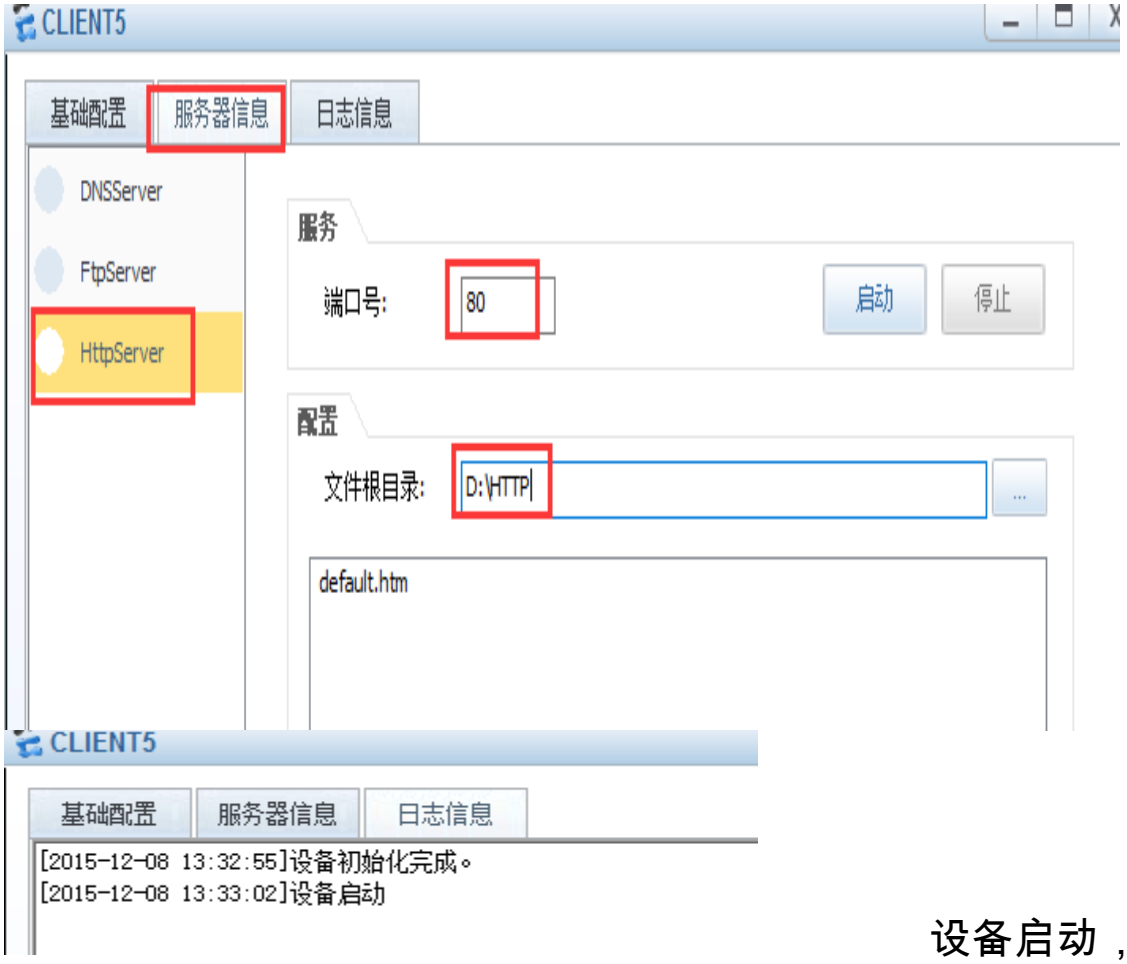
端口号默认 21，文件目录在 D 盘，FTP 文件夹，可以自行设定，启动



启动之后，日志信息显示 listening 就正常工作了

设置 HTTP Web 服务器

在 D 盘建立文件夹，用记事本建立 default 文件，改后缀名为 htm, 内容为 Hello,world!



设备启动，显示就成功运行了。

2.创建安全区域

路由器用域间防火墙特性来提高安全性，在 R1 上建立 3 个部门的安全区域 HR、 SALES、 IT。

HR　　区域的安全级别设置为 12
SALES　区域的安全级别设置为 10
IT　　区域的安全级别设置为 8

另外，还需要创建 Trust 区域，设置 Trust 区域的安全级别为 14，将 FTP 、Web 服务器放在 Trust 区域。

trust　区域的安全级别设置为 14

AR 系统路由器默认可以设置　16 种安全级别，取值 0-15, 15 保留给 Local 区域使用

配置 R1 ，并将接口划分不到同的区域中

R1：
firewall zone trust
priority 14
firewall zone HR
priority 12
firewall zone SALES
priority 10
firewall zone IT
priority 8
q

int g4/0/0
zone trust
int g0/0/0
zone HR
int g0/0/1
zone SALES
int g0/0/2
zone IT

配置完成后，查看相应的区域信息
<R1>display firewall zone

```
[R1]display firewall zone
zone IT
 priority is 8
 interface of the zone is (total number 1):
 GigabitEthernet0/0/2

zone SALES
 priority is 10
 interface of the zone is (total number 1):
 GigabitEthernet0/0/1

zone HR
 priority is 12
 interface of the zone is (total number 1):
 GigabitEthernet0/0/0

zone trust
 priority is 14
 interface of the zone is (total number 1):
 GigabitEthernet4/0/0
```

3.配置安全策略

把接口加入到相应的区域后，就可以实施基于安全区域的 ACL。

在配置时，要注意路由器的防火墙特性：流量方向。

从较高安全级别区域去往较低安全级别区域的报文称为 outbound 报文

从较低安全级别区域去往较高安全级别区域的报文称为 inbound 报文

AR 系统路由器的防火墙特性允许管理员在不同的区域之间进

行报文的过滤处理。

==========

禁止 SALES 和 HR 部门之间的互访

启用 SALES 和 HR 区域之间的防火墙。命令中的 SALES 和 HR 没有先后关系。
防火墙启用之后，安全级别高的区域能访问安全级别低的区域，并且应答报文也能够返回到安全级别较高的区域，但安全级别低的区域无法访问安全级别高的区域。
R1：
firewall interzone SALES HR
firewall enable

[R1]display firewall interzone SALES HR
默认的 inbound 报文被拒绝通过，而 outbound 报文被允许通过。

```
[R1]display firewall interzone HR SALES
interzone HR SALES
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
```

HR 区域安全级别为 12， SALES 区域安全级别为 10
HR 区域到 SALES 区域是 outbound 报文可以通过，而从 SALES 区域到 HR　区域是 inbound 报文被拒绝
用两台 PC 做测试　，PC1pingPC2 可能通 .

PC>ping 172.16.2.1

```
PC>ping 172.16.2.1

Ping 172.16.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
From 172.16.2.1: bytes=32 seq=2 ttl=127 time=15 ms
From 172.16.2.1: bytes=32 seq=3 ttl=127 time=16 ms
From 172.16.2.1: bytes=32 seq=4 ttl=127 time<1 ms
From 172.16.2.1: bytes=32 seq=5 ttl=127 time=15 ms
```

PC2pingPC1 则不通

为了禁止 SALES 和 HR 这两个部门之间的互访，管理员可以在它们之间使用 ACL 达到目的。由于默认 SALES 区域不能访问 HR 区域，不需要做过滤。只需在 outbound 方向上将 HR 去往 SALES 的报文全部过滤掉即可。

创建高级 ACL 3000 来定义从 HR 到 SALES 的报文，在 outbound 方向上引用 ACL 3000

R1:
acl 3000
rule deny ip source 172.16.1.0 0.0.0.255 destination 172.16.2.0 0.0.0.255

q

firewall interzone SALES HR
packet-filter 3000 outbound

[R1]display firewall interzone SALES HR

```
[R1]display firewall interzone HR SALES
interzone HR SALES
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3000 outbound
```

用 PC 测试一下，PC1 去 ping PC2 应该是不通的，说明相应的安全需求已经得到实现。
PC>ping 172.16.2.1

```
PC>ping 172.16.2.1

Ping 172.16.2.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
```

==========

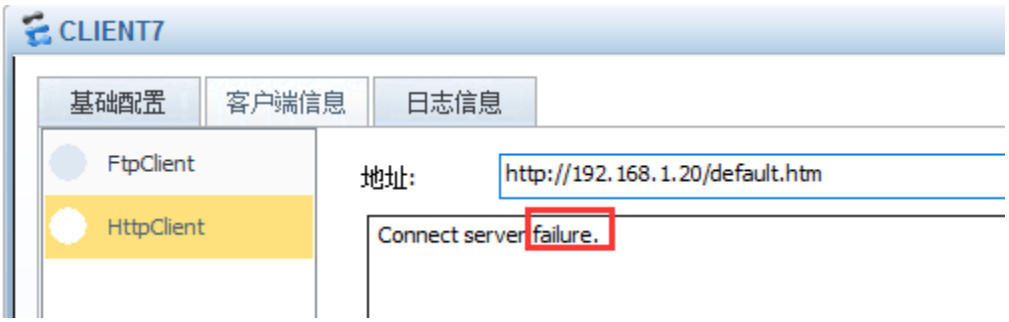
控制 Web 和 FTP 服务器的访问

SALES 部门的用户可以访问公司的 Web 服务器，但禁止访问 FTP 服务器。
SALES 安全级别为 10， trust 安全级别为 14，流量方向为 inbound,防火墙默认是禁止的。因此，创建 3001 在 inbound 方向上明确放行 SALES 区域访问 Web 的报文，其他访问报文

被默认拒绝通过。

R1：
firewall interzone SALES trust
firewall enable

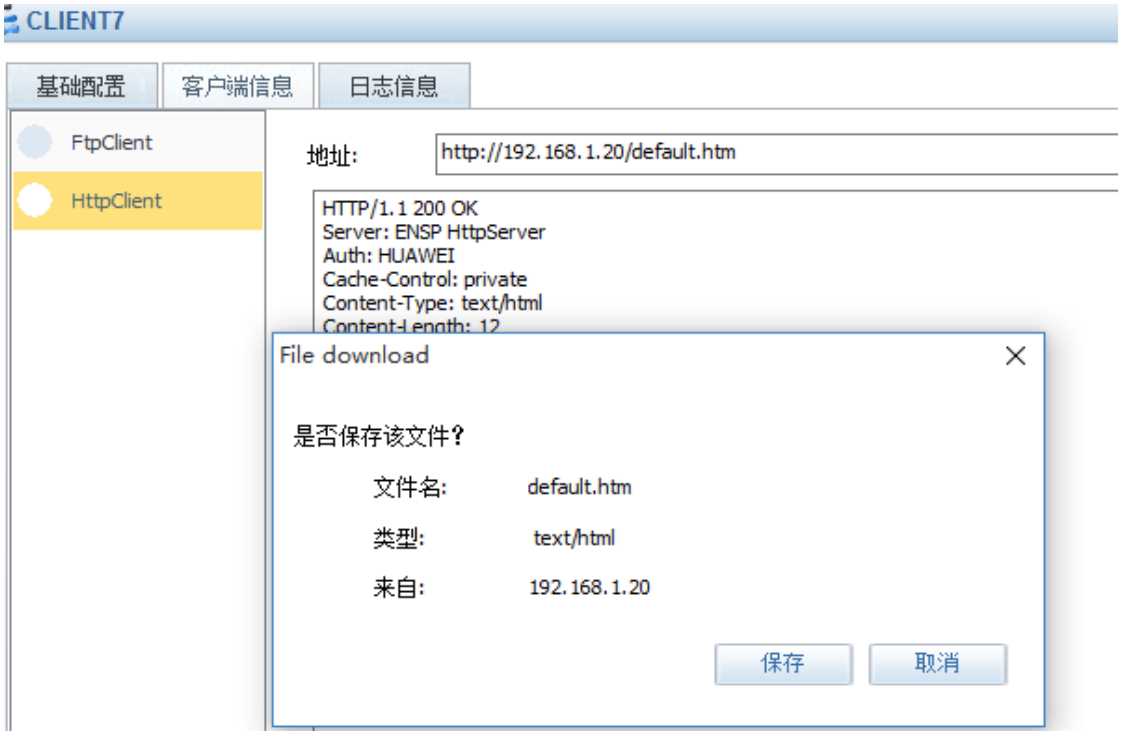
启用之后，PC-2 无法访问 Web 服务器
http://192.168.1.20/default.htm

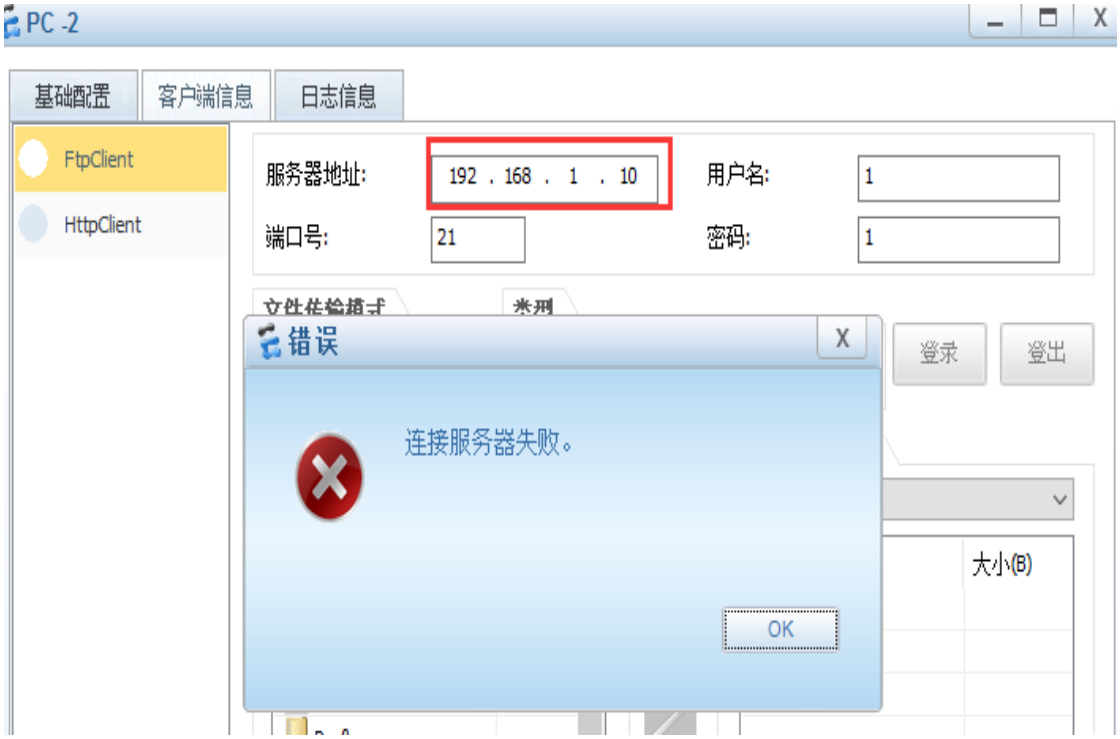


创建 ACL 3001,允许 SALES 部门的用户访问 Web 服务器，并应用在 SALES 和 trust 的区域之间
R1：
acl 3001
rule permit tcp source 172.16.2.0 0.0.0.255
destination 192.168.1.20 0 destination-port eq 80
q

firewall interzone SALES trust
packet-filter 3001 inbound

可以看到 PC-2 可以访问 Web 服务器，但无法访问　FTP 服务器
http://192.168.1.20/default.htm


CLIENT7
基础配置
客户端信息
日志信息
FtpClient
HttpClient
地址:
http://192.168.1.20/default.htm
HTTP/1.1 200 OK
Server: ENSP HttpServer
Auth: HUAWEI
Cache-Control: private
Content-Type: text/html
Content-Length: 12
File download
是否保存该文件?
文件名: default.htm
类型: text/html
来自: 192.168.1.20
保存
取消


PC -2
基础配置
客户端信息
日志信息
FtpClient
HttpClient
服务器地址:
192 . 168 . 1 . 10
用户名:
1
端口号:
21
密码:
1
登录
登出
错误
连接服务器失败。
OK
大小(B)

另一个需求：

IT 部门可以访问 FTP 服务器，但只能在每天的 14:00-16:00 才能访问 Web 服务器，还要求 IT 部门的用户能够随时 ping 通 FTP 和 Web 服务器。

开启 IT 和 trust 之间的防火墙，配置时间为每天的 14:00-16:00。创建 ACL 3002, 放行 IT 到 trust 的 inbound 方向的 FTP 、Web 、ICMP 的报文。
R1 :

```
firewall interzone IT trust
firewall enable
q
time-range web 14:00 to 16:00 daily

acl 3002
rule permit tcp source 172.16.3.0 0.0.0.255
destination 192.168.1.20 0 destination-port eq 80
time-range web
rule permit tcp source 172.16.3.0 0.0.0.255
destination 192.168.1.10 0 destination-port eq 21
rule permit icmp source 172.16.3.0 0.0.0.255
destination 192.168.1.10 0
rule permit icmp source 172.16.3.0 0.0.0.255
destination 192.168.1.20 0

firewall interzone   IT trust
packet-filter 3002 inbound
```

查看配置，display firewall interzone IT trust

```
[R1]display firewall interzone IT trust
interzone trust IT
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3002 inbound
```

==========

对设备的安全控制和管理

为实现对 R1 的安全控制和管理，现在只允许 SW1 上的 VLANIF 1 接口的 IP 地址 192.168.1.1 能够作为源地址登录到 R1. 在 R1 上配置 VTY 用户接口，允许远程主机通过 telnet 管理 R1。使用基本 ACL 对路由器的 VTY 终端进行保护，只允许源地址为 192.168.1.1 的报文访问 R1 的 VTY 终端。

R1:
user-interface vty 0 4
authentication-mode password

acl 2000
rule permit source 192.168.1.1 0
q
user-interface vty 0 4
acl 2000 inbound

在 SW1 上使用 telnet 输入密码后就能登录，<SW1>telnet 192.168.1.254

```
<SW1>telnet 192.168.1.254
Trying 192.168.1.254 ...
Press CTRL+K to abort
Connected to 192.168.1.254 ...

Login authentication


Password:
```

将 SW1　的 VLANIF 1 接口的 IP 地址修改为 192.168.1.2
SW1:
int vlanif 1
ip add 192.168.1.2 24

再测试一下是否能登录到 R1，更换 IP 地址后，便无法登录到 R1.
<SW1>telnet 192.168.1.254

```
<SW1>telnet 192.168.1.254
Trying 192.168.1.254 ...
Press CTRL+K to abort
```

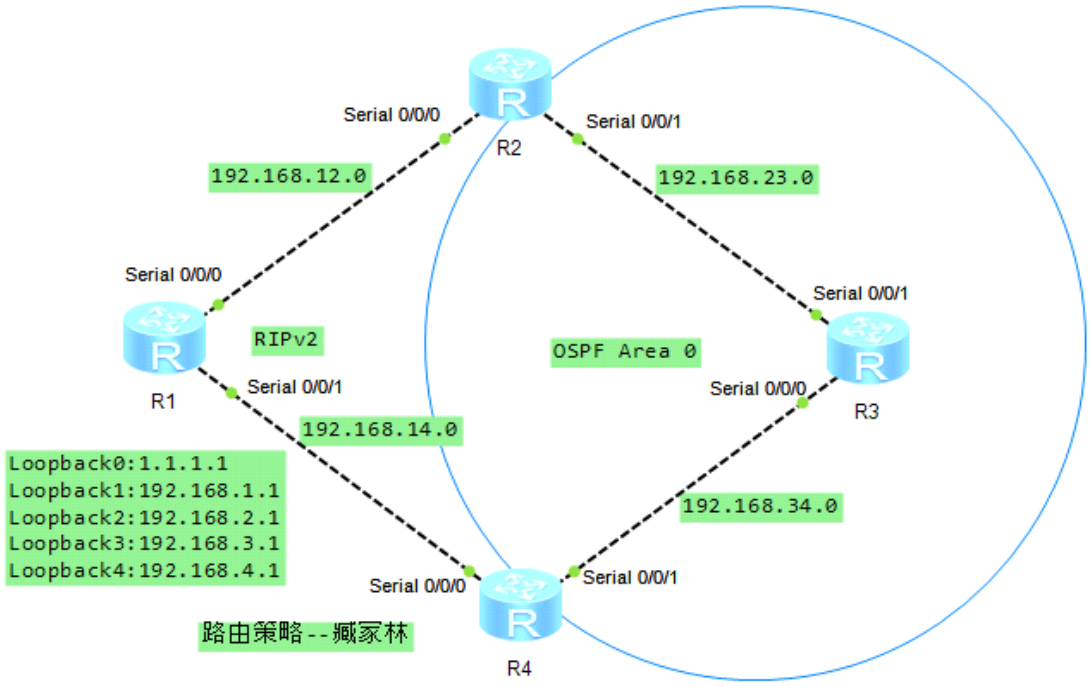
=========

路由控制实验 2：路由策略

路由策略 Route-policy 的应用非常广泛。例如，它可以规定路由器在发布路由时只发布某些满足特定条件的路由，在接收路由时只接收某些满足特定条件的路由，在引入路由时只引入某些特定条件的路由，如此等等。

Route-policy 由一个或多个节点（Node）构成，Node 之间是“或”的关系。每个 Node 都有一个编号，路由项按照 Node 编号由小到大的顺序通过各个 Node。每个 Node 下面可以有若干个 if-match 和 apply 子句（特殊情况下可以完全没有 if-match 和 apply 子句），if-match 之间是“与”关系。If-match 子句用来定义匹配规则，即路由项通过当前 Node 所需要满足的条件，匹配对象是路由项的某些属性，比如路由前缀，Next Hop ,cost ，路由优先级等，apply 子句用来规定处理动作。

路由策略实验 1：基本配置



要求 R3 去往 R1 的，192.168.1.0 和 192.168.3.0 路径为 R3-R2-R1

R3 去往 R1 的，192.168.2.0 和 192.168.4.0 路径为 R3-R4-R1

基本配置
R1:
```
undo ter mo
sys
sysname R1
user-interface console 0
idle-timeout 0 0
int loop 0
ip add 1.1.1.1 24
int loop 1
ip add 192.168.1.1 24
int loop 2
ip add 192.168.2.1 24
int loop 3
ip add 192.168.3.1 24
int loop 4
ip add 192.168.4.1 24
int s0/0/0
ip add 192.168.12.1 24
int s0/0/1
ip add 192.168.14.1 24
q
```

R2:
```
undo ter mo
sys
sysname R2
user-interface console 0
idle-timeout 0 0
int s0/0/0
ip add 192.168.12.2 24
int s0/0/1
ip add 192.168.23.2 24
```

q

R3 :
undo ter mo
sys
sysname R3
user-interface console 0
idle-timeout 0 0
int s0/0/1
ip add 192.168.23.3 24
int s0/0/0
ip add 192.168.34.3 24
q

R4:
undo ter mo
sys
sysname R4
user-interface console 0
idle-timeout 0 0
int s0/0/0
ip add 192.168.14.4 24
int s0/0/1
ip add 192.168.34.4 24
q

R1 R2 R4 之间运行 RIP 协议，R2 R3 R4 运行 OSPF
R1:
rip
version 2
net 1.0.0.0
net 192.168.1.0
net 192.168.2.0
net 192.168.3.0

net 192.168.4.0
net 192.168.12.0
net 192.168.14.0
q

R2:
rip
version 2
net 192.168.12.0
ospf router-id 2.2.2.2
area 0
network 192.168.23.2 0.0.0.0
q

R3:
ospf router-id 3.3.3.3
area 0
network 192.168.23.3 0.0.0.0
network 192.168.34.3 0.0.0.0
q

R4:
rip
version 2
net 192.168.14.0
ospf router-id 4.4.4.4
area 0
network 192.168.34.4 0.0.0.0
q

配置完成后在 R2 R4 将 RIP 引入到 OSPF 中
R2:
ospf
import-route rip 1

q

R4:
ospf
import-route rip 1
q

<R3>display ip routing-table R3 能看到很多引入的路由

1.1.1.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.1.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.2.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.3.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.4.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.12.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.14.0/24	O_ASE	150	1	D	192.168.23.2	Serial0/0/1
	O_ASE	150	1	D	192.168.34.4	Serial0/0/0
192.168.23.0/24	Direct	0	0	D	192.168.23.3	Serial0/0/1

利用 Route-policy 对引入的路由进行过滤和修改

先修改 192.168.1.0　192.168.3.0
R2 :
acl 2000
rule permit source 192.168.1.0 0.0.254.255
route-policy 10 permit node 1
if-match acl 2000
apply cost 20

apply cost-type type-1

ospf
import-route rip 1 route-policy 10

R4 :
acl 2000
rule permit source 192.168.1.0 0.0.254.255
route-policy 10 permit node 1
if-match acl 2000
apply cost 30
apply cost-type type-1

ospf
import-route rip 1 route-policy 10

配置完成后，查看<R3>display ip routing-table

192.168.1.1 == 192.168.1.00000001

192.168.1.3 == 192.168.1.00000011

192.168.1.5 == 192.168.1.00000101

=> 192.168.1.[奇数] == 192.168.1.xxxxxxx**1**

192.168.1.2 == 192.168.1.00000010

192.168.1.4 == 192.168.1.00000100

192.168.1.6 == 192.168.1.00000110

=> 192.168.1.[偶数] == 192.168.1.xxxxxxx0

匹配 192.168.2.0 192.168.4.0

R2 :

acl 2001

rule permit source 192.168.0.0 0.0.254.255

route-policy 10 permit node 2

if-match acl 2001

apply cost 30

apply cost-type type-2

R4 :

acl 2001

rule permit source 192.168.0.0 0.0.254.255

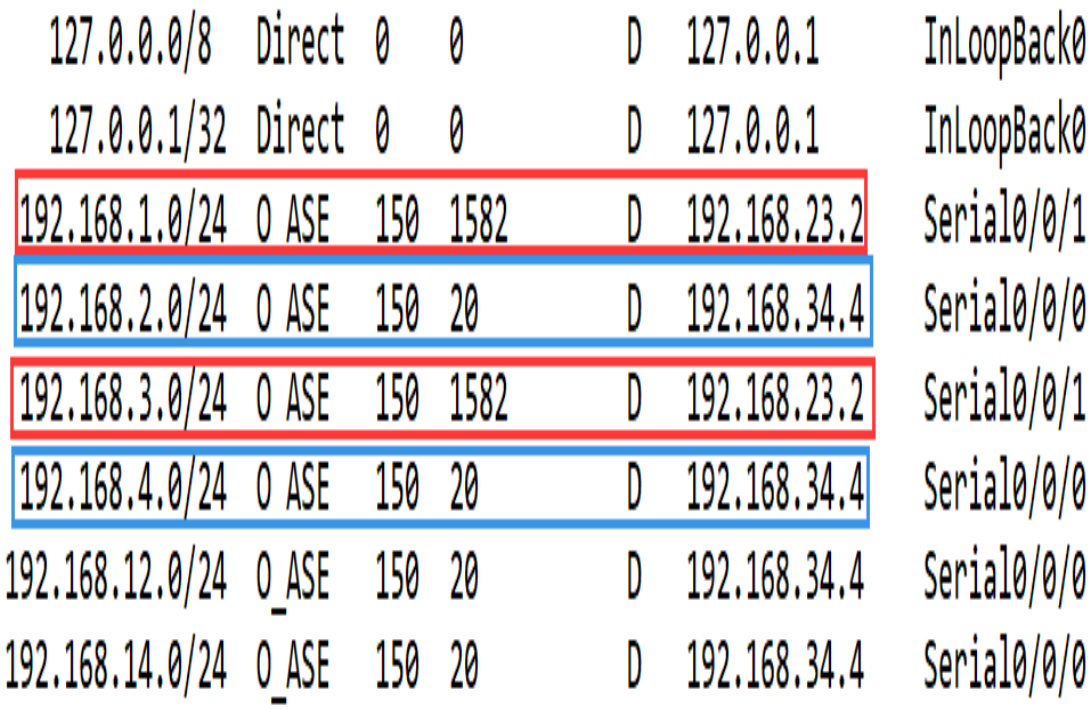
route-policy 10 permit node 2

if-match acl 2001

apply cost 20

apply cost-type type-2

配置完成后，查看<R3>display ip routing-table



127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.1.0/24	O_ASE	150	1582	D	192.168.23.2	Serial0/0/1
192.168.2.0/24	O_ASE	150	20	D	192.168.34.4	Serial0/0/0
192.168.3.0/24	O_ASE	150	1582	D	192.168.23.2	Serial0/0/1
192.168.4.0/24	O_ASE	150	20	D	192.168.34.4	Serial0/0/0
192.168.12.0/24	O_ASE	150	20	D	192.168.34.4	Serial0/0/0
192.168.14.0/24	O_ASE	150	20	D	192.168.34.4	Serial0/0/0

但是在 R3 上没有看到 1.1.1.0 的路由
Route-policy 存在一条默认规则，如果某条路由没有通过 Route-policy 的任何 Node ，则这条路由不会被引入。如果希望将 1.1.1.0 的路由引入 OSPF 中，则需要在 Route-policy 中添加一个 Node 号最大，模式为 permit 的 Node，该 Node 下不需要定义任何内容，其含义是任何路由项都可以通过该 Node。
R2：
route-policy 10 permit node 3
R4：
route-policy 10 permit node 3
配置好之后，R3 上就有 1.1.1.0 的路由了

1.1.1.0/24	O_ASE	150	1		D	192.168.23.2	Serial0/0/1
	O_ASE	150	1		D	192.168.34.4	Serial0/0/0
127.0.0.0/8	Direct	0	0		D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0		D	127.0.0.1	InLoopBack0
192.168.1.0/24	O_ASE	150	1582		D	192.168.23.2	Serial0/0/1
192.168.2.0/24	O_ASE	150	20		D	192.168.34.4	Serial0/0/0
192.168.3.0/24	O_ASE	150	1582		D	192.168.23.2	Serial0/0/1
192.168.4.0/24	O_ASE	150	20		D	192.168.34.4	Serial0/0/0
192.168.12.0/24	O_ASE	150	20		D	192.168.34.4	Serial0/0/0

如果要让 R3 能 ping 通 R1 的环回口，需要将 OSPF 引入 RIP

R2：

rip

import-route ospf 1

R4：

rip

import-route ospf 1

R3 测试一下 ,到 192.168.1.1 是由 R2 过去的

```
[R3]tracert 192.168.1.1

 traceroute to  192.168.1.1(192.168.1.1),
CTRL_C to break

 1 192.168.23.2 60 ms  30 ms  30 ms

 2 192.168.12.1 50 ms  60 ms  100 ms
```