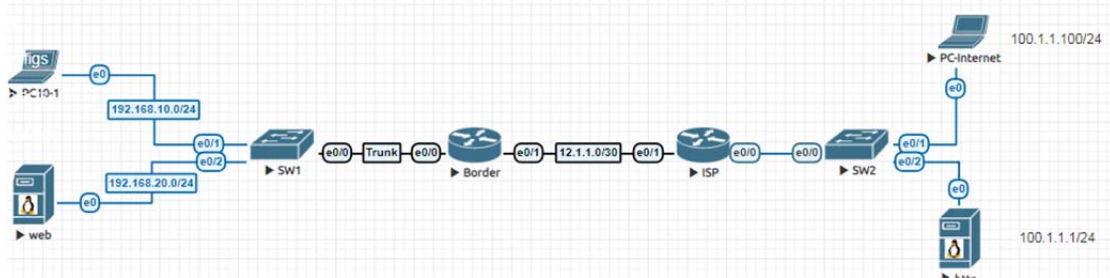


## 自反 ACL 配置

### 一、拓扑



要求：

1. 两侧网络通过 OSPF 路由相通，其中在 Border 上不使用 NAT。
2. 要求 PC10-1 可以正常访问 http 上的网站、ftp 等服务，并且能够通过 icmp 方式访问 PC-Internet 及 http。
3. PC-Internet 只能访问 web 上的网站。
4. PC-Internet 和 http 不能通过 icmp 访问 web 和 PC10-1。

### 二、配置

1.基本 IP 地址配置（省略）。

其中 PC10-1 的 IP 地址为 192.168.10.1/24、web 的 IP 地址为 192.168.20.1/24，网关在边界路由器 Border 上。

PC-Internet 的 IP 地址为 100.1.1.100/24、http 的 IP 地址为 100.1.1.1/24，边界在 ISP 路由器上。

### 二、配置

1.在边界路由器上配置子接口及 OSPF 路由协议

```
Border(config)#interface e0/0.10
Border(config-subif)#encapsulation dot1q 10
Border(config-subif)#ip address 192.168.10.254 255.255.255.0
Border(config-subif)#exit
Border(config)#interface e0/0.20
Border(config-subif)#encapsulation dot1q 20
Border(config-subif)#ip address 192.168.20.254 255.255.255.0
Border(config-subif)#exit
```

```
Border(config)#router ospf 110
Border(config-router)#router-id 1.1.1.1
Border(config-router)#network 12.1.1.0 0.0.0.3 area 0
Border(config-router)#network 192.168.10.0 0.0.0.255 area 0
Border(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

2.在 ISP 路由器上配置 OSPF 路由协议

```
ISP(config)#router ospf 110
ISP(config-router)#router-id 2.2.2.2
ISP(config-router)#network 12.1.1.0 0.0.0.3 area 0
ISP(config-router)#network 100.1.1.0 0.0.0.255 area 0
ISP(config-router)#exit
ISP(config)#
```

3.配置自反 ACL

所谓的自反 ACL，实质上是一种状态化的 ACL，根据题目要求，PC10-1 访问 PC-Internet、http 时必须正常，即对由 PC10-1 主动发起的访问流量是放行的，而由 PC-Internet、http 主动发起的 ICMP 流量是拒绝的，此时如果在边界路由器 Border 的外接口 e0/1 上使用传统的 ACL，就会存在问题。因为，当 PC10-1 通过 ICMP 方式访问 PC-Internet、http 时，传统的 ACL 会将

其返回流量拒绝掉。

为了能够拒绝掉由 PC-Internet、http 主动发起的 ICMP 流量，又能放行 PC10-1 的返回流量，就要配置自反 ACL。

#### ①配置主 ACL

主 ACL，即产生返回流量的 ACL，在本题目中，应当是 PC10-1 访问 PC-Internet、http 的流量，对这个流量必须起一个别名。

```
Border(config)#ip access-list extend ACL_REFLECT
Border(config-ext-nacl)#permit ip 192.168.20.0 0.0.0.255 any
Border(config-ext-nacl)#92.168.10.0 0.0.0.255 any reflect Active_Traffic
Border(config-ext-nacl)#exit
Border(config)#
```

在这个 ACL 中，将由 192.168.10.0 0.0.0.255 网段的主机向外发起的流量起别名为 Active\_Traffic，即对其进行状态化监控。

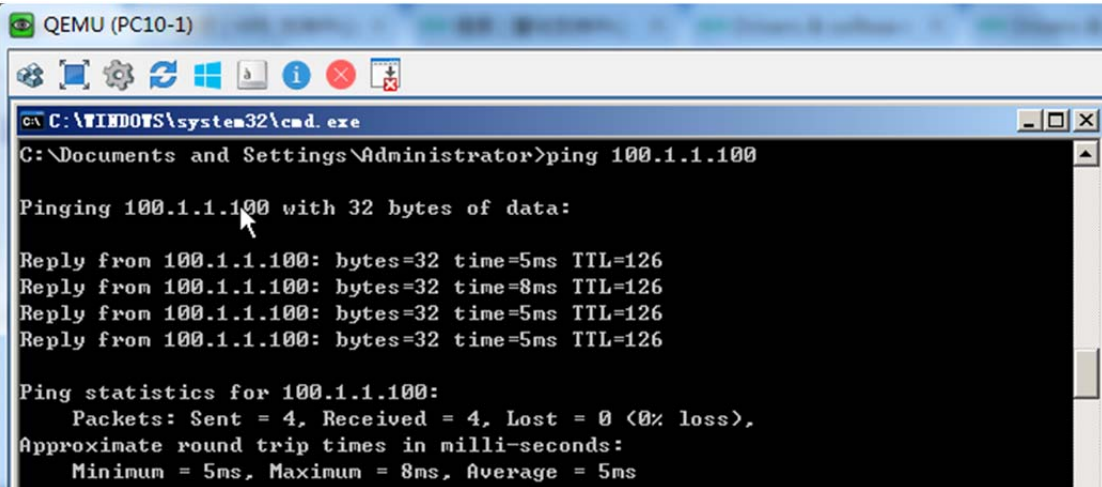
#### ②配置副 ACL

```
Border(config)#ip access-list extend ACL_BACK
Border(config-ext-nacl)#permit ip any 192.168.20.0 0.0.0.255
Border(config-ext-nacl)#evaluate Active_Traffic
Border(config-ext-nacl)#exit
```

在这个 ACL 中，其对别名为 Active\_Traffic 流量的返回流量进行放行。

### 三、测试

#### ①PC10-1 主动访问 PC-Internet 和 http 上的网站



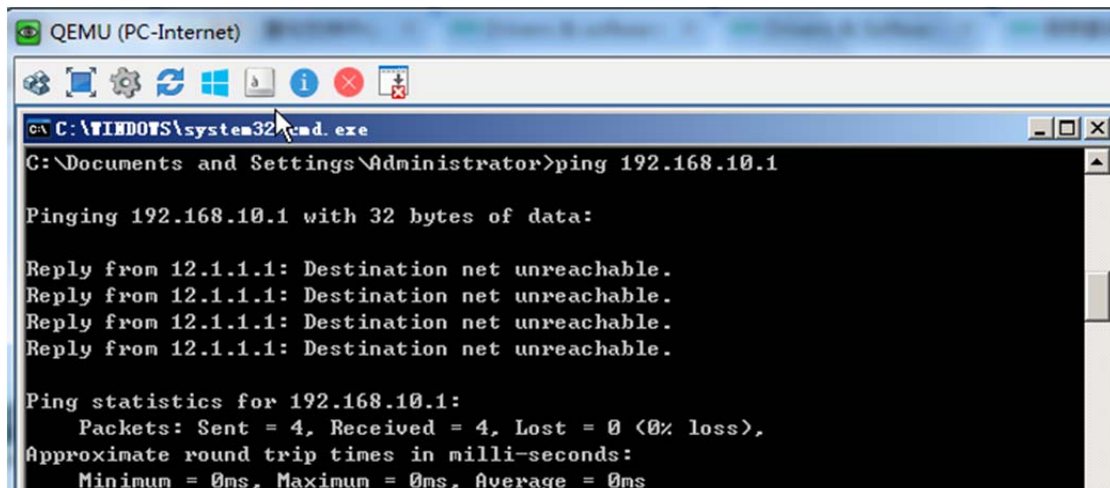
The screenshot shows a QEMU window titled 'QEMU (PC10-1)'. Inside, a Windows-style command prompt is open with the title 'C:\WINDOWS\system32\cmd.exe'. The user has entered the command 'ping 100.1.1.100'. The output shows four successful replies from 100.1.1.100 with varying response times (5ms and 8ms) and a TTL of 126. The ping statistics at the bottom indicate that all 4 packets were received with 0% loss, and the average response time is 5ms.

可以看到 PC10-1 可以主动访问 PC-Internet。



可以看到 PC10-1 正常访问 http 上的网站。

②PC-Internet 主动访问 PC10-1 和 web 上的网站



可以看到 PC-Internet 无法通过 icmp 方式访问 PC10-1。



可以看到 PC-Internet 正常访问 web 上的网站。

总结：

通过自反 ACL，可以完成一些数据流的单向访问，特别是在企业网的内部流量控制中，可以实现财务部或者人事部发送一些通知，或者技术部对其它部门的远程协助。

在上面的自反 ACL 配置中，特别是返回流量的配置中，一定要注意 ACL 的流量控制，在本例中，实质上还要放行 OSPF 流量，

```
Border#show ip access-list ACL_BACK
Extended IP access list ACL_BACK
 10 permit ip any 192.168.20.0 0.0.0.255 (10 matches)
 15 permit ospf any any (84 matches)
 20 evaluate Active_Traffic
Border#
```

如果未加上序列为 15 的 ACE，则导致 Border 和 ISP 之间的 OSPF 邻居挂掉。