TTS 9.0 COOKBOOK

(NSD PROJECT1 DAY04)

版本编号 9.0

2018-01

达内 IT 培训集团

NSD PROJECT1 DAY04

1. 案例 1：标准 ACL 的配置（1）

- **问题**

按照图-1 所示拓扑结构，禁止主机 pc2 与 pc1 通信，而允许所有其他流量

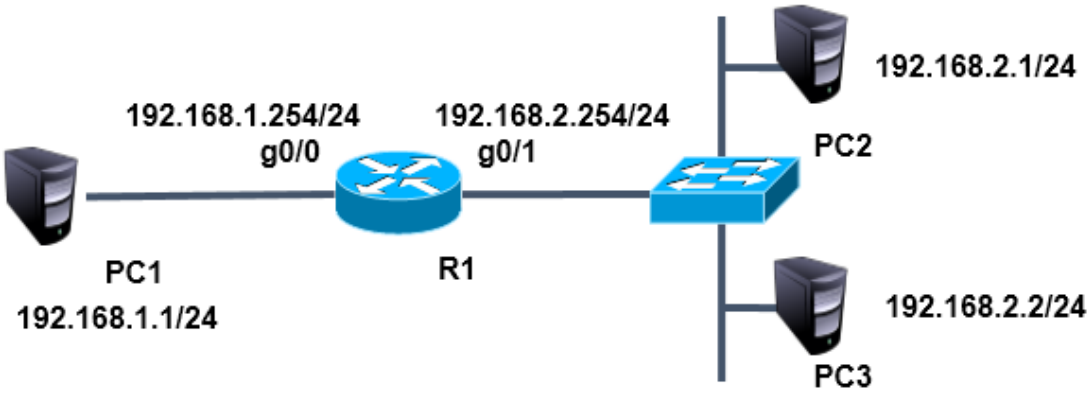

图-1

- **步骤**

1，为路由器 g0/0 接口配置 ip 192.168.1.254，为路由器 g0/1 接口配置 ip 192.168.2.254

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#no shut

Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.2.254 255.255.255.0
Router(config-if)#no shut
```

2，为每台 pc 配置 ip 与网关

3，使用标准 acl 限制 pc2

```
Router(config)#access-list 1 deny 192.168.2.1 0.0.0.0
```

或

```
Router(config)#access-list 1 deny host 192.168.2.1
```

以上两条配置其中一条即可，效果相同。

4，放行其他数据

```
Router(config)#access-list 1 permit any
```

5，在接口中应用 acl

```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip access-group 1 in
```

2. 案例 2：标准 ACL 的配置（2）

- **问题**

按照图-2 所示拓扑结构，允许主机 pc2 与 pc1 互通，而禁止其他设备访问 pc1

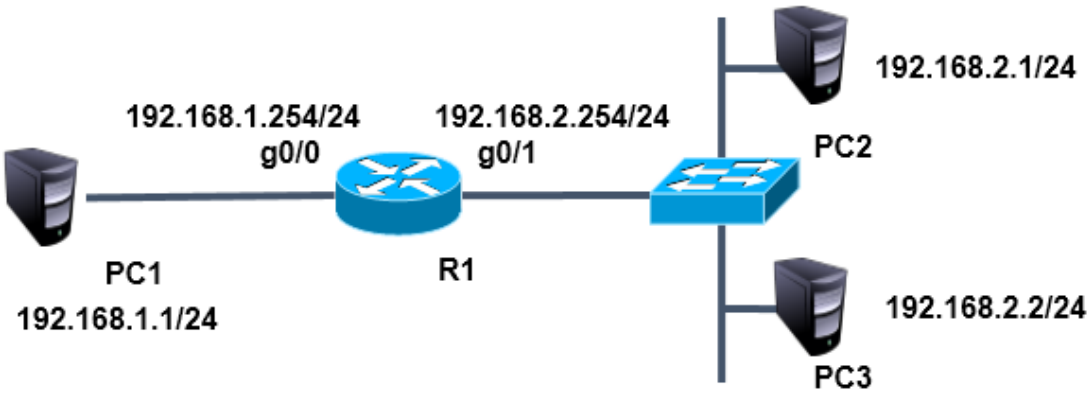

图-2

- **步骤**

注：此配置需要在案例 1 的基础上完成

```
Router(config)#no access-list 1
Router(config)#access-list 1 permit 192.168.2.1 0.0.0.0
```

或

```
Router(config)#access-list 1 permit host 192.168.2.1
```

以上两条配置其中一条即可，效果相同。

3. 案例 3：扩展访问控制列表

- **问题**

按照图-3 所示拓扑结构，禁止 pc2 访问 pc1 的 ftp 服务，禁止 pc3 访问 pc1 的 www 服务，所有主机的其他服务不受限制

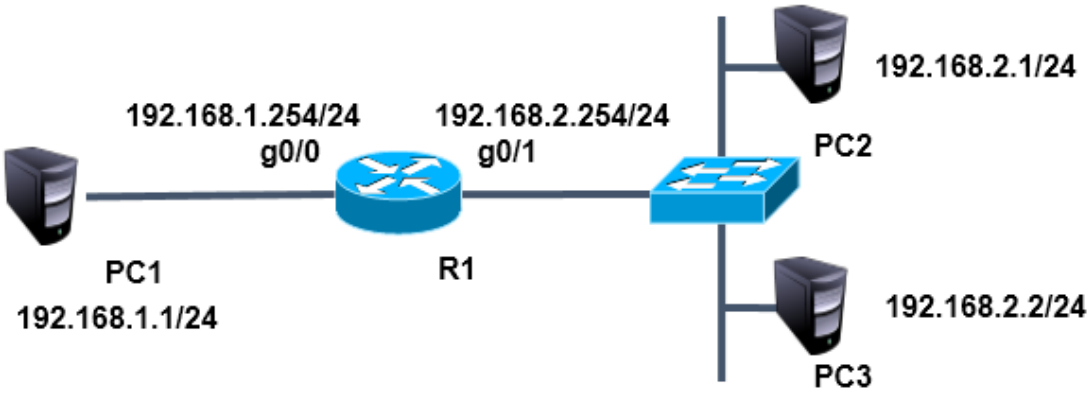

图-3

- **步骤**

注：此配置需要在案例 2 的基础上完成

```
Router(config)#no access-list 1
Router(config)#access-list 100 deny tcp host 192.168.2.1 host 192.168.1.1 eq 21
Router(config)#access-list 100 deny tcp host 192.168.2.2 host 192.168.1.1 eq 80
Router(config)#access-list 100 permit ip any any
```

在接口中应用 acl

```
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip access-group 100 in
```

4. 案例 4：配置静态 NAT

- **问题**

按照图-4 拓扑图所示，在 R1 上配置静态 NAT 使 192.168.1.1 转换为 100.0.0.2,192.168.1.2 转换为 100.0.0.3，实现外部网络访问

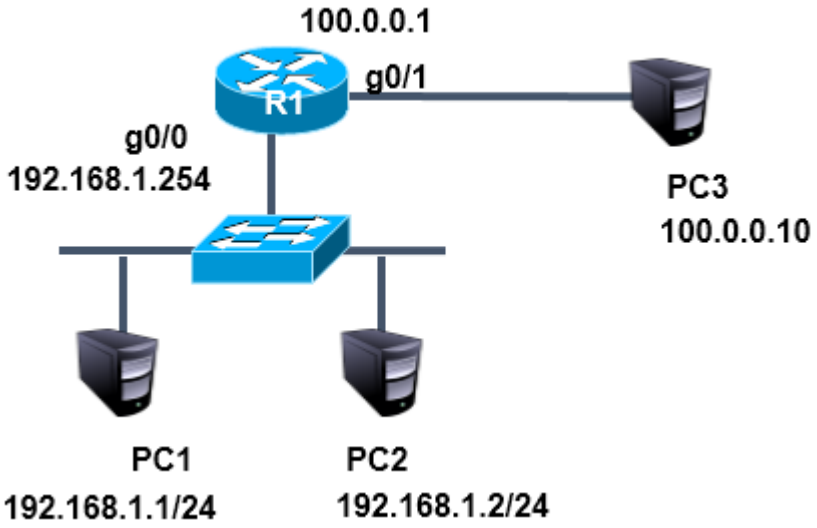

图-4

- **步骤**

1，首先配置路由器的接口地址

```
Router(config)#interface g0/1
Router(config-if)#ip address 100.0.0.1 255.0.0.0
Router(config-if)#no shut
Router(config)#interface g0/0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#no shut
```

2，配置静态 nat 转换

```
Router(config)#ip nat inside source static 192.168.1.1 100.0.0.2
Router(config)#ip nat inside source static 192.168.1.2 100.0.0.3
```

3，在内部和外部端口上启用 NAT

```
Router(config)#interface g0/1
Router(config-if)#ip nat outside
Router(config)#interface g0/0
Router(config-if)#ip nat inside
```

4，为 pc 配置 ip 地址与网关，pc3 无需配置网关

5. 案例 5：端口映射

- **问题**

按照图-5 所示拓扑结构，在 R1 上配置端口映射，将 192.168.1.1 的 80 端口映射为 100.0.0.2 的 80 端口，将其 web 服务发布到 Internet。

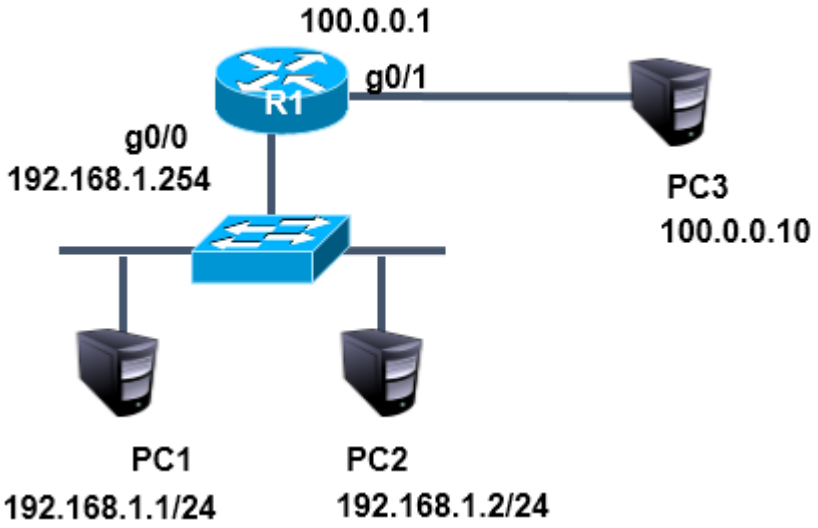

图-5

- **步骤**

注：此配置需要在练习 4 的基础上完成

```
Router(config)#no ip nat inside source static 192.168.1.1 100.0.0.2
Router(config)#no ip nat inside source static 192.168.1.2 100.0.0.3

Router(config)#ip nat inside source static tcp 192.168.1.1 80 100.0.0.2 80
```

6. 案例 6：端口多路复用

- **问题**

按照图-6 所示的拓扑结构，在 R1 上配置 PAT 端口多路复用使企业内网 192.168.1.0/24 复用 g0/1 端口的 ip，实现外部网络的访问

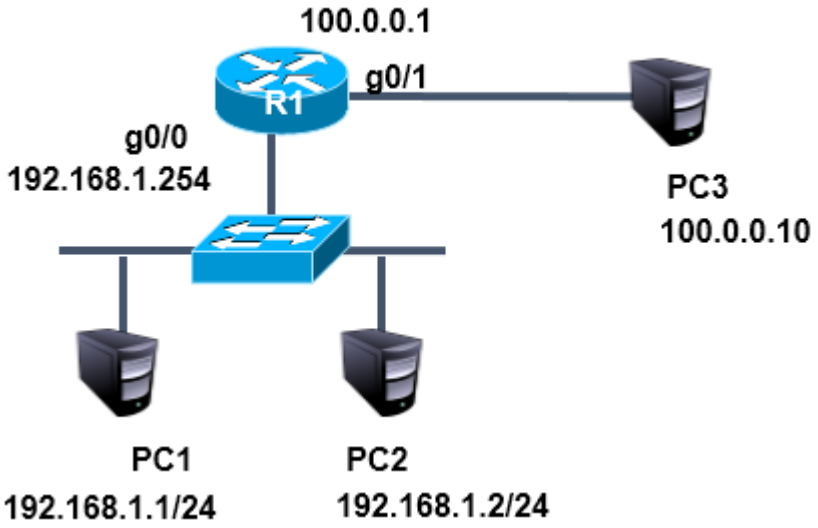

图-6

- **步骤**

注：此配置需要在案例 5 的基础上完成

```
Router(config)#no ip nat inside source static tcp 192.168.1.1 80 100.0.0.2 80
```

使用 acl 定义内部 ip 地址

```
Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

使用 pat 复用外网接口地址

```
Router(config)#ip nat inside source list 1 interface g0/1 overload
```