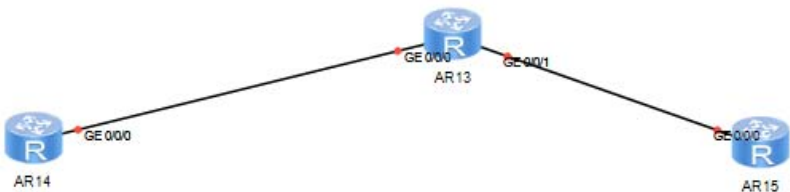


网络系统建设与运维课程教案

周次	6	课次	2	学时	4
本次课题	访问控制列表高级配置				
教学目标	知识目标： 掌握标准 ACL 和扩展 ACL 的配置能力目标： ①能对标准访问控制列表和扩展访问控制列表配置 ②能对标准访问控制列表和扩展访问控制列表在路由接口应用				
教学重点	重点：标准 ACL 的配置				
教学难点	难点：扩展性 ACL 的配置				
训练项目（任务）或案例	实验目的： 1、掌握标准 ACL 的配置； 2、理解标准 ACL 在接入控制中的运用 实验环境：华为路由器 3 台  图 4.1 实验内容： (1) 按图 4.1 所示连接网络； (2) 在 R2 三部署标准访问控制列表，只允许 192.168.12.0/24 网段的用户穿越 R2 访问 3.3.3.3，其他进入 R2 S0/0 接口的流量全部丢弃。 (3) R1 配置：				

```
R1# configure terminal
R1(config)# Interface serial0/0
R1(config-if)# Ip address 192.168.12.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface loopback0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# exit

R1(config)# ip route 0.0.0.0 0.0.0.0 192.168.12.2
```

(4) R2 配置:

```
R2# configure terminal
R2(config)# interface serial0/0
R2(config-if)# clock rate 64000
R2(config-if)# ip address 192.168.12.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# interface serial0/1
R2(config-if)# clock rate 64000
R2(config-if)# ip address 192.168.23.2 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit

R2(config)# ip route 1.1.1.1 255.255.255.255 192.168.12.1
R2(config)# ip route 3.3.3.3 255.255.255.255 192.168.23.3
```

(5) R3 配置:

	<pre>R3# configure terminal R3(config)# interface serial0/0 R3(config-if)# ip address 192.168.23.3 255.255.255.0 R3(config-if)# no shutdown R3(config-if)# interface loopback0 R3(config-if)# ip address 3.3.3.3 255.255.255.255 R3(config-if)# exit R3(config)# ip route 0.0.0.0 0.0.0.0 192.168.23.2</pre> (5) ACL 配置: <pre>R2(config)# access-list 1 permit 192.168.12.0 0.0.0.255 R2(config)# interface serial 0/0 R2(config-if)# ip access-group 1 in !!将 ACL 应用在 R2 的 S0/0 口 in 方向</pre> 与这一来从 R1 上直接 ping 3.3.3.3 是通的 ,因为数据的源地址是 192.168.12.1 ,而使用 1.1.1.1 为源去 ping 3.3.3.3 ,却无法 ping 通 ,因为此刻的源地址是 1.1.1.1 ,所以被 ACL 干掉了 : <pre>R1#ping 3.3.3.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 48/74/120 ms R1#ping 3.3.3.3 source 1.1.1.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds: Packet sent with a source address of 1.1.1.1 U.U.U Success rate is 0 percent (0/5)</pre>
教学方法	教师讲授法、案例分析法、实验法
教学环境	专用计算机房，华为模拟软件，广播软件
课后作业	

实验要求：

- 1.北京总部内网全网互通！其中要求部署DHCP服务器，使所有部门PC可以自动获取IP
- 2.要求总部可以全部上网，禁止互联网的路由器R4配置任何路由！
- 3.将总部的web服务器对外发布，要求互联网的PC可以成功总部内网的web服务器。
- 4.要求禁止销售部上网！
- 5.要求广州的员工可以安全访问总部的web服务器，但不能访问总部其他员工

教 学 过 程 设 计						
教学环节 时间分配		教学内容	教师活动	学生活动	技术与资源应用	设计意图
课前准备		复习动态 NAT 基本配置	提问	回答和操作	使用资源中的课件资源	回顾上节课内容
课中	环节一	教师教授访问控制列表 ACL 配置方法和命令	介绍并演示访问控制列表 ACL 配置方法和命令	了解访问控制列表 ACL 配置方法和命令	使用资源中的课件资源和视频资源	让学生了解访问控制列表 ACL 配置方法和命令
	环节二	学生练习访问控制列表 ACL 配置方法和命令	巡视和回答学生问题	动手进行访问控制列表 ACL 配置	使用资源中的课件资源和视频资源	让学生动手进行访问控制列表 ACL 配置
课后拓展		让学生在完成访问控制列表 ACL 配置实验后完成实验报告	布置课后练习	按要求完成	使用资源中的课件资源	巩固课程中学习的内容
教学反思						