ACL 实验

【实验目的】

ACL广泛应用于 NAT、IPv4-IPv6 地址翻译、VPN、QoS 中。本实验在路由器上配置基于时间的 ACL 实现主机对服务器的访问控制。

【实验拓扑】

两个网络通过一台路由器相连，如图 1 所示。

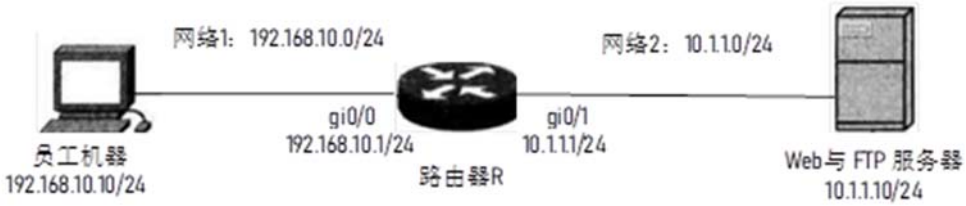

图 1 实验拓扑图

- 网络 1 ：
  - 员工机器：IP: 192.168.10.10/24, 与路由器 gi0/0 接口连接。
  - 路由器 R 的 gi0/0 端口： IP: 192.168.10.1/24。

- 网络 2：
  - 服务器机器：IP:10.1.1.10/24，与路由器 gi0/1 接口连接，其上部署 Web 服务器和 FTP 服务器。
  - 路由器 R 的 gi0/1 端口: IP: 10.1.1.1/24。

【实验内容】

1. 搭建实验拓扑：正确配置员工机器和服务器机器的 IP 地址、子网掩码、网关。复习网络配置等命令，以检查机器是否正确配置了网卡地址等。
2. 搭建实验拓扑：正确配置路由器的 2 个路由端口。
   复习路由器的配置命令，复习如何查看路由器的运行配置，以检查是否正确配置了路由器接口的 IP 地址、子网掩码等。
3. 安装 Web 和 FTP 服务器：在服务器机器上，正确安装 Web 与 FTP 服务器并启动它们。FTP 服务器至少创建一个用户名和密码。
4. 在路由器上设置基于时间的 ACL ：实现员工机在工作时间（9：00-18：00）仅可以访问 FTP 服务器，不可以访问 Web 服务器；在非工作时间仅可以访问 Web 服务器，不可以访问 FTP 服务器。

【实验步骤】

步骤 1：搭建实验拓扑

- 按照拓扑图连接设备
- 配置两台计算机（员工与服务器）的 ip 地址、子网掩码、网关
- 检查计算机与服务器的连通性
- 在服务器上安装 Web 和 FTP 服务器。FTP 服务器需要至少创建一个用户名和密码

Web 服务器（Apache）简化版安装教程

（1） 解压：解压 Apache24文件夹放置在 C 盘根目录。

（2） 安装：管理员身份运行cmd，进入C:/Apache24/bin，运行命令 httpd -k install -n "Apache"。

（3） 运行：文件管理器打开上述文件夹，运行A...Monitor.exe；打开图形界面（桌面左下角图标），第一行显示Apache24，点击 start。

（4） 验证：浏览器地址栏：http://127.0.0.1, 有显示页面即配置成功，tips:默认端口号为 80，如果 www 服务启动不了，可以尝试修改端口，比如从 80 修改为 8080 等，相关资料请自行查阅学习。

安装并启动 FTP 服务器 ：ftpserver 开启方式有多种，推荐使用Mobaxterm
mobaxterm-->server-->FTP server

步骤 2：配置路由器

```
// 进入RCMS路由器管理
Router#configure terminal
Router(config)#interface gigabitethernet 0/0
Router(config-i)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#exit
Router(config)#interface gigabitethernet 0/1
Router(config-if)#ip address 10.1.1.1 255255.255.0
Router(config-if)#exit
```

步骤 3：验证设备连通性

（1） 验证员工机器与服务器的网络连通性。

（2） 验证员工机能否登录 Web 和 FTP 服务器。

步骤 4: 在路由器上配置基于时间的访问控制列表（参考版本如下）

```
// 定义工作时间段
Router(config)#time-range work-time
// 这里的工作时间考虑实验方便自行调整
Router(config-time-range)#periodic weekdays 09:00 to 18:00
Router(config-time-range)#exit

Router(confia)#ip access-list extended accessctrl
// !只允许员工的主机在上班时间访问FTP服务器
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host 10.1.1.10 eq
ftp time-range work-time
Router(config-ext-nacl)#permit tcp 192.168.10.0 0.0.0.255 host 10.1.1.10 eq
ftp-data time-range work-time
// !不允许员工的主机在上班时间访问www服务器
***
// !允许员工的主机在非上班时间访问www服务器
***
```

Router(config-ext-nacl)#exit

步骤 5: 在路由器上端口上应用 ACL

Router(config)#interface gigabitethernet 0/0
Router(config-if)#ip access-group accessctrl in
Router(config-if)#end

步骤 6: 验证 ACL 的有效性

在使用基于时间的 ACL 时,要保证设备(路由器或交换机)的系统时间的准确性，因为设备是根据自己的系 统时间(而不是主机时间)判断当前时间是否在时间段范围内。可以在特权模式下使用 show clock 命令 查看当前系统时间,并使用 clock set 命令调整系统时间。通过调整设备的系统时间实现在不同时间段测 试 ACL 是否生效。

（1） 查看路由器的系统时间:使用show clock 命令判断当前时间段

（2） 在员工机器上，登录 FTP 服务器,并通过 http://10.1.1.10 访问 Web 服务器,在非工作时间内是否能登录和访问？工作时间内能否访问？登录 FTP 时分别通过 DOS 命令与浏览器方式，结合捕获进行报文分析

（3） 捕获主机访问服务器时的数据包，并进行分析。

重要配置、实验过程和实验结果请截图并完成相应实验报告。