**【实验名称】：ACL访问控制列表实验项目**

**学生姓名：苏家铭 合作学生：莫益萌**

**实验地点：济世楼330 实验时间：2023年11月8日**

**【实验目的】**

**包过滤机制是路由器基本处理机制,加入过滤规则,可以实施基本的网络安全控制。阻隔访问敏感网站和关键主机,均可以使用访问控制列表作为过滤规则实施。学习访问控制列表，不但可以了解基本网络安全知识,而且还可以提高路由器使用水平。本实验利用路由器的访问控制列表功能,使得特定的 IP 地址不能访问,实现网络安全管理务。**

**(1)了解路由器包过滤基本原理**

**(2)了解访问控制列表实施原理**

**(3)利用控制列表实施网络安全**

**【实验原理】**

**路由器包过滤机制是指路由器在转发 IP 数据包时,需要对每一个 IP 数据包头部进行分析,检查头部是否损坏并用于计算路由,为转发服务。**

**访问控制列表(Access Control Lists,ACL),是指路由器在包过滤时,以IP 数据包头部中的信息,诸如以源地址和目的地址等数据域作为规则条件,制订访问控制规则,只允许让满足条件的 IP 数据包通过,达到访问控制的目的,从而提高网络可管理性和安全性。在工程应用中,可以设置规则不允许访问某些网站,比如禁止访问一些不健康网站;也可以对自身网络中某段地址进行保护,比如保护网站服务器。典型的 Web 应用，一般有 Web 服务器和数据库两种服务器,Web 服务器必须让外界直接访问,但数据库服务器就不应让外部直接访问,避免遭受攻击。通过访问控制列表,可以允许外部网能访问 Web 服务器地址,但不允许访问数据库服务器地址。**

**【实验设备】**

**济事楼330机房电脑2台，两台路由器和一台交换机**

**【实验步骤】**

**(1)使用单根串行交叉线将两个路由器的串口对接起来;将路由器以太网端口和两台计算机网卡都用网线直接连接到交换机,由交换机招当网络连接:通过串行线将计算机串口 com同路由器 console 口连接起来两台计算机超级终端作为路由器管理的操作平台。为处理方便,所有子网掩码设置成 255.255.255.0。配置参数如下**

1. **路由器 A:以太网端口 g/0,IP 地址设置为 192,168.1.1,串口地址设置为 202,1681.1**
2. **路由器 B:以太网端口 g0/0,IP 地址设置为 192,168.2.1,串口地址设置为 202.168.1.2.**
3. **host1 承担测试任务,网卡地址设置在 192,168.10/24 网段,网卡地址将根据实验要求,在 192.168.1.15 和 192.168.1.17 之间进行切换,网关地址设置成 192.168.1.1。**
4. **host2 网卡地址设置为 192.168.2.254,网关地址设置成 192.168.2.1。**

**按照实验环境要求,完成实验拓扑结构连接，并打开相关设备电源。(2)测试 Host1 网卡使用 192.168.1.15 和192.168.117 地址是否都能连通 Host2.配置主机 Hostl 网卡地址。限于篇幅,请参考 14.1小节,主机网卡IP 地址设置如下:**

**Hostl;IP地址=192.168.1.15,子网掩码=255.255.255.0,网关=192.168.1.1团测试子网连通。**

**(3)RouterA 配置访问控制列表。在完成静态路由配置成功基础上修改，配置访问控制组及实施。注意不要同时为 RouterB配置访问控制列表。**

1. **进入配置模式。**
2. **进入特权模式;routerA>en,EnableSecret Password=cisco查看静态路由表,routerA>shiproute,核实静态路由已配置完毕进人配置模式:routerA#configt@建立访问控制组,访问控制策略是允许访问 192.168.1.1-192.168.115 地址段routerA(config)#access-list 1 permit 192.168.1.0 0.0.0.15查看访问控制组(可选):routerA#shaccess-list**
3. **设置以太网端口作为访问列表控制策略实施端口，允许外部进站访问,也可以采用串口作为实施点，但控制方向是出站:**

**进入以太网端口配置模式:routerA(config)#ing0/0实施访问控制策略:routerA(config)#ipaccess-grouplin退出配置模式，使配置生效:routerA(config-if)end**

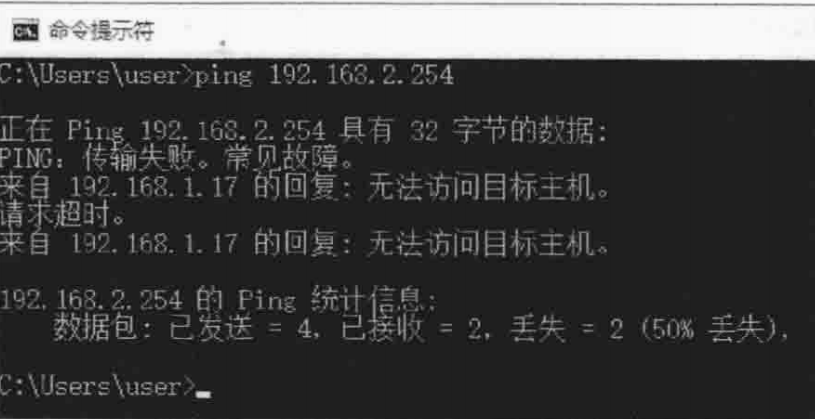
**(4)重新测试连通。**

**修改Host1的IP地址。Hostl;IP地址=192.168.1.17,子网掩码=255.255.255.0,网关=192.168.1.1。**

**重新测试，测试 Host1地址为197.158.1.17 时是否连通计算机2**

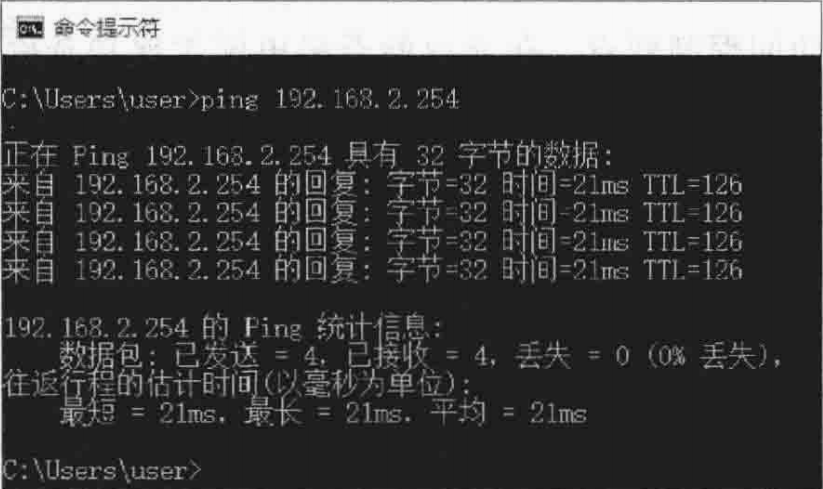
**【实验现象】**

**Host1打开命令窗口键入“ping 192.168.2.254”,不连通就表示访问控制表发生作用,192.168.1.17 地址没有得到允许访问,所以无法访问。**



**Host1地址改回192.168.115,并重新测试,可能需要重复几次**

**键入“ping 192.168.2.254”,连通就表示实验成功,表示控制列表访问组起作用,允许访问192.168.1.15 地址。**



**【分析讨论】**

**ACL（Access Control List）具有多种作用，主要用于管理资源的访问权限和确保系统的安全性。**

**1. 控制访问权限：ACL允许系统管理员或资源所有者定义谁可以访问特定资源以及以何种方式访问这些资源。这有助于限制对敏感信息和系统资源的访问。**

**2. 实施身份验证：ACL可以验证用户或实体的身份，以确保只有经过授权的用户或实体能够访问资源。**

**3. 精细化控制：ACL允许定义精确的权限，例如读、写、执行、删除等，以及控制这些权限的具体用户或用户组。**

**4. 保护机密信息：ACL可以用于保护敏感数据、文件或资源，确保只有授权的用户可以查看或修改这些信息。**

**5. 确保数据完整性：ACL可以用于控制谁有权对数据进行修改，从而保护数据的完整性，防止未经授权的更改。**

**6. 管理文件和文件夹权限：在文件系统中，ACL可用于控制文件和文件夹的权限，以确保只有特定用户或用户组能够访问、编辑或删除它们。**

**7. 支持多用户环境：在多用户环境中，ACL允许管理不同用户之间的访问权限，以维持系统的多样性和安全性。**

**8. 合规性和审计：ACL的使用可以有助于满足合规性要求，并提供审计跟踪功能，以跟踪资源的访问历史，以便在需要时进行审计和调查。**