**ACL实验**

**实验9-1 ACL实验**

**学习目标**

* 了解ACL协议原理。

**原理**

随着大规模开放式网络的开发，网络面临的威胁也就越来越多。网络安全问题成为网络管理员最为头疼的问题。一方面，为了业务的发展，必须允许对网络资源的开发访问，另一方面，又必须确保数据和资源的尽可能安全。网络安全采用的技术很多，而通过访问控制列表（ACL）可以对数据流进行过滤，是实现基本的网络安全手段之一。本章只研究基于IP的ACL。

ACL 概述

访问控制列表简称为ACL，它使用包过滤技术，在路由器上读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。ACL 分很多种，不同场合应用不同种类的ACL。

1. 标准ACL

标准ACL 最简单，是通过使用IP 包中的源IP 地址进行过滤，表号范围1-99；

2. 扩展ACL

扩展ACL 比标准ACL 具有更多的匹配项，功能更加强大和细化，可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP 连接建立等进行过滤，表号范围100-199；

3. 命名ACL

以列表名称代替列表编号来定义ACL，同样包括标准和扩展两种列表。

在访问控制列表的学习中，要特别注意以下两个术语。

1. 通配符掩码：一个32 比特位的数字字符串,它规定了当一个IP 地址与其他的IP 地址进行比较时，该IP 地址中哪些位应该被忽略。通配符掩码中的“1”表示忽略IP 地址中对应的位，而“0”则表示该位必须匹配。两种特殊的通配符掩码是“255.255.255.255”和“0.0.0.0”，前者等价于关键字“any”，而后者等价于关键字“host”；

2. Inbound 和outbound：当在接口上应用访问控制列表时，用户要指明访问控制列表是应用于流入数据还是流出数据。总之，ACL 的应用非常广泛，它可以实现如下的功能：

1. 拒绝或允许流入（或流出）的数据流通过特定的接口；

2. 为DDR 应用定义感兴趣的数据流；

3. 过滤路由更新的内容；

4. 控制对虚拟终端的访问；

5. 提供流量控制。

**拓扑图**



图1拓扑

**操作步骤**

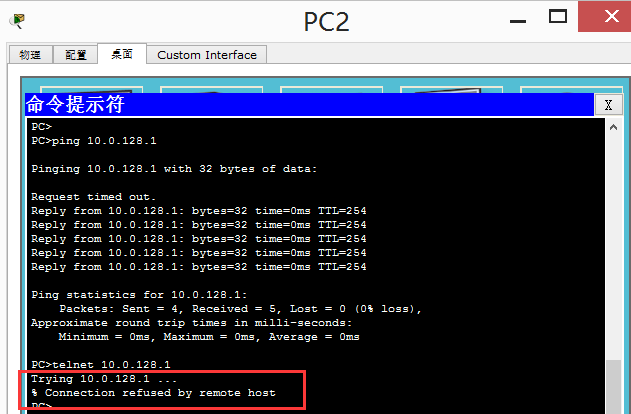
将《GRE实验》中保存的拓扑打开，要求校园网所有设备只允许图书馆所在网段进行telnet；服务器不允许宿舍终端访问。

1. 配置telnet安全防护
2. 在设备上设定ACL，并在line 0 4 中应用，以R1为例，其他设备配置相同。

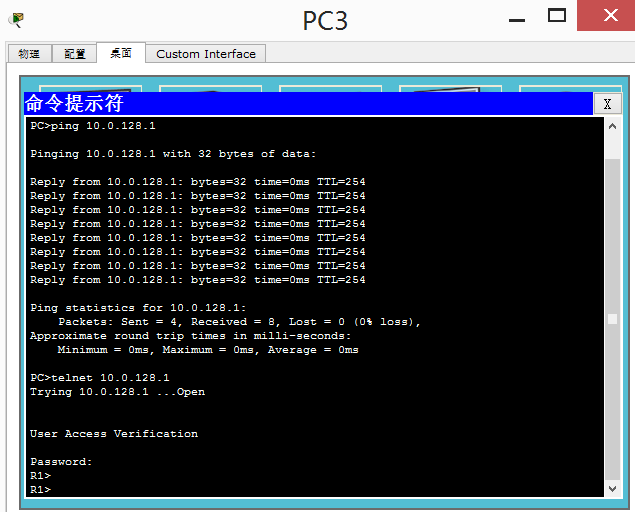
|  |
| --- |
| *R1>enable*  *R1#conf t*  *R1(config)#access-list 1 permit 10.0.2.0 0.0.0.255 //设置只允许图书馆网段*  *R1(config)#line vty 0 4*  *R1(config-line)#access-class 1 in //只允许acl1 允许地址telent本设备* |

1. 使用PC2 和PC3进行测试。

PC2所在网段不能telnet R1



PC3所在网段能telnet R1，符合项目要求。



1. 在SW1和SW2上部署ACL，实现不允许宿舍访问服务器。
2. 在SW1上部署ACL

|  |
| --- |
| *SW1(config)#access-list 10 deny 10.0.1.0 0.0.0.255 //设置ACL*  *SW1(config)#access-list 10 deny 10.0.3.0 0.0.0.255*  *SW1(config)#access-list 10 permit any*  *SW1(config)#interface vlan 101*  *SW1(config-if)#ip access-group 10 out*  *Sw1(config-router)#exit //调用ACL* |

1. 在SW1上查看ACL

|  |
| --- |
| *SW1#show ip access-lists*  *Standard IP access list 10*  *deny 10.0.1.0 0.0.0.255*  *deny 10.0.3.0 0.0.0.255*  *permit any* |

1. 在SW2上部署ACL

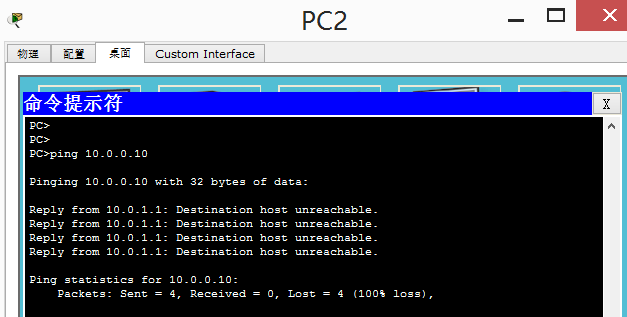
|  |
| --- |
| *SW2(config)#access-list 10 deny 10.0.1.0 0.0.0.255 //设置ACL*  *SW2(config)#access-list 10 deny 10.0.3.0 0.0.0.255*  *SW2(config)#access-list 10 permit any*  *SW2(config)#interface vlan 101*  *SW2(config-if)#ip access-group 10 out*  *Sw2(config-router)#exit //调用ACL* |

1. 在SW2上查看ACL

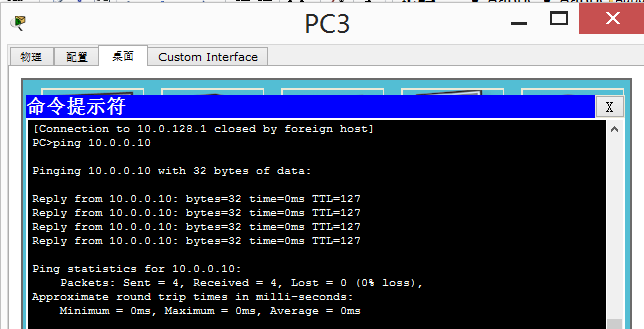
|  |
| --- |
| *SW2#show ip access-lists*  *Standard IP access list 10*  *deny 10.0.1.0 0.0.0.255*  *deny 10.0.3.0 0.0.0.255*  *permit any* |

1. 使用PC2和PC3进行测试

PC2不能访问服务器地址10.0.0.10，符合项目需求



PC3可以能访问服务器地址10.0.0.10，符合项目需求



1. 在SW1上查看ACL

|  |
| --- |
|  |

1. **保存配置**
2. 全网设备保存配置，防止掉电配置丢失。

参考配置：

*R1#wr //各设备特权模式下保存配置*

*Building configuration...*

*[OK]*

*R1#*

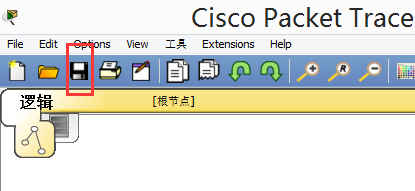
1. 查看全网设备配置保存是否成功，防止掉电配置丢失。

参考配置：

*R1#show startup-config //特权模式下查看保存的配置*

1. 保存拓扑。

单击“保存”，保存拓扑信息。



1. 以学号+名字+日期命名拓扑并保存，用U盘带走文件。

