访问控制列表简介

ACL（访问控制列表--AccessControlList）是一种路由器配置和控制网络访问的一种有力的工具。适用于所有的路由协议。

一、作用

1、控制路由器应该允许或拒绝数据包通过

2、监控流量

3、检查网络的安全性（自上向下），检查和过滤数据和限制不必要的路由更新，让网络资源节约成本

注：路由表属于控制层面，ACL 属于数据层面

二、两个动作、ACL 分类以及匹配规则

2.1、动作：

deny 拒绝

permit 允许

2.2、ACL 分类

1.标准 ACL1-99 仅仅匹配源 ip 地址，尽量靠近目标

2.扩展 ACL100-199 关注源 ip、目标 ip、协议号或端口号，尽量靠近源，ACL 不能拒绝自身产生的流量

2.3、匹配规则

从上往下依次匹配一旦匹配不再往下查询，末尾隐藏拒绝所有

三、ACL 写法（编号写法和命名写法）

3.1、标准 AC

①编号写法

```
R3(config)#access-list1deny192.168.1.20.0.0.0 拒绝 192.168.1.2 的流量

R3(config)#access-list1permitany 允许其它流量通过
```

切记:拒绝某个地址的流量一定写在前面,然后 permitany 才是正确的写法。

调用

```
R3(config)#interfacef0

1

R3(config-if)#ipaccess-group1out 在出的接口限制流量
```

②命名写法

```
R3(config)#ipaccess-liststandardxx

R3(config-std-nacl)#denyhost192.168.1.2

R3(config-std-nacl)#permitany
```

3.2、扩展 ACL

①编号写法

```
R1(config)#access-list100denyiphost192.168.1.2host192.168.2.2
```

```
R1(config)#access-list100permitipanyany
```

调用

```
R1(config)#interfacef0
0
R1(config-if)#ipaccess-group100in
```

②命名写法

```
R1(config)#ipaccess-listextendedccna
R1(config-ext-nacl)#denyiphost192.168.1.2host192.168.
2.2
R1(config-ext-nacl)#permitipanyany
```

ACL 是保证网络安全最重要的核心策略之一，配置 ACL 后，可以限制网络流量，允许特定设备访问，指定转发特定端口数据包等。ACL 既可以在路由器上配置，也可以在具有 ACL 功能的业务软件上进行配置。在实际生活中作用很大，需要我们熟练掌握和使用!