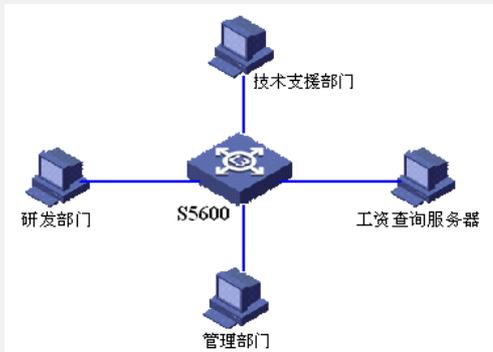


S5600系列交换机访问控制列表 (ACL) 的配置

1、组网图:



1. 公司企业网通过Switch的千兆端口实现各部门之间的互连。管理部门由GigabitEthernet1/0/1端口接入，技术支持部门由GigabitEthernet1/0/2端口接入，研发部门由GigabitEthernet1/0/3端口接入。
2. 工资查询服务器子网地址129.110.1.2，MAC为00e0-fc01-0303，技术支持部门IP为10.1.1.0/24，研发部门主机MAC为00e0-fc01-0101。

2、组网需求:

1. 要求正确配置ACL，限制研发部门在上班时间8:00至18:00访问工资查询服务器。
2. 通过基本访问控制列表，实现在每天8:00~18:00时间段内对源IP为10.1.1.1主机发出报文的过滤。
3. 通过二层访问控制列表，实现在每天8:00~18:00时间段内对源MAC为00e0-fc01-0101目的MAC为00e0-fc01-0303报文的过滤。

3、配置步骤:

1. 定义时间段

```
[Quidway] time-range huawei 8:00 to 18:00 working-day
```

2. 进入3000号的高级访问控制列表视图

```
[Quidway] acl number 3000
```

3. 定义访问规则

```
[Quidway-acl-adv-3000] rule 1 deny ip source any destination 129.110.1.2 0.0.0.0 time-range huawei
```

4. 进入GigabitEthernet1/0/1接口

```
[Quidway-acl-adv-3000] interface GigabitEthernet1/0/1
```

5. 在接口上用3000号ACL

```
[Quidway-GigabitEthernet1/0/1] packet-filter inbound ip-group 3000
```

6. 进入2000号的基本访问控制列表视图

```
[Quidway-GigabitEthernet1/0/1] acl number 2000
```

7. 定义访问规则

```
[Quidway-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range Huawei
```

8. 进入GigabitEthernet1/0/2接口

```
[Quidway-acl-basic-2000] interface GigabitEthernet1/0/2
```

9. 在接口上应用2000号ACL

```
[Quidway-GigabitEthernet1/0/2] packet-filter inbound ip-group 2000
```

10. 进入4000号的二层访问控制列表视图

```
[Quidway-GigabitEthernet1/0/2] acl number 4000
```

11. 定义访问规则

```
[Quidway-acl-ethernetframe-4000] rule 1 deny source 00e0-fc01-0101 ffff-ffff-ffff dest 00e0-fc01-0303 ffff-ffff-ffff time-range Huawei
```

12. 进入GigabitEthernet1/0/3接口

```
[Quidway-acl-ethernetframe-4000] interface GigabitEthernet1/0/3
```

13. 在接口上应用4000号ACL

```
[Quidway-GigabitEthernet1/0/3] packet-filter inbound link-group 4000
```

4、配置关键点:

1. time-name 可以自由定义。
2. 设置访问控制规则以后，一定要把规则应用到相应接口上。
3. S5600系列交换机只支持inbound方向的规则，所以要注意应用接口的选择。

