S5000PV3/5130/5150系列交换机允许指定范围内的主机互相访问配置方法（命令行版）

ACL Godiva612 2018-11-28 发表

组网及说明

1.1 适用产品系列

本案例适用于如S5024PV3-EI-HPWR、S5048PV3-EI、S5120V2-52P-LI、S5120V2-28P-SI、S5130-52S-EI、S5130S-28S-EI、S5150X-16ST-EI等S5000PV3、S5120V2、S5130、S5150系列的交换机。

1.2配置注意事项

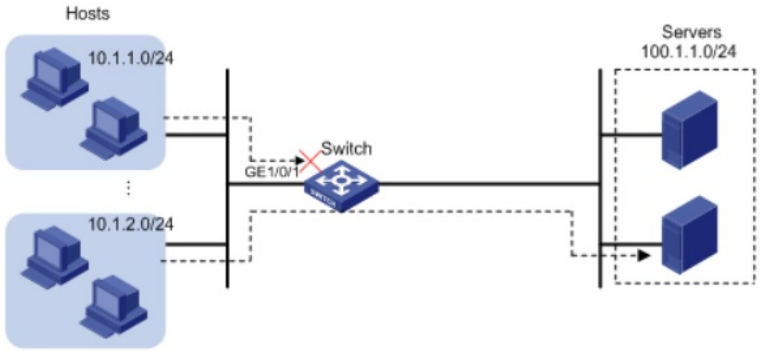
在ACL规则中，设备通过通配符掩码（如0.0.0.255）来确定要匹配的IP地址范围。例如要匹配源地址为1.1.0.0/16网段，规则中应输入source 1.1.0.0 0.0.255.255。

在配置时要特别注意ACL规则的配置顺序，如果先配置了拒绝所有IP报文通过的规则，则指定网段之间的IP报文也将被过滤，无法实现组网需求。

1.3配置需求及实现的效果

交换机的GigabitEthernet1/0/1端口下连接了两个网段的主机，要求通过配置ACL，仅允许10.1.2.0/24网段访问100.1.1.0/24网段的报文通过，而拒绝其它报文通过。

2 组网图



配置步骤

3.1配置acl，接口下下发过滤策略，调用acl

创建IPv4高级ACL 3000，配置两条规则，分别为允许源地址为10.1.2.0/24网段，目的地址为100.1.1.0/24网段的IP报文通过，以及拒绝其它IP报文通过。

```
<H3C> system-view
[H3C] acl number 3000
[H3C-acl-ipv4-adv-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination 100.1.1.0 0.0.0.255
[H3C-acl-ipv4-adv-3000] rule deny ip
[H3C-acl-ipv4-adv-3000] quit
```

说明：如果acl number 3000无法写上去的话可能是由于交换机的软件版本不同导致，此时修改为acl advanced 3000的写法就可以了。

配置包过滤功能，应用IPv4高级ACL 3000对端口GigabitEthernet1/0/1收到的IP报文进行过滤。

```
[H3C] interface gigabitethernet 1/0/1
[H3C-GigabitEthernet1/0/1] packet-filter 3000 inbound
```

3.2检查配置效果

执行display packet-filter命令查看包过滤功能的应用状态。

```
[H3C] display packet-filter interface GigabitEthernet 1/0/1
  Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 3000, Successful
```

上述信息显示GigabitEthernet1/0/1端口上已经正确应用了包过滤功能。

在10.1.2.0/24网段的主机上以100.1.1.0/24网段内的服务器为目的进行ping操作，返回正常应答信息；在其它网段的主机上执行此操作返回请求超时信息。

4保存配置信息

```
[H3C]save force
```

配置关键点