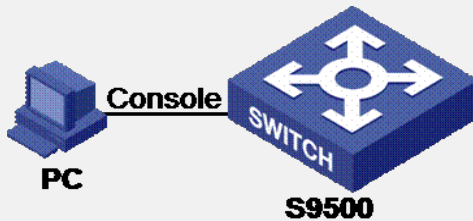


H3C S9500交换机防范TTL等于1的IP报文攻击的配置

一、组网需求:

配置当交换机收到TTL等于1的IP报文时，不向报文发送端发送“time exceeded”的ICMP报错报文，避免攻击者连续发送给交换机TTL等于1的IP报文时，交换机就会不停地向其发送“time exceeded”的ICMP报错报文，从而造成交换机CPU资源的耗损的情况出现。

二、组网图:



三、配置步骤:

软件版本: S9500交换机全系列软件版本

硬件版本: S9500交换机D类单板

配置当交换机收到TTL等于1的IP报文时，不向报文发送端发送“time exceeded”的ICMP报错报文

```
[S9500]ip icmp-time-exceed enable
```

四、配置关键点:

1. 非D类单板，可以通过配置ACL规则过滤TTL等于1的报文。需要注意的是，配置ACL规则对TTL等于1的报文进行过滤后，所有TTL等于1的报文都会被过滤，在使用时需要特别小心。一般情况下，建议在确认设备遭受攻击后通过该方法过滤攻击报文。