H3C 3600系列交换机采用自定义ACL实现ARP欺骗防攻击的配置

周宣余 2006-12-20 发表

H3C 3600采用自定义ACL实现ARP欺骗防攻击的配置

> 一　组网需求：
> 配置自定义ACL，通过匹配报文对应的协议号、MAC地址及IP地址等字段，过滤攻击主机发出的冒充网关的ARP报文。
> **二　组网图：**
> 略
> 三　配置步骤：
> 1．定义5000的ACL
> [Switch] acl number 5000
> 2．把arp Reply协议报文中Sender ip address为端口所在VLAN网关192.168.0.1的ARP报文过滤掉（16和32分别是协议字段和Sender ip address字段的偏移量）
> [Switch-acl-user-5000]rule 0 deny 0806 ffff 16 c0a80001 ffffffff 32
> 3．在除连接网关之外的所有端口下下发自定义ACL对入方向的ARP欺骗报文进行过滤
> [Switch]interface Ethernet 1/0/1
> [Switch-Ethernet1/0/1]packet-filter inbound user-group 5000
> 四　配置关键点：
> 1. 如果开启了QinQ功能后，不建议应用用户自定义acl。
> 2. 一定要除连接网关之外的所有端口下下发该ACL，否则没有下发ACL的端口将继续收到ARP欺骗报文，从而无法达到防欺骗的效果。
> 3. 对于H3C 5600 arp报文协议号（0806）、Sender IP的偏移量将分别为20、36。