S9500交换机支持哪些防攻击功能

孟维佳 2006-12-22 发表

随着互联网规模的扩大和互联网用户的增加，网络设备在运行中会受到攻击的可能性也在增大。S9500交换机针对一些典型的攻击方式，专门设计了一套防报文攻击的方案，可以防止IP、ARP、802.1x、未知组播等报文的攻击。

所谓IP报文攻击，是指S9500接收到过多的目的地址和VLAN接口地址在同一网段，且在交换机上没有相应的转发表项的IP报文，该类报文会上送CPU进行处理，占用大量CPU资源，严重时会影响正常数据业务的转发。所谓ARP报文攻击，是指S9500收到大量的源MAC地址相同或者相近的arp请求报文，影响正常的arp学习。所谓802。1x报文攻击，是指S9500收到大量的源MAC地址相同或者相近的802。1x认证报文，占用CPU资源。

系统默认IP防攻击启用，ARP和802.1x防攻击不启用。启用防攻击后，当IP、ARP和802.1x报文达到一定限度时，系统会自动限制这些报文，不让这些报文冲击CPU，对CPU起到保护作用，避免系统一直在处理这些攻击报文，而影响对正常业务的处理。

各种报文的防攻击可以根据用户和组网需要启动或者关闭，配置命令（系统视图下）如下：

IP报文防攻击启动：anti-attack ip enable

IP报文防攻击关闭：anti-attack ip disable

ARP报文防攻击启动：anti-attack arp enable

ARP报文防攻击关闭：anti-attack arp disable

802。1x报文防攻击启动：anti-attack dot1x enable

802。1x报文防攻击关闭：anti-attack dot1x disable

1278及以后版本还支持防TTL=1报文攻击

TTL=1报文防攻击启动：anti-attack ttl1 enable

TTL=1报文防攻击关闭：anti-attack ttl1 disable