S7500系列交换机是如何进行防攻击

曹皓 2006-12-24 发表

H3C S7500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，是指交换机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，是指交换机收到大量的源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，是指交换机收到大量的源MAC地址相同或者相近的802.1x认证报文，占用CPU资源。
H3C S7500的防攻击功能是缺省打开的。
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。
H3C S7500交换机可以防范的攻击报文包括以下类型：

802.1x broadcast 802.1x to cpu
arp broadcast arp to cpu
bpdu-tunnel bpdu tunnel to cpu
bridgemac bridge mac to cpu
dhcp broadcast dhcp to cpu
dip-miss dip miss to cpu(opcode=0x100)
dldp dldp cpu
gmrp gmrp to cpu
gvrp gvrp to cpu
igmp igmp multicast to cpu
ip-option-err ip option error to cpu(opcode=0x2000)
ipx ipx to cpu
isis isis to cpu
lacp lacp to cpu
ndp hgmp to cpu
ntp ntp to cpu
ospf-multicast ospf multicast to cpu
ospf-unicast ospf unicast to cpu
other-pkt other pkt to cpu
other-unicast other type unicast to cpu
pim-multicast pim multicast to cpu
pim-unicast pim unicast to cpu
rip-multicast rip multicast to cpu
rip-unicast rip unicast to cpu
stp stp to cpu
tcp tcp(dip is vlan interface ip) to cpu
unknown-multicast unknown multicast to cpu(opcode=0x800)
vrp-mac l3 interface mac to cpu(opcode=0x100)
vrrp vrrp multicast to cpu