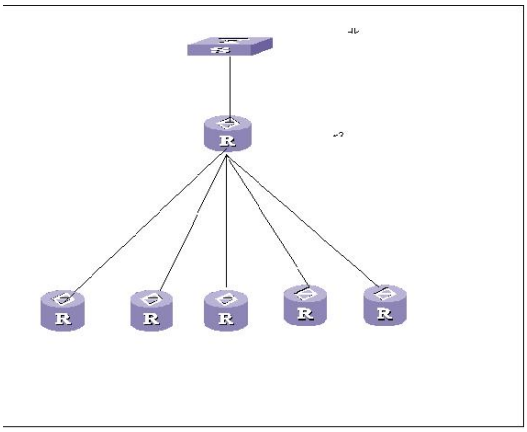
路由配置错误和病毒攻击引起R3680路由器转发性能问题

王雪梅 2006-02-15 发表

路由配置错误和病毒攻击引起R3680路由器转发性能问题

拓扑图如下：



3680路由器的版本很老。用户说丢包严重。

Sh run 未发现问题

Sh ver 居然是vrp 1.2(当时就有一个念头：先升一下)

Sh int 发现了一些问题：观察某些端口流量很大，以太网口达到60M。s9:1的流量大于2M且output queue 71/75/xxxxxx 输出对列丢弃了n多的包，且一直在上升。好多2m口输出对列都有丢弃的报文。怀疑有病毒造成拥塞。pings9:1挂的路由器丢包很严重，到此一直未出现死机。

在北电交换机上做端口镜像分析以太网口的数据报，内网未发现病毒报文。用户说他们的局网中有防病毒系统。那病毒有可能是来自其他地市。

考虑到路由器上流量很大，如果debug ip pa R3680肯定会直接down掉。这时可以配一些acl看一下匹配项可知是否有异常报文。试着ping几个下挂的路由器，没出现丢包。只有s9:1下挂的点丢包。Sh int s9:1时没看到过有链路层错误，怀疑路由有问题，sh ip rout后居然发现一条默认路由下一跳是s9:1下挂的路由器端口地址上。应该不是3680死机，是配置问题。

Sh ip ospf lsa ase 发现s9:1下挂的网络中居然有n个路由器配了默认路由且引入了ospf。

0.0.0.0 200.65.14.30 200.65.15.41 1186 36 8000019f 2 1
0.0.0.0 200.65.13.30 200.65.15.37 -1 36 80000232 2 1
0.0.0.0 200.65.11.30 200.65.15.29 2737 36 80000016 2 1
0.0.0.0 200.65.10.30 200.65.15.25 197 36 80000040 2 1
0.0.0.0 200.65.9.30 200.65.15.21 2710 36 8000004d 2 1
0.0.0.0 200.65.8.30 200.65.15.17 1437 36 8000004f 2 1
0.0.0.0 200.65.7.30 200.65.15.13 600 36 800000ec 2 1
0.0.0.0 200.65.6.30 200.65.15.9 485 36 800001a6 2 1
0.0.0.0 200.65.4.30 200.65.15.1 784 36 800006cb 2 1
0.0.0.0 200.65.14.20 200.65.14.30 1190 36 8000018f 2 20
0.0.0.0 200.65.10.20 200.65.10.30 137 36 80000038 2 20
0.0.0.0 200.65.9.11 200.65.9.30 -1 36 80000040 2 20
0.0.0.0 218.11.140.1 200.65.1.200 1017 36 80000036 2 20

让用户找相关单位解决配置问题。然后在3680上配了一系列的acl下发到所有端口，边下发系统边报出：!! System maybe under attack.

In one minute, there are 604978 InBound packets filtered, and 487835 are rejected by access-list, 0 rejected defaultly!

居然有80%的报文被滤掉了。

Sh acl 可看到 135 445端口 被匹配了n次。

101 deny tcp any any eq 135 (1576667 matches, 76468180 bytes -- rule 1)
101 deny tcp any any eq 445 (16597245 matches, 812969402 bytes -- rule 6)

总结这次故障就是：病毒+错误路由