网管心得：网络丢包究竟为何如何解决？ PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/0/2021_2022__E7_BD_91_E7_AE_A1_E5_BF_83_E5_c99_211.htm 网络丢包是我们在使用ping对目站进行询问时，数据包由于各种原因在信道中丢失的现象。ping使用了ICMP回送请求与回送回答报文。ICMP回送请求报文是主机或路由器向一个特定的目的主机发出的询问，收到此报文的机器必须给源主机发送ICMP回送回答报文。这种询问报文用来测试目的站是否可到达以及了解其状态。需要指出的是，ping是直接使用网络层ICMP的一个例子，它没有通过运输层的UDP或TCP。 网络丢包的原因主要有物理线路故障、设备故障、病毒攻击、路由信息错误等，下面我们结合具体情况进行说明。 物理线路故障 网管员发现广域网线路时通时断，发生这种情况时，有可能是线路出现故障，也可能是用户方面的原因。为了分清是否是线路故障，可以做如下测试。 如果广域网线路是通过路由器实现的，可以登录到路由器，通过扩展ping向对端路由器广域网接口发送大量的数据包进行测试。 如果线路是通过三层交换机实现，可在线路两端分别接一台计算机，并将IP地址分别设为本端三层路由交换机的广域网接口地址，使用“ ping 对端计算机地址 -t ”命令进行测试。 如果上述测试没有发生丢包现象，则说明线路运营商提供的线路是好的，引起故障的原因在于用户自身，需要进一步查找。 如果上述测试发生丢包现象，则说明故障是由线路供应商提供的线路引起的，需要与线路供应商联系尽快解决问题。 由物理线路引起的丢包现象还有很多，如光纤连接问题，跳线没有对准设备接口，双绞线

及RJ-45接头有问题等。另外，通信线路受到随机噪声或者突发噪声造成的数据报错误，射频信号的干扰和信号的衰减等都可能造成数据包的丢失。我们可以借助网络测试仪来检查线路的质量。 设备故障 设备故障主要是指设备硬件方面的故障，不包含软件配置不当造成的丢包。如网卡是坏的，交换机的某个端口出现了物理故障，光纤收发器的电端口与网络设备接口，或两端设备接口的双工模式不匹配。 笔者近日在工作中发现一交换机端口的光纤模块故障造成的丢包现象，该交换机在通信一段时间后死机，即不能通信，重启后恢复正常。在经过一段时间观察后发现，某光纤模块存在问题，取一块新的模块替换，一切正常。究其原因，交换机会对所有接收到的数据包进行CRC错误检测和长度校验，将检查出有错误的包丢弃，正确的包转发出去。但这个过程中有些有错误的包在CRC错误检测和长度校验中都均未检测出错误，这样的包在转发过程中不会被发送出去，也不会被丢弃，它们将会堆积在动态缓存中，永远无法发送出去，等到缓存中堆积满了，就会造成交换机死机的现象。最终结果是，数据包无法到达目的主机。 网络拥塞 网络拥塞造成丢包率上升的原因很多，主要是路由器资源被大量占用造成的。 如果发现网速慢，并且丢包率呈现上升的情况，这时应该show process cpu和show process mem，一般情况下发现IP input process占用过多的资源。接下来可以检查fast switching在大流量外出端口是否被禁用，如果是，则需要重新使用。 再看一下Fast switching on the same interface是否被禁用，如一个接口配有多个网段并且这些网段间流量很大时，路由器工作在process-switches方式，这种情况下要在接口上执行命令

“ enable ip route-cache same-interface ”。 接下来，用show interfaces和show interfaces switching命令识别大量包进出的端口。一旦确认进入端口后，打开IP accounting on the outgoing interface看其特征，如果是攻击，源地址会不断变化但是目的地址不变，可以用命令“ access list ”暂时解决此类问题(最好在接近攻击源的设备上配置)，最终解决办法是停止攻击源。应用中遇到的造成网络拥塞的情况还有很多，如大量的UDP流量，可以用解决spoof attack的步骤解决此问题。大量的组播流、广播包穿越路由器，路由器配置了IP NAT并且有很多DNS包穿越路由器等。上述情况造成网络拥塞后，通信双方采取流量控制，丢弃不能传输的包。 路由错误 网络路径错误也会导致数据包不能到达目的主机，如主机的默认路由配置错误，主机发出的访问其他网络的数据包会被网关丢弃。但此类丢包属于正常情况下的丢包，是意料之中的，不会对网络造成影响。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com