网络中检测共享（NAT）的原理分析 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022__E7_BD_91_E7_BB_9C_E4_B8_AD_E6_c101_142684.htm 网络尖兵原来采用的检测技术主要是：1、检查从下级IP出来的IP包的IP-ID是否是连续的，如果不是连续的，则判定下级使用了nat. 2、检查从下级IP出来的IP包的ttl值是否是32、64、128这几个值，如果不是，刚判定下级使用了nat. 3、检查从下级IP出来的http请求包中是否包含有proxy的字段，如果有，则下级用了http代理。 由于检测和防检查技术的对抗升级，现在可能增加了检测的内容：一、通过行为统计：1. 在三秒内同一IP以上的站行Request，此IP透NAT行。" 2. 在秒，若同一IP同一站，行次以上的Request，此IP透NAT行。二、深度检测数据包内容：1.检测并发连接数量来源：www.examda.com 2.检测下级IP出来的QQ号码数量，如果同时有5个QQ号，则判定为共享。3.更多的检测方法 Detecting NAT Routers Thursday, April 24 2003 @ 08：35 AM CDT Contributed by： opticfiber A great paper written by Peter Phaal explains the simple method used in his companies product, Sflow, to detect multiple host behind a NAT firewall. The secret, it would seem is simply monitoring of the TTL of out going packets and comparing them to a host know not to be using a NAT firewall. Another method only touched upon by Phaal is passive OS finger printing, although this method is less reliable, an statistical analasys could determine if multiple operating systems were using the same network network device. If this were the case it would be reasonable to assume that that host was in fact a NAT device. ATamp.T uses, relies on the fact that most operating systems （excluding Linux and Free BSD） use IP header IDs as simple counters. By observing out of sequence header IDs, an analasys can calculate how many actual hosts are behind a NAT device./ Each of these methods can be easily defeated through better sterilization by the router itself. In the first example, if the TTL for each TCP packet was re-written by the router for each packet to the value of 128, the first method would no longer function. For the second method, sterilizing IP header information and stripping unneeded TCP flags would successfully undermine this scheme. For the last Method, counting hosts behind a router. Striping the fragmentation flag for syn packets, and setting the IP ID to 0, （like Linux and Free BSD both do） would make it impossible to count hosts behind a NAT router. P