Linux下网络分析例解 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/252/2021_2022_Linux_E4_B8_8B_E7_BD_c103_252908.htm Linux作为网络服务器，特别是作为路由器和网关时，数据的采集和分析是必不可少的。所以，今天我们就来看看Linux中强大的网络数据采集分析工具——TcpDump。 顾名思义，TcpDump可以将网络中传送的数据包的“ 头 ”完全截获下来提供分析。它支持针对网络层、协议、主机、网络或端口的过滤，并提供and、or、not等逻辑语句来帮助你去掉无用的信息。 和Linux终端状态下的其他软件一样，TcpDump也是依靠参数来工作，本文将结合实例来说明。 数据过滤 不带任何参数的TcpDump将搜索系统中所有的网络接口，并显示它截获的所有数据，这些数据对我们不一定全都需要，而且数据太多不利于分析。所以，我们应当先想好需要哪些数据，TcpDump提供以下参数供我们选择数据： -b 在数据-链路层上选择协议，包括ip、arp、rarp、ipx都是这一层的。 例如：tcpdump -b arp 将只显示网络中的arp即地址转换协议信息。 -i 选择过滤的网络接口，如果是作为路由器至少有两个网络接口，通过这个选项，就可以只过滤指定的接口上通过的数据。例如： tcpdump -i eth0 只显示通过eth0接口上的所有报头。 src、dst、port、host、net、ether、gateway这几个选项又分别包含src、dst 、port、host、net、ehost等附加选项。他们用来分辨数据包的来源和去向，src host 192.168.0.1指定源主机IP地址是192.168.0.1，dst net 192.168.0.0/24指定目标是网络192.168.0.0。以此类推，host是与其指定主机相关无论它是源还是目的，net是与其指定网络

相关的，ether后面跟的不是IP地址而是物理地址，而gateway则用于网关主机。可能有点复杂，看下面例子就知道了：tcpdump src host 192.168.0.1 and dst net 192.168.0.0/24 过滤的是源主机为192.168.0.1与目的网络为192.168.0.0的报头。 tcpdump ether src 00:50:04:BA:9B and dst…… 过滤源主机物理地址为XXX的报头（为什么ether src后面没有host或者net？物理地址当然不可能有网络喽）。 Tcpdump src host 192.168.0.1 and dst port not telnet 过滤源主机192.168.0.1和目的端口不是telnet的报头。 ip icmp arp rarp 和 tcp、udp、icmp这些选项等都要放到第一个参数的位置，用来过滤数据报的类型。例如： tcpdump ip src …… 只过滤数据-链路层上的IP报头。 tcpdump udp and src host 192.168.0.1 只过滤源主机192.168.0.1的所有udp报头。 数据显示/输入输出 TcpDump提供了足够的参数来让我们选择如何处理得到的数据，如下所示： -l 可以将数据重定向。如tcpdump -l ＞tcpcap.txt将得到的数据存入tcpcap.txt文件中。 -n 不进行IP地址到主机名的转换。 如果不使用这一项，当系统中存在某一主机的主机名时，TcpDump会把IP地址转换为主机名显示，就像这样：eth0 ＜ ntc9.1165＞ router.domain.net.telnet，使用-n后变成了：eth0 ＜ 192.168.0.9.1165 ＞ 192.168.0.1.telnet。 -nn 不进行端口名称的转换。 上面这条信息使用-nn后就变成了：eth0 ＜ ntc9.1165 ＞ router.domain.net.23。 -N 不打印出默认的域名。 还是这条信息-N 后就是：eth0 ＜ ntc9.1165 ＞ router.telnet。 -O 不进行匹配代码的优化。 -t 不打印UNIX时间戳，也就是不显示时间。 -tt 打印原始的、未格式化过的时间。 -v 详细的输出，也就比普通的多了个TTL和服务类型。 100Test 下载频道开通，各类