TCPDUMP入门Linux下的网络协议分析工具 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/240/2021_2022_TCPDUMP_E5_85_A5_c103_240656.htm TCPDUMP简介 在传统的网络分析和测试技术中，嗅探器(sniffer)是最常见，也是最重要的技术之一。sniffer工具首先是为网络管理员和网络程序员进行网络分析而设计的。对于网络管理人员来说，使用嗅探器可以随时掌握网络的实际情况，在网络性能急剧下降的时候，可以通过sniffer工具来分析原因，找出造成网络阻塞的来源。对于网络程序员来说,通过sniffer工具来调试程序。 用过windows平台上的sniffer工具(例如，netxray和sniffer pro软件)的朋友可能都知道，在共享式的局域网中，采用sniffer工具简直可以对网络中的所有流量一览无余！Sniffer工具实际上就是一个网络上的抓包工具，同时还可以对抓到的包进行分析。由于在共享式的网络中，信息包是会广播到网络中所有主机的网络接口，只不过在没有使用sniffer工具之前，主机的网络设备会判断该信息包是否应该接收，这样它就会抛弃不应该接收的信息包，sniffer工具却使主机的网络设备接收所有到达的信息包，这样就达到了网络监听的效果。 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。 用简单的话来定义tcpdump，就是：dump the traffice on a network，根据使用者的定义对网络上的数据包进行截获的包分析工具。 作为互联网上经典的的系统管理员必备工具，tcpdump以其强大的功能，灵活的截取策略，成为每个高级的系统管理员分析网络，排查问题等所必备的东东

之一。 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。 tcpdump提供了源代码，公开了接口，因此具备很强的可扩展性，对于网络维护和入侵者都是非常有用的工具。tcpdump存在于基本的FreeBSD系统中，由于它需要将网络界面设置为混杂模式，普通用户不能正常执行，但具备root权限的用户可以直接执行它来获取网络上的信息。因此系统中存在网络分析工具主要不是对本机安全的威胁，而是对网络上的其他计算机的安全存在威胁。 普通情况下，直接启动tcpdump将监视第一个网络界面上所有流过的数据包。 ―――――――――――――――――――――――――――― bash-2.02# tcpdump tcpdump: listening on eth0 11:58:47.873028 202.102.245.40.netbios-ns > 202.102.245.127.netbios-ns: udp 50 11:58:47.974331 0:10:7b:8:3a:56 > 1:80:c2:0:0:0 802.1d ui/C len=43 0000 0000 0080 0000 1007 cf08 0900 0000 0e80 0000 902b 4695 0980 8701 0014 0002 000f 0000 902b 4695 0008 00 11:58:48.373134 0:0:e8:5b:6d:85 > Broadcast sap e0 ui/C len=97 ffff 0060 0004 ffff ffff ffff ffff ffff 0452 ffff ffff 0000 e85b 6d85 4008 0002 0640 4d41 5354 4552 5f57 4542 0000 0000 0000 00 ^C ――――――――――――――――――――――――――――― 首先我们注意一下，从上面的输出结果上可以看出来，基本上tcpdump总的的输出格式为：系统时间 来源主机.端口 > 目标主机.端口 数据包参数 