从入门到精通：网络监听技术全解 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/269/2021_2022__E4_BB_8E_E5_85_A5_E9_97_A8_E5_c67_269710.htm 网络监听，在网络安全上一直是一个比较敏感的话题，作为一种发展比较成熟的技术，监听在协助网络管理员监测网络传输数据，排除网络故障等方面具有不可替代的作用，因而一直倍受网络管理员的青睐。然而，在另一方面网络监听也给以太网安全带来了极大的隐患，许多的网络入侵往往都伴随着以太网内网络监听行为，从而造成口令失窃，敏感数据被截获等等连锁性安全事件。 网络监听在安全领域引起人们普遍注意是在94年开始的，在那一年2月间，相继发生了几次大的安全事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令。上述事件可能是互联网上最早期的大规模的网络监听事件了，它使早期网络监听从"地下"走向了公开，并迅速的在大众中普及开来。 关于网络监听常常会有一些有意思的问题，如："我现在有连在网上的计算机了，我也有了窃听的软件了，那么我能不能窃听到微软(或者美国国防部，新浪网等等)的密码？ 又如：我是公司的局域网管理员，我知道hub很不安全，使用hub这种网络结构将公司的计算计互连起来，会使网络监听变得非常容易，那么我们就换掉hub，使用交换机，不就能解决口令失窃这种安全问题了么？ 这是两个很有意思的问题，我们在这里先不做回答，相信读者看完全文后会有自己正确的答案。 基本概念：认清mac地址和ip地址 首先，我们知道，一台接在以太网内的计算机

为了和其他主机进行通讯，在硬件上是需要网卡，在软件上是需要网卡驱动程序的。而每块网卡在出厂时都有一个唯一的不与世界上任何一块网卡重复的硬件地址，称为mac地址。同时，当网络中两台主机在实现tcp/ip通讯时，网卡还必须绑定一个唯一的ip地址。下面用一个常见的unix命令ifconfig来看一看作者本人的一台正常工作的机器的网卡
：[yiming@server/root]# ifconfig -ahme0: flags=863 mtu 1500inet 192.168.1.35 netmask ffffffe0ether 8:0:20:c8:fe:15 从这个命令的输出中我们可以看到上面讲到的这些概念，如第二行
的192.168.1.35是ip 地址，第三行的8：0：20：c8：fe：15是mac地址。请注意第一行的BROADCAST，MULTICAST，这是什么意思？一般而言，网卡有几种接收数据帧的状态，如unicast，broadcast，multicast，promiscuous等，unicast是指网卡在工作时接收目的地址是本机硬件地址的数据帧
。Broadcast是指接收所有类型为广播报文的数据帧。Multicast是指接收特定的组播报文。Promiscuous 则是通常说的混杂模式，是指对报文中的目的硬件地址不加任何检查，全部接收的工作模式。对照这几个概念，看看上面的命令输出，我们可以看到，正常的网卡应该只是接收发往自身的数据报文，广播和组播报文，请大家记住这个概念。 对网络使用者来说，浏览网页，收发邮件等都是很平常，很简便的工作，其实在后台这些工作是依靠tcp/ip协议族实现的，大家知道有两个主要的网络体系：OSI参考模型和TCP/IP参考模型，OSI模型即为通常说的7层协议，它由下向上分别为物理层、数据链路层、网络层、传输层、会话层、表示层、应用层，而tcp/ip模型中去掉了会话层和表示层后，由剩下的5层构成了互联网的

基础，在网络的后台默默的工作着。 下面我们不妨从tcp/ip模型的角度来看数据包在局域网内发送的过程：当数据由应用层自上而下的传递时，在网络层形成ip数据报，再向下到达数据链路层，由数据链路层将ip数据报分割为数据帧，增加以太网包头，再向下一层发送。需要注意的是，以太网的包头中包含着本机和目标设备的mac地址，也即，链路层的数据帧发送时，是依靠48bits的以太网地址而非ip地址来确认的，以太网的网卡设备驱动程序不会关心ip数据报中的目的ip地址，它所需要的仅仅是mac地址。 目标ip的mac地址又是如何获得的呢？发端主机会向以太网上的每个主机发送一份包含目的地的ip地址的以太网数据帧(称为arp数据包)，并期望目的主机回复，从而得到目的主机对应的mac地址，并将这个mac地址存入自己的一个arp缓存内。 当局域网内的主机都通过HUB等方式连接时，一般都称为共享式的连接，这种共享式的连接有一个很明显的特点：就是HUB会将接收到的所有数据向 HUB上的每个端口转发，也就是说当主机根据mac地址进行数据包发送时，尽管发送端主机告知了目标主机的地址，但这并不意味着在一个网络内的其他主机听不到发送端和接收端之间的通讯，只是在正常状况下其他主机会忽略这些通讯报文而已！如果这些主机不愿意忽略这些报文，网卡被设置为promiscuous 状态的话，那么，对于这台主机的网络接口而言，任何在这个局域网内传输的信息都是可以被听到的。 