局域网实现监听的基本原理 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E5_B1_80_E5_9F_9F_E7_BD_91_E5_c101_251007.htm 对于目前很流行的以太网协议，其工作方式是：将要发送的数据包发往连接在一起的所有主机，包中包含着应该接收数据包主机的正确地址，只有与数据包中目标地址一致的那台主机才能接收。但是，当主机工作监听模式下，无论数据包中的目标地址是什么，主机都将接收（当然只能监听经过自己网络接口的那些包）。 在因特网上有很多使用以太网协议的局域网，许多主机通过电缆、集线器连在一起。当同一网络中的两台主机通信的时候，源主机将写有目的的主机地址的数据包直接发向目的主机。但这种数据包不能在IP层直接发送，必须从TCP/IP协议的IP层交给网络接口，也就是数据链路层，而网络接口是不会识别IP地址的，因此在网络接口数据包又增加了一部分以太帧头的信息。在帧头中有两个域，分别为只有网络接口才能识别的源主机和目的主机的物理地址，这是一个与IP地址相对应的48位的地址。 传输数据时，包含物理地址的帧从网络接口（网卡）发送到物理的线路上，如果局域网是由一条粗缆或细缆连接而成，则数字信号在电缆上传输，能够到达线路上的每一台主机。当使用集线器时，由集线器再发向连接在集线器上的每一条线路，数字信号也能到达连接在集线器上的每一台主机。当数字信号到达一台主机的网络接口时，正常情况下，网络接口读入数据帧，进行检查，如果数据帧中携带的物理地址是自己的或者是广播地址，则将数据帧交给上层协议软件，也就是IP层软件，否则就将这个帧

丢弃。对于每一个到达网络接口的数据帧，都要进行这个过程。 然而，当主机工作在监听模式下，所有的数据帧都将被交给上层协议软件处理。而且，当连接在同一条电缆或集线器上的主机被逻辑地分为几个子网时，如果一台主机处于监听模式下，它还能接收到发向与自己不在同一子网（使用了不同的掩码、IP地址和网关）的主机的数据包。也就是说，在同一条物理信道上传输的所有信息都可以被接收到。另外，现在网络中使用的大部分协议都是很早设计的，许多协议的实现都是基于一种非常友好的、通信的双方充分信任的基础之上，许多信息以明文发送。因此，如果用户的账户名和口令等信息也以明文的方式在网上传输，而此时一个黑客或网络攻击者正在进行网络监听，只要具有初步的网络和TCP/IP协议知识，便能轻易地从监听到的信息中提取出感兴趣的部分。同理，正确的使用网络监听技术也可以发现入侵并对入侵者进行追踪定位，在对网络犯罪进行侦查取证时获取有关犯罪行为的重要信息，成为打击网络犯罪的有力手段。 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