1.1.2 数据包嗅探器工作过程

数据包嗅探过程中涉及软件和硬件之间的协作。这个过程可以分为成个步骤。

第一步：**收集**，数据包嗅探器从网络线缆上收集原始二进制数据。通情况下，通过将选定的网卡设置成混杂模式来完成抓包。在这种模式下，卡将抓取一个网段上的所有网络通信流量，而不仅是发往它的数据包。

第二步：**转换**，将捕获的二进制数据转换成可读形式。高级的命令行据包嗅探器就支持到这一步骤。到这一步，网络上的数据包将以一种非常础的解析方式进行显示，而将大部分的分析工作留给最终用户。

第三步（最后一步）：**分析**，对捕获和转换后的数据进行真正的深入析。数据包嗅探器以捕获的网络数据作为输入，识别并验证它们的协议，后开始分析每个协议的特定属性。