分析网络中传输数据包的最佳方式很大程度上取决于你手头拥有什么设备。在网络技术发展的早期阶段（使用 HUB 或集线器的共享网络时代），答案很简单，只须将线路插在一台集线器上，一切就搞定了——那就是使用协议分析仪。

协议分析仪就是能够捕获网络报文的设备。协议分析仪的正当用处在于扑捉分析网络的流量,以便找出所关心的网络中潜在的问题。例如,假设网络的某一段运行得不是很好,报文的发送比较慢,而我们又不知道问题出在什么地方,此时就可以用协议分析仪来作出精确的问题判断。

协议分析仪在功能和设计方面有很多不同。有些只能分析一种协议，而另一些能够分析几百种协议。一般情况下，大多数的嗅探器至少能够分析下面的协议：

以太网

TCP/IP

IPX

DECNet

其它……

协议分析仪通常是软硬件的结合，通常使用专用硬件或设置为专用方式的网卡实施对网络中的数据扑捉。捕获在网络中传输的数据信息方法称为 sniffing（嗅探）。

以太网协议是在同一回路向所有主机发送数据包信息。数据包头包含有目标主机的正确地址。一般情况下只有具有该地址的主机会接受这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方式通常称为“混杂”模式(P 模式)。这是协议分析仪扑捉数据的基础，它的产生是由共享网络的方式而来的。

对于今天的以太网交换机，答案开始变成“视情况而定”。根据设计，大多数交换机不允许用户查看从服务器到工作站的流量状况（用户正在使用的那台工作站除外）。事实上，这种情况通过端口映射技术可能解决。具体来讲，就是将传送到交换机上某个端口的传输流复制到另一个端口。但需要注意的是，目前的交换机又分为可管理的交换机和不可管理的交换机，不可管理的交换机价格比可管理的交换机要便宜，但通常缺少进行端口映射的能力。有些交换机虽然自称是可管理的，但实际上可能不过是支持 SNMP，也许仍不具有端口映射功能。在用户为网络购买新交换机时，这是一个需要搞清楚的重要问题。

如果用户的交换机不支持端口映射，也有方法来解决。这些方法对于在交换环境下的协议分析工作来说更加常用：

廉价和方便的方法：可以在被测试的工作站与网络之间安装一台集线器。将协议分析仪连接到这台集线器上，观察两个方向的传输流。昂贵和专业的方法：使用专业的以太网测试接口盒（TAP）联机安装在被测网络上，

无需在使用的分析仪内执行额外的过滤就可查看一个方向的会话情况。这意味着用户不能同时看到全部的会话，因此也许需要进行一些额外的数据包捕获，来掌握全部情况。

协议分析仪原本是网络工程师的常用工具，不过被人利用来做其他的目的也是非常常见的。现今的黑客们都熟练地使用着功能强大的协议分析仪，这本来就是一个工具的两面性。

对于能使用协议分析仪的人员来说，本身他的权利就是很大的，如果他用这东西来干些什么，很难阻止的。这个工具用在安全角度，即有用又有害。就象刀子一样，看它拿在谁的手中了。……

以上内容整理自《安恒网络维护论坛》

编辑本段原理

协议分析仪 protocol analyser 的工作从原理上要分为两个部分：数据采集数据扑捉、协议分析。对这两部分的工作从实现的形式上来说有以下常见的几种形式：

纯软件的协议分析系统，如：Fluke 的 OptiView-PE。大多数的纯软件协议分析仪是可以使用普通的网卡来完成进行简单的数据采集工作的，这就是使用率最多的协议分析软件+PC 网卡。这种方式的协议分析仪通常有两种原因存在的。①简单廉价的软件，或自由软件，小巧实用，功能较弱②运行在 PC 或报价本电脑上的协议分析仪的软件部分，本来协议分析工作就是基于软件分析的工作。所以再高端的协议分析仪其软件部分也是要由计算机平台实现的。 基于笔记本+数据采集箱的便携式协议分析仪这种方式与上述采用协议分析软件+PC 网卡的主要区别就是专用的数据采集系统，在对复杂和高速的网络链路上要想全线速地扑捉或更有效地进行实时数据过滤采用专用的数据采集方式是必须的。 手持式综合协议分析仪从协议分析仪发展的角度来说，网络维护人员越来越需要使用功能强大并能将多种网络测试手段集于一身的综合式测试分析手段，典型的协议分析仪上的功能延展就是加入网管功能、自动网络信息搜集功能、智能的专家故障诊断功能， 并且移动性能要有效。这种综合的协议分析仪或者说是综合的网络分析仪成为了当今网络维护和测试仪的主要发展趋势，象 Fluke 的 OptiView INA 自上市来在网络现场分析、故障诊断、网络维护方法得到了相当广泛的应用和发展。分布式协议分析仪随着网络维护规模的加大，网络技术的变化，网络关键数据的采集也越来越困难。有时为了分析和采集数据，必须能在异地同时第进行采集，于是将协议分析仪的数据采集系统独立开来，能安置在网络的不同地方，由能控制多个采集器的协议分析仪平台进行管理和数据处理，这种应用模式就诞生了分布式协议分析仪。通常这种方式的造价会非常高的。