拿什么来分析网络故障以及诊断网络性能[2] PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/256/2021_2022__E6_8B_BF_E4_BB_80_E4_B9_88_E6_c67_256493.htm 传统的基于SNMP的通用网管软件仅能对网络的整体流量进行监控，而无法对具体协议种类和应用流量组成进行进一步分析，它无法回答当前网络流量分别由哪些应用（协议）组成、各占多大的比例，哪些用户的访问数据量最大，分别使用什么协议，数据源和目的地是什么等问题。而基于基于网络探针（Probe）的分析方法中，“ 探针 ”和软件之间的接口一般是私有接口，第三方软件无法使用，所以此种软硬件结合的方案价格昂贵，部署不是很方便。 基于Flow的分析方法中，网络流（network flow）通常被定义为给定源节点和目的节点之间传输的单向数据包/帧序列。通常，网络设备（3层交换机、路由器等）本身提供了基于IP包头的分析功能，负责网络流数据的分析和整理，按照一定的条件和定义良好的数据格式向流采集器（Flow Collector）输出数据，然后再有相关的软件将采集到的流数据进行整理、分析和客户端展现。这种方法具有价格低廉、部署和配置方便的特点，可适应长期的、大流量环境下的数据采集和分析。最近，IETF的技术人员正在制订IPFIX（IP Flow Information Export）规范，使得网络中流量统计信息的格式趋于标准化。IPFIX基于Cisco的NetFlow V9设计，是一种针对数据输出的、基于模板的格式，具有很强的可扩展性。 NetFlow何处用武？ 基于NetFlow的应用系统，根据其侧重点不同，可以分成多种类型的应用： 网络流量分析及容量规划 基于NetFLow的应用系统可以根据NetFlow记录的源/目

的IP地址、源/目的端口、L3协议类型、Flow开始/结束时间、包数、字节数等字段，进行综合的静态和动态分析，获取大量的有用信息，如网络在某一时间段内的具体协议、流量大小分布，TopN的流量用户排行、TopN的应用排行，用户之间的详细通信会话，各种应用的流量随时间的变化趋势等等。 经过长时间的数据采集，可以了解整体网络流量和重要应用带宽的占用状况及其变化趋势，用户的使用模式等信息，为今后的网络规划和升级提供决策参考。 流量计费 基于NetFlow可实现多种计费方式，如基于流量、不同的时间段、QoS、应用类型、自治域计费等。 安全监测 根据采集的NetFlow数据，可综合进行模式匹配、基线分析等，进行DoS/DDoS攻击和蠕虫等病毒检测，从而快速定位网络中的异常行为。 传统的安全解决方案不能定位攻击的来源，只能被动防御，如果采用FLOW技术，那么可以很清晰地定位攻击的源地址，目的地址，以及从哪个路由器的物理接口进来，从哪个物理接口出去，这样可以在物理接口上配置ACL，适时地切断蠕虫或者DDOS的流量，进而保护整个网络不受影响。 