拿什么来分析网络故障以及诊断网络性能[1] 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_256492.htm 随着IT、网络技术的迅猛发展和企业信息化程度的不断提高，各种网络应用越来越丰富，各种应用时时刻刻都在争夺有限的网络带宽，从而导致网络管理的难度不断增大。因此，如何保证网络的可用性和关键业务的畅通运行，对企业发展将起到至关重要的作用。企业需要有相应的技术手段，明确了解网络上各种应用的带宽占用情况，分析用户流量行为，以便合理的规划和分配网络带宽，有效地保障关键业务应用的正常运行。 与此相适应，网络管理也从过去的设备级管理上升为今天的业务管理。因此，专业的网络流量和协议分析软件也应运而生，他们帮助用户具体了解当前的流量组成、协议分布和用户行为。 网络流量分析是指捕捉网络中流动的数据包，并通过查看包内部数据以及进行相关的协议、流量分析、统计等来发现网络运行过程中出现的问题，它是网络和系统管理人员进行网络故障和性能诊断的有效工具。常用的网络流量和协议分析有四种方法。 1、基于SNMP 本方法仅能对网络设备端口的整体流量进行分析，可以获得设备端口的实时或者历史的流入/流出带宽、丢包、误包等性能指标，但无法分析具体的用户流量和协议组成。通过扩展实现RMON和RMON II，该方法可在一定程度上（网络2层到4层）实现有限的端到端通信会话数据分析、TopN用户统计等功能。相关的产品有HP的OpenView NNM，CA的 UniCenter，MRTG等。因其具有实现简单、标准统一、接口开放的特点，被业界广泛采用。 2

、基于网络探针（Probe） 本方式的数据抓包、分析和统计等功能一般都在网络“ 探针 ”上以硬件方式实现，分析的结果存储在探针的内存或磁盘之中，具体的前端展现依赖与之对应的专门软件。因此具有效率高、可靠性高、高速运行不丢包的特点。本种方式可深入的对网络2层、3层甚至7层的特性进行详细分析。常见的产品有Agilent的 NetMetrix 及其Probes，NetScout 的nGenius Performance Manager 及其Probes等。 3、基于实时抓包分析 基于实时抓包的分析技术提供详细的从物理层到应用层的数据分析。但该方法主要侧重于协议分析，而非用户流量访问统计和趋势分析，仅能在短时间内对流经接口的数据包进行分析，无法满足大流量、长期的抓包和趋势分析的要求。常见的产品有NAI 的Sniffer Pro，免费的tcpdump、ethereal等。 4、基于流（Flow）的流量分析 目前基于流的分析技术主要有两种：sFlow和NetFlow。sFlow是由InMon、HP和Foundry Networks联合开发的一种网络监测技术，它采用数据流随机采样技术，可以适应超大网络流量（如大于10Gbps）环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。目前，仅有HP、Foundry和 Extreme Networks等厂商的部分型号的交换机支持sFlow。 NetFlow是Cisco公司开发的技术，它既是一种交换技术，又是一种流量分析技术，同时也是业界主流的计费技术之一。它可以回答有关IP流量的如下问题：谁在什么时间、在什么地方、使用何种协议、访问谁、具体的流量是多少等问题。NetFlow因为其技术和Cisco网络产品的市场占有率优势而成为当今主流的流量分析技术之一。 基于Flow的分析方法将成为趋势 在上面所提到的四种方法中，基于Flow的分析

方法应该是网络流量分析技术的趋势。这是它的技术实现理论所决定的。 流量管理方式比较表（Y=Yes；N=No；P=Perhaps） 