第3章

网络流量测量与分析

随着网络应用的不断发展，以 IP 数据包交换为特征的计算机网络已经逐渐替代以电路交换为特征的传统网络。以 Internet 为代表的 IP 网络规模不断扩大，各种新的网络设备、基于不同流量模型的业务应用的不断出现使得网络拓扑结构、网络应用及网络管理日益缤纷复杂。人们也逐渐认识到对网络行为的深入理解是保障网络健康运行的决定性因素之一，是网络容量规划、流量工程、故障诊断、性能提升的科学决策依据，是保障网络高可靠、低延迟/丢包、降低操作复杂性的基础。

对网络提供者、网管人员而言，网络的流量采集、测量与分析预测都有着非常重要的意义。对网络提供者来说，通过流量测量，网络提供者可以采用更为灵活的计费方式，比如基于用户使用网络的时间，基于用户占用的带宽和流量，基于用户的业务类型和服务质量等。再通过流量的预测，可以了解到自治域之间、网络之间的流量情况及其趋势，这些数据可以用于网络优化应用中，以便更好地进行路由设计和负载均衡的设计。对网管人员来说，通过对网络流量的测量与预测，可以制定网络拥塞控制策略。这样就可以降低因网络拥塞带来的信息丢失和延迟，充分利用网络资源，提高服务质量。

网络管理员目前一般采用若干标准的工具与技术，例如 Ping、TraceRoute 和 SNMP (simple network management protocol)实现网络监控管理，这些工具、技术目的明确，但功能单一，对满足网络监控从网络设计、容量规划到流量工程、安全检测故障调试等多种多样的需求来说还是远远不够的。

网络流量是单位时间内通过网络设备或传输介质的信息量(报文数、数据包数或字节数)。网络流量的测量与分析系统一般由数据采集、数据存储和数据分析三个部分组成。数据采集负责捕获流量信息，并把它们发送到数据存储设备进行存储，数据分析负责对存储的流量数据和模型进行分析处理。

3.1 网络流量采集

网络流量采集技术是网络流量分析和处理的基础，网络管理信息来源多、种类多，网络流量的变化可综合反映诸多网络运行中故障、性能等方面的信息。只有对网络运行历史有定量化记录才能对网络运行可靠性等信息有准确的认识，才能科学地制定出提高网络可靠性和升级的方案。

在一般网络设备例如路由器和交换机的 MIB 库中，一般都包含设备的网络端口信息，包括端口的类型、速率、最大流出量、最小流出量、最大流入量、最小流入量等。根据这些值，可以计算出平均流出量、平均流入量、链路利用率等监测网络的链路流量信息，可以基于 SNMP 协议设计 SNMP 的 Manager 程序，对这些 MIB 数据进行采集处理来得到链路的流量状况。流量采集系统的易用性直接影响到分析与预测子系统开发的难度和效率，流量采集系统的广度和深度直接影响到分析与预测子系统的准确性和广泛性。面对大量需要采集的信息，构建高效稳定健壮的底层数据采集系统是实现可靠网络流量采集与分析系统的基础。

3.1.1　几种主要的流的定义

“流(flow)”的定义是流量工程一个重要概念。根据具体研究目的的不同，“流”的定义可以有多种方式，许多厂家也有各自不同的具体实现，但随着“流”在网络流量测量中的地位愈来愈重要，越来越受关注，其标准化工作也在持续进行中。下面简要介绍一下几个主要的“流”的定义。

1. CBP flow

K. C. Claffy 等人在研究中最早总结出有关“流”的定义，他们认为“一个流是活动的，就是指在一个定义好的时限内(timeout)可以观察到属于给定条件的流的 IP 分组(packets)”。他们给出了参数化的 IP 流结构描述，即根据流的方向(单向或双向)、单端点(endpoint)或双端点聚合方式(源、目的端点，或源-目的端点对)、端点描述的颗粒度(IP 地址、网络号、AS 号或 IP 地址＋端口号)及功能协议层(TCP、UDP 或应用层)等四个方面定义“流”。这个流的定义对于以后有关流及因特网行为研究产生了深远影响。

2. Cisco NetFlow

Cisco 的 NetFlow 是指从给定源节点到目的节点的单一方向上的 IP 分组流(stream)，它使用源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议类型、TOS、输入逻辑接口号来标记网络“流”。

NetFlow 记录的“流”包含了丰富的信息，它主要在 Cisco 的路由器和交换机产品系列实现，主要用于网络监测、应用监测、用户监测、容量规划和安全分析等。

3. IETF RTFM

RTFM 是 IETF 建立的一个工作组，提供了一个描述和测量网络流的通用框架。RTFM 中的“流”是指根据端点的有关属性来定义的 IP 分组集合，这些属性包括：

- 完整的 5 元组信息(源 IP 地址、目的 IP 地址、源端口号、目标端口号、协议类型)；
- 网络地址块对(network block pairs，如 192.168.1/24 和 192.168.2/24)；
- 地址块列表等。

RTFM 仅关注端点之间“会话”(sessions)行为，端点的属性值(如地址和类型等)在两个方向上是相同的，且单向流可以被看作是一种双向的退化情况(degenerate case)。因此，RTFM 流是双向的(bi-directional)。NetraMet 是第一个实现 RTFM 的流量测量工具，被广泛使用。

4. IETF IPFIX

IETF 的 IPFIX(IP flow information export)是以 Cisco 的 NetFlow 的第九版为基础制定的。根据 RFC3917 的定义,一个"流"是指在一个特定的时间间隔内通过网络中的观测点(observation point)的 IP 分组集合,属于同一个特定的分组流具有相同的属性集合。每个属性都是直接来源于以下值或者某种规则的组合:

- 一个或者多个分组的头部信息(如目的 IP 地址)、传输层协议信息(如目的端口号)、应用层协议信息(如 RTP);
- 一个或多个分组本身的信息(如 MPLS 标签号);
- 一个或多个与分组转发的属性(如下一跳的 IP 地址、输出端口号)。

为了较完整的输出数据,IPFIX 使用以下七元组来确定一个流:源 IP 地址、目的 IP 地址、源端口、目的端口、三层协议类型、服务类型字节和输出逻辑接口。七元组相同的 IP 分组被归入同一个流。需要说明的,目前 IPFIX 中的流仍然是源 IP 地址和目的 IP 地址之间传输的单向数据流(与 NetFlow 类似)。

上述的不同版本的"流"的定义中,差异通常直观地表现在其输出报文格式上,这些 Flow 所定义的字段和数量随着厂商及协议版本的不同而各有不同(如包含自治域号、下一跳等)。由于 IPFIX 有关流的定义更具有普遍性,其标准化的进程进展非常顺利,目前已有多家著名网络厂商开始或即将支持 IPFIX。

3.1.2 流量采集算法

流数据采集是网络流量分析与控制的基础技术,可以掌握网络某节点或链路的流量细节,如运输协议、应用协议、流量强度情况和用户行为特征等来对网络流的特性进行测量和分析。流数据采集有如下方法。

1. 采样算法

由于高速网络流量给流量监测带来的困难,使用传统的方式对每个数据报文进行统计是不现实的,为了减少监测操作带来的资源消耗,目前研究了许多新的统计方式如:流量采集、统计算法等,而其中有许多都是基于采样算法实现的。早期经典的采样算法包括:Claffy 提出的基于时间和基于报文到达次序的随机采样分层监测技术,1998 年 Cozzani 研究的基于报文内容采样的监测技术。

随着 2.5Gbps 和 10Gbps 高速主干网络的普遍使用和网络监测技术研究的深入,采样监测技术有了较快的发展。美国 AT&T 实验室的 Duffield 于 2001 年提出了 Trajectory 基于报文内容的采样技术;2003 年 IETF 成立了报文采样测量工作组(PSAMP)专门研究报文采样测量技术。目前采样检测技术也被广泛应用于网络监测设备中,如 Cisco 的 NetFlow 和 NettanMet 测量器等。

但是采样方式存在很多缺点:首先,由于 IP 流存在的分布特性,采样报文需要大量的资源维护流信息;其次,采样信息丢失了部分详细信息,带来了统计等应用的不精确性;此外,大量的采样信息的存储,需要很大的存储空间。

2. 哈希算法

在高速流量监测过程中,如果对每个数据报文的流 ID、大小、地址等信息进行保留,

就需要消耗大量的资源，并且在新的数据报文到达时进行流相关信息的查询速度也很慢。

哈希算法可以很好地解决这些问题，但是存在一定的局限性：传统的哈希算法能够满足流的快速查询、减少流 ID 的存储空间等要求，但是丢失了 IP 流的五元组地址信息；采用 Bloom filter 数据结构的哈希算法能查询一个流是否存在，但是丢失了流大小的相关信息，并且由于对每个报文都进行处理，要求内存速度快，需要用 SRAM 实现。

3. 大象流识别算法

大象流(elephant flow)是那些在网络中持续时间长、发送报文数据多、数据量大、对网络性能影响最显著的流。很多的流量监测应用，只需关注大象流。2002 年 Estan 提出了 Sample and Hold 算法和 Multistage filter 算法来对大象流进行识别和统计。前者的基本思想是对报文进行采样，并对每个报文进行处理，当一个流的一个报文被抽到以后，在内存的哈希表中建立了该流的大小的计数器，这个流的后续报文都需要更新这个计数器，直到监测过程结束，其实质是通过采样来识别流。大象流的报文数目多，因此被采样的概率也大。而后者则是使用过滤器算法模块来独立为每个流建立多个哈希站，每个哈希站都采用独立的哈希函数，当一个流到达时只有所有的哈希站都超过预定义的阈值时才被识别为大象流。

4. 其他算法

由于网络流量监测技术的应用需求不同，还存在对于流分布信息的估计等应用算法，如 Duffield 提出的比例法和 EM 法等多种算法；Cristian Estan 提出的统计活动流数目的一族 Bitmap 算法；Abhishek Kumar 等 2004 年提出的建立流哈希映射，使用 Bayes 统计估计流大小分布的算法等。

3.1.3　流量采集工具

目前，国外技术力量研发的流量采集工具包括 MRTG、Sniffer Portable、libpcap、NetFlow、RMON 和 sFlow 等，由国内技术力量研发的流量采集工具有 KTAM 方案。下面分别对它们进行简单介绍。

3.1.3.1　MRTG

MRTG(the multi router traffic grapher)是监控网络链路流量负载情况的工具软件，是一款免费软件，支持 UNIX 和 Windows 操作系统，其安装过程非常简单，由于其结果输出采用 Web 页面形式，因此需要在相应的平台上安装发布系统，目前已经相当广泛的应用在各种不同领域中作为流量统计工具。它通过 SNMP 协议从路由设备得到网络流量信息，可根据被检测的网络设备或服务器传回的两个主要检测值实时地产生网页及统计图表，并且 MRTG 耗用系统资源很少。MRTG 通常被网管人员用来收集网络节点端口流量统计信息，是典型的监视网络链路流量负荷的工具。MRTG 将真实流量数据统计信息通过 HTML 页面实时输出，使得维护人员可以迅速地发现网络的故障和可能发生故障的节点。MRTG 比较适合用于对网络上的重要节点端口和故障发生频繁的网络设备进行监测。

MRTG 的优点是安装、定制简单，结果采用 Web 方式输出方便实用，而且是开源产

品，在世界各地有很多的开发人员不断对其升级和改进。缺点是功能比较单一，分析功能不强，其收集到的流量信息是基于端口的统计信息，无法实现基于 Payload 级别的流量监测，对网络运营商目前关注的如 P2P 文件共享、VoIP、流媒体等消耗大量带宽的应用无法正确识别。

3.1.3.2 Sniffer Portable

Sniffer Portable 属于 Network General 公司的 Sniffer 产品系列，可以在 PC、笔记本上安装。Sniffer Portable 采集流量的过程是将安装了 Sniffer 的主机接入到交换机的某个端口，然后将需要进行采集流量的交换机端口（可以不在同一交换机上）流量映射到此端口，通过对一个端口的扫描就可以采集到多个端口的流量并保存到数据库中，同时通过其分析部件实时监视和显示数据的统计信息。如果没有购买合适的硬件支持，Sniffer Portable 只能用于 100Mbps 及以下速度链路，特别适合小型网络的性能维护和分析。对于更高速率链路的流量采集，或者是全面收集大型网络的流量时，可以采用 Sniffer 的硬件产品及其分布式系统，但其价格十分昂贵。

3.1.3.3 libpcap

libpcap 是 UNIX/Linux 平台下的网络数据包捕获函数包，常见的基于 libpcap 的抓取系统在监测端口接收到数据包以后，由网卡驱动程序转发到位于操作系统内核的 TCP/IP 协议栈中排队等待处理，流量监测分析程序通过操作系统提供的套接字接口（socket）或者注册钩子函数（hook）的方式提取数据包进行解码和分析。在上述数据包的接收过程中，不仅要为数据包动态地分配和释放缓存，更重要的是需要将数据包从操作系统的内核空间拷贝到用户空间，这些操作将产生大量的系统调用开销，耗费 CPU 资源，因此基于此种架构实现的流量监测分析系统很难适用于高速网络链路环境的监测需求。

3.1.3.4 KTAM

KTAM 方案是一种基于 Linux 内核实现的新颖的设计方案，它可以减少系统调用的开销，减轻内存访问的负担，达到减少 CPU 资源开销的目的。KTAM 方案支持三级流量监测分析，分别为数据包级、业务流级和 Payload 级：数据包级监测分析所有的原始数据包，负责提供数据包 2～3 层的协议解码和报文统计信息；业务流级监测分析提供对特定的流监测，例如基于特定应用或 IP 地址、IP 地址段的流量监测；Payload 级监测分析提供对数据包净载荷的检查，能够识别某些端口不确定的应用，例如 P2P 文件共享、VoIP、流媒体等。

3.1.3.5 NetFlow

NetFlow 是 Cisco 公司提出的网络数据包交换技术，它同时可用来将网络流量记录到设备的高速缓存中，从而提供非常精准的流量测量。一个 NetFlow 是从给定的源端到目的端的一系列单向数据包，它使用源和目的端点的 IP 地址和传输层端口号、协议类型、服务类型以及输入接口等来标记网络流。

NetFlow 记录的流包含了丰富的信息，为流量分布、业务分布等性能分析提供最充足的数据(但需要消耗一定的路由器 CPU 和内存)，它可用于多种目的，如网络流量核算、基于使用的网络付费、网络监控以及用于商业目的的数据存储，同时非常适合于网络性能分析。NetFlow 不需要其他硬件流量设备的支持，开启和关闭都非常方便，因此国内外已有许多运营商用它来收集流量，服务于网络规划、设计和优化等领域。NetFlow 的配置非常方便、安装简单，除了需要在路由器上配置之外，只需要一台 UNIX 工作站作为信息采集器，所有路由器或交换机上发送的 NetFlow 流都将送到此工作站集中处理和分析。根据 NetFlow 的特点可知，其非常适用于大型的网络，成本较低，实施方便，而且不受速率的限制。

同时 Cisco 的路由器中还包含了流量集监测功能模块，称为 NetFlow Services。此功能会在路由器转发分组的同时根据配置记录下经过路由器各个端口的分组情况，记录的内容包括：源和目的 IP 地址、下一跳地址、输入和输出物理端口号、某个流的包数、某个流的总字节数、流的起始时间和结束时间、源和目的地址掩码等。经过指定时间，再将这些统计信息以一定的格式(UDP 包，有固定的格式)发送到信息采集器进行处理。信息采集器在特定端口监听等待数据到达，然后根据规定的格式分析、处理和记录数据，得到流经路由器的网络流量状况。严格来说 NetFlow 并不是一个简单的流量采集。

3.1.3.6　RMON

RMON 是 IETF 定义的 MIB(RFC1757)，是对 SNMP 标准的扩展，它定义了标准功能以及在基于 SNMP 管理站和远程监控者之间的接口，主要实现对一个网段乃至整个网络的数据流量的监视功能，目前已成为成功的网络管理标准之一。RMON 是对 SNMP 的重要增强，它所定义的 MIB 被补充为 MIB. II，并且提供了有关互联网络的关键信息，使 SNMP 更为有效、更为积极主动地监控远程设备。

RMON 的规范是 RFC1271 定义的，它定义了标准网络监视功能以及在控制台和远程探测器之间的通信接口。它提供了一个有效的方法，可以在降低其他代理和控制台负载的情况下监视子网行为。RMON MIB 由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。

通常我们将用于研究网络整体流量的设备称为网络探测器，或者网络分析器、探测器。单纯利用 SNMP 的管理者代理作模式，可以获取单个网络设备的信息，但不易获取 LAN 上整个的信息流量。而探测器可以通过监听方式在 LAN 上运行，以监视 LAN 上的每一个包。探测器可以产生统计信息，包括错误统计(如小于规定大小的包的个数和冲突数量)和性能统计(如每秒传递的包数以及包的大小分布)。探测器还可以存储全部或部分报文以供以后分析使用，并使用过滤器根据包的类型或包的其他特性来限制计数或捕获的数据包个数。利用 RMON，可以有效地监视 LAN 上的每一个数据包，同时又不会对网络性能造成较大的影响。

RMON 探测器和 RMON 客户机软件管理站结合在一起在网络环境中实施 RMON，RMON 的监控功能是否有效，关键在于其探测器要具有存储统计数据历史的能力，这样

就不需要不停地轮询。

3.1.3.7 sFlow

sFlow(RFC3176)是2001年被IETF批准成为一项草案标准的一种网络监测技术，它利用对整个网络上传送的局域网和广域网数据包流的随机采样，让用户详细、实时地掌握网络传输流的性能、趋势和问题。与数据包采样技术(如RMON)不同，sFlow是一种导出格式，它增加了关于被监视数据包的更多信息，并使用嵌入到网络设备中的sFlow代理转发被采样数据包，因此在功能和性能上都超越了当前使用的RMON、RMON II和NetFlow技术。

sFlow使用两种独立的采样方法来获取数据：针对交换数据流的基于数据包统计采样方法和针对网络接口统计数据的基于时间采样方法。sFlow使用不同的采样率，对交换机或仅对其中一些端口实施监视，这样保证了在设计管理方案时的灵活性。sFlow需要网络交换设备硬件支持，如果硬件设备不支持，则需要在端系统上开发sFlow Agent。

sFlow技术独特之处在于它能够在整个网络中，以连续实时的方式监视每一个端口，但不需要镜像监视端口，对整个网络性能的影响也非常小。sFlow使拥有高速千兆和万兆端口的网络能够得到精确的监视，同时经过扩展，可以在一个采集点上管理数万个端口。因为sFlow代理嵌入在网络路由器和交换机ASIC中，所以与传统的网络监视解决方案相比，这种方法的实施成本要低得多，而且也不需要购买额外的探针和旁路器，就能全面监视整个网络。与那些需要镜像端口或网络旁路器来监视传输流量的解决方案不同，在sFlow的解决方案中，并不是每一个数据包都发送到采集器(接收sFlow数据包的设备)。

采集到的数据以UDP报文的形式发送到采集器。一个数据包主要分为三大部分：数据的包头部分、样本的具体信息和接口统计信息。以一个sFlow数据版本号为2的基本数据包为例，在数据的包头部分包含sFlow数据的版本信息、Agent的IP地址、采样包的序列号、采样的样本数、系统采样时间等信息。其中采样的样本数，就是指该包中所含sample数据的个数。

3.1.3.8 RMON、NetFlow和sFlow三种产品的比较

SNMP是TCP/IP协议族的一部分，嵌入在各种TCP/IP协议中，提供基本的接口计数信息和协议信息。而RMON、NetFlow和sFlow通常都是采用嵌入式系统实现的Agent系统，因此与SNMP差异较大。以下主要对RMON、NetFlow和sFlow进行比较。

(1) Agent的资源消耗

- 对处理能力的消耗。RMON对每个数据报文进行处理，提取出信息后，存入数据库，把流量信息按照ASN.1的格式进行编码，以SNMP数据包发给管理站。NetFlow既可以处理逐个报文进行处理，在繁忙的时候也进行采样，然后把流量用NetFlow报文发送到管理站。sFlow直接将采样的数据报文头部发送到管理站。因此RMON和非采样NetFlow对Agent处理能力要求最高，采样的

NetFlow 和 sFlow 对处理能力要求低。

- 对内存的消耗。在不同的时间 RMON 和 NetFlow 内存的消耗不一样，sFlow 在固定了采样率和轮训间隔后，内存消耗保持不变。

(2) 报文信息

- 信息的精确性：RMON 和 NetFlow 可以对每个报文进行处理，因此信息的精确性要比采样的 NetFlow 和 sFlow 要高，但是数据量也大。
- 内容的详细程度：RMON 和 NetFlow 都对报文进行过处理，损失了一些报文信息，而 sFlow 则将整个报文头部发送给管理站，信息的内容最为丰富。

3.2　网 络 测 量

对于网络测量的研究始于 20 世纪 70 年代，随着网络技术的飞速发展，网络规模不断扩大，容量不断增加，网络环境变得更加复杂、多变和异构，新的网络行为不断出现，网络中出现的各种难以预测的问题日益增多，因此，网络测量也越来越受到关注。

网络测量可用于故障诊断、协议排错、网络流量特征化、网络性能评价等。

(1) 故障诊断主要是对广播风暴、非法分组长度、地址错误、安全性攻击等故障进行诊断；

(2) 协议排错是指网络测量能够为新协议和应用程序的正确运行提供测试的手段，使其和原标准保持一致，或使老的版本向后兼容；

(3) 网络流量特征化指网络测量可使用统计技术来分析经验数据，从而提取出网络应用或网络协议的特征，以优化其特性；

(4) 性能评价指网络测量可用来考察某个协议或某个应用在网络中的性能水平，帮助确定性能瓶颈。此外，网络测量还有许多其他的用途。例如，用于选择服务器 ISP，验证网络配置设计互联网的新应用，配置网络或服务器，广域网中的负载平衡以及计费等方面。

对于网络测量，目前还没有统一的定义。从技术层面讲，人们形象地将网络测量描述为遵照一定的方法和技术，利用软件和硬件工具来测试或验证网络性能指标的一系列活动的总和。而从测量目的而言，网络测量是对网络行为进行特征化、对各项指标进行量化并充分理解与正确认识互联网的最基本手段，是理解网络行为的最有效的途径。

网络测量包含以下三个要素：

(1) 测量对象，也就是被测量的节点和链路，以及待测量节点、链路或网络的某种或某些特性；

(2) 测量环境，包括测量点的选取，测量时间的确定，测量设备、通信链路的类型等；

(3) 测量方法，也是针对某一具体的网络行为指标，选取合适的测量方法。

其中，测量方法应满足三个方面的要求：

- 稳健性，即被测网络的轻微变化不会使测量方法失效；
- 可重复性，即同样的网络条件下，多次测量结果应该一致；
- 准确性，即测量结果应该能够反映网络的真实情况。

从不同的角度出发，可以对网络测量进行分类，如表 3-1 所示。

表 3-1　网络测量分类

不 同 角 度	网络测量的分类
测量方式	主动测量
	被动测量
测量对象	网络拓扑测量
	网络性能测量
	网络流量测量
测量基准	基于流(flow-based)的测量
	基于网络接口、链接和节点的测量
	基于节点对(node pair-based)的测量
	基于路径(path-based)的测量
测量点的选择	单点测量
	分布式测量

3.2.1　根据测量方式分类

根据测量方式的不同，网络测量可分为主动测量和被动测量。

主动测量是基于端到端的测量，其测量设备向被测量设备网络注入一些以探测网络特征为目的的探测流，并通过分析这些探测流在网络中传输时反映出来的属性来得到网络性能参数和网络行为参数。如 Ping 发送 ICMP 类型数据包，可以获得网络往返时延、丢包率与连通性等参数。

被动测量需要在网络中的一点收集流量信息，如使用路由器或交换机收集数据或者使用一个独立的设备被动地监测通过被测网络链路地流量，通过该点数据流进行收集、分类和提取，然后对记录数据进行归并和处理。观测点一般位于网络中流量聚合的地方。被动测量几乎不会对原有网络流量造成影响，测量得到的网络数据能真实反映当前网络的流量分布特点，因此主要用于测量和分析网络流量分布，从网络流量模型的角度进行网络 QoS 管理和设计。

3.2.2　根据测量内容分类

根据测量对象的不同，网络测量可分为网络拓扑测量、网络性能测量和网络流量测量。

1. 网络拓扑测量

网络拓扑测量是指测量网络的拓扑结构或逻辑拓扑关系，以及具有地理信息的拓扑图，用以指导资源调节和流量分配。如 CAIDA 组织开发的 Skitter 工具收集从几个源节点到成千上万个目的节点的路径信息，通过断层摄影技术，动态发现和跟踪 Internet 拓扑结构，并将其可视化，绘制全球互联网拓扑结构，并且开展了地理信息图方面的研究。

2. 网络性能测量

网络性能测量主要通过监测网络的端到端的时延、抖动、丢包率等特性，了解网络的可达性、利用率以及网络负荷等。如 NPACI 的 Network Weather Service 每隔一定的时间周期性地监视、动态地预报各种网络及计算资源的网络性能，收集某一时刻的数据，通过数据模型预测下一时段的 TCP/IP 端到端的吞吐量延迟，用于广域网上的大规模计算调度和保证元计算软件平台上开发服务质量。

3. 网络流量测量

网络流量测量主要是对网络数据流的特性进行监测和分析，以掌握网络的流量特性，如协议的使用情况、应用的使用情况、用户的行为特征等。网络流量测量是网络流量管理的基础，尤其是对大型复杂的主干网。目前的研究中，网络流量的测量多采用被动方式，其数据采集方法主要有两种：直接读取 MIB 对象的流量信息和网络侦听。

流量测量帮助人们对网络的基本特性有了更深刻的了解。正是在对网络流量的观测和分析的基础上，Leland 等人在 1994 年发现了以太网流量的自相似特性，此后 Paxsont、Crovella 等人验证了网络具有广泛的自相似特性，从而解决了泊松模型和马尔可夫模型不能解释的网络现象。近年来，多分形模型和小波等分析工具纷纷被引入流量分析中，得到了更多的对于网络的认识。

3.2.3　根据测量基准分类

在 IETF 的 TEWG 的网络流量测量框架中，依据的分类方法是测量的对象（或者叫做基准，bases）。测量基准有流、接口、链接和节点、节点对、路径。因此，按测量基准来分，网络测量可分为基于流（flow-based）的测量、基于网络接口（interface-based）、链接（link-based）和节点的测量、基于节点对（node pair-based）的测量和基于路径（path-based）的测量。

1. 基于流的测量

报文是网络中最小的传输单元，最初网络行为研究主要集中在报文层次上，但由于这些研究相对平等地分析每个报文，会导致报文间关系及更高层次信息分析的缺失。

流是在同一组特定的源地址和目标地址、源端口号和目标端口号之间传递的有着固定的协议类型、具有开始和结束时间的数据包的集合。对流特性的研究和分析，可以掌握网络某节点或链路的流量细节，如传输协议、应用协议、流量强度情况和用户行为特征等。而且采用流概念记录测量结果，通常可以大大节省存储空间，因此流测量成为网络测量中的一个热点研究方向。

基于流的测量是以流为基准对网络流量进行测量。测量信息通常包括源和目标的 IP 地址、端口号、协议类型、服务类型、流开始和结束的时间戳、分组计数、字节计数等。这种测量经常用于接入路由器、边界路由器等流量开始或者结束的地方。一般不对核心网络的核心路由器进行基于流的测量。流是一个粒度很小的测量对象。基于流的测量往往不是连续进行的，而是采取采样的方法。

2. 基于网络接口、链接和节点的测量

- 基于网络接口。
- 基于链接：主要针对 MPLS 中的 link building，会聚的链接作为一条链接，以便优

化。这样的链接也应该作为一条链接来测量。

可以对每个网络元素进行被动式的测量。如 SNMP、Tcpdump、Windump、NexXray 等。测量的信息包括：发送/接收的分组个数、字节个数、丢弃的分组个数、出错的分组个数等。

3. 基于节点对的测量

属于主动式测量，弥补被动测量的不足。基于节点对的测量可以用来测量主要的边界路由器之间的一些网络参数。由于路由配置可能发生改变，因此对节点对之间流量的跟踪就会出现丢失的情况。对某个节点对之间的流量可以用结束(或开始)于某个节点的路径的流量来表示。

4. 基于路径的测量

比流有更粗的粒度，适用于 MPLS 路由，用于访问控制、服务质量监视。路径：IP 分组从一个源端节点传送到目标端节点的过程中所经过的一系列连接的集合。基于路径的测量往往是针对 MPLS 路由而言的，因为 MPLS 可以使用相对固定的路径对流量进行路由。进一步，可以开发出基于流量的准入控制机制并对传送的特定服务的性能进行跟踪和评估。跟流一样，路径也是和一个节点对联系在一起。路径的粒度更大一些，因为路径通常传送的是汇聚流量。若路由发生变化，一个路径传送的流量要么不受影响，要么汇合到另外一个路径中去。

3.2.4 根据测量点分类

根据测量点的选择，又可将网络测量分为单点测量和分布式测量。

在测量吞吐量、包到达时间间隔、包长和 Hurst 参数等参数时，只需要布置一个测量点就可以进行测量，这样的测量就是单点测量。在测量延时、抖动和丢包率等参数时，需要布置多个测量点进行测量，这就是分布式测量。

3.3 网络流量测量

流量工程的目标是优化网络工作性能，其研究重点是对自治系统内部的各种业务流进行管理和控制。实施流量工程的一个必要前提就是对网络流量的测量，为网络性能分析提供最原始的数据。流量测量还可用于检测链路拥塞和拒绝服务攻击。

如前所述，根据测量对象的不同，网络测量可分为网络拓扑测量、网络性能测量和网络流量测量。下面对其中的网络流量测量技术及分类进行详细描述。

网络流量测量的主要内容就是对网络中的“流”进行测量和分析，以分析网络状况、掌握网络的流量特性，比如：协议的使用情况、应用的使用情况和用户的行为特征等。

3.3.1 网络流量的定义

根据 IETF 的定义，“流”是指在同一组特定的源地址和目标地址、源端口号和目标端口号之间传递的有着固定的协议类型，具有开始和结束时间的数据包的集合。目前，对网

络流量的测量都以“流”为基本粒度。

“流量(Traffic)”是通过网络上某一观测点的流的总和。流量测量是利用特定的技术手段,记录通过或到达观察点的数据包,并进行统计分析,最终获取网络流量信息。

一般在 IP 网络中可根据 IP 数据包的源 IP 地址、目的 IP 地址、协议号以及 TCP(或 UDP)报头的源端口号、目的端口号来定义网络流。具有相同源 IP 地址、源端口号、目的 IP 地址、目的端口号和协议的网络信息就属于一个流。这样定义的网络流可以适合于多种网络协议栈。通过分析具有相同协议类型的流,研究人员可以据此研究协议的工作性能和开发新的协议与应用。通过对流的分析,为科学地规划网络提供依据,以便更好地管理网络和改善网络的运行服务,并有助于网络管理者了解更多的网络流量情况和尽量多的测量信息。

在网络的链路上,流量是由很多的不同的流聚合而成,而这些流的传输协议类型及参数,以及应用的类型都可能存在很大的差异,因此仅从包级上来分析链路上的流量,就不能区别应用类型、传输协议的类型和单个流的特征,这样得到的分析结果比较片面;另一方面,在数据包级的流量分析需要占用大量的硬件资源,比如 CPU 运算、内存和硬盘空间等,测量和分析相对比较困难。

3.3.2　网络流量测量技术及分类

网络流量测量技术是目前唯一能用于分析网络状况、掌握流量特性的有效方法。流量测量主要是对网络中的“数据流”进行测量和分析,以掌握网络的流量特性,比如协议的使用情况、应用的使用情况、用户的行为特征等。

网络流量测量是网络流量管理的基础,随着网络技术的发展,不断有新的网络流量测量技术推出,其中的一些研究成果被采纳为技术标准并应用于设备中。了解和掌握这些技术有助于更好地利用已有的流量测量技术和工具,可以更方便地实现网络分析和网络管理。

网络流量测量技术可以从不同角度进行分类:

- 从测量工具的角度,可分为基于硬件的和基于软件的流量测量;
- 按照测量工具是否向被测网络中发送数据,可分为被动测量和主动测量;
- 按照对测量结果进行分析的方式,可以分为在线测量和离线测量;
- 从流量测量面向的区域对象来看,可以分为局域测量和广域测量;
- 按与被测网络的关系,可以分为合作测量和非合作测量。

以下分别对不同分类方式下的网络流量测量方法进行介绍。

3.3.2.1　硬件测量和软件测量

流量测量工具分为硬件和软件两种。基于硬件的流量测量工具是专门为采集和分析网络流量而设计生产的设备。基于软件的流量测量工具一般使用普通工作站作为运行平台,通过修改安装于主机上的操作系统的网络接口模块,使之具有捕获数据包的功能,以实现流量信息的收集和分析。

1. 基于硬件的流量测量

基于硬件的流量测量通常采用硬件测量工具来进行流量数据的收集和分析。这种流

量测量方式的测量效率很高，专用性强，但是存在价格昂贵、与网络接口类型和测试目标协议相关、对使用人员的要求较高的缺点。

硬件测量技术的一个典型例子是 Fluke 公司的 OptiView 链路分析仪，该分析仪是目前在千兆以太网领域进行流量测量使用比较普遍的硬件测量工具。它提供 OSI 参考模型全部 7 层的实时流量监测。可以在千兆以太网链路上进行实时的流量分析，能够实现交换式以太网链路的分布式流量分析，具有全双工在线流量分析能力，并且可以通过浏览器或 Telnet 进行设置。

2. 基于软件的流量测量

基于软件的流量测量通常采用软件测量工具来进行流量信息的收集和分析。这种流量测量方法具有价格便宜、实现灵活和可扩展性强等优点，但是其性能要低于基于硬件的测量技术。

软件测量技术的典型例子是 UNIX 下的 TcpDump 软件，它是基于 Berkeley 包过滤器(BPF)实现的 TCP/IP 数据包捕获工具。TcpDump 可以将网络中传送的数据包的包头完全截获下来进行分析。它支持针对网络层、协议、主机和端口的过滤，并提供与、或、非等逻辑语句实现信息过滤，是目前应用最广泛的软件流量测量工具。TcpDump 在 Windows 操作系统下的变形应用是 WinDump，其功能和使用方法与 TcpDump 类似。另一个应用比较普及的流量测量软件是 SnifferPro。SnifferPro 是一个功能十分强大的流量测量软件，它能够抓取网络上的所有数据包，可自定义过滤器，并将收集的数据包分析后转化为图表和报告形式输出，可以很方便地了解网络状况。

3.3.2.2 主动测量和被动测量

流量测量技术的另一种分类方法是按照测量工具是否向被测网络中发送数据划分为被动测量和主动测量两种，如图 3-1 所示。

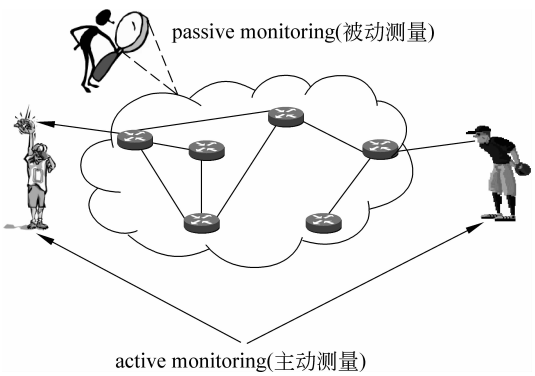

图 3-1 主动测量和被动测量

1. 被动测量

被动测量是指在网络中特定的节点上安装探针和数据采集器等来收集流经该节点的网络流量，然后进行分析，提取业务特征进而获得网络性能数据。被动测量是大多数测量工具采用的方法，例如 TcpDump 和 SnifrerPro 等工具。目前的研究中，网络流量的测量

多采用被动方式。

被动测量方法的优点在于可以有效地获取网络中的流量信息，不需要向网络中注入额外的流量，不会增加和修改网络的数据，对于网络负荷基本上没有影响，能够较为准确地反应网络中的性能。其缺点在于被动测量基本上是基于对单个设备（如路由器、交换机等）的监测，难以获得对网络整体行为的理解和对网络端到端的性能进行分析，并且可能实时采集的数据量过大，另外还存在用户数据泄漏等安全性和隐私问题。因此，被动测量的主要应用是包监听，主要用于单点监测。

2. 主动测量

主动测量是在选定的测量点上利用测量工具向目标链路或者目标节点发送探测数据包，然后根据返回的网络性能参数来研究和分析网络的行为。

主动测量方法的优点是对测量过程的可控性比较高，非常易于在网络测量中实现，而且能以更加直接的方式来分析网络，可以全面掌握整个测量网络的行为特征。缺点是注入的测量流量会改变网络本身的运行情况，使得测量的结果与实际情况存在一定的偏差，而且测量流量还会增加网络负担。

基本网络性能、网络的路由行为分析和网络的拓扑探测及可视化常用到主动测量技术。除此之外，主动测量还应用在 BGP 路由的测量和路由的不对称性分析等方面。要对一个网络进行主动测量，需要一个测量系统，这种主动测量系统一般包括以下四个部分：测量节点（探针）、中心服务器、中心数据库和分析服务器。由中心服务器对测量节点进行控制，由测量节点执行测量任务，测量数据由中心数据库保存，数据分析则由分析服务器完成。

主动测量的典型例子是利用 ping 工具测量到达某个特定节点的网络时延。

例 1：使用 ping 命令进行简单的时延/丢包侦听。

```
C:\Users\Administrator.ZGC-20110221ARD>ping www.uestc.edu.cn

正在 Ping www.uestc.edu.cn [202.112.14.184] 具有 32 字节的数据:
来自 202.112.14.184 的回复: 字节=32 时间=1ms TTL=121
来自 202.112.14.184 的回复: 字节=32 时间=1ms TTL=121
来自 202.112.14.184 的回复: 字节=32 时间=1ms TTL=121
来自 202.112.14.184 的回复: 字节=32 时间=1ms TTL=121

202.112.14.184 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

例 2：使用 traceroute 进行路由行为监测。

```
C:\Users\Administrator.ZGC-20110221ARD>tracert www.uestc.edu.cn

通过最多 30 个跃点跟踪
到 www.uestc.edu.cn [202.112.14.184] 的路由:

  1     1 ms     1 ms     1 ms  222.197.180.1
  2     1 ms     1 ms     3 ms  222.197.180.1
  3     1 ms    <1 毫秒   <1 毫秒 125.71.229.37
  4     1 ms     4 ms    <1 毫秒 125.71.230.69
  5     2 ms     1 ms     1 ms  202.115.0.53
  6     1 ms     1 ms     1 ms  202.115.0.1
  7     *        *        *     请求超时。
  8     3 ms    19 ms     2 ms  www.uestc.cn [202.112.14.184]

跟踪完成。
```

通过以上的介绍我们知道，被动测量只记录可在观测点观察到的数据，而观测点本身不产生任何数据送入被测网络中，因此被动测量是大多数测量工具采用的方法。而主动测量具有响应速度快、适应性强的优点，但是会增加网络的负载，使用时需要注意测量的频度。

因此，主动测量与被动测量各有其优、缺点，而且对于不同的性能参数来说，主动测量和被动测量也都有各自的用途。所以，将主动测量与被动测量相结合将会给网络流量测量带来新的发展。

3.3.2.3 在线测量和离线测量

按照测量工具对测量结果进行分析的方式进行划分，可以分为在线测量和离线测量两种类型。

在线测量工具不仅可以实时收集网络流量数据，还可以立即对收集的数据进行分析，并实时输出分析结果。这对测量工具的能力有很高的要求，一般只有硬件测量工具才能做到。近年随着个人计算机处理能力的增强，很多软件测量工具也能做到一定程度的实时分析，例如 SnifferPro 等。

离线测量工具只能将收集到的流量数据保存下来，在需要的时候进行离线分析。这种方式实现比较简单，流量数据的收集和分析工作相对独立，有利于进行灵活的结果分析。例如我们可以利用 TcpDump 工具记录下网络中的流量信息，在适当的时候利用保存下来的数据进行各种分析工作。

3.3.2.4 局域测量和广域测量

从流量测量面向的区域对象来看，可以将流量测量分为局域测量和广域测量。局域测量针对局域网进行流量测量，广域测量的目标是广域网络。

局域测量的实现通常比较简单，因为局域网络一般都由一个统一的管理机构进行管理，并且构建局域网的基础技术一般都比较单一，例如采用以太网技术。因此在局域网中简单地部署测量设备即可实现流量测量。

广域网络的环境比较复杂，其中既包含了各种不同的基础技术，例如以太网、ATM、帧中继等，有可能由不同的机构进行管理，因此广域测量比较复杂。其复杂性主要体现在两方面：一方面是收集流量数据比较复杂，不仅需要考虑获得测量数据的安全性和有效性，还要考虑观测点分布的合理性；另一方面是流量数据的分析比较复杂，其关键在于如何获得广域网的全局流量信息，而不仅仅是局部的状况。

MRTG 是目前应用最广泛的广域网流量测量工具之一，MRTG 是一个监控网络链路流量负载的工具软件，它通过 SNMP 协议从设备得到流量信息，并将流量负载以包含 PNG 格式图形的 HTML 文档方式显示给用户，以非常直观的形式显示流量负载。

3.3.2.5 单点测量和多点测量

按测量点的分布可分为单点测量和多点测量。单点测量在非合作的情形下能发挥巨大的作用。要测量一个大规模网络的情况，需要在网络中的很多地点进行分布式多点测量，得到比较详尽的、综合的大规模网络数据以及单点测量所得不到的交叉路由信息。现在的多

数网络测量体系都采用分布式多点测量，如 NIMI、NLANR、AMP、Skitter、IEPM 等。

3.3.2.6　合作测量与非合作测量

按与被测网络的关系可分为合作测量和非合作测量。

合作测量对网络运营者来说，能够掌握网络的运行状况、找出瓶颈、业务分布情况等，以便有效地管理网络、充分利用网络资源。

非合作测量是指被测网络不乐意被别人测量，测量目的是窥探对方网络的情况，这在军事上有非常重要的意义。

3.3.3　流量测量基础设施及其体系结构

1999 年 10 月，IETF 的 IPPM 工作组（IP performance metrics working group）在 RFC2722 提出了一个流量测量框架（traffic flow measurement：architecture）。

框架由四部分组成：测量管理器（Manager）、测量设备（Meter）、测量数据读取设备（Meter Reader）、测量数据分析应用（Analysis Application）。

- Manager 负责对 Meter 进行配置，对 Meter Reader 进行控制，同时监视 Meter 和 Meter Reader 的操作行为。
- 测量设备可以对测试数据进行压缩和初步处理，处理后的数据称为“使用数据（usage data）”。
- Meter Reader 负责获取“usage data”并提供给 Analysis Application 进行分析。
- Analysis Application 处理“usage data”，将分析结果提供给网络工程人员和管理人员使用。

图 3-2 说明了 IETF 的流量测量框架结构。框架定义了流量测量的整个过程：监测点部署监测设备，创建配置文件去指定需要监测的流，然后按照一定时间间隔读取、保存网络流量数据，最后进行分析，分析结果用于辅助工程和管理人员进行分析和管理。

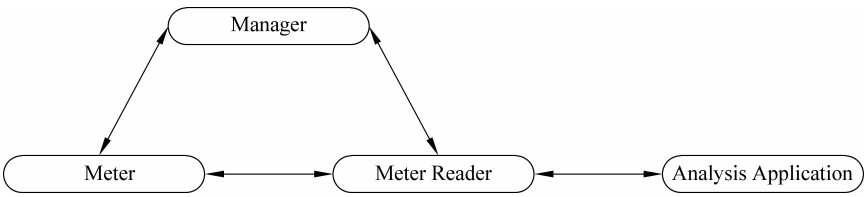

图 3-2　IETF 的流量测量框架结构

3.4　本 章 小 结

本章主要的内容是网络流量采集、网络测量和网络流量测量。其中，网络流量采集包括了几种主要的流的定义以及流量采集算法和工具。网络测量主要从测量方式、测量内容、测量基准和测量点进行分类。网络流量测量包括了网络流量的定义、网络流量测量技术及分类和流量测量基础设施及体系结构。

第4章

网络流量分析

网络的作用是传输应用数据，网络流量的分析就是对在网络中传输的实际数据流进行分析，网络数据流的分析包括从底层的数据流一直到应用层的数据的分析，有的时候也称之为网络协议分析。

4.1 网络流量分析的目的和意义

简单地说，我们对网络流量进行分析的目的是了解、发现和证明。管理好一个网络最重要的就是对网络的了解，包括了解网络拓扑、设备和配置等，但要保证网络的服务质量，这样的了解还远远不够。对网络流量的分析能使网络技术人员更深入地了解网络，包括网络运行规律、网络应用运行规律和网络用户的网络行为。

网络运行规律：每个网络都有自身的运行规律，这和网络的结构、应用特点等紧密相关，通过流量的长期分析，能够了解网络系统运行的规律。

网络应用运行规律：网络上重要的应用在运行时，每一个访问、每一个交易处理，数据都由网络来传输，通过分析应用的流量，能够清楚地了解应用运行的规律，访问量、交易处理数量、响应性能等数据，都可以通过流量分析手段获取。

网络用户的网络行为：每个网络用户的网络行为都是相互影响的，同时会对网络的运行产生影响，伴随每个用户在网络中的每个网络行为都有网络流量产生，通过对网络用户的网络流量进行分析，能够直观地了解网络用户的网络行为。

网络异常的发现是建立在了解网络的基础之上，如果能及时发现网络异常，将使网络管理更主动，将为网络的持续高性能运行提供重要的保障。

(1) 网络运行异常：网络中流量的异常，包括利用率、数据包数的异常。

(2) 网络应用运行的异常：连接数量、应用响应、应用流量的异常，都可以通过长期主动分析来及时发现。

(3) 网络用户的异常网络行为：异常的网络行为也都有明显的流量特征，如感染的蠕虫病毒、安装了后门程序等，长期的流量分析能及时地发现网络用户的这些异常网络行为，及时发现网络用户的异常网络行为是避免其影响网络运行的关键。

网络流量的分析可以为网络和应用问题的分析提供依据，特别是数据包级的分析，而这些依据是真实的，因为它们是实实在在地在网络中传输的数据包，这也是流量分析能够大大提高网络和应用问题分析效率的原因。

网络流量分析是有助于让网络持续、高效和安全运行的一种手段，网络流量分析的意义在于取得对网络运行管理、应用运行管理和网络应用问题分析有意义的数据。不同的网络和不同的应用有完全不同的流量数据，所以这些数据多种多样，像利用率、bps、pps、延迟、重传、连接数量等这些流量分析的数据，都要和实际的网络应用运行情况结合起来才有意义。网络流量分析的数据的意义是建立在了解的基础上的，只有对网络和应用的深入了解，才能使这些数据的价值得到真正的体现。

网络流量分析在网络管理中具有重要的意义，网络流量分析给技术人员提供了有效技术数据，这对了解网络、发现问题、确认原因都有重要意义，而这些能够在网管的整个工作进程中提供有效的帮助。

4.2　网络流量分析方法

网络流量是单位时间内通过网络设备或传输介质的信息量（报文数、数据包数或字节数）。目前，主要的分析方法有流量的统计分析和流量的粒度分析等。

4.2.1　网络流量统计分析

网络流量统计分析是网络运行管理、网络测量、网络性能分析及网络规划设计中的一个重要内容，流量统计分析可以简单地分为基于硬件和基于软件两类。

（1）基于硬件的流量统计

此类分析通常采用硬件测量设备，是一种为特定目的设计的用于收藏和分析流量数据的硬件设备。硬件统计技术的典型例子是 Fluke 公司的 Optiview 链路分析仪 Fluke。

（2）基于软件的流量统计

这种统计分析一般通过修改主机上的操作系统的网络接口模块，使之具有捕获数据包的功能，以实现流量信息的收集和分析。软件技术典型的例子是 NetFlow 软件。其主要原理是根据网络数据包传输时，连续相邻的数据包通常是向目的 IP 地址相同位置传输的特性，配合 Cache 快取机制，当网络管理者开启路由器或交换机接口 NetFlow 功能时，设备会在接收数据包时分析该数据包的包头信息来获取流量资料，并将所接收的数据包流量信息汇聚成一条条的流来进行分析。

基于硬件的流量统计效率很高，专用性强，但价格昂贵，对人员要求高，相比之下基于软件的流量统计有价格便宜、实现灵活、可扩展性强的优点，但其性能要低于基于硬件的统计技术。因此，流量统计方法有待进一步的提高，以适应网络快速发展的需求。

4.2.2　网络流量的粒度分析

网络流量行为特征的分析还可以在不同测量粒度或者不同的层面上展开。

- 比特级（bit-level）流量分析，这种分析主要关注网络流量的数据特征，如网络线路的传输速率，吞吐量的变化等。
- 分组级（packet-level）流量分析，此类分析主要关注的是 IP 分组的到达过程、延

迟、抖动和丢包率等。

- 流级(flow-level)流量分析,flow 的划分主要依据地址和应用协议而展开的,它主要关注流的到达过程、到达间隔及其局部特征。Barakat. C 等人给出的定义是一个由源 IP 地址和端口号、目标 IP 地址和端口号以及应用协议组成的五元组。

上面流量的粒度由小到大递增,时间尺度也逐渐增大,不同时间尺度的网络流量往往表现出不同的行为规律。研究表明:毫秒级的细时间粒度的网络流量行为主要受到网络协议的影响;小时以上的粗时间粒度的网络流量行为主要受到外界因素的影响,而两者之间的秒时间粒度上的网络流量则表现为自相似性。通常,网络设备本身都提供基于 IP 分组头的分析功能。因此,flow-level 的流量分析成为主要发展趋势。

4.3 网络流量分析的典型算法模型

网络流量分析算法可以从不同粒度上进行分类,主要分为:bit-level、packet-level、flow-level、stream-level 四类。下面将依次对这些算法做介绍,其中有些算法模型会在第六章深入讨论,所以在本章只做简要介绍和讨论。

4.3.1 bit-level(超细时间粒度 ms)

4.3.1.1 基于离散小波变换的网络流量分析

近年来,许多关于网络流量特性的研究结果表明,在真实环境中的网络流量呈现出相当明显的尺度特性。网络流量在小时间尺度上呈现出复杂奇异性特征,在大时间尺度上具有长程依赖性(即 LRD 特征)。

常用的小波函数有 Haar 小波、Morlet 小波、Maar 小波等。常见的小波模型均基于 Haar 小波。Haar 小波函数和尺度函数构成了一个简单的小波正交基。Haar 小波的尺度系数和小波系数分别为

$$\psi(t)=\begin{cases}1, & 0\leqslant t<1/2\\ -1, & 1/2\leqslant t<1\\ 0, & \text{其他}\end{cases} \tag{4.1}$$

$$\phi(t)=\begin{cases}1, & 0\leqslant t<1\\ 0, & \text{其他}\end{cases} \tag{4.2}$$

Haar 小波的尺度系数 $U_{j,k}$ 和小波系数 $W_{j,k}$ 有如下关系:

$$\begin{aligned}U_{j,k}&=2^{-1/2}(U_{j+1,2k}+U_{j+1,2k+1})\\ W_{j,k}&=2^{-1/2}(U_{j+1,2k}-U_{j+1,2k+1})\end{aligned} \tag{4.3}$$

据此有

$$\begin{aligned}U_{j+1,2k}&=2^{-1/2}(U_{j,k}+W_{j,k})\\ U_{j+1,2k+1}&=2^{-1/2}(U_{j,k}-W_{j,k})\end{aligned} \tag{4.4}$$

通过用这样的方法来处理离散信号 $X(k)$,并假设 $X(k)$ 的长度为 $2n$,从而 $X(k)$ 与最精细尺度系数关系如下:

$$X(k) = 2^{-n/2}U_{n,k}, \quad k = 0,1,\cdots,2^n - 1 \tag{4.5}$$

从上面的分析可以看到，小波变换具有对信号的自适应性，能够保持分析对象的尺度不变性。由于网络流量的自相似性是在统计意义上具有尺度不变性的一种随机过程，因此，小波变换在数学上具有其特有的优势，下面的小波模型都是建立在对网络流量多尺度分析的基础上。

通过分析流量过程的小波系数的分布特性，可以对网络流量进行分析，为网络流量建模打下基础。

对于一维离散采样信号，Haar 小波变换相当于进行差分运算。

以 $a^j(k)$表示其在第 j 层的尺度系数、$d^j(k)$表示第 j 层的小波系数，Haar 小波变换的系数的递推公式为

$$\begin{aligned} a_X^j(k) &= 2^{-1/2}(a_X^{j+1}(2k) + a_X^{j+1}(2k+1)) \\ d_X^j(k) &= 2^{-1/2}(a_X^{j+1}(2k) - a_X^{j+1}(2k+1)) \end{aligned} \tag{4.6}$$

则

$$\begin{aligned} a_X^{j+1}(2k) &= 2^{-1/2}(a_X^j(k) + d_X^j(k)) \\ a_X^{j+1}(2k+1) &= 2^{-1/2}(a_X^j(k) - d_X^j(k)) \end{aligned} \tag{4.7}$$

4.3.1.2　基于离散小波变换的多重分形模型

多重分形为描述信号在小尺度上的奇异性提供了良好的数学框架，而小波变换对具有长程依赖性的信号起到了去相关的作用，所以在时域里难以分析和建模的 Internet 网络流量过程在小波域里就变得相对容易了。因此，多重分形模型(DWMM)应运而生。通过分析流量过程中小波系数的分布特性，研究者建立了基于 DWT 的新的多重分形模型(DWT multifractal model，DWMM)。

在建立该模型时，要保证尺度系数的非负性，需要满足条件：$a^j(k) \geqslant |d^j(k)|$。当引入一个尺度因子 $\mu^j(k) = d^j(k)/a^j(k)$后，尺度系数非约束条件就变为：$|\mu^j(k)| \leqslant 1$。通过对系数$\{\mu^j(k)\}$分布特性的研究，就可以建立起相应的流量模型。

(1) DWMM 的分析过程如下：

① 设离散序列$\{X^0(k),\ k=0,1,\cdots,2^N-1\}$代表初始的流量数据；

② 对$\{X^0(k)\}$进行 Haar DWT 分解得到相应的尺度系数$\{a^j(k)\}$和小波系数$\{d^j(k)\}$；

③ 计算每一层的尺度因子$\{\mu^j(k) = d^j(k)/a^j(k)\}$，并分析其分布特性；记录最大尺度上的尺度因子 $u^N(0) = d^N(0)/a^N(0)$以及 $a^N(0)$；

④ 根据分析结果，尺度因子$\{u^j(k)\}$在不同的尺度上的分布特性也都近似于零均值的高斯正态分布(尺度越大则越与正态分布吻合)，所以其分布特性就可以用标准差 std(j)以及相应的上下限 $\mu_{\max}(j)$和 $\mu_{\min}(j)$描述。

(2) DWMM 的流量合成过程如下：

① 从最大尺度 $j=N$ 开始，根据 $\mu^N(0)$和 $a^N(0)$可以求出 $d^N(0)$，然后再利用式(4.6)计算出$\{a^{N-1}(0), a^{N-1}(1)\}$；

② 尺度 $j=N-1$：产生标准差为 std(j)的零均值高斯随机数($\mu^j(k)$)，其取值范围为