文章编号:1001-2486(2007)03-0093-05

基于网络监测技术的电信级IP宽带网络研究与实践*

赵 勇
(湖南大学 计算机与通信学院,湖南 长沙 410005)

摘 要:随着数据业务的飞速发展,如何保证宽带IP网络高可靠、高性能、可运营和可管理变得至关重要。针对电信级IP宽带网业务与运维需要,在详细分析IP协议特点的基础上,剖析电信级IP网络提供服务质量保障业务与网络运维面临挑战。为了满足电信级IP网络规划设计、运维管理、提供增值业务的需求,提出网络监测指标体系。结合当前的网络监测技术,提出了基于分布式网络监测分析技术的电信级IP宽带网络的构建方案。该方案已经得到湖南电信实验局验证。

关键词:IP宽带网;网络监测;指标体系
中图分类号:TP390 文献标识码:B

Research on Carrier-class IP Broadband Network Based on Network Measurement and Monitor Technologies

ZHAO Yong
(Institute of Computer and Communication, Hunan Univ., Changsha 410005, China)

Abstract: With the rapid development of digital applications, it is crucial to guarantee the reliability, high-power, operatability and manageability of IP broadband network. According to the requirements of carrier-grade IP broadband network, based on the detailed study of IP protocol, the challenges of carrier-grade IP broadband network on the aspects of service quality, which guarantee the network operation, were analyzed. To satisfy the requirements of network design, operation management and increment businesses, a metrics system is proposed. Then, combined with existing measurement methods, a solution to building carrier-grade IP broadband networks based on network measurement and monitor was proposed.

Key words: IP broadband network; network measurement; metrics system

随着网络应用的不断发展,IP数据包交换网络逐渐替代以电路交换为特征的传统网络,在今后几年内,宽带业务(例如视频电话、视频点播等)将会以较快的速度增长。随着IP宽带网网络规模的不断扩大,并且因新的网络设备、不同流量模型的业务等使得网络日益复杂,人们日益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。建立网络与业务行为模型,是提供电信级宽带网网络容量规划、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。如何使IP宽带网络成为承载关键业务的电信级网络面临巨大的挑战。

宽带网发展迅速,市场竞争激烈,如何构建建立高效、稳定、安全、可靠、互操作性强、可预测的网络,以提高对用户的吸引力,提高用户的忠诚度,降低运营成本,在宽带接入市场中占据优势地位,是宽带接入快速发展阶段的重要课题。传统的网络监控方法已经不能适应高速发展的宽带网的需求,建立一个不同时间刻度、不同信息粒度宽带网络测试的监控平台是非常必须的。

1 电信级IP宽带网络要求

1.1 拓扑设计

IP宽带网骨干网络典型地由高速链路连接汇聚点而成,连接链路由汇聚点间的流量交换矩阵确定,例如在两个流量比较小的汇聚点间增加一条链路,则对网络性能影响非常小;反之,在业务繁忙的汇

* 收稿日期:2006-10-30
基金项目:国家863高技术资助项目(2002AA121032);国家自然科学基金资助项目(60403031)
作者简介:赵勇(1956—),男,高级工程师,博士。

聚点间增加高速链路,将极大地减少业务端到端延迟。汇聚点间的业务流可以通过流量矩阵(traffic matrix)指标获得,流量矩阵表示网络的接入链路(ingress point)/输出链路(egress point)与其他网络交换的业务流,目前一般基于各个链路流量的路由信息,根据统计理论可以推测网络的流量矩阵。测量不同时间粒度、不同级别汇聚链路的流量指标是非常重要的。IP 骨干网络必须满足丢包(packet loss)、延迟(delay)、有效性(availability)等严格要求,精确分析数据包通过单个路由器的延迟/丢包等指标对于估计路径延迟/丢包等端到端的性能是必要的。类似地,只有明确流量突发与路由器处理突发的能力,才可以计算缓存的能力。尽管路由器性能可以在实验室测试环境下进行评估,在实际运行网络中,实际业务流量下的测量数据将为网络设计提供更为科学的设计依据。即使在设备故障发生、软件配置故障、大规模突发流量情况下,网络提供商也希望能够为客户提供可预期的服务质量,因此理解在发生故障情况下的网络动态变化(network dynamics)对于更好地保护网络是非常有价值的。另外,网络必须要求容错发生的短期故障(例如路由器崩溃、软件 Bugs、配置不准确等)、网络故障容错及其恢复的基础是特征化网络事件的频率、特征与影响(例如路由协议收敛时间),这些指标必须通过收集路由器记录、路由更新消息、数据包协议分析等获得。

1.2 容量规划与预测

流量测量与路由信息是高效容量规划的关键,例如通过测试可以获悉网络瓶颈链路,通过升级该链路或者重新规划路由可以消除该瓶颈链路,从而避免网络拥塞。

有效的容量规划除了流量测量以外,必须要求精确的流量增长预测,不准确的流量预测将导致网络在容量浪费与容量不足之间振荡,因而影响性能预测。基于历史流量数据的统计预测过程是预测流量变化的主要方法,不同时间粒度的流量指标是不同流量预测的基础。

1.3 网络运行与管理

网络管理人员负责宽带网的运行与管理,其主要任务包括两个方面:

(1) 流量工程:流量工程的目标是在传输业务时,优化资源利用率,提高应用性能。网络传输的流量与网络路由策略密切相关。例如 ISP 使用链路状态协议(如 IS-IS、OSPF)作为域内路由协议,链路的负载是设置 IS-IS 链路权重的主要参考依据,同样,流量测量也可以显示链路权重的改变对流量的影响。网络测试将帮助管理人员阻止不期望的网络流量,例如 ISP 一般不希望自己的网络成为其他对等 ISP 的中间传输路径,通过按照输入/输出链路、BGP 前缀,网络管理员可以快速分辨并阻断不期望传输的流量。流量测量可以作为流量工程的输入指标,监测分析流量的突变与不稳定。对于日常的流量模式正常流量波动,网络管理员可以根据流量波动模式进行前摄控制(例如在不同的时刻设置不同的链路权重);对于非预期不可控制的变动,例如相邻域的突然拥塞,网络管理员可以将拥塞链路的流量导向负载较小的路径。

(2) 故障诊断与调试:网络管理员的主要职责是鉴别、诊断和修复网络日常故障,详细、及时地测试网络运行状态,分析故障成因并采取正确的应对措施。当前网络管理员对故障管理是被动的,网络测试不仅可以加速故障响应,而且可以在客户发现故障之前采取前摄性的动作。例如,跟踪在链路中传输的数据包可以跟踪与停止 DoS(denial of service)攻击,分析数据包的传输路径可以检查路由器与路由协议是否正确配置。

1.4 提供增值业务

(1) SLA 业务(service level agreements):目前大部分 SLA 指标包括丢包、延迟与链路有效性,丢包与延迟是长时间(例如 1 个月)的网络范围指标,链路有效性指客户连接到 ISP 的连接链路(通常为 ISP 的路由器接口)。缺乏进一步的 SLA 指标的原因是缺乏合适的基础设施来测量流量和为相关的 SLA 指标提供证据。许多运营商经常对抱怨网络故障的用户提供赔偿的方式,并用不同的赔偿方式区分不同的 SLA 业务。尽管客户赔偿的方式可以提高用户的满意程度,但是它将减少运营商的收入,因此运营商必须通过有效的网络运营满足用户的 SLA 指标,并且通过连续、细节性的网络测量精确测定 SLA 相关指标。当前网络运维人员往往采用标准的 Ping、Traceroute 或者其他的一些主动探测工具来测量丢包、延

迟等指标,这些简单的测试方法对测试服务有效性以及不同时间粒度、指标变化等细节统计指标是远远不够的。可以预计,在不久的将来,客户将要求运营商提供端到端的延迟、丢包、服务有效性等统计指标,因此必须研究更加科学的测试方法、部署更加有效的测试分析平台,例如被动采样技术等。

(2) 攻击阻断:客户经常要求宽带网运营商能够阻断发自本网络的 DoS 攻击,并且能够检测攻击发起源。目前,网络管理员在接到客户受到可能的攻击报告时,将采用阻断所有用户流量的方法防止攻击,采用这种方法将使得用户服务完全停止。被动测试方法可以通过捕获数据包并进行协议解析,监测攻击源。在网络测试系统的支持下,网络管理员将基于 BGP 前缀或者链路对可以实时监测业务流,建立业务流的流量模型,通过业务流的异常检测进行攻击预警。

(3) 流量工程实施:宽带网运营商在提供客户 SLA 报告时,经常包含客户业务流量 Hop 数、路径延迟、出口链路等指标,这将有利于客户验证业务在传输中的延迟。例如用户租用运营商的链路建立 VPN (virtual private network),需要知道各个点交换流量矩阵,以在保证性能的情况下,规划租用链路带宽。客户可以通过在本身的网络上安装流量检测系统的方法进行流量统计分析,或者通过发送探测数据包的方法检测宽带网络性能,但往往需要客户具有网络专业背景知识。运营商提供这些指标将提升客户的满意程度。

2　网络监测指标及应用

为了满足不同用途,宽带网运营商需要采集不同的测试指标。

数据包级(packet-level):捕获链路中传输的 IP 数据包或者数据包头,通过高效的协议分析,检测数据包协议分布、链路传输质量等指标。数据包级测试的关键是在采集数据包时,在数据包中加上精确的时间戳。

流级(flow-level)[1]:流是相同属性数据包的集合,通常采用"源地址 - 目标地址 - 源端口号 - 目标端口号 - 协议"(source IP address—destination IP address—source port—destination port—protocol number)五元组来描述流。流级指标包括流中数据包指标(例如目标端口、目标地址等)与数据包推导指标(例如流容量、持续时间、强度等)。流级指标是数据包级指标的汇聚,通过流级数据包内的指标,例如数据包间隔、延迟、延迟抖动等,可以检测业务的 QoS(quality of service)。

路由(routing):主要包含路由器间交换的路由信息与路由器中路由表快照,通过采集路由信息(包括内部路由 IS-IS、OSPF、I-BGP,或者外部路由信息 BGP),可以分析路由稳定性、病态路由等路由行为,更好地进行路由规划[2]。

路径级(path-level):路径级性能对于端到端的业务性能是至关重要的,包括的指标有路径本身的信息(例如 Hop 数)与路径服务质量(例如丢包、延迟、抖动、有效带宽、瓶颈带宽)[3]。

网元级(network element-specific):网络中网元相关指标,例如链路利用率、路由器配置、路由器 CPU 利用率等,一般可以利用 SNMP 收集网元信息。

综上所述,网络运营中需要观测两种类型的指标:大时间刻度的汇聚信息指标与较小时间刻度的数据包级细粒度指标,因此在网络运营支撑系统中必须综合实施不同时间精度的测试。

(1) 在全网范围内实施相对大时间刻度的(min、h)汇聚统计指标(metrics of aggregated statistics)的采集,例如包括链路平均利用率、路由器 CPU 负载等网元级的指标,周期性路由表更新等路由指标以及从数据包级统计分析得到的各种信息(如从分析 IP 数据包头得到数据包大小分布)。利用数据包协议分析技术进行流测试,分析流的汇聚统计指标也经常被应用。流性能指标被周期性地输出到中央采集工作站,从而避免数据包级测试产生大测试流量的缺陷。汇聚统计指标对于监视全网性能与检测异常行为是足够的,可以提供网络管理员全网运行状态的视图。

(2) 从指定的网元中采集高精度的指标。通过数据包捕获与线速协议分析,深度分析网络故障。数据包级指标的测试关键是高性能的采集分析系统,特别在高带宽的链路中,数据包级测试必须依赖高性能的处理器、ASIC、采样技术、高效协议分析技术以及数据存储技术来完成。

3 基于网络监测技术的电信级IP宽带网络构建方案

3.1 IP宽带网络监测系统

一个可行的宽带网络监测系统,必须能够为宽带网络的构建提供可靠、准确的依据和模型[4-6]。结合当前的网络测试技术,网络监测系统必须具有以下功能和特点:

(1) 运用SNMP技术,对所管理的网络进行自动的拓扑发现,并以直观的方式显示,这样网络管理员可以直观地了解和掌握网络拓扑结构以及网元的相对位置。

(2) 实现各种级别(数据包级、流级、路径级和网员级)的监测,为网络性能的分析提供实时和准确的网络运行信息。

(3) 结合各种测试技术(被动测试、主动测试、业务仿真测试),对网络进行全面的监测,为网络性能分析提供尽量多的有用信息。

(4) 对采集的网络运行信息做快速和准确的分析,并以直观的形式显示给网络管理员。分析主要包括:

① 数据包级的协议分析,检测数据包协议分布、链路传输质量等指标。

② 流级的指标分析。流级指标是数据包级指标的汇聚,流级指标包括流中数据包指标(例如目标端口、目标地址等)与数据包推导指标(例如流容量、持续时间、强度等)。通过流级数据包内的指标,例如数据包间隔、延迟、延迟抖动等,检测业务的QoS(quality of service)。

③ 路径级分析主要包括分析路径本身的信息(例如Hop数)与路径服务质量(例如丢包、延迟、抖动、有效带宽、瓶颈带宽)。

④ 网元级分析网络中网元相关指标,例如链路利用率、路由器配置、路由器CPU利用率等,这些信息一般通过SNMP技术获得。

(5) 当网络运行出现故障时,快速定位故障源,并给出推荐的解决方案。

(6) 当网络中某个设备或者链路状态超过了网络管理员所设置的阈值或者呈现某种异常趋势时,向管理员告警,并给出异常源和推荐解决方案。

(7) 通过网络测量、测试与管理技术,监控网络运行状态,提供运营商之间、运营商与用户之间完整的SLA指标体系,量化现有网络能力与业务能力,为制定SLA服务规范、服务流程、建立SLA服务保障机制提供科学的决策机制。

(8) 解决传统网管系统以网络设备为主要管理对象的局限性,真正站在用户的角度进行端到端用户业务监测。

(9) 监测系统中的测试探针需要分布在网络业务的汇聚点,实现分布式的测试。而对各种采集和测试所得信息统一地由控制分析中心分析。

(10) 分布的测试探针需要具有高性能的网络处理器,并提供各种高速接口。

(11) 监测分析系统本身必须稳定,具有很高的容错能力和可靠性。

3.2 监测系统的部署

IP宽带网监测系统采用分布式采集、集中式分析架构,系统由两个组件构成:网络探针和网络控制分析中心。探针的主要功能是从综合信息网网元处采集实时的流量信息、从网管系统收集网管数据及进行端到端的性能测试。信息采集探针由分布于综合信息网的流量采集探针、端到端性能测试探针和基于各级网管系统的网管探针组成,可进行实时的流量监视和测量。网管探针是驻留在网管系统的软件模块,主要是将网管系统的各种数据上传至监测分析系统。探针根据用户配置需求定时向控制分析中心发送测试结果数据,并可进行本地测试结果数据存储。控制分析中心功能包括自动网络拓扑发现与设备管理、轮询和接收探针测试结果、SNMP轮询与Trap信息接收、实时事件关联与后台历史数据专家分析,提供全面的网络操作监视平台。网络探针分布于网络业务的汇聚点、接入层和骨干网络上,这样就可以对网络的各级运营情况进行高效而准确的采集;而集中的控制分析中心为方便的网络管理提

供了基本的保证。监测系统可按照图 1 所示来部署。

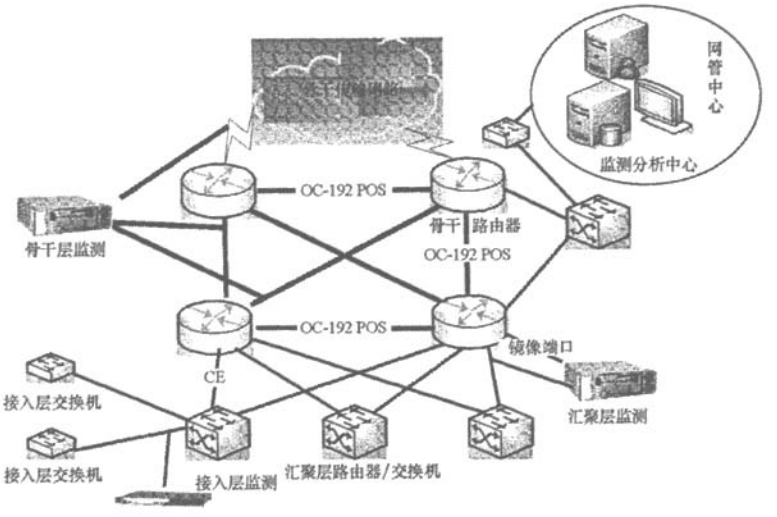

图 1　IP 宽带网络监测系统

Fig.1　IP boardband network measurement system

IP 宽带网络监测系统不仅能够独立地进行数据的采集和分析,而且还需要通过适当的方式(比如通信 API 等)为其他系统如 BSS/OSS(business support system/operation support system)等提供指标的查询并可以接受这些系统的管理。图 2 说明了监测系统与其他系统共享数据的逻辑结构。

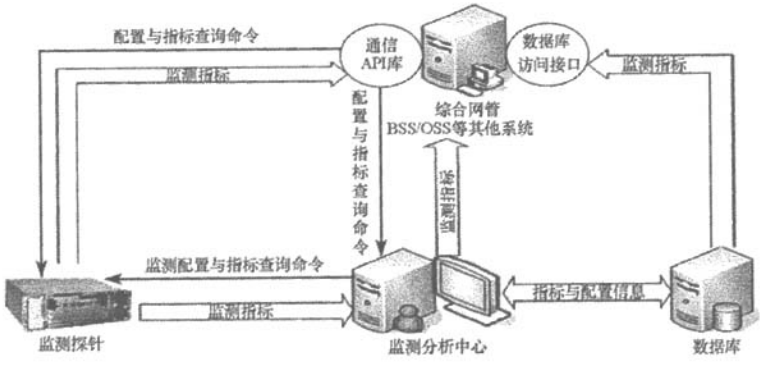

图 2　IP 宽带网络监测系统与其他系统数据共享

Fig.2　Correlation of IP measurement system with the other system

4　结束语

针对电信级 IP 宽带网业务与运维需要,分析了电信级 IP 网络提供服务质量保障业务与网络运维面临挑战,提出了网络监测指标体系。结合当前的网络监测技术,提出了基于分布式网络监测分析技术的电信级 IP 宽带网络的构建方案。

参 考 文 献:

[1] Brownlee N, Mills C, Ruth G. Traffic Flow Measurement: Architecture[R]. RFC 2722, October 1999.
[2] Laboviz C. Multithreaded Routing Toolkit-final Report to the National Science Foundation[R]. Merit Network Inc., Technical Report(MERIT-960501),1996.
[3] Cerf V G. Guidelines for Internet Measurement Activity[R]. RFC1262. October 1991.
[4] Case J D, Fedor M, Schoffstall M L, et al. Simple Network Management Protocol (SNMP)[R]. RFC, May 1990.
[5] 马维雯,李忠诚,叶晨.一种分布式的被动测量系统设计[J].计算机应用研究,2004,21(10).
[6] Bhattacharyya S, Iannaccone G, Moon S, et al. Network Measurement and Monitoring: A Sprint Perspective[R]. draft-ietf-monitoring-sprint-03.txt, 2003.