基于 WSDM 的校园网流量监测系统设计与实现

左 靖，王海龙，杨奔全
(张家界航空工业职业技术学院 信息系，湖南 张家界 427000)

摘 要：设计了一种基于 WSDM 的校园网流量监测系统。以校园网为实验环境，设计并实现了该流量监测系统的原型。通过测试结果分析，证明该系统比传统流量监测系统具有更多的流量采集方式，更好的松耦合性，更容易进行扩展以及服务管理，对基于分布式计算的网络管理系统模型的开发和设计有较好的借鉴价值。

关键词：Web 服务分布式管理；校园网；流量监测；网络管理
中图分类号：TP393 **文献标识码**：A

Design and implementation of campus network traffic measurement system based on WSDM

ZUO Jing, WANG Hai Long, YANG Ben Quan
(Department of Information, Zhangjiajie Aviation Industry Vocational and Technical College, Zhangjiajie 427000, China)

Abstract: In this paper, a campus network traffic measurement system based on WSDM is designed. Under the environment of campus network, this paper designs and implements a traffic measurement prototype. Through analysis of test results, it is proved that this system has more methods of traffic collection, and all module parts of the system are more loosely coupled, and is easier to do expansion and service management. Moreover, this system can be used for designing the network management system model based on distributed computing.

Key words: WSDM; campus network; traffic measurement; network management

以 Internet 为代表的信息网络是现代信息社会最重要的基础设施之一，它已渗透到社会生活的各个领域，并成为学校教育中资源共享、信息交流的必要网络平台，因此，校园网的网络管理越来越受到广泛关注。

流量监测正是网络管理的前提和基础。从网络体系架构分析，网络流量是一切研究的基础，它能直接反映网络性能的好坏，更能帮助判断网络故障及网络安全等状况[1]。目前的校园网具有以下特点：(1)覆盖范围广，一般都要跨越多个校区；(2)使用的网络设备多样，例如服务器（DNS 服务器、MAIL 服务器、WWW 服务器等）、交换机、路由器等；(3)网络设备的生产厂家各异。这些都给网络流量监测带来了很大的困难。同时，现有的流量监测系统存在如下问题：(1)市场上的网管软件(例如 SunNet Manager、OpenView 和 NetView) 虽然管理功能完善，但价格比较昂贵，而且为了充分发挥功能需要二次开发[2]；(2)采集手段单一，通常只使用 SNMP 模式[3]；(3)分析方法简单，所得的分析结果不能为网络性能分析和安全监控提供充分的参考。因此，本文设计了一种基于 Web 服务分布式管理 WSDM (Web Service Distributed Management)的校园网流量监测系统。

1 系统设计

面向服务架构(SOA)是一种软件体系结构的思想，它需要依赖具体的实现技术。本文采用 WSDM 标准[4]来支持面向服务架构(SOA)的实现。WSDM 是一个用于描述特定设备、应用程序或者组件的管理信息和功能的标准。所有描述都是通过 Web 服务描述语言 WSDL(Web Services Description Language)进行的。WSDM 标准实际上由 WSDM-MUWS、WSDM-MOWS 两个不同的标准组成。

网络流量监测有主动监测和被动监测 2 种不同的实现方法[5]。由于主动测量方法的不足，本系统采用被动监测技术。网络流量采集使用 3 种技术：(1)基于网管设备 MIB 的 SNMP 模式；(2)基于网络探针技术的 IP 流量数据捕获模式；(3)基于 NetFlow 技术的数据流捕获模式。针对基于 SNMP 模式的技术，可以参考文献[6]实现的基于 WSDM 的 SNMP 网关，通过该网关收集 SNMP 设备上的 MIB 信息；针对基于网络探针技术模式，可以参考文献[7]实现的基于 WSDM 的网络探针服务；针对基于 NetFlow 技术模式，也可以参考文献[7]，但流量数据

是通过 NetFlow 的主动式数据推送机制获得的，网络设备中的 NetFlow 代理通过规范的报文格式将流量数据送往指定主机(须事前指定 IP 地址、协议和端口)，因此，WSDM 服务提供了接收和传输 NetFlow 流量数据的功能。3 种采集流量的 WSDM 服务(SNMP 网关、网络探针服务以及 NetFlow 的相关服务)都可以称作流量采集器或者 WSDM Agent。

1.1 总体架构

本文设计的校园网流量监测系统在体系结构上划分为 3 个层次，由底至上依次为资源层、管理服务层、展示层，如图 1 所示。

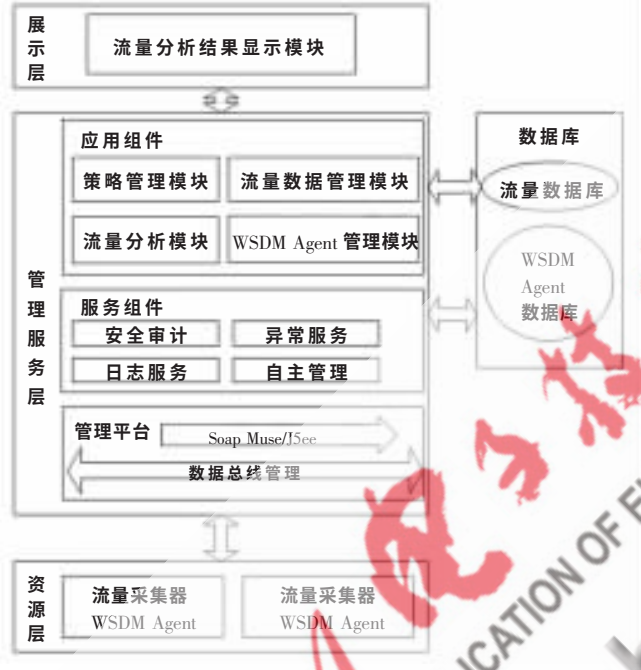

图 1 系统架构

1.1.1 资源层

资源层包括提供流量采集服务的分布式流量采集器 WSDM Agent，它们通过调用管理服务层的 WSDM Agent 注册服务实行自主注册，具备向管理服务层主动汇报、自主管理和主动服务等功能。进行流量采集时的方法各异，结构也不尽相同，但是对外包装成统一的 WSDM 服务接口，可以方便地通过管理服务层对 WSDM Agent 进行管理。

1.1.2 管理服务层

管理服务层包括应用组件、服务组件、管理平台以及数据库。其中，应用组件是对展示层提供支持的各种管理服务，包括策略管理模块、WSDM Agent 管理模块、流量数据管理模块以及流量分析模块等系统功能实现的模块。服务组件是对资源层的各种 WSDM Agent 资源的支持，包括安全审计、日志服务、异常服务、自主管理等，主要是管理服务器自主实现的一些功能。数据库部分是应用组件中各模块对应的数据存储。中间层的管理平台是管理服务层的核心，是对应用组件、服务组件以及数据库的支持，包括 Web 服务、WSDM 服务的引擎和 API 等。

策略管理模块：主要是底层流量采集器 (WSDM Agent)的使用策略以及流量采集策略的管理。

WSDM Agent 管理模块：为合法的流量采集器(WSDM Agent) 提供注册以及更改 WSDM Agent 运行状态服务，再根据 WSDM Agent 的使用策略调用符合条件的 WSDM Agent 提供的流量采集服务。WSDM Agent 开发人员可以将新开发的服务通过 WSDM Agent 管理模块注册发布到管理服务层，从而方便地实现系统扩展开发。

流量数据管理模块：对资源层送来的流量数据进行融合处理，为流量分析模块提供原始的流量数据，并写入原始流量数据库中；通过对网络原始流量数据的分析得到整个网络的流量统计信息，并将该统计结果存入流量统计结果数据库中，为展示层的流量时空状态显示模块提供态势展示数据。

流量分析模块：对采集到的网络原始流量数据进行完整的测量数据统计和分析，进行网络带宽分布分析、网络瓶颈分析、网络流量异常分析、网络应用流量监测等，对网络健康状况及未来的发展趋势做出准确判断。

1.1.3 展示层

展示层包括流量时空状态显示模块。该模块可以从流量数据库中取得所要查询的网络流量历史信息，也可以调用管理服务层提供的服务触发流量信息更新采集实时的流量数据，还可以通过服务将合法用户的操作信息送到管理服务层，根据用户需求采用图形用户界面 GUI 将流量态势分析的结果展示出来。提供包括实时报表、日报表、周报表、月报表等多种格式的流量报表，还可以以直方图，二维、三维坐标曲线，扇形图等形式向用户展示实时的网络链路流量信息以及大规模网络流量态势分析的结果。

1.2 物理视图

系统的物理部署情况如图 2 所示。由于系统采用 3 种方式进行流量采集，因此，针对 SNMP 设备则使用 SNMP

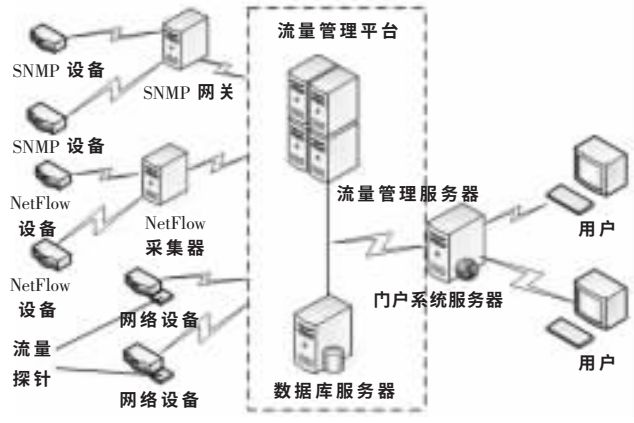

图 2 系统物理视图

网关（采集器），针对 NetFlow 设备则使用 NetFlow 采集器。另外还部署了网络探针(采集器)，这些采集器都部署在网络的核心节点或关键链路处，将通过路由器或交换机采集到的原始流量数据发送到流量管理平台，流量管理服务器及流量数据库服务器进行交互，对分布式的网络流量数据进行分析与处理，并将原始的流量数据与统计分析之后的态势数据存入流量数据库中，门户系统服务器通过调用流量管理平台提供的服务满足用户的查询请求。

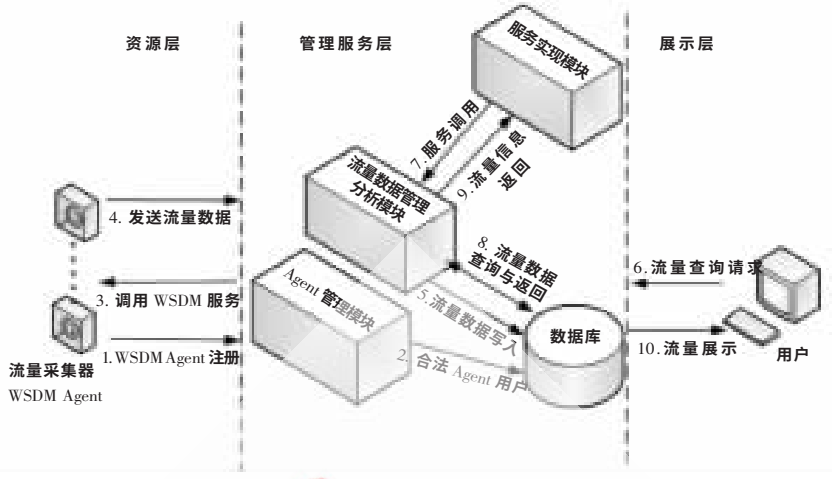

图 3 系统处理视图

1.3 处理视图

系统的处理视图如图 3 所示。具体的处理流程如下：

(1) 流量采集器 (WSDM Agent) 通过调用管理服务层对合法 WSDM Agent 提供的注册服务进行注册。

(2) 合法 WSDM Agent 的注册信息写入流量 WSDM Agent 注册数据库，此时表明该 WSDM Agent 正常工作。

(3) 管理服务层按照流量采集器(WSDM Agent)使用策略调用已注册 WSDM Agent 的服务。

(4) 流量采集器(WSDM Agent)返回采集的流量数据。

(5) WSDM Agent 送来的流量数据经过流量数据管理模块与流量分析模块的交互处理后，将经过融合处理的分布式流量数据以及得出的统计分析数据写入流量数据库。

(6) 用户进行流量查询请求。

(7) 服务实现模块将用户的请求转换成对流量数据管理模块和流量分析模块的服务调用。

(8) 流量数据管理与流量分析模块从流量数据库中查询得到用户请求的流量数据。

(9) 服务实现模块得到所请求的流量数据。

(10) 服务实现模块将请求的流量数据送到位于展示层的流量时空状态显示模块中，将流量信息展示给用户。

1.4 流量分析系统架构

流量分析系统是整个流量监测系统的核心，其系统架构如图 4 所示。该架构分为 5 个模块：流量采集模块、数据接收模块、数据传输模块、流量分析模块、数据存储与管理模块。由流量监测系统总体架构可知，流量分析系统结构中的这 5 个功能模块分别位于总体架构的各个层次。

位于资源层中的流量采集模块和数据接收模块，通过网络数据流采集技术采用某种机制(例如基于 NetFlow 的流信息数据采集）实现分布式的网络流量数据的采集，构成流量采集器(WSDM Agent)；然后由数据传输模块负责将这些分布式的流量采集器(WSDM Agent)采集到的原始流量数据上传至位于管理服务层的流量管理平台中；由流量管理平台中的流量分析模块对这些分布式的网络流量数据进行全网络的 OD 流[8]的计算，之后对 OD 流进行进一步的统计和分析判定，提供包括确定网络关键链路、瓶颈节点、识别网络中的大象流及判定异常流等功能，并将得到的这些分析统计结果保存到流量数据库。流量数据库由数据存储与管理模块进行维护。该模块设计为存储网络实时流量和历史流量数据以及统计分析结果数据，由流量管理平台中的流量数据管理模块将资源层发送上来的经过预处理的原始流量数据保存到该模块所属的原始流量数据库中。

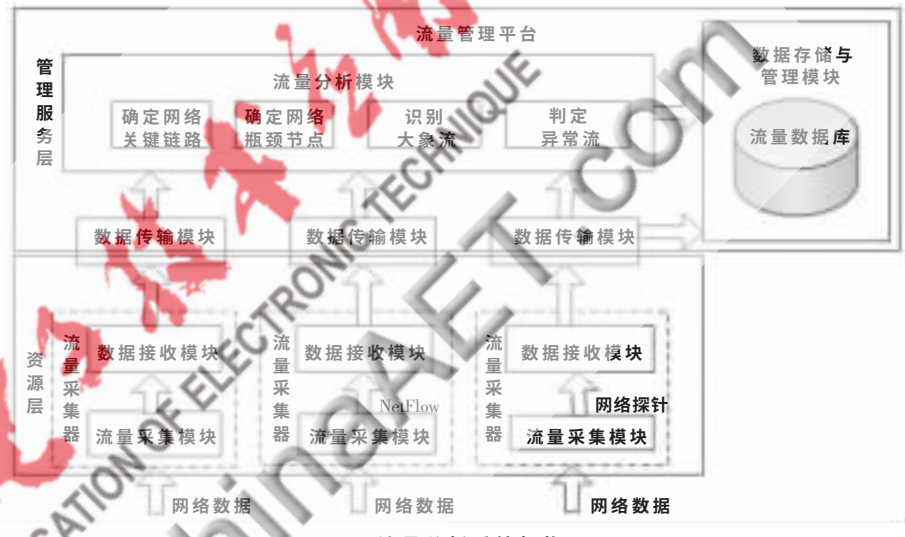

图 4 流量分析系统架构图

2 系统实现

2.1 系统实现的关键技术

本文设计的校园网流量监测系统相对于传统的系统，没有采用面向服务架构的监测系统，具有更好的松

耦合性，并且更容易进行扩展。为了进一步验证其可以应用于现实的校园网流量监测中，并验证所设计系统的创新性与实用性，本文基于校园网实现了一个原型系统。实现中涉及的关键技术如下：

(1)基于 Glassfish 平台的 Agent 服务开发技术。Glassfish 是 Sun 公司新推出的一款 Java EE 服务器，与 Tomcat 相比，Glassfish 服务器拥有延迟加载、动态映射等技术，并且与其他商用组件和开源组件具有很好的兼容性，所以在 XML 处理以及 Web Service 方面有很大的优势。

(2) 基于 Apache Muse 的 WSDM Agent 开发，将流量采集功能包装成标准的 WSDM 服务。Apache Muse 通过 Java 实现了 WSDM 规范，用户可以使用它为可管理的资源创建 Web 服务接口。基于 Muse 建立的应用程序可以部署在 Java EE 环境中。

(3) 将 WSDM Agent 注册模块集成到 Glassfish 平台中，这个过程修改和调用了 Glassfish 的内部相关接口。

(4) 流量分析模块中确定关键链路、确定瓶颈节点、识别大象流以及判定异常流的相关方法的实现。

(5) 流量数据库的数据存储以及分析结果显示技术。采用基于 JDBC 的数据库连接进行流量数据的存储以及显示。

2.2 运行测试

首先测试系统中流量分析模块实现的确定网络关键链路、识别大象流、判别异常流 3 种功能。流量分析模块采用 Perl 语言编程实现，可以同时在 Windows 系统或者 Linux 系统上运行，运行结果先输出为文本文件，后导入 MySQL 数据库中。图 5~图 7 展示了系统中流数据分析模块的运行效果。

图 5 关键链路测试

图 6 识别大象流测试

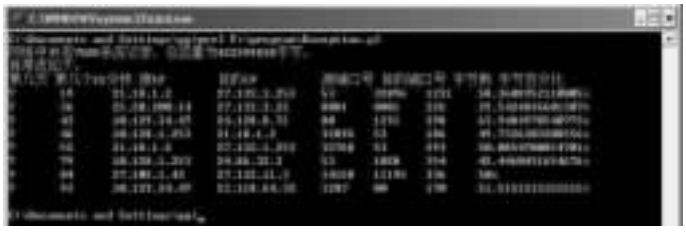

图 7 判别异常流测试

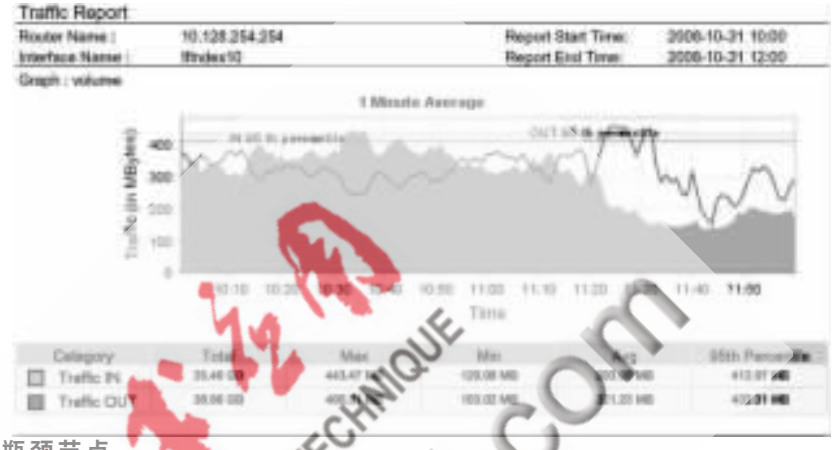

图 8 路由器接口流量

图 8 是对校园网中 IP 地址为 10.128.254.254 的 Router 的 IfIndex10 接口的流量监测服务的测试报告图。测试时间为 2008 年 10 月 31 日，上午 10 点至 12 点，图中显示出该路由器接口的流量。该流量测试报告显示了网络实时流量随时间变化的状态，在该时间段内，流入该接口的网络流量最大值为 443.47 MB，平均值为 293.09 MB，流出该接口的最大网络流量值为 460.31 MB，平均值为 321.23 MB。

本文设计的基于 WSDM 的校园网流量监测系统，不仅能够通过多种手段采集流量数据，而且具有确定关键链路、确定瓶颈节点、识别大象流以及判定异常流的流量分析功能，为流量控制提供了有价值的参考信息。同时，由于系统各部分松耦合，WSDM 标准提供了统一的方式来访问被管资源，能满足分布式环境下对象处理的可靠性、可重用性和位置透明性要求，所以该系统模型能很好地适用于分布式环境下的网络管理[9]。下一步将设计并实现一个流量控制系统，针对流量监测系统的分析结果，对校园网流量进行管理，进一步提高校园网的网络性能。

参考文献

[1] 关卿.分布式网络流量数据分析与管理技术研究与实现.国防科学技术大学硕士学位论文，2008.

[2] 赵新元，王 能.基于 Web 的网络流量监测系统的设计.计算机工程，2007,33(3).

[3] 崔金玲，闫娟.基于 SNMP 的校园网网络性能管理系统的实现.河南师范大学学报(自然科学版)，2007，35(1).

[4] OASIS.WSDM.TC,http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsdm, 2008-04-25.

[5] 张卫东, 王伟, 韩维桓.网络流量测量与监控系统的设计与实现[J].计算机工程与应用, 2005(7):14-15.

[6] 杨岳湘, 刘蓉, 唐川.面向SNMP代理的WSDM转化网关研究. CNCC2007, 全国计算机大会, 2007.

[7] 殷泰晖.网络流量探针的关键技术研究. 国防科学技术大学硕士学位论文, 2007.

[8] JUVA I, KUUSELA P, VIRTAMO J. A case study on traffic matrix estimation under Gaussian distribution. In: Proc. of the 17th Nordic Teletraffic Seminar, 2004:49-60.

[9] 何明, 龚正虎, 卓莹.基于WSDM Agent的分布式拓扑发现系统设计与实现[C].计算机技术与应用进展2008, 合肥:中国科学技术大学出版社, 2008:1286-1291.

(收稿日期:2009-03-04)

APPLICATION OF ELECTRONIC TECHNIQUE
www.chinaAET.com