本文引用格式：谭志勇,林艳华,顾家铭.融合 Zabbix 和 SNMPv3 的网络流量监控方法[J].自动化与信息工程,2025,46(3):52-57.
TAN Zhiyong, LIN Yanhua, GU Jiaming. Zabbix-SNMPv3 integrated network traffic monitoring approach[J]. Automation & Information Engineering, 2025,46(3):52-57.

融合 Zabbix 和 SNMPv3 的网络流量监控方法*

谭志勇　林艳华　顾家铭
（武汉软件工程职业学院（武汉开放大学）信息化中心，湖北 武汉 430033）

摘要：网络的飞速发展带来了流量的快速增长，流量监控在网络管理中尤为重要。针对网络设备配套的流量监控功能存在兼容性、扩展性不足，以及第三方流量监控系统存在的管理维护繁琐、安全风险高、应用普适性欠佳等问题，提出一种融合 Zabbix 和 SNMPv3 的网络流量监控方法。该方法在 Linux 系统部署开源网络监控软件 Zabbix，通过 SNMPv3 协议采集网络设备关键端口的流量数据，并将流量数据保存到数据库中，最后将流量数据预处理后以图形化方式在 Web 端展示。应用结果表明，该方法可直观呈现网络流量数据，方便网络管理人员监控网络流量。

关键词：网络管理；流量监控；Zabbix；SNMPv3
中图分类号：TP393.07　　**文献标志码：**A　　**文章编号：**1674-2605(2025)03-0008-06
DOI：10.12475/aie.20250308　　开放获取

Zabbix-SNMPv3 Integrated Network Traffic Monitoring Approach

TAN Zhiyong　LIN Yanhua　GU Jiaming
(Department of Information Technology, Wuhan Vocational College of Software and Engineering (Wuhan Open University), Wuhan 430033, China)

Abstract: The rapid evolution of networks has triggered exponential growth in traffic volumes, making traffic monitoring particularly crucial for network management. To address the limitations of native traffic monitoring features in network equipment—such as compatibility constraints and scalability deficiencies-along with the drawbacks of third-party monitoring systems (including cumbersome maintenance and management, elevated security risks, and suboptimal applicability), this paper proposes a Zabbix-SNMPv3 integrated network traffic monitoring approach. The method deploys open-source Zabbix monitoring software on Linux systems, collects traffic data from critical interfaces of network devices via the SNMPv3 protocol, persists the data in a database, and finally visualizes preprocessed traffic metrics through graphical representations on a web interface. Experimental results demonstrate that this methodology delivers intuitive visualization of network traffic data, significantly facilitating monitoring operations for network administrators.

Keywords: network management; traffic monitoring; Zabbix; SNMPv3

0　引言

网络管理是计算机网络三大经典问题（路由、流量控制和网络管理）之一[1]。近年来，随着网络技术的飞速发展，各种新型网络应用层出不穷，网络的规模不断扩大，结构日趋复杂，流量快速增长，这些都对网络管理提出了更高的要求。网络流量监控作为网络管理的基础，不仅能呈现当前的网络状态，还能用于网络性能优化，满足行为监控、流量工程、异常检测、故障分析等方面的需求[2-3]。因此，网络流量监控方法一直是网络研究领域的热点问题[4]。

针对网络流量监控的现实需求，大多数网络设备的主流制造商都提供了配套软件。但这些软件通常为商用版，部署需要额外的成本；且兼容性和扩展性较差，往往仅能监控对应厂商的设备，无法兼容其他厂

* 基金项目：湖北省中华职业教育社课题研究项目（HBZJ2023503）

商的设备[5]；用户无法在现有软件的基础上通过二次开发来满足自身业务场景需求。此外，在网络设备种类繁多的环境中，如数据中心，通过多个不同的软件来监控网络会增加网络管理的复杂性。

近年来，相关学者针对网络流量监控做了很多探索与实践。文献[6]利用开源流量监测工具——多路由器流量图示器（multi router traffic grapher, MRTG）来部署网络流量监控系统，实现对核心网络设备上下行流量的监控；但该系统监控多台设备时，需要运行多个命令行窗口，且可视化页面不在同一 Web 页面展示，管理维护较为繁琐。文献[7]在 Windows Server 2003 环境部署了图形化网络监测工具 Cacti，结合图形插件模块来监控网络设备端口流量；但因其部署使用的操作系统版本较低，在实际应用中可能存在兼容性问题或安全性风险。文献[8-9]基于 Netflow 技术监测分析网络流量，但支持的网络设备厂商以 Cisco、Juniper 为主，应用普适性欠佳。

Zabbix 作为企业级的分布式开源监控解决方案[10]，相较于 Cacti、Nagios 等开源监控系统，具有更强的告警方式、详细的审计系统、灵活的用户权限管理、完备的支持文档和相对较低的学习成本等特点[11-12]，在实际应用环境中能满足网络管理与流量监控的需求[13-15]。简单网络管理协议（simple network management protocol, SNMP）、公共管理信息服务/公共管理信息协议（common management information service/common management information protocol, CMIS/CMIP）是两种网络管理标准。其中，CMIS/CMIP 制定的服务标准较全面，但因其实现难度较大，目前支持 CMIS/CMIP 的产品较少[16]；SNMP 提供了一系列标准，可访问任何生产厂商的任何网络设备，具有应用简单、容易实现和易于部署等特点，应用广泛[17]，并不断演变产生多个版本，其中 v2c 和 v3 版为应用主流，且 v3 版的安全性更高。

本文提出一种融合 Zabbix 和 SNMPv3 的网络流量监控方法。该方法在 Linux 系统部署开源网络监控软件 Zabbix，通过 SNMPv3 协议采集网络设备关键端口的流量数据，将流量数据预处理后以图形化方式在 Web 端展示，具有易于实现，普适性较强的特点。

1　关键技术分析

1.1　Zabbix

Zabbix 作为一款高度集成的网络监控软件，提供了网络发现、数据采集、数据存储、通知告警、可视化图形等功能，可以监控众多网络参数以及服务器的健康度和完整性。Zabbix 所有的逻辑运算都在服务器端执行，对被监控对象的性能影响很小[18]。Zabbix 监控系统主要包括 Zabbix Server、Zabbix Web、Database、Zabbix Proxy、Zabbix Agent 等组件，其结构如图 1 所示。

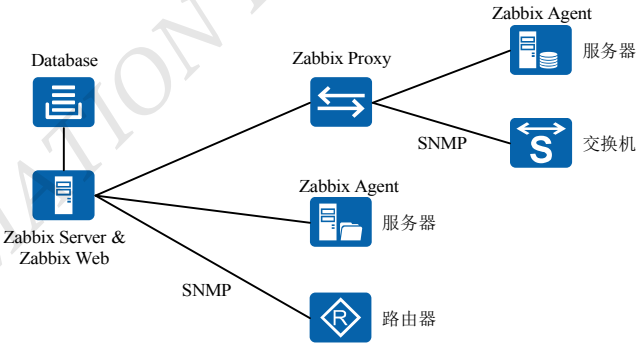

图 1　Zabbix 监控系统结构图

Zabbix Server 作为监控系统的核心组件，负责将采集的监控数据存储到 Database 中，并支持 MySQL、Oracle 等主流数据库。为满足用户使用浏览器访问、配置、管理系统的需求，Zabbix 监控系统提供了基于 PHP 的 Web 功能。Zabbix Web 和 Zabbix Server 通常部署在同一台服务器上。Zabbix Server & Zabbix Web 和 Database 是 Zabbix 监控系统的必选组件。

Zabbix Proxy 可协助 Zabbix Server 采集监控数据，降低了 Zabbix Server 的负载，是 Zabbix 监控系统的可选组件。Zabbix Agent 部署在被监控对象上，负责监控服务器的本地资源和应用程序，并将采集的监控数据发送给 Zabbix Server，是 Zabbix 监控系统的可选组件。

1.2　SNMPv3

SNMPv3 主要包括网络管理系统（network

management system, NMS）、被管代理进程（agent）和管理信息库（management information base, MIB）等部分，其模型如图 2 所示。

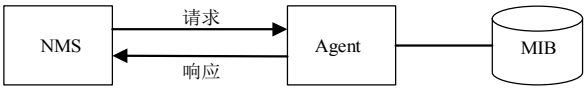

图 2　SNMPv3 模型

Agent、MIB 安装在被管理设备上，如交换机等。其中，Agent 负责响应来自 NMS 的信息查询请求（Get）或修改请求（Set）；MIB 是一个数据库，定义了被管理设备上的一系列被管理对象，如 CPU 利用率、端口状态等。每个被管理对象均通过对象标识符唯一标识，并以树型结构存储[20]。Agent 通过对 MIB 的操作来完成 NMS 的请求。

SNMPv3 在兼容之前版本的基础上增加了安全特性，其中基于用户的安全模型（user-based security model, USM）在 SNMPv3 的安全运行中发挥了关键作用。在具体应用中，需要为 SNMPv3 用户分别配置认证密码和加密密码。以 Get 操作为例，Agent 收到 NMS 发来的 Get 请求后，先对其进行身份认证；认证通过后，再对其数据单元进行解密；解密成功后，在 MIB 中查询相应的节点，并将查询得到的值封装到 Response 报文中，加密后发送。

2　方法设计

2.1　设计目标

核心层是网络的枢纽中心，其设备承担着网络流量的转发任务。因此，对核心层设备的网络流量进行监控尤为重要。核心层设备网络流量的监控主要集中在上联端口，包括出（out）、入（in）方向的流量数据。通过采集这两个方向的流量数据，并以图形化的方式直观展示流量的实时数据和历史数据，不仅便于发现网络运行过程中的潜在问题，还能为网络出口带宽扩容提供依据。

2.2　整体架构

融合 Zabbix 和 SNMPv3 的网络流量监控方法整体架构由监控服务端、被监控端和用户端 3 部分组成，如图 3 所示。

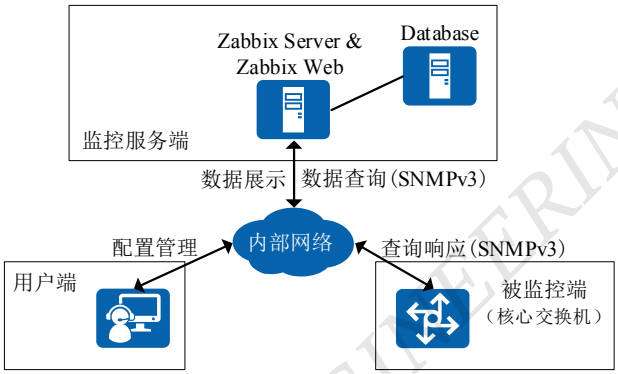

图 3　整体架构图

监控服务端主要由 Zabbix Server & Zabbix Web 和 Database 组成，负责采集、存储、展示流量数据；被监控端为核心层网络设备，如核心交换机等，由于网络设备无法安装 Zabbix Agent，因此监控服务端与被监控端采用安全性较高的 SNMPv3 协议进行交互，即监控服务端向被监控端发送 Get 请求来查询端口流量数据，被监控端查询 MIB 后，将结果响应给监控服务端；用户端通过监控服务端的前端页面进行配置管理，并查看监控服务端展示的流量数据。

3　技术实现

3.1　监控服务端

监控服务端采用 LAMP（Linux+Apache+My-SQL+PHP）环境。其中，Zabbix Server & Zabbix Web 部署在同一台服务器上，Database 部署在另一台服务器上。相关软件版本、操作系统、IP 地址、主机名等信息如表 1 所示。

表 1　监控服务端相关软件及操作系统部署信息

软件	操作系统	IP 地址	主机名
Zabbix Server & Zabbix Web 5.0	CentOS 7.6	192.168.0.1/24	zabbix-server
PHP 7.2	CentOS 7.6	192.168.0.1/24	zabbix-server
MySQL 5.7	CentOS 7.6	192.168.0.2/24	zabbix-mysql

1）系统环境准备。根据表 1 的信息，分别在两台服务器上安装 CentOS 7.6 操作系统、配置 IP 地址、

修改主机名；服务器可以是实体机，也可以是虚拟机，如 VMware 等。

2） 在 zabbix-server 服务器上安装 Zabbix Server Web 5.0，安装前关闭系统防火墙与 selinux。首先，安装 zabbix 包管理器即 YUM 源并将源中的镜像站点地址替换为阿里云镜像；然后，安装 Zabbix Server，即 zabbix-server-mysql。

3） 在 zabbix-server 服务器上安装 Zabbix Web 5.0。首先，卸载系统自带的低版本 PHP 并安装高版本的 PHP 7.2；然后，激活 Zabbix 前端源并使用 yum 命令安装 Zabbix 前端包，即 zabbix-web-mysql-scl 和 zabbix-apache-conf-scl。

4）在 zabbix-mysql 服务器上安装 MySQL 5.7 数据库。由于 CentOS 7.6 自带 MariaDB 数据库，为避免冲突，先卸载 MariaDB 数据库，再安装 MySQL 5.7 数据库。安装完成后，启动数据库的 mysqld 服务，并执行 mysql_secure_installation 运行安全配置向导。

5） 在 MySQL 数据库中创建数据库 Zabbix，并创建该数据库的管理用户（zabbix）及密码（pwd!2345），再向 Zabbix 数据库中导入 sql 文件。关键命令如下：

```
mysql -uroot -p -e "create database zabbix character set utf8 collate utf8_bin;"
mysql -uroot -p -e "grant all privileges on zabbix.* to 'zabbix'@'192.168.0.%' identified by 'pwd!2345';"
zcat /usr/share/doc/zabbix-server-mysql-*/create.sql.gz | mysql -uroot –p zabbix
```

sql 文件导入成功后，利用 vim 编辑器打开 /etc/zabbix/zabbix_server.conf 文件，找到以下 4 个 key（即“=”左边），取消 key 前面的注释符号#，并根据之前设置的数据库信息为其赋予相应的 value（即“=”右边）：

```
DBHost=192.168.0.2
DBName=zabbix
DBUser=zabbix
DBPassword=pwd!2345
```

6）在 zabbix-server 服务器上启动 zabbix-server、httpd 和 rh-php72-php-fpm 等服务。

3.2 被监控端

被监控端的核心交换机以华为 S12700 为例，其管理地址为 192.168.100.254/24，该地址需要与 zabbix-server 服务器的 IP 地址 192.168.0.1 互通。S12700 通过 SNMPv3 与 Zabbix Server 通信，SNMPv3 用户组为 grp、用户为 usr，认证算法选用 SHA，认证密码为 pwd12345，加密算法选用 AES128，加密密码为 pwd54321。关键命令如下：

```
snmp-agent
snmp-agent sys-info version v3
snmp-agent group v3 grp privacy
snmp-agent usm-user v3 usr
snmp-agent usm-user v3 usr group grp
snmp-agent usm-user v3 usr authentication-mode sha cipher pwd12345
snmp-agent usm-user v3 usr privacy-mode aes128 cipher pwd54321
```

配置完成后，在 zabbix-server 服务器上利用 snmpwalk 命令获取交换机的端口描述信息，可得到交换机端口在 MIB 表中的编号：

```
snmpwalk -v 3 -u usr -a SHA -A pwd12345 -x AES -X pwd54321 -l authPriv 192.168.100.254 ifDescr
```

3.3 用户端

通过浏览器访问 http://192.168.0.1/zabbix，即可进入 Zabbix 的 Web 页面。首次登录需按照页面提示依次完成 Check of pre-requisites 环境预检、Configure DB connection 数据库连接配置、Zabbix server details 服务器参数设置等步骤，才能进行以下配置。

1） 添加主机。在 Zabbix 前端页面通过“配置→主机→创建主机”添加主机。其中，“接口”项选择 SNMP；IP 地址填写核心交换机的管理地址即 192.168.100.254；端口号保持默认的 161；SNMP 版本选择 SNMPv3；安全级别选择 authPriv；验证协议、验证口令、隐私协议、私钥等按 3.2 中配置的信息选择或填写。

2） 添加监控项。先在 Zabbix 前端页面点击步骤 1）中添加的主机，再通过“监控项→创建监控项”

来监控核心交换机上联端口的网络流量。由于端口流量分为出（out）、入（in）方向，因此需要创建两个监控项：出流量监控项的 OID 为 IF-MIB::ifHCOutOctets.x，入流量监控项的 OID 为 IF-MIB::ifHCInOctets.x，其中，x 表示端口编号，可通过 3.2 中的 snmpwalk 命令获取。监控项的单位为 b/s，由于从交换机返回的数据单位为 byte，且是一个随时间不断增加的总量，因此 Zabbix Server 将其存储到数据库之前需进行预处理，即在“预定步骤”中先添加“每秒更改”，再添加“自定义倍数”，参数填 8（1 byte = 8 bit）。

3） 创建图形。首先，在 Zabbix 前端页面点击步骤 1）中添加的主机；然后，通过“图形→创建图形”添加网络流量的可视化图形，可以分别为出流量与入流量各创建一个图形，也可以在一个图形中同时展示出流量与入流量；最后，在“监控项”选择步骤 2）中创建的监控项即可。核心交换机上联端口流量监控图如图 4 所示。

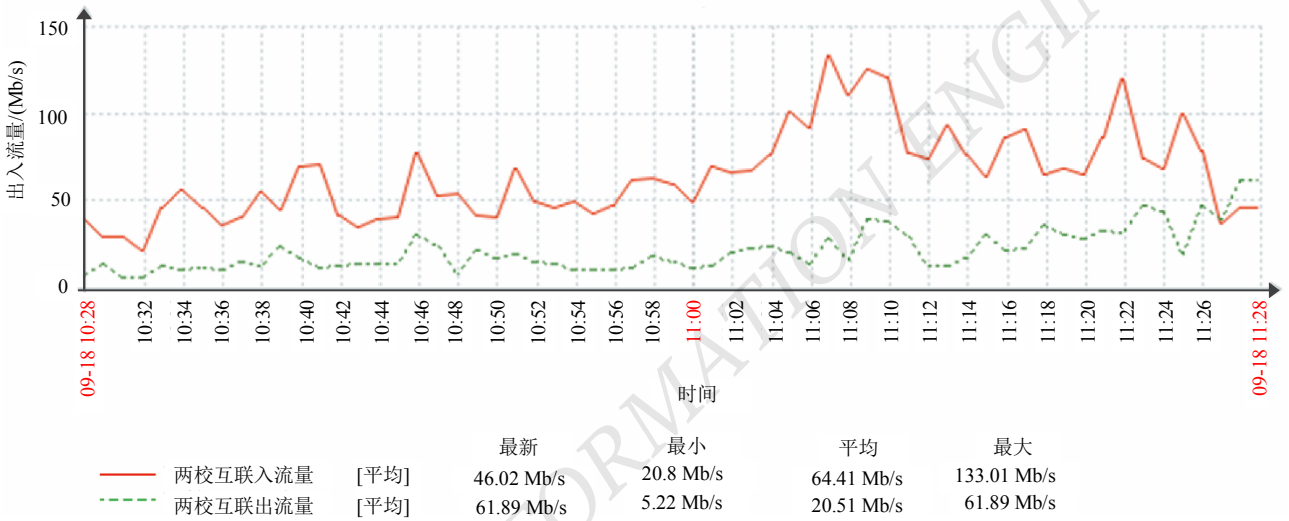

图 4 核心交换机上联端口流量监控图

图 4 展示了两校互联链路在某时间段的流量出入情况，观察发现，入流量显著高于出流量，出流量相对稳定，但入流量从 11 点开始出现明显突增，提示网络管理人员有必要对这一现象进行排查。

4 结论

本文在分析 Zabbix 和 SNMPv3 技术原理的基础上，提出一种融合 Zabbix 和 SNMPv3 的网络流量监控方法。该方法易于实现，普适性强。Zabbix 的功能不限于流量监控，还包括通过创建监控项触发器配置告警动作、监控服务器等关键设施的资源使用情况等，这些功能也是网络管理领域值得深入研究与应用的重要方向。

参考文献

[1] 王宏,王承松,郦苏丹.计算机网络管理困境与对策[J].计算机工程与科学,2021,43(11):1952-1958.

[2] 张恒,蔡志平,李阳.SDN 网络测量技术综述[J].中国科学:信息科学,2018,48(3):293-314.

[3] 沈萍,陈俊丽,张汉举.增强的 Zeek 网络流量采集与监控分析系统设计[J].计算机技术与发展,2024,34(10):77-83.

[4] 朱相楠.轻量级细粒度网络流量监控机理与仿真实现[D].成都:电子科技大学,2021.

[5] 姜欢.SDN 网络流量监控方法研究及系统设计[D].桂林:桂林电子科技大学,2022.

[6] 刘鹏,王光武.基于 MRTG 的校园网络流量监控系统部署与实现[J].中国教育信息化,2017(1):94-96.

[7] 王宁邦,刘江涛,梁红飞,等.Cacti 在可视化校园网络管理中

的应用[J].云南民族大学学报(自然科学版),2018,27(2):129-135.
[8] 李春平,王东,张淑荣,等.基于 Netflow 的网络流量监测与分析[J].现代计算机,2022,28(4):45-51.
[9] 王庆刚,顾峰,张雪梅,等.基于校园网流量分析的安全预警系统[J].网络安全技术与应用,2022(7):73-76.
[10] 薛康佳,张玉亮,王林,等.CSNS 加速器服务器监控系统设计[J].核电子学与探测技术,2023,43(2):404-408.
[11] 李晨,解思江,郝颖,等.信息系统安全运行自动化手段在电力公司的探索[J].电信科学,2017,33(S1):123-128.
[12] 乔石.面向算力网络的资源监控及预测系统的设计与实现[D].北京:北京邮电大学,2023.
[13] 梁鹏,岳宗敏.基于 Zabbix 的矿山物联网络监控系统研究[J].单片机与嵌入式系统应用,2021,1(6):39-42.
[14] 张红金;刘维.国产云平台安全体系策略探究[J].自动化与信息工程,2022,43(2):23-28.
[15] 周美佳,赵科.基于 Zabbix 的 VMware 产品的自动监控系统设计[J].上海船舶运输科学研究所学报,2022,45(2):63-68.
[16] 田昊,王超.基于国密 SM3 和 SM4 算法的 SNMPv3 安全机制设计与实现[J].计算机科学,2024,51(S1):931-937.
[17] 张子尧,吴黎兵,夏振厂,等.一种 SDN 环境的 SNMP Trap 报文聚合方法[J].小型微型计算机系统,2023,44(9):2059-2067.
[18] 贾宝军,徐雷,郭玉华,等.跨数据中心的统一监控研究与实现[J].电信科学,2016,32(3):2-6.
[19] 郭光海,周建胜,潘培华.计算机监控系统改进设计与应用[J].机电工程技术,2022,51(6):255-259.
[20] 梁勇,宫翔,熊林林,等.面向服务的一体化网络监测技术研究[C].第十六届全国信号和智能信息处理与应用学术会议论文集.北京:计算机工程与应用,2022:269-273.

作者简介：

谭志勇，男，1985 年生，工程师，硕士研究生，主要研究方向：计算机网络。E-mail: tanzy@mails.ccnu.edu.cn

林艳华，女，1982 年生，高级工程师，硕士研究生，主要研究方向：教育信息化。

顾家铭，女，1984 年生，工程师，硕士研究生，主要研究方向：物联网。