第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·网络与通信· 文章编号：1000—3428(2008)07—0104—03 文献标识码：A 中图分类号：TP393.4

下一代互联网网络管理系统的设计与实现

杨 柳[1,2]，李振宇[2]，杜 宁[1,2]，张大方[1]，谢高岗[2]
(1. 湖南大学计算机与通信学院，长沙 410082；2. 中国科学院计算技术研究所，北京 100080)

摘 要：随着网络规模的迅速增长和 IPv6 协议的发展，互联网网络管理工具变得越来越重要。该文设计了 IPv4/IPv6 兼容的简单网络管理协议底层通信机制和一种基于简单网络管理协议的拓扑发现方法，实现了下一代互联网网络管理系统。该系统由拓扑发现、网络性能分析以及故障管理 3 大功能模块组成，目前已成功应用在实际的网络环境中。

关键词：网络管理；下一代互联网；简单网络管理协议；拓扑发现

Design and Implementation of Network Management System for Next Generation Internet

YANG Liu[1,2], LI Zhen-yu[2], DU Ning[1,2], ZHANG Da-fang[1], XIE Gao-gang[2]
(1. School of Computer and Communication, Hunan University, Changsha 410082;
2. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

【Abstract】With the rapid growth of Internet scale and the development of IPv6 protocol, network management tools for next generation Internet become more and more important. This paper designs an IPv4/IPv6 compatible SNMP communication mechanism, and a topology discovery algorithm based on SNMP. On this basis, a network management system for next generation Internet is designed and implemented. The system mainly consists of three modules: topology discovery module, network performance analysis module and fault management module, respectively. This system has been applied in practical network environment successfully.

【Key words】network management; next generation Internet; SNMP; topology discovery

1 概述

网络管理技术已成为网络构建和维护中必不可少的重要因素，IPv4, IPv6 混合网络环境下的网络管理意义尤为重要。ISO 将网络管理的关键功能分为 5 类：故障管理，配置和名称管理，计费管理，性能管理，安全管理。

简单网络管理协议(SNMP)是目前最常用的网络管理协议，提供了一种从网络上的设备中收集网络管理信息的方法。网络中的资源通过用管理信息库(MIB)中的对象来表征实现管理，管理工作站通过 SNMP 协议与管理代理通信，获得保存在设备 MIB 中的信息。MIBⅡ(RFC 1213)是最重要的 MIB 规范，是 IPv4 环境下可获得的路由器 MIB 信息的最小集合。随着 IPv6 网络规模的日益发展，IETF IPNG 小组发展了 IPv6 标准 MIB，用于 IPv6 环境下的网络管理[1]，包括 IPv6 MIB(RFC 2465)和 ICMPv6 (RFC 2466)。本文设计和实现的网络管理系统在 SNMP MIB 基础上实现了配置管理、故障管理、性能管理和安全管理等功能，并在 IPv4/IPv6 环境下兼容。

正确的网络拓扑是进行网络管理的基础。由于大型网络并没有一个单独的管理者，拓扑复杂动态的特性决定了手动收集大型网络的拓扑信息是不现实的。基于拓扑发现对网络管理的关键性，本文介绍了基于 SNMP 的路由器层和子网内设备拓扑发现算法。

2 下一代网络管理系统的设计与实现

2.1 系统结构

下一代网络管理系统根据功能主要分为拓扑发现、网络性能监测和故障管理 3 大模块，按照系统流程分为底层通信、中间数据处理、应用显示三层构架。系统结构如图 1 所示。

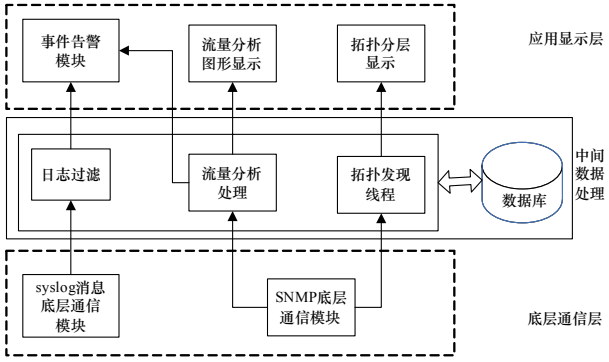

图 1 下一代网络管理系统结构

2.2 关键技术

2.2.1 SNMP 底层通信

SNMP 底层通信模块在 IPv4/IPv6 环境下兼容，根据对象标识符(OID)读取代理设备 MIB 信息。SNMP 消息具有 5 种 PDU(协议数据单元)类型：GetRequest PDU, GetNextRequest PDU, SetRequest PDU, GetResponse PDU 和 Trap PDU[2]，这 5

基金项目：国家自然科学基金资助项目(60403031, 90604015, 60473031)

作者简介：杨 柳(1982－)，女，硕士研究生，主研方向：网络管理，网络测试；李振宇，博士研究生；杜 宁，硕士研究生；张大方，教授、博士生导师；谢高岗，副研究员、博士

收稿日期：2007-05-28 **E-mail：**luluwillow@163.com

种 SNMP 消息对支持 SNMP 实体进行管理。

目前比较流行的底层通信 API 是基于 SNMP 网管程序的 WinSNMP，它为 SNMP 通信提供了必须遵循的开放式单一接口规范，在其之上可以建立强大的 SNMP 应用程序，但是 WinSNMP 不支持 IPv6 环境下通信。针对这一问题，开发了 SNMP over IPv4/IPv6 底层通信模块，利用面向对象的思想设计并实现了 SNMP 通信的建立、目标代理配置、变量绑定的设置、报文的收发以及返回值的解析等基本功能。通过 GetRequest PDU, GetNextRequest PDU, SetRequest PDU, GetResponse PDU 4 个原语实现了对指定 OID 对象的单个值以及表的读取。SNMP 底层通信的基本流程如图 2 所示。

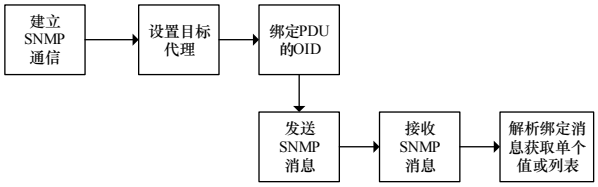

图 2　SNMP 底层通信流程

2.2.2　数据处理

通过 SNMP 底层通信和 Syslog 消息底层通信读取数据后，后台进行相应数据处理。由于设备流量数据大，信息量丰富，系统采用基于 Oracle 数据库的数据存储和读取，根据 MIB 中设备信息的结构设计数据库中的表。按照设置的轮询时间间隔，系统在后台自动定时读取设备信息并存储到相应的数据库表中。对于比较大的数据表，如 IPv6 端口性能指标高达 25 项，系统采用存储过程来实现大数据表的复杂操作。

2.3　拓扑发现模块

拓扑自动发现方法主要分为 3 大类：基于管理协议(如 SNMP)，基于通用协议(如 ICMP)，基于路由协议(如 BGP)。基于 ICMP 协议的方法不存在访问权限的限制，因此在发现公共网络的拓扑时最有效[3]。但是该方法构建的拓扑图准确性不高，产生的冗余信息太多，由于地址同名(Alias)的原因导致拓扑图中路由器间的连接关系处理复杂。更重要的是基于 ICMP 的方法利用 Traceroute 工具探测路径信息，通过发送 TTL 值递增的 ICMP 回显请求报文到一个不可达端口获取到达目的节点所经过的设备端口地址。其主动探测的特征导致同一个端口被探测点重复访问，给被管理网络增加了大量的冗余流量[4]。基于 SNMP 的方法要求所有的设备必须支持 SNMP 协议，才能利用 MIB 中路由表的信息进行拓扑发现。这种方法基本的限制是并非所有设备都支持 SNMP，MIB 信息的标准化、一致化也是问题，并且网络管理员不希望其他人获取他们的设备信息。访问 MIB 需要具备对路由器设备的访问权限，即团体字，因此该方法不能应用于所有环境。但是如果运用于私有网络，基于 SNMP 方法的优点非常明显。当网络一旦发生变化，设备 MIB 信息也会自动变化，结果正确率高，而且信息获取速度很快，网络开销小，实现简单。利用路由协议发现网络拓扑的一些方法也被提出，如通过 Open Shortest Path First(OSPF)发现路由器层的拓扑，利用 Neighbor Discover Protocol(NDP)发现 IPv6 网络拓扑等。本文所提出的系统用于私有网络管理，采用基于 SNMP 的拓扑发现方法。

IPv4 环境中，基于 SNMP 的三层拓扑发现(路由器层)是关键，包括了路由器及其相连的子网信息发现，通过读取路由器设备的路由表(ipRouteTable)中下一跳地址实现。若对应的路由类型为 3 则连接一个子网，若对应的路由类型为 4 则连接一个路由器。同名问题(Alias)通过读取设备的地址表(ipAddrTable)解决。本系统采用的路由器拓扑发现算法如下：

```
Foreach IPi    ∀ IPi∈IPSet// IPSet为IP地址范围内的IP地址集
IF GetSystem(IPi) = = 三层设备 && GetIPForwarding(IPi) = = 网关
Begin
//该IP地址对应一个路由器设备
IPAlias = GetIPAddrTable(IPi)//该路由器对应的多个地址(Alias)
VisitedSet += IPAlias          // VisitedSet为已访问设备列表
SubNetDiscoverThread(IPi )     //启动子网发现线程
ConnectedSet = GetRouteTable(IPi)
Foreach IPj ∈ ConnectedSet
Begin
  IF (GetIPRouteType(IPj )= = 4) &&( IPj ∉ VisitedSet) //下一跳//为路由器
    AddRouter;                 //发现路由器及连接关系
    RouterDiscover（IPj）      //递归调用
  IF GetIPRouteType(IPj )= = 3  //下一跳是子网
    AddSubNet;                 //发现子网及连接关系
 End
 End
```

三层拓扑仅仅覆盖了 IP 网络的小部分连接关系，二层拓扑(交换机等)对于网络管理人员来说十分重要，它对诊断端到端的连接、判断链路和设备失败的潜在影响具有明显意义。基于 SNMP 的子网发现包括发现子网内部设备(交换机、主机等)及其相连关系。该系统采用的子网拓扑发现算法如下：

```
GetNetToMediaTable(IPi)    //读取ARP表
GetIPAddrTable(IPi)        //读取地址表
Foreach ipNetToMediaNetAddress   //连接设备IP
Begin
  IF ipAdEntIfIndex = = ipNetToMediaIfIndex    //地址表和//ARP表通过端口索引匹配
  Begin
      //一个端口可对应多个子网掩码
      NetMask = ipAdEntNetMask
       IF (ipNetToMediaNetAddress & NetMask) = = (ipAdEntAddr & NetMask)
          SubNet = ipNetToMediaNetAddress & NetMask
  End
  GetSystem(ipNetToMediaNetAddress)  //根据sysServeices判//断设备类型
End
```

通过 ARP 表(ipNetToMediaTable)获取路由器相连的设备，ARP 表存储的是一段时间内路由器相连的所有设备信息，该方法获取的连接信息虽然并不完全，但是反映了最实时的连接关系。由于一个端口可对应多个子网掩码，在判断设备所在子网时，增加了一个条件限制，从地址表(IPAddrTable)获得端口掩码后，与路由器端口地址计算所得的子网地址相比较。如果等于由设备地址计算的子网地址，则设备在该子网中。实验证明该判断条件明显提高了子网内设备发现的正确性。

仅仅获取二层拓扑的设备信息是不完整的，发现二层设备的连接关系也十分重要。贝尔实验室 Lucent 技术小组提出了一个新算法，主要研究异构(heterogeneous)IP 网络的物理拓扑[5]。它在 Bridge MIB(RFC 1493)的基础上获取异构网络(例如适应多个 ISP)的二层拓扑，主要是利用数学图论的方法

解决二层设备的拓扑连接关系。这个方法对网络环境要求很高，Brue Lowekamp[6]在它的基础上改进了算法，使其对网络要求条件显著降低。

IPv6 环境下，利用 IPv6 标准 MIB 理论上可构造网络拓扑，但是目前基于 SNMP 拓扑发现方法仍存在很大限制。虽然大部分设备生产商都已将 IPv6 作为产品开发的一个重要部分，但在实际网络环境中仍然有许多正被使用的设备对 IPv6 MIB 不支持或支持得不够。比如，Hitachi 路由器 GR2000 部分支持 IPv6 标准 MIB(RFC 2465)，Cisco 路由器(IOS Version 12.2(2600))支持 SNMP over IPv6，但不支持 IPv6 相关的 MIB。另外，大部分 IPv6 路由协议使用本地链路地址来定义路由表的下一跳对象[7-8]，所以目前基于 SNMP 的拓扑发现方法是不现实的。系统目前仅支持 IPv4 环境下的拓扑自动发现，对 IPv6 设备支持手动添加。本文根据 IPv4 MIBII 提出的路由器拓扑发现和子网设备发现算法思想对 IPv6 标准 MIB 也是成立的，随着设备更加普遍地支持 IPv6 标准 MIB，未来基于 SNMP 的 IPv6 拓扑发现必定能在实际网络环境中实现。

笔者利用所开发的系统，进行了大量的实验。图 3 显示了系统发现的某单位的三层拓扑图，隐去了 IP 地址的后 2 B。

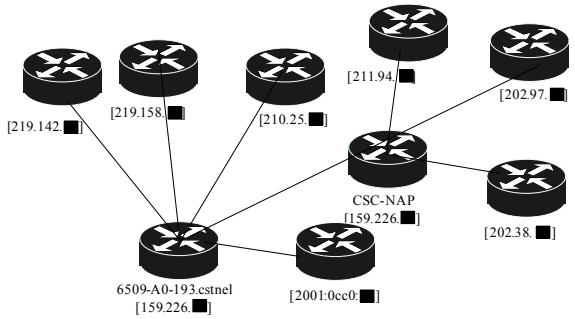

图 3　某单位的三层网络拓扑图

2.4　网络性能分析模块

图 4 显示了某设备端口的进/出流量的性能分析图，对流量最大值、最小值和平均值进行了统计分析。

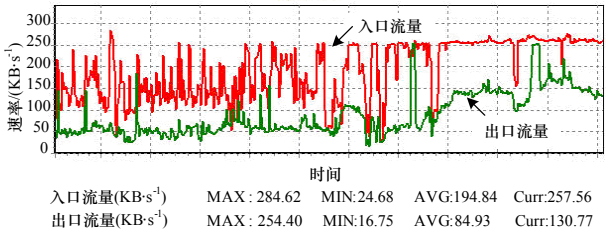

图 4　端口性能

网络性能分析模块实现对拓扑图中性能参数的实时分析和历史分析。标准 MIB 根据不同的协议流量进行分组，该模块主要分析指标包括端口流量和端口利用率、IP 层统计流量、传输层统计流量、应用层统计流量。MIB 中流量由一个累加的计数器统计包或字节数，流量值由式(1)计算，表示为包或字节数的变化速率。其中，*interval* 表示为采样时间间隔；*ΔtrafficSum* 表示当前采样点和上一采样点的包数或字节数变化值。对于端口利用率，采用式(2)的方法计算，*ΔinTraffic*，*ΔoutTraffic* 和 *ifSpeed* 分别表示采样时间间隔内端口收到的总字节数(B)、采样时间间隔内端口传输的总字节数(B)以及端口当前数据速率容量(b/s)。流量数据通过后台定时轮询记录到数据库中。

$$traffic = \Delta trafficSum / interval \tag{1}$$

$$interUtl = \frac{(\Delta inTraffic + \Delta outTraffic) \times 8 / inteval}{ifSpeed} \tag{2}$$

2.5　故障管理模块

故障管理模块用于检测和报告故障，当链路、设备发生异常或接收到 Syslog 消息时能够根据严重性以多种方式进行预警或告警，及时定位异常发生位置，同时支持事件日志的历史查询。链路异常指链路利用率超过设定阈值。设备状态异常指设备不可达或者设备 CPU 利用率、内存利用率以及温度超过设定阈值。设备流量异常是指设备的端口流量、IP 层统计流量、传输层统计流量、应用层统计流量超过设定阈值。根据异常的严重性程度触发事件告警模块。

Syslog 消息为设备事件日志，Syslog 协议(RFC3164)支持设备通过 IP 网络发送事件消息(Syslog 消息)到接收器，即 Syslog 服务器。

Syslog 消息由 3 部分组成：PRI, HEADER, MSG。PRI 表示该 Syslog 消息的优先级(priority)，优先级值由设备(facility)和严重等级(severity)计算获得。HEADER 包含了 Syslog 消息发出的时间戳和发送设备名或 IP 地址。MSG 包含了该日志事件的细节信息。系统的 Syslog 消息底层通信由 2 个线程完成：侦听 Syslog 消息线程和数据库写进程。当侦听到 Syslog 消息，将该消息插入消息队列，同时触发数据库写事件，取队列中的第 1 个消息出队，解析该消息写入数据库中。

3　结束语

本文实现了基于 SNMP 的下一代网络管理系统，主要介绍了拓扑发现、设备流量监测、故障告警 3 大模块。该系统能够有效保证拓扑覆盖率；IPv4/IPv6 兼容的 SNMP 底层通信模块对于下一代网络设备流量性能分析具有十分重要的意义；设备状态、流量、Syslog 日志以及链路的全方位故障管理，充分保证精确地进行故障地点和影响的定位。

参考文献

[1] Keeni G M, Koide K, Hakraborty D C. SNMP in the IPv6 Context[C]//Proc. of the Symposium on Applications and the Internet Workshops. Florida, USA: [s. n.], 2003: 254-257.

[2] Stallings W. SNMP 网络管理[M]. 胡成松, 汪　凯, 译. 北京: 中国电力出版社, 2001.

[3] Waddington D G, Chang Fangzhe, Viswanathan R, et al. Topology Discovery for Public IPv6 Networks[J]. ACM SIGCOMM Computer Communication Review, 2003, 33(3): 59-68.

[4] Donnet B, Raoult P, Friedman T, et al. Efficient Algorithms for Large-scale Topology Discovery[C]//Proc. of ACM SIGMETRICS. New York, USA: ACM Press, 2005: 327-338.

[5] Breitbart Y, Garofalakis M, Martin C, et al. Topology Discovery in Heterogeneous IP Networks[C]//Proc. of IEEE INFOCOM'00. Piscataway, NJ, USA: IEEE Press, 2000: 265-274.

[6] Lowekamp B, O'Hallaron D R, Gross T R. Topology Discovery for Large Ethernet Networks[J]. Computer Communication Review, 2001, 31(4): 237-248.

[7] Malkin G, Minnear R. RIPng for IPv6[S]. RFC 2080, 1997.

[8] Coltun R, Ferguson D, Moy J. OSPF for IPv6[S]. RFC 2740, 1999.