ISSN1000-9825 Journal of Software 软件学报 2000,11(4):468~472

基于 Web 和数据库的网络管理系统的设计与实现*

段海新 杨家海 吴建平

(清华大学信息网络工程研究中心 北京 100084)

E-mail: dhx@bjnet.edu.cn

摘要 提出了一个基于 Web 和关系数据库的网络管理系统的管理模型,并描述了一个基于该模型的网络管理系统——Super-Domain 的组成结构及其具体实现机制.讨论了系统实现中的关键技术问题及其解决方法,其中包括管理信息的存储模型、数据一致性维护、基于 Web 的实时告警机制、系统安全机制等.

关键词 计算机网络,网络管理,Web,管理信息模型,安全机制.

中图法分类号 TP393

计算机网络的复杂性和异构性使得网络管理问题上升到网络建设的战略性地位,国内外许多学术机构、企业和标准化组织在网络管理技术方面都做了大量的工作[1~5].Web 技术的发展使网络管理模式从规模系统趋向单元结构,使得直接面向应用的网络管理系统的开发已经变得相对容易,而传统的平台式网络管理厂商的优势地位不再明显.基于 Web 的网络管理已经成为当前技术研究和产品开发的热点,如 Advent 公司的 NetMonitor[6]和 IBM 公司的 WebBin 系统[7].

但是,由于基于 Web 管理模式下的许多问题(如安全问题、实时告警问题等)未能很好地得到解决,而且受传统的管理平台体系结构的制约,现有的商品化管理系统(如 HP/OpenView,IBM/NetView 等)基于 Web 的管理能力往往仅限于静态信息的浏览.另外,平台式网络管理产品中往往只提供网络的配置管理、故障管理和性能管理功能.对于我国网络建设最为迫切的计费管理和安全管理功能,却很少实现或根本没有.

在国家"九五"科技攻关项目"先进网络管理与运行技术"的资助下,结合中国教育与科研网络管理中心多年的运行管理经验,我们研究和开发了一个直接面向大规模网络管理应用的、完全基于 Web 和数据库的网络管理系统——Super-Domain,实现了网络的配置、性能、故障、安全和计费的基本管理功能.本文介绍该系统基于 Web 和数据库的管理模型及其总体结构,并着重介绍实现中的关键技术问题及其解决方法,主要包括被管对象管理信息的存储模型和数据库一致性维护、基于 Web 的实时告警机制和安全机制等,最后给出该系统与其他网络管理系统相比较的特点.

1 系统总体结构

系统总体结构如图 1 所示.数据采集模块读取被管对象(路由器、交换机、主机、应用服务等)状态信息和各种运行参数,存储在关系数据库中,由各个功能模块共享.对象操作模块通过修改被管对象的属性来控制和调整网络的运行.系统配置与维护模块负责整个网络管理服务器系统的配置,包括用户管理、被管对象的界定、数据采集任务的管理、阈值的定义等等.各功能模块之间通过内部消息传递机制传递控制信息,通过数据库交换数据.管理员通过 Web 浏览器访问网络管理系统,进而监控整个网络.下面简单介绍各个模块的功能及其工作方式.

---

* 本文研究得到国家"九五"重点科技攻关项目基金(No.97-743-01-01)资助.作者段海新,1972 年生,博士生,主要研究领域为计算机网络管理,计算机网络安全体系结构.杨家海,1966 年生,副教授,主要研究领域为计算机网络体系结构,网络管理及应用.吴建平,1953 年生,教授,博士生导师,主要研究领域为网络协议测试,网络管理,网络体系结构.

本文通讯联系人:段海新,北京 100084,清华大学信息网络工程研究中心

本文 1999-01-26 收到原稿,1999-04-21 收到修改稿

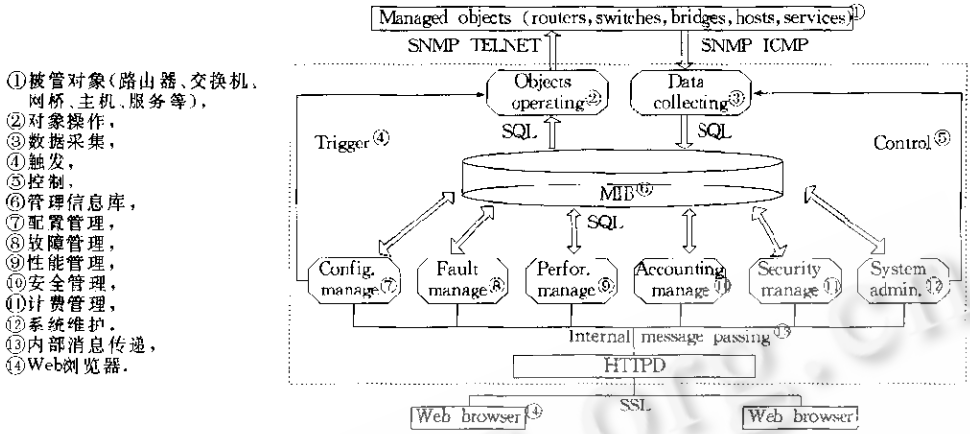


Fig. 1 The architecture of Super-Domain
图1 Super-Domain网络管理系统总体结构

(1) 配置管理模块.配置管理包括以下步骤:自动发现被管对象、配置信息获取与查询、自动构造和编辑拓扑图以及配置信息的修改更新.配置管理模块首先通过自动发现初始化数据库中的被管对象集合,收集、分析配置信息(如接口参数、路由表等),并以结构化的形式存储在数据库中.然后,根据被管对象的配置信息,特别是互连设备的配置,构造网络拓扑图.由于自动布局产生的拓扑图极其复杂、庞大,我们实现了拓扑图的编辑功能,可以用层次结构来组织被管对象.系统向管理员提供被管对象的基本配置工具,如配置路由器的接口参数、路由协议等信息.保持网络管理系统数据库与被管对象配置信息的一致性,是对象操作需要解决的关键问题,本文在第2.2节中给出了一致性问题的一种解决办法.

(2) 性能管理模块.性能管理模块从数据库系统读取被管对象的相关数据,如线路的流量、丢包率和延迟,主机或路由器的负载、存储介质的利用率等,对超过系统性能阈值的参数向管理员告警;对各种性能参数,系统生成不同时间粒度的性能曲线图,以反映网络当前的使用情况和历史发展趋势.系统分析网络流量数据,用饼形图反映网络中各种应用服务所占的比例,用直方图反映线路流量的分布和通断统计情况,以分析网络的利用率和可用性,生成性能监测报告.

(3) 故障管理模块.故障管理模块过滤数据采集模块转发来的事件,并根据事件之间的联系,归并到故障卡片(trouble ticket),把需要处理的故障向管理员告警.系统提供一整套基于Web的排错工具和排错向导,能够使管理员有效地定位和排除故障.系统自动记录管理员的所有排错动作,使事件—故障—处理形成一个整体流程.

(4) 安全管理模块.安全管理模块的功能体现在网络管理系统本身的安全和被管对象的安全两个方面.系统提供用户认证、访问控制、数据传输和存储的保密机制,并通过维护系统日志使管理员对系统的使用和对被管对象的修改有据可查.对于被管对象的安全管理,本系统实现了3个方面的功能:一个是通过管理防火墙或网关路由器的访问来控制链表,控制对网络资源的访问;另一个是接收与被管对象安全相关的事件报告(如SNMP认证失败);再一个是定期探测系统的安全漏洞,并给出补救建议.

(5) 计费管理模块针对计费管理的需要,数据采集模块(本系统使用了一台微机)在网络出口处监听、记录所有进出流量,归并、整理后存入数据库.计费管理模块计算联网用户的网络流量,根据定义的计费政策计算相应的网络费用,并通过浏览器向联网用户提供远程查询界面.Super-Domain系统可以同时输入多套计费政策,管理员可以比较同一计费数据在不同政策下的计算结果,进而为计费决策提供支持.

2 管理信息的存储模型及数据一致性

2.1 管理信息的存储模型

管理信息结构(SMI)[6]所定义的树形结构的管理信息库(MIB)只是逻辑概念上的数据库,各被管对象的管理信息库在内部的实现和存储形式对外是透明的.要完成管理信息在关系数据库中的集中存储,首先要解决的

问题是存储模型的转换.目前可用的信息模型有两种,一种是面向对象模型(OO),另一种是实体-关系模型(ER).SNMP 的 MIB 是一个逻辑上的树形结构,并不是面向对象模型,因为它没有类的概念,只是以层次结构组织的变量的集合.实体-关系模型可以很好地表示被管对象之间的包容(containment)关系,而且这种模型很容易在目前比较成熟的关系数据库系统中实现.由于 MIB 中变量的标识符只在一个被管对象中是唯一的,为表示不同被管对象的某个 MIB 变量,还需要引入一个唯一的被管对象标识符 objectID.

对图 2 中 MIB-2 树形结构的数据,我们建立如图 3 所示的实体-关系图.子树(subtree,如 system,interface,ip 等)下的标量可以作为被管对象的属性,而对于向量(即 table)需要另建一种实体,该实体与被管对象的关系由 objectID 来联系.

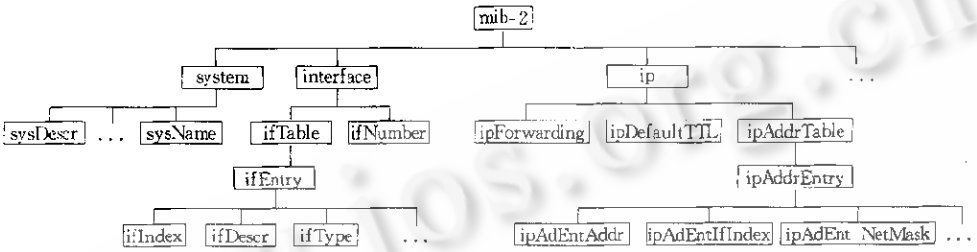


Fig. 2　SUMP MIB tree
图2　SUMP MIB树

2.2　数据一致性的维护

存储在网络管理服务器上的管理信息应该与相应被管对象的状态保持一致,当被管对象状态或配置发生变化时,必须立即更新网络管理数据库.然而,要实现严格的数据一致性是很困难的.一方面,由于网络本身的延迟,同时修改数据库和被管对象的原语操作不可能实现.另一方面,无法防止管理员不经网络管理系统而直接修改被管对象的配置.这些都是引起数据不一致性的主要原因.我们通过两种办法来解决数据的一致性问题.首先,网络管理系统修改管理信息遵循以下步骤:

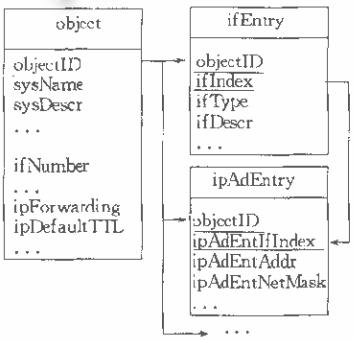


Fig. 3　Entity-Relationship model of MIB
图3　MIB信息的实体-关系模型

(1) 先锁定数据库的相关字段,这时,如果其他进程也要访问同一字段就必须等待;

(2) 系统修改数据库之后触发对象操作模块,形成特定对象的操作命令序列来操作被管对象;

(3) 如果对象操作模块返回失败信息,则恢复对数据库的修改,否则直接执行步骤(4);

(4) 解锁数据库.

其次,系统定期轮询被管对象的配置信息,并与数据库内容相比较,如果发现不一致之处便通知管理员,由管理员决定是更新数据库还是恢复被管对象的配置.

3　基于 Web 的实时告警机制

Web 是一种以拉(pull)为主的技术,即一般只有当用户主动请求服务器时才能返回信息.但网络管理要求对网络中出现的各种事件的实时响应,需要服务器系统在发现网络故障后主动、实时地向浏览器上的管理员发送告警信息.HTTP 协议本身的功能对此略显不足,这也是基于 Web 的网络管理的主要约束之一.

目前,实现 Web 服务器主动向浏览器发送数据的技术主要有 3 种:Client Pull,Server Push 和 Java Applet.Client Pull 技术由于实现简单目前使用较为普遍,浏览器以一定的周期访问服务器,用检查有无新事件的发生.如果周期太长,则事件的延迟太大;如果周期太短,则不仅会给系统增加负担,还会增加网络开销.

我们在实现中考察了后两种技术.Server Push 是一种 CGI 编程技术,由 Web 服务器派生一个进程,执行一

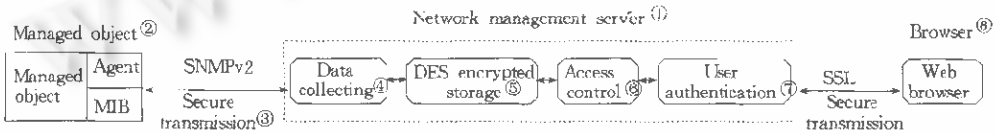
个 NPH(non-parse header)的 CGI 程序与浏览器建立一个 TCP 连接.这样,各功能模块产生的告警信息通过内部消息传递、广播给各 NPH 进程,由这些进程 Push 给浏览器.Server Push 实现的优点是 NPH 进程运行在服务器,对客户浏览器的要求较少.但是,因为服务器要为每个浏览器派生一个 NPH 进程,这就加重了服务器的负担.

Java Applet 实现的告警机制可以有效地平衡客户与服务器之间的负载,因为 Java Applet 运行在客户端浏览器上,每个 Applet 与服务器上的消息传递守护进程建立一个 TCP 连接,在消息传递进程收到各功能模块的告警事件后,通过 Java Applet 向管理员报告.可以看出,Java Applet 的实现把告警事件的处理交给了浏览器,其缺点是要求浏览器必须能够支持 Java.

为了避免由于 Java 版本升级而造成的版本不一致问题,我们在系统中使用了 Server Push 技术.实践证明,这种方式由于运行效率高而实时性更强.

4 系统安全机制

网络管理系统自身的安全可靠对网络的正常运行至关重要,因为网络管理服务器存储着重要的管理信息和强有力的管理工具.不幸的是,基于 Web 的管理给网络管理带来了新的不安全因素,因为 Web 应用的平台独立性和地理无关性使得任何人、从任何地方都可能访问网络管理服务器.为此,我们利用以下安全技术来保证网络管理系统的安全:基于证书的用户认证、DES 数据加密存储、SNMPv2 和 SSL 协议数据保密传输、基于用户组和访问控制链表的访问控制,各种机制之间的关系如图 4 所示.



①网络管理服务器,②被管对象,③数据保密传输,④数据采集,⑤存储,⑥访问控制,⑦用户认证,⑧浏览器.

Fig. 4 Security mechanisms of Super-Domain system

图4 系统安全机制

Web 界面是网络管理系统唯一的访问点,系统对用户的认证是由 Web 服务器完成的.由于用户名/口令认证机制的众所周知的弱点,我们在浏览器与服务器之间使用了安全套接字协议 SSL,利用 SSL 基于公开密钥的证书来认证系统用户.为此,我们维护一个独立的 CA(certificate authority)为网络管理服务器和每个用户签发证书.除了认证以外,SSL 还保证了浏览器与服务器之间数据传输的保密性与完整性.

用户(即管理员)按照角色的不同分成不同的用户组,每个用户组中的用户具有相同的权限,只有具备足够权限的用户才能执行相应的操作(如读、修改、增加或删除).用户对被管对象的操作可用以下三元组来表示:

(用户组 GID,对象 OID,操作模式).

系统查找用户所在的用户组,然后查找系统访问控制表,以检索用户对该对象的操作权限来决定是否允许访问.

对于支持 SNMPv2 的设备,被管对象与网络管理服务器之间使用 SNMPv2 通信协议.在配置了 party 和认证密钥以后,SNMPv2 利用 Keyed-MD5 来认证数据源的可靠性和数据完整性,防止了假冒和篡改类型的攻击.其次,对于采集来的敏感信息,我们使用 DES 加密算法加密之后存储在数据库中.

5 系统应用情况及特点

Super-Domain 网络管理系统在 1999 年初通过了由科技部委托、教育部组织的技术鉴定,认为该系统达到同类网络管理系统的国际先进水平.目前,该系统在 CERNET 网络运行中心(NOC)长期运行,管理 CERNET 国家骨干网络 40 多台路由器和管理中心 12 台服务器.与我们以前使用的 IBM/NetView(版本 4.1)相比,该系统有以下优点:

(1) 全中文的 Web 界面,集成了本系统所有的网络管理功能;

(2) 实现了流量计费管理功能,对同一流量数据可以应用多个计费策略,为计费决策提供支持;

(3) 实现了管理系统本身的安全机制,并实现了部分安全管理功能;

(4) 故障管理功能融入了我们的运行管理经验,提供了从故障监测到故障定位和故障修复全过程的半自动管理流程,并提供了一般故障的排错向导(wizard);

(5) 增强了环境的定制能力,因为系统实现以CGI技术为主,增加新应用只需开发相应的CGI模块即可,无需改动整体结构和其他功能模块.

6 今后的工作

由于开发时间较短,系统还存在着一些不足.从体系结构上看,下一步我们计划将目前的集中式管理扩展成多管理者的分布式管理结构,以增强系统的可扩展性.在故障管理中,我们正在引入人工智能技术,实现故障自动定位.对于安全管理,我们计划增加网络入侵检测的能力,实现网络安全控制与检测的结合,增强系统对安全事件的实时响应能力.

参考文献

1 Case J D, Fedor M, Schoffstall M L *et al*. Simple network management protocol (SNMP). RFC 1157, 1990, http://www.ietf.org/rfc/rfc1157.txt

2 Davin J, Galvin J, McCloghrie K. SNMP administrative model. RFC 1351, 1992, http://www.ietf.org/rfc/rfc1351.txt

3 Black U. Network Management Standards: SNMP, CMIP, TMN, MIBs, and Object Libraries. New York: McGraw-Hill, 1995

4 Sun Microsystems Inc. Java management API architecture. Technical Report, 1996, http://java.sun.com/products/Java-Management/overview.html

5 Object Management Group. The Common Object Request Broker: Architecture and Specification. 1998, ftp://ftp.omg.org/pub/docs/formal/98-07-01.pdf

6 Advent Net Inc. AdventNet NetMonitor——a builder tool to create applets that monitor and control SNMP devices. Technical Report, 1998, http://adventnet.com/products/netmonitor/index.html

7 IBM Inc. Webbin——a platform-independent plug-in for Web servers. Technical Report, 1997, http://www.alphaworks.ibm.com/formula/webbin

8 IETF SNMPv2 Working Group. Structure of management information for SNMPv2. RFC1902, 1996, http://www.ietf.org/rfc/rfc1902.txt

Design and Implementation of a Network Management System Based on Web and Database

DUAN Hai-xin YANG Jia-hai WU Jian-ping

(*Network Research Center Tsinghua University Beijing* 100084)

Abstract A management model is proposed for the network management system based on Web and relational database in this paper. With this model, the components and implementation of a management system, Super-Domain, are described. Some key problems and their solutions, which include the storage model of management information, the maintenance of data consistency, the mechanism of real time alarming based on Web and the mechanism of system security, are also discussed.

Key words Computer network, network management, Web, management information model, security mechanism.