网络管理协议的分析与展望

李天剑　曾文方(成都 四川大学西区计算机系　610065)

摘要:网络管理协议是网络管理的要素之一。本文分析、比较了 CMIP、SNMP、CMOT 这三种当前最著名的网络管理协议,并着重介绍了简单网络管理协议(SNMP)的发展历程,在此基础上,对三种网络管理协议的发展进行了展望。

关键词:网络管理　网络管理协议　SNMP　CMIP　CMOT

一、引言

传统的网络管理系统主要包括管理者(Manager)、代理(Agent)和网络管理协议三大要素,如图 1 所示。

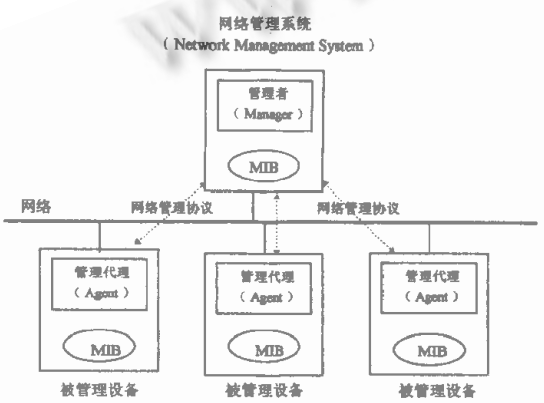

图 1　传统网络管理系统

其中,管理者可以自动或按照用户规定去轮询被管理设备中的管理信息,并对其进行分析和处理,以达到对被管理设备进行监视和控制的目的。代理则负责收集被管理设备的信息及响应管理者发来的轮询,还可以根据用户设定的变量阈值在被管理设备出现问题时产生陷阱(Trap),向管理者发出告警。网络管理协议则是管理者和管理代理之间进行通信的标准。著名的网络管理协议有基于 OSI 的公共管理信息服务/公共管理信息协议(Common Management Information Services/ Common Management Information Protocol,简称 CMIS/ CMIP)、基于 TCP/ IP 的简单网络管理协议(Simple Network Management Protocol,简称 SNMP)和过渡性的在 TCP/IP 之上的公共管理信息服务与协议(Common Management information service and protocol Over TCP/ IP,简称 CMOT)。其中,SNMP 以其简单和易于实现得到广大厂商的普遍支持,是目前使用最广泛的网络管理协议。

二、公共管理信息协议(CMIP)

CMIP 是国际标准化组织 ISO 制定的公共管理信息协议,主要针对 OSI 七层协议参考模型而设计,用来提供标准的公共管理信息服务(CMIS)。CMIP 通信的体系结构如图 2 所示。

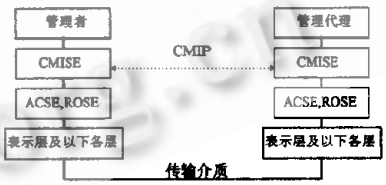

图 2　CMIP 通信体系结构

其中,CMISE、ACSE 和 ROSE 是应用层中与网络管理有关的三个重要元素,简介如下:

· CMISE:Common Management Information Service Element,即公共管理信息服务元素,它负责网络管理信息的逻辑通信。

· ACSE:Association Control Service Element,即联结控制服务元素,它负责建立和拆除两个系统(管理者、管理代理)之间应用层的通信联结。

· ROSE:Remote Operation Service Element,即远程操作服务元素,它负责建立和释放应用层的连接。

在 OSI 七层协议参考模型中，ISO 对每个通信协议都是分成两部分进行定义：一是协议对上层实体提供的通信服务，二是对等协议实体之间的信息传输服务。CMIS/ CMIP 也不例外。在 OSI 管理信息通信中，管理者和管理代理调用 CMISE 来进行管理信息的交换。CMISE 向上提供服务访问点与管理者或代理交换原语，向下通过 ACSE 和 ROSE 的服务按照公共管理信息协议(CMIP)收发 CMIP PDU(协议数据单元)。CMIP PDU 需要传输层提供面向连接的传输服务。

三、简单网络管理协议(SNMP)

SNMP 是 Internet 组织为适应 Internet 的发展而制定的基于 TCP/IP 的网络管理协议，主要用于解决近期内 TCP/IP 网络的管理问题。SNMP 推出后便以其简单和易于实现而取得了出人意料的成功，使得这一原本“暂时”的网络管理解决方案成为事实上的工业标准。

1. 第一版简单网络管理协议(SNMP v1)

1987 年，几个工程师开发了简单网关监控协议(Simple Gateway Monitoring Protocol，简称 SGMP)，用来对网关进行监视和管理。随着网络管理需求的进一步增加，互联网工程任务组(Internet Engineering Task Force，简称 IETF)在改造 SGMP 的基础上于 1988 年 8 月推出了第一版的简单网络管理协议，即 SNMP v1，它采用的管理信息结构定义是 Internet 管理信息结构(SMI)和 Internet 管理信息库(MIB)。

SNMP 提供的管理操作简单而实用，即采用“取/存”机制：管理者可以通过“取”操作从代理获取所需的管理信息，也可通过“存”操作对被管理对象的值进行修改和设置，从而达到对被管理对象进行控制的目的。具体来说，SNMP v 1 提供了 Get、Get-next、Set 和 Trap 四类管理操作。

·Get：从代理处获取特定的 MIB 对象值。

·Get-next：从代理处获取所提供的 MIB 对象在字典顺序上的后继对象值。这种操作提供了强大的通过遍历 MIB 而获取大量管理信息的能力。

·Set：修改、设置 MIB 对象的值。

·Trap：代理向管理者报告重要的事件。Trap 操作提供了一种异步报告机制，使管理者能及时了解代理方出现的问题，从而提高管理效率。

2. 第二版简单网络管理协议(SNMP v2)

SNMP v1 以其简单、实用而受到普遍欢迎，但是，正由于 SNMP v1 的设计初衷是力求简单，因而没有过多考虑安全性问题。应广大用户和厂商的要求，IETF 于 1992 年开始了对 SNMP v2 的研究和开发。同年 7 月，一组被称为安全 SNMP(即 S-SNMP)的文档作为建议标准发布。不久，简单管理协议(SMP)也被提出。SMP 增强了 SNMP v1 的功能，并融合了 S-SNMP 的安全机制，因而成为 SNMP v2 开发的基准。

IETF 于 1994 年和 1996 年两次推出 SNMP v2，它与 SNMP v1 相比较，有如下改进：

·吸纳了 S-SNMP 对 SNMP v1 的安全增强，提高了安全性。

·支持分布式管理，提供管理者之间进行管理信息交换(Manager－to－Manager)的有效机制，使中层管理者能够分担主管理者的任务并使管理体系层次化，从而有利于大型网络的管理。

·增加了 Get-bulk 和 Inform 操作：Get-bulk 可以用来获取代理方的大量数据；Inform 操作则用于一个管理者向另一个管理者发送请求信息。

3. 第三版简单网络管理协议(SNMP v3)

虽然 SNMP v2 对 SNMP v1 作出了一些改进，但仍不尽完善，尤其是存在 SNMP v2 * 和 SNMP v2u 两种方案在安全性问题上的争执，以致许多与安全性有关的内容并未被写进正式的 SNMP v2 文本。因此，1997 年 4 月，IETF 成立了 SNMP v3 工作组，决心进一步提高安全性，并定义一个可以长久使用的框架，工作重点是统一和使用 SNMP v2 * 及 SNMP v2u 已经取得的成果。经过历时一年多的努力，工作组于 1998 年 10 月向 IESG 提交了所有的文档作为草案标准(Draft Standard)。

SNMP v3 的意见请求 RFC(Request For Comments)包括四类，如下所示：

· 数据定义语言：包括 RFC 1902、RFC 1903 和 RFC 1904。

· MIB 模块：包括 RFC 1907。

· 协议操作和传输映射：包括 RFC 1905 和 RFC 1906。

· 安全和管理：包括 RFC 2271 到 RFC 2275。

其中，前三类继承了 SNMP v2 的内容，第四类是从 SNMP v2 * 和 SNMP v2u 两种方案中提取出来，补充到 SNMP v3 中去的，是 SNMP v3 中新的内容，因此对这个部分略作解释。

· RFC 2271：“An Architecture for Describing SNMP Management Frameworks”，描述了 SNMP 管理框架的体系结构，并着重于与安全和管理有关的方面。

· RFC 2272："Message Processing and Dispatching for the SNMP"，描述了对在 SNMP 的体系结构内的 SNMP 报文的处理和调度，包括将不同版本的 SNMP 报文分派到合适的 SNMP 报文处理模块以及协议数据单元(PDU)和 SNMP 应用程序之间的调度。

· RFC 2273："SNMP v3 Applications"，描述了五类和 SNMP 引擎有关的应用，它们是命令发出者(Command Generators)、命令响应者(Command Responders)、报告发送者(Notification Originators)、报告接收者(Notification Receivers)和委托助理(Proxy Forwarders)。

· RFC 2274："The User - based Security Model (USM)for SNMP v3"，描述了 SNMP v3 的基于用户的安全模型。USM 能够抵御常见的几种安全威胁，它们是：修改信息(modification of information)、伪装(masquerade)、修改报文流(message stream modification)和泄密(disclosure)。在这里，SNMP v3 中的安全主要是指在报文级别实现的安全。

· RFC 2275："View - based Access Control Model (VACM)for the SNMP"，描述了在 SNMP 体系结构中基于视图的访问控制模型的使用，定义了对管理信息的访问加以控制的过程元素(elements of procedure)。访问控制是在协议操作级别实现的安全，加上 SNMP v3 在报文级别实现的安全，二者共同实现 SNMP v3 的安全管理框架。

四、TCP/IP 之上的公共管理信息服务与协议(CMOT)

Internet 组织推出 SNMP 的目的是要在短期内满足网络管理的需要，而从长远来看，网络管理协议应该向 OSI 国际管理标准，即 CMIS/CMIP 靠拢。因此，Internet 组织又推出了 CMOT 这一在 TCP/IP 之上的提供 CMIS 服务的网络管理协议，以满足未来 Internet 网络的管理需要。CMOT 通信的体系结构如图 3 所示。其中，CMISE、ACSE、ROSE 与 CMIP 部分介绍的相同，不再赘述。LPP 是轻量表示协议(Lightweight Presentation Protocol)，用来衔接 OSI 的应用层与 Internet 的 TCP/IP 协议的 TCP/UDP 传输层。这样，CMOT 就实现了在 TCP/IP 网络上提供 CMIS 服务。

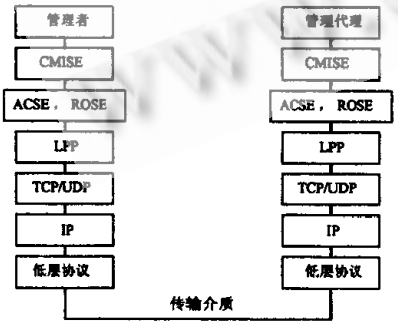

图 3　CMOT 通信体系结构

五、三种协议的比较

以上分别对 CMIS/ CMIP、SNMP 和 CMOT 这三种网络管理协议作了介绍，下面从几个角度出发对它们作一比较。

·协议的体系结构不同。图 4 为三种协议在 OSI 七层协议参考模型中所处位置的比较。

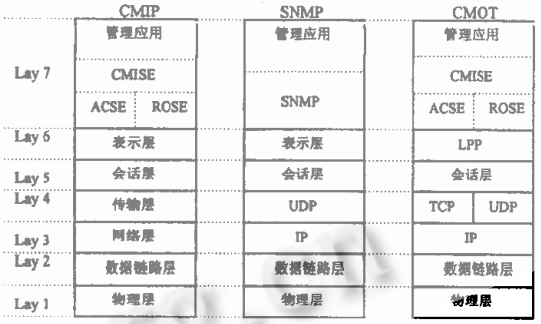

图 4　三种协议在 OSI 七层协议参考模型中的位置

CMIS/ CMIP 是国际标准化组织 ISO 主要针对 OSI 七层协议参考模型而制定的；SNMP 是为 Internet 网络而设计的；CMOT 则是为了在 TCP/ IP 网络上提供 OSI 网络管理服务而制定的一种折衷方案。

·从需要的传输支持服务来看，CMIP 要求下层提供面向连接的服务；SNMP 只要求无连接服务(UDP)；而 CMOT 在面向连接的 TCP 和无连接的 UDP 支持下都可工作。

· 从协议的操作方式来看，虽然三种协议都采用"请求 - 响应"型的操作方式，但 CMIP 和 CMOT 的操作指令比 SNMP 的复杂，当然，功能也更强大。

六、结束语

CMOT是一种过渡性方案，由于SNMP的成功而被放弃使用。作为国际标准的CMIP是一个通用协议，能够管理一切网络设备，功能也很强大，但实现起来比较复杂，而且必须依赖OSI七层协议参考模型下几层的实现，因此离实际应用还有很大距离。相反，SNMP简单、容易实现，两次版本的升级更使得SNMP在完成一般网管工作的基础上朝着进一步提高安全性和进行层次化管理的方向发展。最新版本的SNMP(SNMP v3)已经能够满足一般网络管理在内容和安全性上的要求。因此，有理由相信，简单网络管理协议不会在短期内被符合国际标准的CMIP取代，而是在网络管理中继续保持强大的生命力。

参考文献

[1] Introduction to SNMP v3 (http://www.int.snmp.com) Nov.1998

[2] Ray Hunt. SNMP, SNMP v2 and CMIP - the technologies for multivendor network management. Computer Communications 1997 - 20

[3] 岑贤道，安常青.网络管理协议及应用开发.清华大学出版社，1998

[4] 胡谷雨.现代通信网和计算机网管理.北京：电子工业出版社，1996

（来稿时间：1998年12月）