校园网网管分析与实践

李兴国　顾震苏

(四川大学信息管理中心　成都 610065)

摘　要　随着校园网的迅速发展,合理、有效的网络管理也成了校园网管理工作的重要方面。校园网络管理的主要目的就是保障网络运行的品质,如维持网络传送速率、降低传送错误率、确保网络安全等。所以校园网络管理可借助网络管理工具或技术人员本身的技术经验实施网络管理。本文介绍了网络管理的相关概念及协议,分析了校园网络管理的现状,提出了校园网络管理具体内容及方法,供大家参考和交流。

关键词　校园网,网络管理,SNMP

关于网络管理,国际上已制定相关标准,许多专业部门、网络公司也推出了诸多解决方案。但因为校园网投入资金以及网络技术和管理等一系列问题的存在,各校园网管理的具体问题仍需认真调研和仔细分析。随着校园网的不断发展和应用,网络管理和安全防范问题也越来越复杂。虽然已经有越来越多的管理人员开始关注网络的管理,但是由于对于网络管理意识薄弱、投入大小、自身技术人员知识掌握程度、重硬轻软、先期没有完整的规划、设计等因素,造成当前校园网建设者存在较大误区。对于校园网络管理,在管理什么和如何管理方面是智者见智,仁者见仁。

1　网络管理

1.1　网络管理的定义

网络管理(Network Management)就是通过某种方式对网络状态进行调整,使网络能正常、高效地运行。其目的很明确,就是使网络中的各种资源能够更加高效地利用,当网络出现故障时能及时作出报告和处理,并协调、保持网络的高效运行等。

网络管理包含五部分:网络性能管理、网络设备和应用配置管理、网络利用和计费管理、网络设备和应用故障管理以及安全管理。ISO 建立了一套完整的网络管理模型,其中包含了以上五部分的概念性定义。

性能管理:衡量及利用网络性能,实现网络性能监控和优化。网络性能变量包括网络吞吐量、用户响应次数和线路利用。

配置管理:监控网络和系统配置信息,从而可以跟踪和管理各种版本的硬件和软件元素的网络操作。

计费管理:衡量网络利用、个人或小组网络活动,主要负责网络使用规则和帐单等。

故障管理:负责监测、日志、通告用户,(一定程度上可能)自动解决网络问题,以确保网络的高效运行,这是因为故障可能引起停机时间或网络退化等。故障管理在 ISO 网络管理单元中是使用最为广泛的一个部分。

安全管理:控制网络资源访问权限,从而不会导致网络遭到破坏。只有被授权的用户才有权访问敏感信息。

常见的网络管理协议主要有由 IETF 定义的简单网络管理协议 SNMP(Simple Network Management Protocol)。远程监控(RMON)是 SNMP 的扩展协议;另一种是由 ISO 定义的通用管理信息协议 CMIS/CMIP(the Common Management Information Service/Protocol)。典型地,网络管理系统包括四个部分:若干被管的代理(Managed Agents)或探测器(Probe),主要负责收集众多网络节点上的数据;至少一个网络管理器(Network Manager)或控制台(Console),主要负责集合并分析探测器收集的数据,提取有用信息和报告;一种公共网络管理协议(Network Management Protocol);一种或多种管理信息库(MIB,Management Information Base)。其中网络管理协议是最重要的部分,它定义了网络管理器与被管代理间的通信方法,规定了管理信息库的存储结构、信息库中关键字的含义以及各种事件的处理方法。

网络管理结构:如图 1 所示。

1.2　网管协议

(1)SNMP

SNMP 是专门设计用于在 IP 网络管理网络节点(服务器、工作站、路由器、交换机及 HUBS 等)的一种标准协议,它是一种应用层协议。SNMP 使网

李兴国　工程师,硕士;顾震苏　工程师。

络管理员能够管理网络效能，发现并解决网络问题以及规划网络增长。通过 SNMP 接收随机消息(及事件报告)网络管理系统获知网络出现问题。

SNMP 管理的网络有三个主要组成部分：管理的设备、代理和网络管理系统。管理设备是一个网络节点，包含 ANMP 代理并处在管理网络之中。被管理的设备用于收集并储存管理信息。通过 SNMP，NMS 能得到这些信息。被管理设备，有时称为网络单元，可能指路由器、访问服务器，交换机和网桥、HUBS、主机或打印机。SNMP 代理是被管理设备上的一个网络管理软件模块。SNMP 代理拥有本地的相关管理信息，并将它们转换成与 SNMP 兼容的格式。NMS 运行应用程序以实现监控被管理设备。此外，NMS 还为网络管理提供了大量的处理程序及必须的储存资源。任何受管理的网络至少需要一个或多个 NMS。

目前，SNMP 有 3 种：SNMPV1、SNMPV2、SNMPV3。第 1 版和第 2 版没有太大差距，但 SNMPV2 是增强版本，包含了其它协议操作。与前两种相比，SNMPV3 则包含更多安全和远程配置。为了解决不同 SNMP 版本间的不兼容问题，RFC3584 种定义了三者共存策略。

SNMP 还包括一组由 RMON、RMON2、MTB、MTB2、OCDS 及 OCDS 定义的扩展协议。

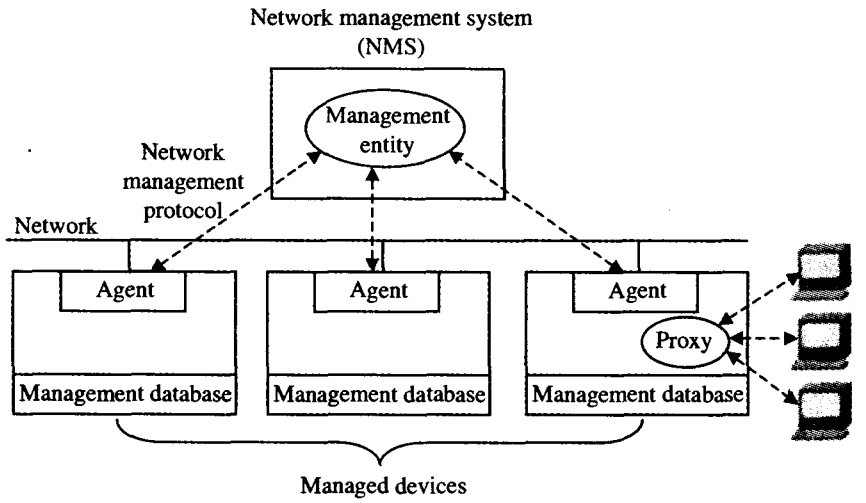

图 1　网络管理结构

(2)RMON

远程监控(RMON)是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

RMON 最初的设计是用来解决从一个中心点管理各局域分网和远程站点的问题。RMON 规范是由 SNMP MIB 扩展而来。RMON 中，网络监视数据包含了一组统计数据和性能指标，它们在不同的监视器(或称探测器)和控制台系统之间相互交换。结果数据可用来监控网络利用率，以用于网络规划，性能优化和协助网络错误诊断。

当前 RMON 有两种版本：RMONv1 和 RMONv2。RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMONv2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。

RMON 监视系统有两部分构成：探测器(代理或监视器)和管理站。RMON 代理在 RMON MIB 中存储网络信息，它们被直接植入网络设备(如路由器、交换机等)，代理也可以是 PC 机上运行的一个程序。代理只能看到流经它们的流量，所以在每个被监控的 LAN 段或 WAN 链接点都要设置 RMON 代理，网管工作站用 SNMP 获取 RMON 数据信息。

(3)CMIS/CMIP

通用管理信息协议(CMIP：Common Management Information Protocol)是与通用管理信息服务(CMIS：Common Management Information Services)同时使用的一种 ISO 协议，支持网络管理应用程序和管理代理之间的信息交换服务。CMIS 定义了一个网络管理信息服务系统。CMIP 提供的一个接口支持 ISO 和用户定义(user-defined)管理协议。TCP/IP 网络中的 CMIP 规范称之为 CMOT(即 CMIP Over TCP)；而 IEEE 802 LAN 中的版本称之为 CMOL(即 CMIP Over LLC)。此外，CMIP/CMIS 是作为 TCP/IP 协议组中简单网络管理协议(SNMP：Simple Network Management Protocol)的一种竞争协议提出的。

CMIP中采用可靠ISO(ISO-reliable)面向连接传输机制并内置安全机制,其功能包括:访问控制、认证和安全日志(security log)。管理信息在网络管理应用程序和管理代理之间交换。管理对象是管理设备的一个特征且可以被监控、修改或控制等,并能完成各种作业。

CMIP并没有指定网络管理应用程序的功能,只定义了管理对象的信息交换机制,而没有定义信息的使用和说明。

与SNMP相比,CMIP的主要优势在于:

CMIP变量不仅用于传发信息还可以完成各种作业;而SNMP不具备这种功能。

CMIP更加安全,它内置安全机制,功能包括访问控制、认证和安全日志(security log)。

CMIP功能强大,在单个请求下可以实现多种功能。

CMIP在异常网络条件下具有更好的报告功能。

对管理对象中的管理信息的访问由通用管理信息服务元素(CMISE)提供,CMISE使用通用管理信息协议(CMIP)为管理服务发布请求。由CMIP/CMISE提供的管理服务可分成两组:管理操作服务(management operation service),即指管理器请求代理提供一定服务或信息的过程;通知服务(notification service),即指管理代理通知管理器已经发生的事件或事件集。

1.3 网管软件

网管软件平台提供网络系统的配置、故障、性能及网络用户分布方面的基本管理,是网管系统的核心。在功能上,网管软件可以归纳为体系结构、核心服务和应用程序三个部分。首先,从基本的框架体系方面,网管软件需要提供一种通用的、开放的、可扩展的框架体系。网管软件既可以是分布式的体系结构,也可以是集中式的体系结构,实际应用中一般采用集中管理子网和分布式管理主网相结合的方式。同时,网管软件是在基于开放标准的框架的基础上设计的,它应该支持现有的协议和技术的升级。而且网管软件还应该能够提供一些核心的服务来满足网络管理的部分要求。核心服务应该包括网络搜索、查错和纠错、支持大量设备、友好操作界面、报告工具、警报通知和处理、配置管理等等。此外,网管软件还有必要加入一些有价值的应用程序,以扩展网管软件的基本功能。常见网管软件中的应用程序主要有:高级警报处理、网络仿真、策略管理和故障标记等。

2 校园网网管现状

网络管理是指规划、监督、控制网络资源的使用和网络的各种活动,以使网络的性能达到最优。其目的在于提供对计算机网络进行规划、设计、操作运行、管理、监视、分析、控制、评估和扩展的手段,从而合理地组织和利用系统资源,提供安全、可靠、有效和友好的服务。随着高校信息化建设不断的发展深入,校园网在信息化建设领域发挥着越来越重要的地位。网络中心承担着校园网的规划、建设、运营和维护等义务,它的工作无疑是非常沉重的。其中的网络管理更是重中之重。

很多高校网络管理者只是对网络设备、线路和用户进行了严格的管理,而没有建立综合网管系统,以实现包括全网故障分析和故障定位、全网性能综合分析等功能的全网的综合管理。校园网的规模一般都比较大,少则上千大则上万个信息点,小的学校整个网管中心只有几个人,大的学校相对要多一些,只有设备提供商提供的网管软件,而对于整个网络以及网络应用在管理上存在较大偏差。而网络的管理绝不仅仅局限于此,设备提供商所提供的管理软件虽然在网络拓扑发现、对傻设备可进行有效管理以及提供全网拓扑等方面有独到之处,但这主要只是对网元进行了管理,并且该类网管系统对于其他厂商设备以及业务应用等方面的管理存在欠缺。

而通过正确而又适合自身的网络管理,高校不但可以提高网络可靠性,还可为网络提高效益。网络管理的最终目的在于最大限度地增加网络的可用时间,提高网络单元的利用率、网络性能、服务质量、安全性和经济效益,简化多制式、多厂商混合网络环境下的管理和控制网络运行成本,提供网络规划的依据。

由于管理意识、技术水平、对网络管理的投入等原因,过去造成网络建设者存在重硬轻软的意识,而且第三方的管理软件也存在价格高、需要更好的技术人员维护管理等因素。但是,在一个平台上对网络进行多层次、多方面的管理已成为了当前网络建设者的共识,实现真正地网络管理已开始在高校中逐渐启动。

3 校园网网络管理

有效地管理网络,更大程度地提高网络管理质量和品质,是每个高校网络管理员所追求的目标。

一般而言,校园网的网络管理的也包括五大功能,它们是:网络的失效管理、网络的配置管理、网络的性能管理、网络的安全管理、网络的计费管理。

3.1 网络故障管理

为确保网络系统的高稳定性,在网络出现问题时,必须及时察觉问题的所在。它包含所有节点运作状态、故障记录的追踪与检查及平常对各种通讯协议的测试。

网络故障管理，是当今网络管理体系结构的一个主要组成部分，含盖了诸如检测、隔离、确定故障因素、纠正网络故障等功能。设立故障管理的目标是提高网络可用性，降低网络停机次数并迅速修复故障。

一个故障管理系统所具备的基本必要条件有：

监控和收集网络设备、流量情况以及实时过程方面的统计信息，以避免和预测可能性故障。

设置极限并对可能发生的网络故障发出警报，以警告网络管理端。

设置警报，报告网络设备和链路上的性能退化情况。

设置警报网络资源（诸如硬盘空间）使用和限制问题。

遥控网络设备的重启、关机等操作。

集中化的 Consol 以实现以上所有功能。

典型的故障管理系统遵循以下步骤：

探测		分析		采取措施
差错检测 数据汇集 差错处理	→	诊断 事件记录	→	开始作用 服务重启 黑名单 (Black-Listing)

一旦出现故障，会产生一个报告并被发送至故障分析器。故障分析器诊断并记录故障问题。最后，系统或个人根据故障分析器上的信息采取适当措施，如隔离差错、黑名单或故障部件；自动重启/修复服务以及更换系统管理员。

3.2 网络配置管理

随时掌握网络内任何设备的增减与变动，管理所有网络设备的设置参数。当故障发生时，管理人员得以重设或改变网络设备的参数，维持网络的正常运作。

网络配置管理主要涉及网络设备（网桥、路由器、工作站、服务器、交换机及其它）的设置、转换、收集和修复等信息。

任何大小的网络流量都处于常量（Constant State）状态。任何网络工程师都可以随时更换交换机和路由器的配置。配置更换会对网络可靠性及服务造成破坏性影响。网络配置管理的目标是节约用户时间 & 降低网络设备误配置引起的网络故障。网络配置管理系统允许用户控制网络变换，简化网络管理工作并迅速修复配置差错。

配置适当设备与网络安全性之间具有直接相连的关系。当今网络配置管理方案主要注重于实现网络自动转换处理、安全保护和设备管理等。无论配置更换是由恶意攻击、手动修正差错引起，还是由网络产品本身的缺限所引起，都会使设备易于遭受攻击并因此影响商业运行。

目前，基本上有两种主要的网络配置工具：一种是由设备供应商提供的工具（如北电的 JDM）；另一种是由第三方公司提供的工具（如 HP Openview）。

供应商指定工具，如思科、北电产品，只能与他们自己的对应设备共同使用，这对于同种设备的情形（配置采用单个供应商设备）而言是个很好的选择。

通常网络中采用的是由多供应商提供的一系列设备。在这种情形下，由第三方公司提供的包含多供应商设备的这种工具将会是一个很好的选择。

3.3 网络性能管理

在于评估网络系统的运作，统计网络资源的运用及各种通讯协议的传输量等，更可提供未来网络提升或更新规划的依据。

网络性能管理指的是一种网络容量规划（Capacity Planning）过程，提供基于帐单的使用，帮助理解流量的服务质量，并向客户/用户提供报告以遵循服务等级协议（SLA），从而使网络管理端获取有关网络的补充信息。

网络性能管理由两部分组成：1）一组功能单元，预计和报告网络设备行为以及网络或网络元素的效力；2）一组子功能单元，包括收集统计信息、维护和检查历史日志、决定自然条件和人为条件下的系统性能以及改变操作的系统模型。

基本衡量标准有：带宽、数据包传输速率、数据包延迟、往返时间和 RTT 变化、数据包损失、可达到性、电路性能。

一个理想的性能管理机制必须是一个独立的、可扩展的并可以提供综合完整的网络覆盖能力的平台。这样网络管理端可以监控正在进行的物理网络性能，分析其数据以实现终端对终端服务性能的相互连接，并在对网络行为具有完全理解的基础上采取行为措施。完善的性能管理应该贯穿网络技术每一层。结合配置技术综合考虑，网络管理端可以认识到性能管理对其用户的影响。

3.4 网络安全管理和访问控制

为防范不被授权的用户擅自使用网络资源，以及用户随意破坏网络系统的安全，要随时做好安全措施，如合法的设备存取控制与加密等。

网络安全管理主要涉及访问控制或网络资源管理。访问控制管理指的是安全性处理过程，即妨碍或促进用户或系统间的通信，支持各种网络资源如计算机、Web 服务器、路由器或任何其它系统或设备间的相互作用。

认证过程主要包含两个步骤：

1）认证：登录过程；

2）自主访问控制（Discretionary Access Control）：校验用户决定他们是否有权访问具有更高安

（下转第 43 页）

用SAL下的sal-smc工具对NSPK协议的认证性进行了分析，找到了一个已知的认证性攻击。通过生成的反例发现存在如下的攻击序列：

(1)$A \rightarrow I$: $\{N_a, A\}_{Ki}$

(2)$I(A) \rightarrow B$: $\{N_a, A\}_{Kb}$

(3)$B \rightarrow I(A)$: $\{N_a, N_b\}_{Ka}$

(4)$I \rightarrow A$: $\{N_a, N_b\}_{Ka}$

(5)$A \rightarrow I$: $\{N_b\}_{Ki}$

(6)$I(A) \rightarrow B$: $\{N_b\}K_b$

入侵者在第(1)步解密消息，获得Na，并在第(2)步通过获得的Na冒充A与B进行通信，第(3)步B与I(B认为是A)进行通信，第(4)步I将B发给它的消息重放给A，第(5)步I解密A发送回来的消息得到Nb，第(6)步I冒充A向B发送得到的N_b。I假冒A成功。这样，B认为是与A建立了认证关系，而实际上一直与B进行通信的是I。

结束语 本文对SAL框架下的安全协议分析技术进行了研究，介绍了SAL中间语言对安全协议的描述方法，给出了在SAL框架下对入侵者模型和通信模型的刻画方法，并以经典的NSPK协议为例，找到了一个已知的认证性攻击。下一步的研究方向是针对开端问题等目前安全协议形式化分析领域所面临的公开问题[6]，尝试在SAL下对这类问题的验证方法进行研究，以求SAL在安全协议领域应用能不断拓展。

参考文献

1 Rajan S, Shankar N, Srivas M K. An integration of model checking with automated proofchecking. In: Proceedings of the 7th International Conference On Computer Aided Verification, volume 939 of LNCS, Liege, Belgium, Springer Verlag, 1995. 84～97

2 Bensalem S, Ganesh V, Lakhnech Y, et al. An overview of SAL. In: Holloway C M ed. Fifth NASA Langley Formal Methods Workshop (LFM 2000), 2000. 187～196

3 Owre S, Rushby J, Shankar N. PVS: A prototype verification system. In: Proc. 11th International Conference on Automated Deduction (CADE), volume 607 of Lecture Notes in Artificial Intelligence, Saratoga, NY, 1992. 748～752

4 de Moura L. SAL: Tutorial. Available at: http:// sal. csl. sri. com/doc/salenv_tutorial. pdf

5 Needham R, Schroeder M. Using encryption for authentication in large networks of computers. Communications of the ACM, 1978, 21(12): 993～999

6 Meadows C. Formal methods for cryptographic protocol analysis: Emerging issues and trends. IEEE Journal on Selected Areas in Communication, January 2003, 21(1): 44～54

(上接第36页)

全控制权限的敏感区域和文件的认证级别。

安全审计是安全管理中访问控制过程的一部分。审计系统可以追踪到特殊登录用户以及其访问资源。

代理服务器和防火墙是安全管理中的两个特定访问控制系统，主要用于防止公共网络如因特网成员访问内部网络资源。代理服务器允许内部用户作为用户代理访问因特网。因此内部IP地址可以隐藏，从而降低外部攻击的可能性。另外代理服务器也允许网络管理端管理内部用户的因特网访问权限。

在一定的规范和原则下，防火墙允许外部用户访问内部网络资源。

3.5 网络的计费管理

收集、缓冲、付款传送和计费信息。校园网络要做到可运营、可管理和用网公平性，网络使用身份验证、授权和计费是必不可少的，而且要实现灵活计费的策略。

另外，日志管理也是网络管理的重要组成部分之一。当网络发生问题时，如何第一时间找到问题的根源？如何满足公安部追查用户上网行为的要求？应用资源众多，如何掌握用户的上网习惯等。采用强大多样的日志保存方式，有效记录这些信息、保存日期较长的日志，管理员坐在办公室就可以轻松的掌握办公区、学生区、家属区等各层用户的上网行为；当出现问题时，也可以迅速找到问题的根源。

最后，对整个校园网中的硬件及软件都要分门别类地进行建档，有完整地使用日志、维护日志等。参数的调整、配置的改动都要有详细的记录，不会因为人员的调动或不到场网络管理就停顿下来，管理日志也为以后的网络管理积累经验和技术文档。建立健全各种规章制度，如网络使用规范、上网规范、操作管理制度、维修保养制度等。

总结 总之，校园网络管理实际上是一件既技术性很强又琐碎的事情，在旁人看来，即使没有人去管它，建好网也正常运转着，如果平时没有对网络进行诊断和管理，一旦出了故障，能否及时修复就成问题了。作为网络管理人员如果不能紧跟技术发展潮流，随时学习新的网络知识最后很可能被淘汰。所以在平时的工作中不断地学习新的知识，多多实践。

网络管理本身还有许多空间和领域值得我们去学习和创新，希望本文能够使大家对网络管理和维护的理解有所帮助。

参考文献

1 Tanenbaum A S, The Netherlands. 计算机网路(第四版). 潘爱民译. 清华大学出版社，2004

2 http://www. zdnet. com. cn/

3 http://tech. ccidnet. com/