基于 SNMP 的 IPMAC 绑定系统的研究与设计

洪 诗,李晓强
(上海大学 计算机工程与科学学院,上海 200072)

摘 要:针对当前网络中 IP 地址管理混乱的状况,根据网络管理需求,设计并实现了 IP-MAC-PORT 绑定系统。通过简单网络管理协议(SNMP)定期对路由及交换设备进行数据采集和分析,对网络进行实时监控,追踪并定位出 IP 地址异常主机的具体位置,然后利用交换机支持端口管理的特性,实现对 IP 盗用者的有效网络隔离。

关键词:简单网络管理协议;管理信息库;代理
中图分类号:TP393 **文献标识码**:B **文章编号**:1674-7720(2011)17-0060-04

Research and design of the IPMAC binding system based on SNMP

Hong Shi, Li Xiaoqiang
(Computer Engineering and Science Institute, Shanghai University, Shanghai 200072, China)

Abstract: Aiming at the situation of current network IP address's management chaos, this article designs and implements an IP-MAC-PORT binding system according to the network management needs. Through the simple network management protocol(SNMP), the system collects and analysis the data of routing and switching equipment periodically, monitors network in real-time, and tracks the specific locations of the hosts with abnormal IP addresses. Then, the system realizes the effective separation from IP embezzler's network based on the characteristics of switches supportting port management.

Key words: SNMP; MIB; agent

Internet 的迅速发展和企业网络系统的不断扩展推动了基于 IP 协议的通信量的巨增,随之而来的是 IP 地址管理问题,特别是局域网内部 IP 地址管理,而 IP 地址管理中最重要的就是网络安全问题。影响网络安全的因素有很多,IP 盗用或地址欺骗就是其中一个常见且危害极大的因素。如果缺乏有效的管理,就会导致网络可用性和服务质量的下降,甚至网络的崩溃。面对这种情况,本文在研究简单网络管理协议 SNMP(Simple Network Management Protocol)网络管理模型的基础上设计并实现了 IPMAC 绑定系统。该系统能实时监控网络的运行状态,能及时、准确地发现网络中 IP、MAC 和端口之间的异常变动并发出报警信息,便于网络管理人员及时处理安全隐患,提高了网络的安全性。

1 相关概念

1.1 SNMP 的管理模型

SNMP 是为基于 TCP/IP 的多厂商异构互连网的管理而设计的。它作为工业标准,已被广泛接受,其应用已扩展到其他协议组。

SNMP 的网络管理模型[1]由多个管理代理、至少一个管理工作站、一种通用的网络管理协议、一个或多个管理信息库 MIB(Management Information Base)等组成[2],其模型如图 1 所示。

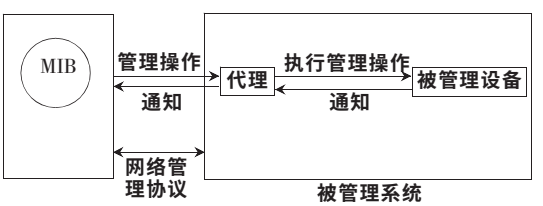

图 1 管理者-代理者-被管理设备关系模型

管理者(Manager)可以是工作站、个人计算机等,它负责发出管理操作的指令,并接收来自代理的信息。

代理(Agent)驻留在被管对象中,对来自管理者的请求进行应答,并随机为管理者报告一些重要的意外事件。

管理信息 MIB 是对通过网络管理协议可以访问信

息的精确定义，通常就是被管理设备的数据库。

网络管理协议是管理者与代理之间通信的协议，它提供一种访问任何厂商生产的网络设备并获得一系列标准值的一致性方式。

1.2 SNMP 协议

SNMP 是一种应用层协议，它只要求使用无连接服务的数据传送服务，自身具有纠错能力，因此减少了网络负担。SNMP 的基本功能包括：监视网络性能、监测并恢复网络故障以及配置网络设备等。SNMP 的协议体系结构由 SMI、MIB 和 SNMP 本身三部分构成。SMI 描述了互连网中受管对象的识别方案和结构；MIB 描述了 SNMP 所用到的管理信息库的结构以及其中变量的定义，SMI 和 MIB 都是用 OSI 的 ASN.1 定义的；SNMP 的 MIB 用于存放网络元素的各种管理参数，SNMP 本身提供在网络管理站和被管对象之间交换管理信息的方法。

网络管理站和被管对象之间通过发送 SNMP 报文来彼此通信。实现 SNMP 协议有两种操作：取值和设置值。为此，SNMP 协议定义了 5 种 PDU (Protocol Data Unit)[3]，即：GetRequest－PDU、GetNextRequest－PDU、SetRequest－PDU、GetReponse－PDU 和 Trap－PDU。其中，GetRequest－PDU 用于访问代理，并从 MIB 中获得变量值；GetNextRequest－PDU 取下 1 条 MIB 值，它提供了一种连续读取 MIB 变量的方法；SetRequest－PDU 用于设置 MIB 中变量的值；GetReponse－PDU 用于对上述 3 个请求的响应；Trap－PDU 用于代理报告一些异常事件，如系统重新初始化、局部链路失效、链路功能恢复以及邻居没有响应等。

每个 SNMP 报文被封装成一个 UDP 数据报，并通过 IP 层发送出去。协议指定在 161 端口接收除“Trap”以外的所有报文，而在 162 端口接收“Trap”报文。这 5 种报文的操作如图 2 所示。

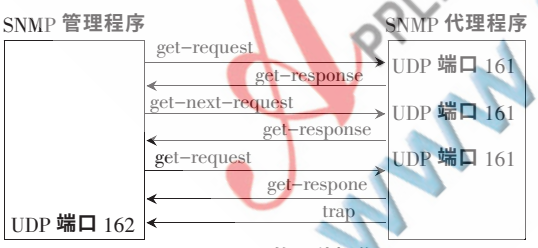

图 2 SNMP 的 5 种操作

1.3 IP 冒用

IP 冒用是指使用者使用未经授权的 IP 地址来配置网上的计算机。由于 IP 地址是一个协议逻辑地址，需要用户设置并随时修改其值，因此无法限制用户修改本机的 IP 地址。如果用户在配置或修改配置时，使用的不是合法获得的 IP 地址，就形成了 IP 冒用。

1.4 IP－MAC 捆绑技术

交换机是局域网的主要网络设备，它工作在数据链路层，基于 MAC 地址来转发和过滤数据包。因此，每个交换机均维护着一个与端口对应的 MAC 地址表。任何与交换机直接相连或处于同一广播域的主机的 MAC 地址均会被保存到交换机的 MAC 地址表中。因此，可以在交换机上使用 IP－MAC 绑定，在交换机上形成一个静态的 IP－MAC 对应表，以达到非法 MAC 无法通过交换机登录网络的目的。

1.5 多层 B/S 结构

多层 B/S 体系结构的优越性体现在以下几点：将表现与功能进一步分离，可独立优化各层以提高系统的可伸缩性与综合性能；平台通用性强，功能模块可重用；对客户端的要求与限制大大减低，维护与升级方便；开发过程的有限并行等。同时，中间件技术也被引进来，它是一些独立的代码封装体，提供特定的服务[3]。

2 系统总体设计

2.1 设计思路

以太网交换机根据端口号与节点 MAC 地址的对应关系建立“端口号/MAC 地址映射表”。当有帧从某端口到达交换机时，交换机的交换控制中心将根据“端口号/MAC 地址映射表”的对应关系找出对应帧目的地址的输出端口号，为输入端口到输出端口建立连接，这种端口之间的连接可以根据需要同时建立多条。根据以太网交换机工作原理可知，在整个网络中，某个确定节点的 MAC 地址与交换机端口号的对应关系只可能出现在下列两种情况中：(1)出现在与之直接相连的交换机的“端口号/MAC 地址映射表”中，且其对应的交换机端口号必为该节点物理连接的端口号；(2) 出现在与之不直接相连的交换机的“端口号/MAC 地址映射表”中，则其对应的交换机端口号必为该交换机与其他交换机的级连端口上。而如果交换机的某个端口用于级连，也就是不接主机，显然不引入安全问题，这种情况不用考虑。因此，如果在所有交换机的“端口号/MAC 地址映射表”中出现两个或两个以上非级连端口与某个确定主机的 MAC 地址对应，说明必然有人使用了他人主机的 MAC 地址(修改了其本机的 MAC 地址)。也就是说，如果能够动态获得整个网络中各交换机非级连端口与节点 MAC 的映射表，就可以发现异常 MAC 地址。

在 TCP/IP 网络中，主机的 IP 地址只是主机在网络层中的地址，不能直接用来进行通信。若要将网络层中传送的数据包交给目的主机，必须知道该主机的 MAC 地址。因此，必须在 IP 地址和主机 MAC 地址之间进行转换。在以太网上，IP 地址到 MAC 地址的转换由地址转换协议(ARP)来完成。为了找出与某个 IP 地址对应的 MAC 地址，主机要采用 MAC 广播地址发送 ARP 请求包，带有 MAC 广播地址的帧到达本地网络的每个网络接口。ARP 请求包基本询问这样一个问题“我这里拥有 IP 地址所对应的 MAC 地址是什么？”，一般只有与指定 IP 地址一致的主机才响应这个 ARP 请求，其他主机一概忽视该 ARP 请求。ARP 请求的目标主机将发送一个

数据包作为接收到的IP数据包的答复。回答需要了解ARP广播请求包发送者的IP地址及MAC地址的联系。为了加速IP地址解析的过程，每一个主机都有一个ARP Cache，里面保存了一些最近访问的一些节点的IP与MAC地址的对应信息。如果能够获得这些IP与MAC地址的对应信息，就可以发现异常IP地址。监听出口路由器的ARR Cache，可以找到网络上活动节点的IP地址和MAC地址的对应信息，但这可能会增加路由器的负担，影响出口速度，最好能从各交换机获取活动IP与MAC的对应信息。

通过对Internet MIB和SNMP的研究，发现MIB中的管理对象有一个IP地址翻译实体(AT组)，其MIB对象标识为iso-org-dod-internet-mgmt-mib2-at-atTable(oid=1.3.6.1.2.1.3.1.1.2)。为了进行一步了解交换机的MIB，本设计通过编程获取了Intel Express 500T Ethernet Switch的MIB，并对此MIB进行了分析，发现交换机的每个端口均有一个IP地址翻译实体，其对象标识为：1.3.6.1.2.1.3.1.1.2.x(x为端口号)。定时查询网络上每个交换机的非级连端口的IP地址翻译实体，便可以动态获取各交换机端口号-主机MAC地址映射及主机IP地址-主机MAC地址映射信息。对Intel交换机MIB的进一步分析后发现，与端口工作状态有关的MIB对象标识为1.3.6.1.2.1.2.2.1.7.x(x为端口号)，该值为1时，该端口启用，该值为2时，该端口禁用。MIB对象的命名方法[4]如图3所示。

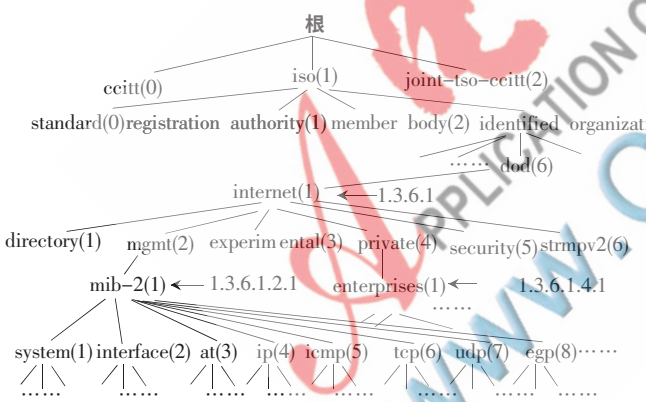

图3 管理信息库的对象命名举例

2.2 系统业务流程

本系统实现了以下4个业务：

(1)实时IP-MAC-PORT信息的显示。获取整个网络中的实时表。实时表主要包含设备IP、MAC、上联端口索引等信息。管理员可对某一IP地址范围进行查询，对已获取的实时表可执行同步到基准，或删除操作。

(2)基准IP-MAC-PORT信息的显示。该业务主要用于对基准信息的维护及管理(注：系统首次初始化时基准IP-MAC-PORT信息由实时表同步得到，并保存在数据库中)，具体包含对基准信息的查询、修改、删除以及设置基准的比较状态。

(3)接口下联设备列表显示。用于查询接口的实时状态。

(4)IPMAC定位。管理员可以根据IP或MAC迅速定位设备在网络中的具体位置。

系统整体的业务流程为：系统启动，系统初始化并开始轮询整个网络的FDB和ARP信息(系统启动后默认设置是每隔5 min轮询一次)，将获取到的信息生成实时IP-MAC-PORT表，将实时表与基准表做差异判断，如有不同信息则生成差异表并根据系统已设置的方式报警通知管理员，以便能及时做出处理，图4为IPMAC系统的整体业务流程。

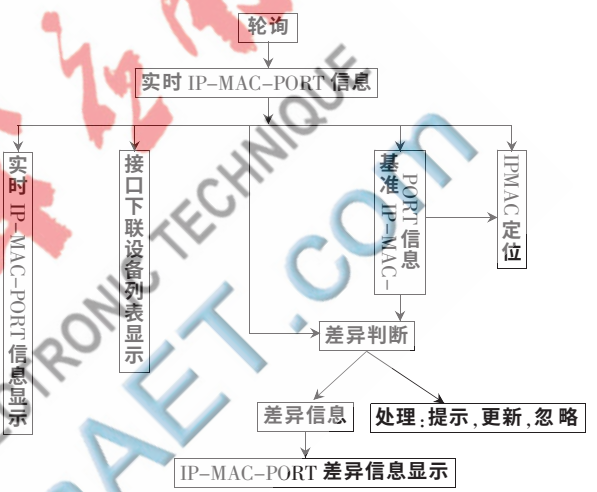

图4 IPMAC系统业务流程图

2.3 功能模块设计与实现

本系统由参数设置、数据采集、数据分析、配置管理和信息发布5个模块组成。

2.3.1 参数设置模块

参数设置模块用于设置和修改系统运行所需的参数，包括：数据采集的时间间隔，需要监测的交换机非级连端口信息(每个端口信息由所在交换机的IP地址和端口号组成)，发现异常对应，是否禁用发现异常的交换机端口。这些参数设置保存在文本文件(ipman.sys)中，系统运行时读入内存。

2.3.2 数据采集模块

数据采集模块按预定的时间间隔从各交换机的MIB采集非级连端口的ARP Cache数据，并将采集的数据生成实时表保存在内存中，它由交换机IP地址、交换机端口号、主机IP地址、与该IP地址对应的MAC地址等信息组成。

2.3.3 数据分析模块

当采集模块完成某次数据采集并与各交换机断开连接后，系统自动启动数据分析模块。数据分析模块从实时表读取采集模块最近一次采集的数据，将每条记录与基准表比较，判断是否存在IP地址-MAC地址或

MAC 地址-交换机端口号异常对应，如存在异常对应，将异常信息生成差异表，它由差异描述、差异分类、时间、操作等数据项组成。其中，异常的类别有 IP 变更、新增终端和终端变更三种。如果发现异常，该模块将向管理员发送报警电子邮件(提示声或短信)，并根据系统设置是否禁用该端口。

2.3.4 配置管理模块

当异常排除后，网管人员可用配置管理模块开启某个交换机的端口，管理员也可用此模块来对交换机端口的一些参数进行配置。

2.3.5 信息发布

采用 CGI 程序从差异表中读取数据，将差异表异常信息通过 IIS 4.0 发布，这样网络管理人员可随时随地浏览查看 IP 地址安全管理日志。

3 系统测试

在一个拥有 50 多台终端的局域网中对 IPMAC 绑定系统做了监控与管理测试，该局域网中包括了各种型号的路由器、交换机、多种平台的服务器等标准 SNMP 设备，测试的结果符合真实网络运行中包含多种网络设备的实际情况。图 5 所示为系统在运行期间获得的差异表。

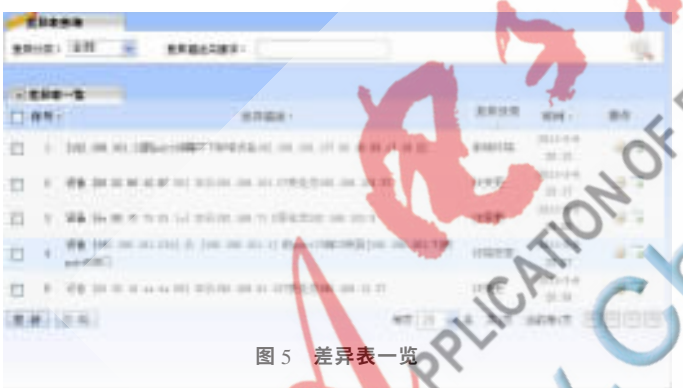

图 5 差异表一览

从图 5 可以看出，无论是网络中新增加一个设备、把设备移到别的端口下，还是修改了设备的 IP 地址，系统都能及时、准确地发现并报警。这就使得网络管理人员能及时地发现网络中出现的异常变动，便于对可能出现的网络安全隐患采取相应的措施。系统在运行期间是全自动的，网络管理人员即使不在电脑旁也能通过系统发送的短信报警信息及时发现网络的常异变动，这就极大提高了网络的可维护性和安全性，减轻了网络管理人员的负担。

针对当前网络运行和管理中存在的 IP 地址理管混乱、IP 冒用等问题，本文在研究 SNMP 网络管理模型的基础上，仔细探讨了 IPMAC 绑定系统的设计与实现，并通过在局域网中的使用测试得到了良好的预期效果：

(1) 系统能有效地发现和阻止 IP 地址及 MAC 地址盗用，提高了网络的安全性和管理水平。

(2)IPMAC 系统具有网络配置工作量小、用户透明、对网络的性能影响小等优点。

(3) 随着计算机网络规模不断扩大以及复杂度的不断提高，SNMP 在提高网络系统的可管理性、可靠性和安全性等方面将发挥越来越大的作用。

参考文献

[1] WALDBUSSER S. RFC1757-Remote network monitoring management information base [DB/OL]. Camegie Mellon University, 1995,2.

[2] 于小红.网络管理软件的选择和应用[J].计算机应用研究,2001(2):25-28.

[3] 岑贤道,安常青.网络管理协议及应用开发[M].北京:清华大学出版社,1999.

[4] STEVEN W R.TCP/IP 详解卷 1:协议[M].北京:机械工业出版社,2008.

(收稿日期:2011-04-14)

作者简介：

洪诗，男，1984 年生，硕士研究生，主要研究方向：网络管理，数据库技术。

李晓强，男，1973 年生，副教授，硕士研究生导师，主要研究方向：多媒体计算与安全。