

宿舍网运营管理系统的设计与实现

许卓斌, 李录章, 郑海山

(厦门大学信息与网络中心, 福建 厦门 361005)

摘要:简单网络管理协议(SNMP)是各类网络设备中通用程度最高的协议之一,通过该协议可以实行对各类网络设备的控制及管理.本文给出了基于SNMP技术,对拥有各类不同品牌网络接入设备的复杂校园宿舍运营网的计费及控制管理系统的实现方法.

关键词:SNMP MIB;网络管理;宿舍网运营

中图分类号:TP 393

文献标识码:A

文章编号:0438-0479(2007)S2-0121-05

随着校园学生宿舍网络的扩大与运营化,实现一个高效率,能兼容多种不同混杂设备的网络管理系统变得十分必要.为了简化和统一网络管理,业界多年来提出了数种网络管理框架,协议标准和服务,其中简单网络管理协议(SNMP)由于易于实现和TCP/IP事实广泛的应用基础而被众多的厂商支持和实现.在20世纪80年代,Internet体系结构委员会提出了简单网络管理协议的第一个版本SNMP v1.1993年正式发表了SNMP v2,设计了更有效和功能更强的网络管理协议.SNMP v3正在逐渐扩充和发展,将能够支持更多的网络应用.SNMP v3保持了SNMP v1和SNMP v2易于理解和实现的特性,并增强了网络管理的安全性能、验证和访问控制等安全管理特性.目前普遍应用的SNMP的局限性主要表现在使用查询操作,不适合强介入模式网管;MIB模式有限,不能支持安全网管,不适合获取大量数据等等,并只能适用与TCP/IP网络.但这些局限性对于使用包月制的简单网络管理行为的校园网络管理,是可以接受的.

1 简单网络管理协议(SNMP)

1.1 管理信息库(MIB)

SNMP网络管理中,MIB是被管资源可以通过网络管理协议访问的信息对象集合.这些资源以对象来表示,每一个对象表示被管理资源的一项属性,这些对象的集合形成了管理信息库.管理信息库使用类似于DNS规则的树型数据结构.

1.2 SNMP报文操作

SNMP定义了5种协议数据单元(PDU),用于管理进程和代理进程之间的信息交换.

(1) `get_request` 用于操作管理进程从代理进程上提取一个或者多个MIB参数值,这些参数值均在MIB中用ASN.1来定义.

(2) `get_next_request` 用于操作管理进程从代理进程上遍历MIB树,提取一个或多个参数的下一个参数值.

(3) `set_request` 用于操作管理进程来设置代理进程的一个或多个MIB参数值.在本文讨论的管理系统中大量用于控制设备手段.

(4) `get_response` 操作代理进程返回一个或多个MIB参数值,是前面3种操作的响应操作.

(5) `trap` 操作代理进程主动向管理进程发出的报文,标记一个可能需要特殊关注的事件的发生,如重新启动或者故障触发Trap操作.

图2给出了SNMP管理操作的数据流程:

2 赛尔宽带厦门大学校园宿舍网络的特殊性

在赛尔宽带厦门大学学生宿舍网络建立之初,当时面临着宿舍网需要进行可收费的运营化管理,需要管理的设备为大量不同品牌,不完全支持SNMP的桌面级交换机.在计费策略上,由于高校学生的经济承受能力不高,对网络的使用量巨大,包月制计费是唯一可被接受的收费制度.而计具体时长,计流量这些在商业计费系统里必须的功能,在赛尔宽带厦门大学学生宿舍网络的运营管理中并不必要.在设备兼容度上,赛尔宽带厦门大学学生宿舍网络建立之初,设备品牌组成复杂,更由于成本的问题,部分片区还有尚不能支持

SNMP管理的桌面接入设备,由设备厂商推出的管理系统不能很好的对其他厂商的产品提高全面的兼容.在用户使用方面,学生同社会宽带用户相比又具有一定的管理难度,如大量出现地址盗用,病毒爆发频繁,试图侵入管理系统等等情况.因为上述的特殊性,该校园宽带管理系统主要需求是适应包月制运营管理,兼容多种低端设备,能解决 IP盗用.具体而言,即按策略实现桌面端口的自动开通和关断,能自动绑定 MAC地址,对布线实现信息化管理,以改变原先设备,布线,用户等基础管理信息依赖手工操作,各区布线人员使用各自独立的数据表格的情况,实现网络运营管理信息系统的统一数据库,由系统取代人工来完成 MAC端口绑定,桌面端口准时开关,IP地址盗用扫描这些耗用人力巨大的工作.这些功能在现在看来,如使用品牌统一,管理功能完善的中高端桌面交换机,配合厂商提供的集中管理系统不难实现,但在设备品牌构成复杂,对管理功能支持不完全的当时,开发这套管理系统是必需而且没有其他现成产品可供选择的.同时,对于在校园网里广泛使用的许多低成本桌面交换机而言,相当部分较早期的设备不提供对 SNMP管理的支持,常常仅提供 WEB访问管理和 Telnet命令式管理.为了对此类设备也能进行必要的管理,需针对不同的管理访问接口编写代码,对此则开发了相应的程序,模拟浏览器和 telnet客户端对这类管理访问接口的设备进行管理操作.同时,针对校园宽度网面临安全威胁较重的情

况,在安全方面采用了封闭的独立设备虚拟网,加密的 HTTPS访问协议等手段.

3 赛尔宽带厦门大学学生宿舍网络管理系统的功能设计

3.1 该管理系统的设计功能主要有

(1)对桌面交换设备,宿舍布线实际地址与设备端口对应关系,用户信息等数据实行统一管理.

(2)自动按照用户缴付信息控制设备端口的开放和到期后关闭.

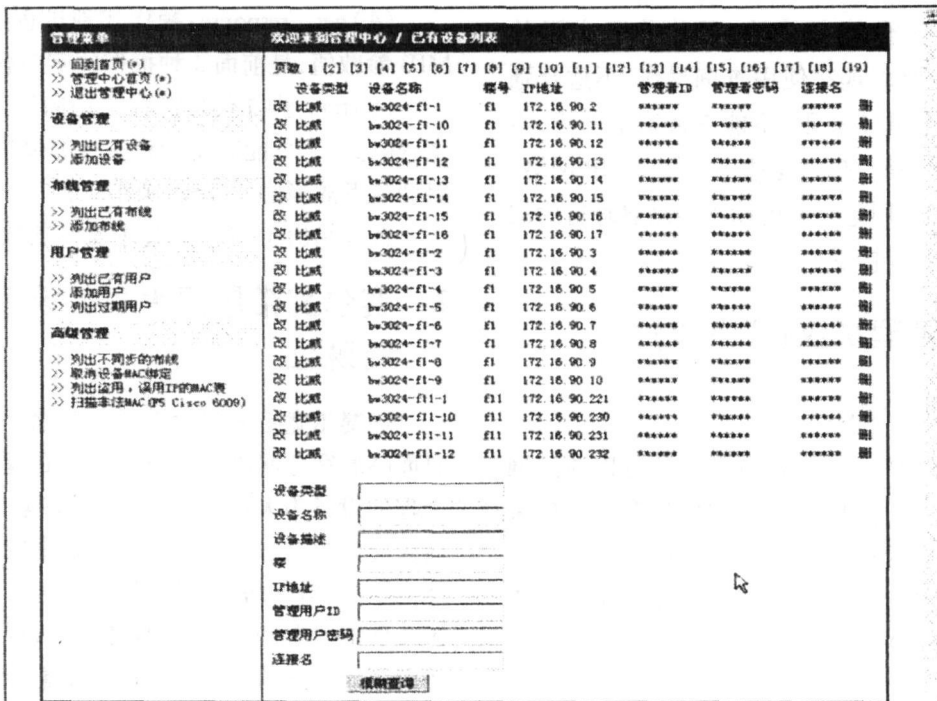
(3)自动完成用户网卡 MAC地址同桌面交换机端口的绑定(仅在支持该功能的设备上实现).

(4)按需扫描路由器 ARP表,比对用户 MAC记录以捕获用户盗用 IP信息.

3.2 整个系统以 B/S界面提供给管理人员操作,分为以下功能模块

(1)交换设备管理模块

登记各楼层交换机的型号,地理部署地址,IP地址,SNMP访问密码等设备基础信息.一方面电子化这些数据以后为系统自动按规则维护设备提供了必须的原始参数,另一方面也为设备物理管理提供了统一的、可电子统计、查询的记录,改变了系统实施前使用低效的手工统计的状况,见图 1.



(2) 布线信息管理模块

该模块主要实现对各个宽带用户的桌面到交换机之间布线的基础信息的记录和控制,为系统自动按规则维护端口通断提供了必须的原始参数;为布线和端口的物理管理提供了统一的、可电子统计、查询的记录,改变了系统实施前使用低效的手工统计的状况,并允许管理人员使用系统通过 snmp 直接控制设备端口的通断,见图 2

(3) 用户信息管理模块

该模块主要实现对各个宽带用户的基础信息的记录,为系统自动按规则维护用户通断提供了必须的原始参数,同时为用户管理提供了统一的、可使用 SQL 统计、查询的记录,改变了系统实施前使用低效的手工统计的状况,并允许管理员在这个界面中直接控制单个用户的端口通断状态,见图 3

(4) 不良网络行为控制模块

该模块可通过 SNMP 查询各交换机端口状态,发现并列出未和管理系统数据一致的端口和布线,以纠正必须由人工完成的布线和设备设置一些环节中可能出现的错误操作,并针对宿舍网络的特点,开发了基于 telnet 协议的机器人程序来读取扫描汇聚成路由器 ARP 表,同系统内数据库比对后列出盗用、误用 IP 的 MAC 表,以达到控制用户盗用 IP 的行为。

后台服务管理模块,该模块包含若干模块:

端口控制模块:根据用户数据库自动到期开放和关闭用户的端口。

MAC 绑定模块:根据用户 MAC 数据自动设置交换机限制端口仅允许该用户 MAC 使用。

设备检查模块:根据数据库自动检查各交换机工作状态,及时发现故障并通过邮件报警。

ARP 表扫描模块:扫描汇聚成路由器 ARP 表,同系统内数据库比对后列出盗用,误用 IP 的 MAC 表,

管理菜单		欢迎来到管理中心 / 已有布线列表												
>> 回到首页 (s)		页数 1 [2] [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13]												
>> 管理中心首页 (s)		布线架 布线序号 插座 设备名 设备口 物理线路状态 期望状态 实际状态 类型												
>> 退出管理中心 (s)														
设备管理		改 s1	101	1	bw3024-s1-1	1	断	开	开	1	删			
>> 列出已有设备		改 s1	101	2	bw3024-s1-1	2	断	开	开	1	删			
>> 添加设备		改 s1	101	3	bw3024-s1-1	3	断	开	开	1	删			
布线管理		改 s1	101	4	bw3024-s1-1	4	断	开	开	1	删			
>> 列出已有布线		改 s1	102	1	bw3024-s1-1	5	断	断	断	1	删			
>> 添加布线		改 s1	102	2	bw3024-s1-1	6	断	断	断	1	删			
用户管理		改 s1	102	3	bw3024-s1-1	7	断	断	断	1	删			
>> 列出已有用户		改 s1	102	4	bw3024-s1-1	8	断	断	断	1	删			
>> 添加用户		改 s1	103	1	bw3024-s1-1	9	断	断	断	1	删			
>> 列出过期用户		改 s1	103	2	bw3024-s1-1	10	断	断	断	1	删			
高级管理		改 s1	103	3	bw3024-s1-1	11	断	断	断	1	删			
>> 列出不同步的布线		改 s1	103	4	bw3024-s1-1	12	断	断	断	1	删			
>> 取消设备MAC绑定		改 s1	104	1	bw3024-s1-1	13	断	断	断	1	删			
>> 列出盗用,误用IP的MAC表		改 s1	104	2	bw3024-s1-1	14	断	断	断	1	删			
>> 扫描非法MAC (FS Cisco 6009)		改 s1	104	3	bw3024-s1-1	15	断	断	断	1	删			
		改 s1	104	4	bw3024-s1-1	16	断	断	断	1	删			
		改 s1	105	1	bw3024-s1-1	17	断	断	断	1	删			
		改 s1	105	2	bw3024-s1-1	18	断	断	断	1	删			

图 2 布线信息管理模块

管理菜单		欢迎来到管理中心 / 已有用户列表									
>> 回到首页 (s)		页数 1 [2] [3]									
>> 管理中心首页 (s)		用户名	楼 序号	插座位置	IP地址	MAC	真实姓名	用户类型	用户状态		
>> 退出管理中心 (s)		改 99071032	s1	601	4	218.193.15.8	0000B91120C 王耀	1	1	删	开户历史
设备管理		改 99071042	s1	601	3	218.193.15.9	00B04C101CC9 曹元路	1	1	删	开户历史
>> 列出已有设备		改 00062033	s1	603	4	218.193.15.7	00104C813D96 潘瑞	1	1	删	开户历史
>> 添加设备		改 00062002	s1	603	2	218.193.15.6	0094B3400736 陈瑞琳	1	1	删	开户历史
布线管理		改 99060012	s1	703	1	218.193.15.10	00B04C006C5A 付朋卿	1	1	删	开户历史
>> 列出已有布线		改 99032005	s1	705	3	218.193.15.5	00B04C6010E3 黄乙	1	1	删	开户历史
>> 添加布线		改 00062029	s1	701	3	218.193.15.13	00B04CE31206 林登彬	1	1	删	开户历史
用户管理		改 00031039	s1	308	4	218.193.15.12	0040B6009491 杨玲	1	1	删	开户历史
>> 列出已有用户		改 00031043	s1	308	3	218.193.15.11	00B04C60A1B6 陈静	1	1	删	开户历史
>> 添加用户		改 01072018	s1	602	1	218.193.15.14	5254A84F54B0 陈顺雄	1	1	删	开户历史
>> 列出过期用户		改 00031015	s1	204	1	218.193.15.15	00B000860B0A 杜志瑞	1	1	删	开户历史
高级管理		改 00031011	s1	101	4	218.193.15.18	00B04C398949 黄建	1	1	删	开户历史
>> 列出不同步的布线		改 00031011	s1	101	4	218.193.15.24	00B04C303A70 田国萍	1	1	删	开户历史
>> 取消设备MAC绑定		改 00031002	s1	101	3	218.193.15.22	0008743B721F 陈芳	1	1	删	开户历史
>> 列出盗用,误用IP的MAC表		改 99100011	s1	503	3	218.193.15.25	00B000A2F884 范建峰	1	1	删	开户历史
>> 扫描非法MAC (FS Cisco 6009)		改 00031018	s1	204	4	218.193.15.20	00B04C6010C1 桂明	1	1	删	开户历史
		改 01322011	s1	108	1	218.193.15.19	0030184C0E89 姚玉萍	1	1	删	开户历史
		改 01322018	s1	108	2	218.193.15.16	00B04C73B996 麻杨乐	1	1	删	开户历史
		改 00031003	s1	101	1	218.193.15.17	00B04C3989FA 肖利	1	1	删	开户历史
		改 00031003	s1	101	1	218.193.15.21	00B04C303A38 何青慧	1	1	删	开户历史

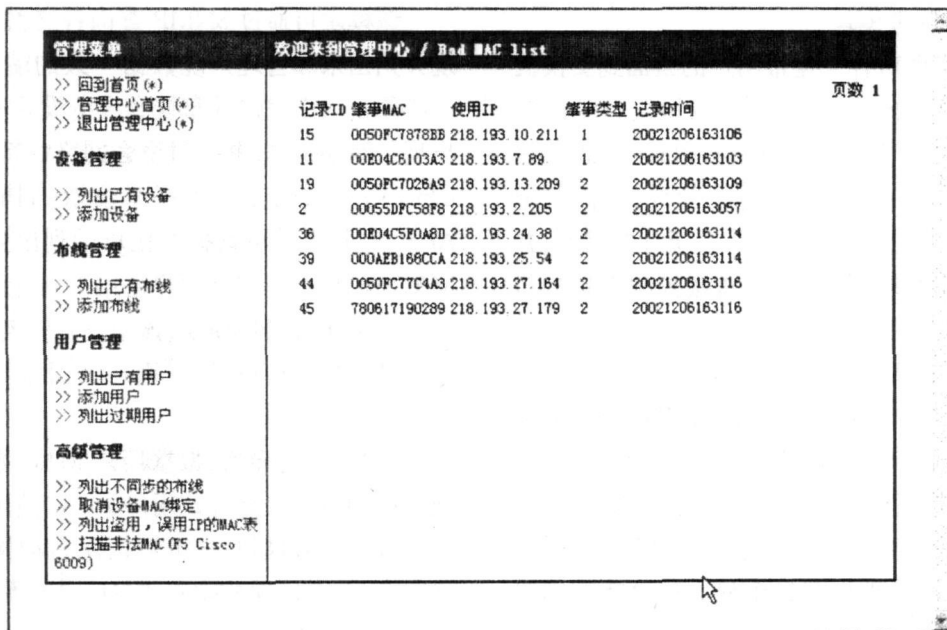


图 4 不良网络行为控制模块

见图 4

(5)系统安全管理

该模块包含了系统本身用户的分级权限管理界面,对系统用户分成多项权限的独立授权,并使用 MD5 密码进行身份校验,同时采取了一系列措施来保护系统安全:

在访问协议上,使用数据加密的 HTTPS 协议;

在操作系统级上使用防火墙规避系统被非法侵入,使用 TCP/IP 访问策略禁止一切管理员以外的 IP 访问,以此来提高系统的安全性;

在部署上,将设备管理 IP 和管理服务器部署在独立的 VLAN 内,同用户网络完全隔断。

4 系统实现及总结

基于当时的网络的设备品牌构成,管理界面各异,对 SNMP 不完全支持这些特点,我们使用 SNMP 作为主要管理手段,虚拟 Web 和虚拟 telnet 模拟管理为辅助管理手段,针对网络中的不同品牌和型号的桌面交换机开发了管理接口。在服务器操作系统方面,我们选择了 Redhat Advance Server SNMP 控制方面使用了 PERL 语言来编写脚本控制设备,对于不同设备根据设备提供的管理接口不同选择 PERL 调用设备的 Web 管理界面和直接操作 snmp 原语分别实现,并且记录操作过程和结果以备复查。系统本身的 Web 管理采用 PHP 编写。设备和用户信息数据库使用了开源的

mySQL 中国知网 <https://www.cnki.net>

(1)PERL 调用设备 Web 管理界面的部分代码示

例

我们首先对设备进行分析,找到 Web 管理界面相关功能的链接,并且提交数据,分析返回的结果,然后编写代码来完成上面的人工操作步骤。

/管理功能 Web 链接,已经包含相关数据

```
my $myurl = "http://$adminuser:$adminpasswd@$ipaddress/config/";
```

```
"port_security.htm?address=$mac&unit=$unit&page=portSecurity&port=$port";
```

```
"&status=$status&$actionstr";
```

/提交数据并获取结果

```
my $request = new HTTP::Request('GET', $myurl);
```

```
my $response = $ua->request($request);
```

/根据预期的正确信息对结果进行比较,这个例子只需直接比较结果,不用分析结果

```
my $SuccessMsg = "<html><head><meta http-equiv=refresh content=0; url=/config/ctrl_sec_secmod.htm></head></html>\n";
```

/结果正确则返回操作成功

```
return ($response->content eq $SuccessMsg);
```

(2)PERL 操作 snmp 原语的部分代码示例

通过查找 snmp 协议规范,找到操作的 snmp 原语,设置值。

/以下例子为设置某个端口管理状态

```
$snmpStr = "snmpset $IPaddress $Password interfaces ifTable ifEntry ifAdminStatus $integer $ADMINSTATUSUP";
```

/运行并获取结果

```
return (0 == system($snmpStr))
```

总体来说,该系统实现的管理功能虽然相对简单,

但具有以下优点:

(1)支持的设备广泛,甚至不支持 snmp 的低端交换机均可纳入该系统的管理.对网络设备硬件的要求低.

(2)系统平台均使用开源软件,降低了系统整体成本.

(3)功能吻合高校实际包月制网络运营的管理需求.

(4)硬件资源消耗低,并在我校的实际使用中系统表现非常稳定,在稳定方面甚至优于许多昂贵的商业网络管理系统.

该系统功能简明但足以满足包月制网络运营的需求,同时具有成本优势和面对廉价交换设备的兼容优

势,对比市面上价格昂贵,功能繁多的商业网络管理系统,相信使用 SNMP定制吻合自身实际需求的网络管理系统,仍是许多网络运营应用建设中的一个选择.该系统从 2002年至 2007年在赛尔宽带厦门大学学生宿舍网的实际运营管理中取得了不错的效果.

参考文献:

- [1] 雷振甲. 计算机网络管理及系统开发 [M]. 北京: 电子工业出版社, 2006
- [2] RFC1158 1213 Management Information Base for Network Management of TCP/IP-based internets MIB-II[S].
- [3] RFC 2270-RFC2275 Simple Network Management Protocol Version 3[S].

The Management System of Campus Dormitory Network

XU Zhuo-bin LI Lu-zhang ZHENG Hai-shan

(Network Information Center Xiamen University, Xiamen 361005, China)

Abstract Simple Network Management Protocol (SNMP) is one of the most universal protocol for network management. We can control and manage network device by this protocol. The paper based on SNMP, and described how to design and implement a simple network management system.

Key words SNMP MIB; network manager; dorm network