

基于 Linux 的网络系统管理 及其 Internet 服务的配置^①

郭东辉 李立峰 纪安妮 刘瑞堂

(厦门大学技术物理所 物理学系 厦门 361005)

摘要 基于 Linux 操作系统开放性的特点, 选用 Linux 做为 Intranet 的网络管理平台. 介绍了实验室中 Intranet 的结构以及如何在 Linux 平台上实现的 Internet 服务管理及其资源共享.

关键词 Linux 系统, 网络管理, Internet 服务, 资源共享

中国图书分类号 TP 316, TP 393.2

近年来随着计算机的普及, 高校中各个教研室或实验室的工作人员为了工作方便几乎都配备了计算机. 但对于缺乏经费的单位来讲, 要集成其所有的计算机设备建立一个系统资源共享同时能提供 Internet 服务的 Intranet(实验室内部网)就有一定的困难. 除了需要购买 Switch(交换机)或 Hub(集线器)外, 还需要考虑购置如 Router(路由器)、Firewall(防火墙)、RAS(Remote Access Server, 即拨入服务器)等其他网络设备以及管理软件的 License(版权). 鉴于 Linux 操作系统^[1]开放性的特点, 我们选择 Linux 这一自由免费软件作为实验室 Intranet 的网络管理平台. 在不增加经费购买其他网络设备和管理软件的情况下, 启用一台濒临报废的 486 机器作为网络管理服务器, 成功地建立起一个集 Router、Firewall、RAS 等于一体可实现 Internet 服务管理及资源共享的实验室内部网.

为了阐述本实验室 Intranet 的组建技术, 本文首先介绍实验室 Intranet 的网络结构及功能方案, 然后具体描述如何在 Linux 平台上实现 Internet 服务管理及资源共享的功能.

1 实验室的网络结构及功能

目前本实验室共有 SUN 工作站 10 台, PC 兼容机 35 台. 其中, 10 台 SUN 工作站的机型分别是 3 台 Ultra1、1 台 Sparc10、4 台 Sparc5、2 台 Sparc2; 而 35 台 PC 兼容机中仅有 7 台为有盘机器, 这 7 台有盘机器中还有 1 台为 486/100 的旧机器. 目前我们主要负责管理我校“211”重点学科中 EDA(电子设计自动化)工具的应用和科研开发工作, 为了能够合理利用这些机器资源, 在 SUN 工作站上分别装了各种有浮动版权的 EDA 工具软件, 组成了 EDA 中心的 EDA 工具服务器群; 同时, 精心地配置了 7 台有盘的微机, 即 1 台 Linux 网络服务器, 1 台 WinNT 服务器, 1 台 SQL 服务器, 4 台 Win95 机器, 以及 28 台无盘机器, 组成一个独立的实验室内部局域网. 在实验室里, Linux 网络服务器是由 486/100 机器装成的用来实现网络管理和配置; WinNT 服务器是

^① 本文 1999-05-19 收到; 国家教委留学回国人员启动基金、福建省自然科学基金重点资助项目(F982001)和国家自然科学基金“863”预研资助项目(69886002)

由PII300机器装成的,用来作为其他28台无盘机器的Win95启动服务器和内部拨号服务器;SQL服务器也是PII300机器装成的,用来实现实验室数据管理;2台Win95机器给网络管理员使用,另外2台Win95机器给学生和教师作为软件安装测试及软件调试实验机器.本实验室的8位研究工作人员和研究生的日常工作均使用Win95无盘机器,另外的20台无盘Win95机器用来建成一个供学生进行EDA软件培训的微机实验室,同时也便于用来对学生进行相关课程

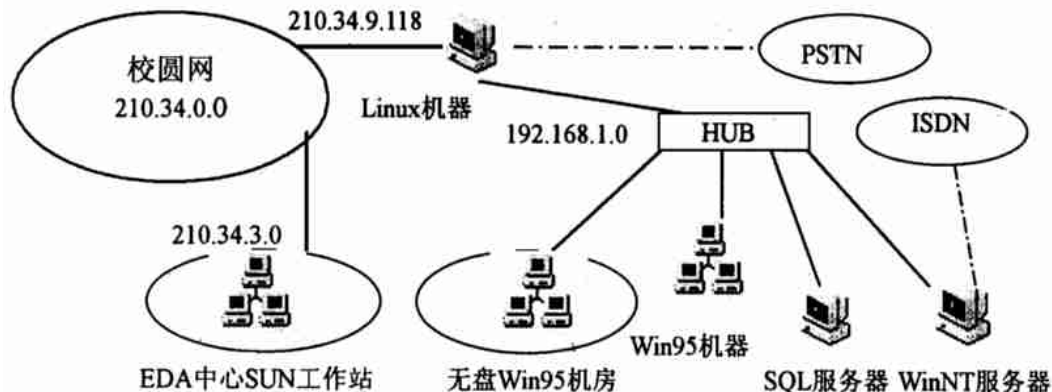


图1 实验室网络拓扑结构图

Fig. 1 Network s structure of our laboratory

的教学.总之,这些机器所建立的网络拓扑结构如图1所示.

由于本实验室主要是利用SUN工作站上的EDA工具进行科研与教学工作的,因此,通过Linux网络服务器的网络地址转换办法,让局域网内的有盘和无盘Win95机器能透明地登录EDA中心的SUN工作站上调用EDA工具.此外,由于采用无盘工作方式,工作人员和学生的文件数据分别由Linux服务器和WinNT服务器分配硬盘存储.为了能让工作人员从家中或外地直接进入实验室内部网工作,我们的Linux服务器和WinNT服务器也分别配上了Modem卡和ISDN卡来实现拨号服务.EDA中心的用户使用数据和本内部局域网的网络管理数据均送入SQL服务器,由SQL服务器对网络使用情况实现统计管理.

本实验室内部网是经校园网与Internet互联的,为了能使实验室的所有机器正常使用一些常用Internet服务功能,同时能让社会同行及时了解我们的工作,我们用该Linux服务器实现了如E-mail、WWW、FTP、DNS、Router/Firewall等服务功能.本文在下一节将着重描述用Linux实现网络服务配置的具体方法.

2 网络服务功能的配置

Linux服务器上采用的是Slackware3.5版本的Linux操作系统^[2].为了满足本实验室的需要,进行了如下的网络服务配置:

1) E-mail服务:利用SMTP和POP3协议实现对本实验室人员的E-mail服务,Linux的安装软件本身带有Sendmail和POP3d.只要系统安装好后在系统引导时启动/etc/rc.d中的Sendmail daemon,系统就具备了本地内部网上邮件发送的功能.具体方法是在rc.M中加入以下语句:

```
if [ -x /usr/sbin/sendmail ]; then
    echo "Starting sendmail daemon."
    /usr/sbin/sendmail -bd -q15m
fi
```

pop3 是由 inetd 启动的, 需修改配置文件(/etc/inetd.conf), 即把 pop3 服务的那一行

```
"pop3 stream tcp nowait root / user/sbin/tcpd /usr/sbin/in.pop3d"
```

的注释去掉, 再重新启动 inetd 服务。

2) WWW 服务: 利用 Apache 的 WWW 服务器软件系统作为本实验室的信息发布平台。Slackware3.5 版本的 Linux 系统本身带有 Apache 的 WWW 服务器软件。系统安装后, WWW 的根目录在 /var/lib/httpd, 系统的可执行程序为 /usr/sbin/httpd, 系统所要发布的信息文件都放在 /var/lib/httpd/htdocs 下。而 WWW 服务的配置文件在 /var/lib/httpd/conf。一般情况下, 只要在 /etc/inetd.conf 中加入一行

```
"http stream tcp nowait ftp /var/lib/httpd/httpd httpd"
```

来启动 httpd(或在 /etc/rc.d/ 目录下加入在系统启动时启动 httpd 的脚本), 这样缺省的配置就能够运行 www 服务。为了更好地使用和维护 WWW 服务, 我们另调整了以下配置文件:

A. 在 httpd.conf 文件中加入 "ServerName www.eda.xmu.edu.cn" 来确定本服务器的别名。

B. 在 srm.conf 文件中加入 "UserDir public-html" 让本实验室人员在自己用户目录下建立一个 public-html 目录来维护自己的网页。

C. 在 access.conf 文件中加入

```
< Directory /home>
    AllowOverride None
    Options Indexes Includes
< /Directory> "
```

使各用户能够访问主目录下的文件。

3) FTP 服务: Linux 服务器上装有一个 8G 的硬盘, 用来存放一些常用的软件和资料, 其中 FTP 服务主要是为了便利这些软件和资料的内外交流。Slackware3.5 版本的 Linux 系统带的是 wu-ftp 服务软件^[3], 当 Linux 系统安装好之后, FTP 的配置文件放在 /etc 目录下, 主要为 ftpaccess 和 ftpusers。其中, ftpaccess 用于定义允许访问的 IP 范围, ftpusers 用于定义哪些用户不能用 ftp 登录本服务器。而 ftp 的共享文件是放在 ftp 的主目录 "home/ftp/" 下。

4) DNS 域名服务: 由于 SUN 工作站装有不同的 EDA 工具, 且各 PC 兼容机作为不同的用户机使用, 为了便于记忆和数据处理, Linux 服务器上也装上了的域名服务。其中, 我们所装的 DNS 服务软件是免费的 bind 域名服务器软件, 它可从如 "http://www.isc.org/bind.html" 站点上下载后编译安装。该域名服务的可执行程序为 /usr/sbin/named, 配置文件为 /etc/named.conf, 在那里定义 named 的主目录, 一般为 /var/named。

5) RAS 服务: 用 modem 接收拨入, 作为远程访问的服务器, 以便研究人员在家登入访问实验室的网络资源。虽然 Slackware3.5 版本的 Linux 系统带有 agetty 拨号服务软件, 但它不接受

Win95 的 pap 认证。为此, 我们在 "http://sunsite.unc.edu" 站点上下载了 mgetty + sendfax 软

件,并修改文件“`/etc/inittab`”。用 `mgetty` 处理来自 modem 的输入,其中, `mgetty` 的配置文件缺省在 `/usr/local/etc/mgetty+sendfax` 目录下,可执行文件为“`/usr/local/sbin/mgetty`”。这样就可以方便地从 win95 拨号登录到 linux 服务器上。其中,需在 `/etc/ppp/options.ttyS*` 文件中定义拨入机器的 IP 和路由。

6) Router 与 Firewall 服务:该服务的设置主要是为了保证网络内部资源不受攻击,并管理内部机器访问 Internet 的权限。我们利用网络地址转换机制来实现堡垒主机的防火墙功能,即在 Linux 服务器上装双网卡把内部网和校园网分开,并定义一定的过滤规则,一方面方便了内部网访问校园网,另一方面也限制校园网对内部网的访问。为了实现本服务功能,需要重新编译 Linux 内核,使它能支持双网卡工作。在编译内核后,需启用 `ip-firewall`、`ip-forward` 和 `ip-masq` 等功能,然后修改文件“`/etc/rc.d/rc.local`”,即用 `ipfwadm` 把相应规则加入,这样,重新启动后 Linux 的该项服务就启用了。具体设置服务方法如下:

假定内部网为 192.168.1.0,缺省内部网的机器可以访问外面的任何机器,则在 `rc.local` 的设置为:

```
/sbin/ipfwadm -F -p deny
```

```
/sbin/ipfwadm -F -a m -S 192.168.1.0/24 -D 0.0.0.0/0
```

```
/sbin/insmod /lib/modules/2.0.30/ipv4/ip-masq-ftp.o
```

第一条语句定义缺省的规则为禁止 IP 转发;

第二条语句允许内部网的机器 192.168.1.* 访问外面的任何机器;

第三条语句加载特殊的模块使 `ftp` 能正确允许,因为 `ftp` 的数据连接需要从外部网的主机主动发起连接,缺省是不允许这样的,加载了本模块后就能正确处理这种情况,允许 `ftp` 建立数据连接。

7) 文件共享服务:本服务可以保证在 Win95 机器上用网上邻居直接访问 Linux 机器上的共享文件。Slackware3.5 版本的 Linux 软件自带的 Samba 软件包可实现此服务功能,它允许把一台 Unix 机器仿真成一台 WinNT 服务器,这样,Win95 机器可以方便地共享 Linux 服务器资源。其中,其他免费的 Samba 软件可以从一些站点上下载。Samba 软件安装后,它的配置文件为 `/etc/smb.conf`,用来定义 Samba 模拟 WinNT 的一些属性和需要共享的资源,比如文件夹或打印机;同时,可以用命令 `smbpasswd` 来设定访问 samba 共享资源的用户密码,密码文件一般放在 `/usr/private/smbpasswd` 文件里。

3 结 论

经过一年多来的运行,基于 Linux 操作系统建立起来的 Intranet(实验室内部网)工作相当稳定。在 Internet 服务功能的使用过程中,我们也深深体会到 Linux 系统的功能强大、配置灵活、网络运行效率高等优点。最令人放心的是,它做为自由软件,没有商业许可证问题,实验室安装不受数量限制,便于科研开发。即使出现技术难题,现在也有大量的免费咨询站点给你提供帮助,而且还有许多公司给予有偿的技术支持。总而言之,本文希望通过阐述本实验室基于 Linux 系统平台的网络管理和 Internet 服务配置,将我们使用 Linux 的经验和看法介绍给同行。

参 考 文 献

- 1 Goncalves M. Linux at Work: Building Strategic Applications for Business. New York: John Wiley & Sons, 1999
- 2 Reichard K. The Linux Internet Server. Foster City: IDG Books Worldwide, 1997
- 3 Sobell M G. A Practical Guide to Linux. San Francisco: Addison-Wesley, 1997

Network Management and Internet Configuration by Linux

Guo Donghui Li Lifeng Ji Anni Liu Ruitang

(Institute of Technical Phys., Dept. of Phys., Xiamen Univ., Xiamen 361005)

Abstract Due to its opening and effectuation, Linux is selected as the network s operating system for the LAN platform in our laboratory. This paper will show with the network s architecture of our LAN and detail about the implementation of network s management for internet server and sharing information by Linux operating system.

Key words Linux, Internet, Network management