2002年12月 成都师范高等专科学校学报 第21卷 第4期
Dec, 2002 Journal of Chengdu Teachers College Vol. 21, NO. 4

用 Linux 在局域网中实现 Intranet

余 伟

(成都师范高等专科学校计算机科学系 四川 彭州 611930)

摘 要 本文提出了一种用 Red Hat Linux 在局域网中建设 Internet/Intranet 的 Web 服务器、FTP 服务器、Mail 服务器和防火墙的方案。并说明了设置各种服务器的主要配置文件，详细解释了配置文件的重要参数和命令。

关键词 Linux 操作系统 服务器 Intranet

中图分类号 TP393.18 文献标识码 A 文章编号 1009-833](2002)04-024-05

1 引言

近几年来，个人计算机性能不断提高，而成本不断下降，建设局域网的复杂程度降低，成本也下降了很多，因此许多学校和企业都建设了自己的局域网。另一方面，Internet 在我国迅速普及，学校、企业内部的信息系统建设得到快速发展。将 Internet 技术和现存的校园、企业网络相结合，能更好地满足企业发展的需求。Intranet 是基于 Internet 的 TCP/IP 协议，使用环球网 WWW 工具，采用防止外界侵入的安全措施，连接 Internet 的企业内部网络。学校、企业建立了 Intranet，就可以像上 Internet 一样，在 Intranet 上浏览网页、发布信息，改善学校、企业的通信能力，可使内部信息资源共享，更好地发挥已有网络的作用。

在网络系统的建设中除了网络硬件的选型与集成外，一项非常重要的工作就是网络操作系统的选择、安装、配置和维护。Linux 操作系统功能十分强大，系统稳定，而且完全免费，源代码开放，对于经费比较有限的一些中、小企业、学校来说是一个很好的选择。

2 局域网的建设

本文中的局域网为以太网，因此每台服务器和工作站都要安装有以太网卡，作为防火墙的计算机应至少有两块网卡，一块通过网线与路由器相连，一块通过网线与交换机相连。局域网通过路由器与 Internet 相连。

2.1 安装 Linux

本文所有内容都以 Red Hat Linux7.2 为例。Linux 有多种安装方法，在这里，不详细叙述具体的安装过程，只讨论两个关键的问题。第一，在选择所要安装的各种服务器组件时，一定要将本文所涉及的 Apache 等服务器及其相关的包选中，当然也可以选中 Everything，不过此时要保证硬盘有足够的空闲空间，至少要有 3GB 以上。第二，在安装过程中，系统会检测到网卡，可以进行网络设置，如主机名、域名、主机 IP 地址、子网掩码等。

2.2 启动需要的服务

要让 Apache 等服务器工作，必须首先启动它们，这可以通过 Xwindow 中的一个系统工具 Service Config

来实现，十分方便。在本文中，讨论修改 services 配置文件来实现。Services 文件比较大，包含内容很多，这里只列出一些本文后面要用到的选项。

```
ftp-data 20/tcp                          //关于 FTP 的配置
ftp-     21/tcp
smtp     25/tcp      mail                //关于 SMTP 的配置
http     80/tcp      WWW WWW-http        //关于 HTTP 有配置
pop3     110/tcp     pop-3               //关于 POP3 的配置
mysql    3306//tcp                       //关于 MYSQL 的配置
swat     901/tcp                         //SAMBA 基于 Web 的配置
```

2．3　配置 Linux 的 Samba 服务器

Samba 程序让 Linux 服务器懂得 SMB（Server Messages Block）协议，从而实现在 Linux 服务器和 Windows98 工作站之间的打印共享和文件共享。

配置 Samba 服务器的文件是/etc/samba/smb．conf。文件中设定了系统与其他机器共享的资源及访问权限。文件由许多部分组成，每一部分定义一项服务，本文只讨论用到的选项。

```
[global]              // [global] 段控制整个 SMB 服务器的参数，还提供了其他段的默认值
    workgroup = MYGROUP
    server string = Samba Server
    security = share
[homes]               // [homes] 段允许网络客户连接到服务器上某个用户的主目录
    comment = Home Directories
    browseable = no
    writable = yes
[printers]            // [printers] 段为客户列出所有 printcap 定义的打印机
    comment = All Printers
    path = /var/spool/samba
    browseable = no
    guest ok = yes
    writable = no
    printable = yes
```

2．4　配置 Windows98 工作站

在 Windows98 工作站上安装 TCP/IP 协议，过程如下：启动 Win98 工作站，顺序打开“控制面板”、“网络”、“添加”、“TCP/IP 协议”、“属性”、设置 IP 地址与 DNS 参数。重新启动计算机后就可以通过“网上邻居”来访问 Samba 服务器了。

3　构建 Intranet 服务器

3．1　Web 服务器

Apache 是 Red Hat Linux 默认安装的 Web 服务器。Apache 服务器的配置文件主要有：/etc/httpd/conf 目录下的 httpd．conf，auess．conf，srm．conf．其中，httpd．conf 是其主要配置文件，通过配置 httpd．conf 文件，完全可以不用另外两个文件。httpd．conf 主要用来设置与服务器有关的系统及基本信息。一般情况下，

httpd. conf 中的大部分缺省值可保留。需要注意以下几项：

```
Server Type StandAlone          //Web 服务器运行方式，这里为单机方式
ServerRoot /etc/httpd/          //服务器目录的绝对路径，即服务器到哪里去找所有资源和配置文件
Server Name www. yuwei. com     . //服务器主机名
Listen192. 168. 120. 246:80     //侦听 192. 168. 120. 246（本文主机 IP）的 80 端口
Listen * . 80                   //侦听所有主机 IP 的 80 端口
Listen 127 0. 0. 1: 901         //侦听本机的 901 端口，Samba 服务使用的端口
Port 80                         //指定端口为 80
DocumentRoot/var/WWW/html       //文档目录树的绝对路径
UserDir Public-html             //和本地用户主目录相对的目录，可将公共 Html 文档放入其中
```

3. 2 DNS 服务器

域名服务（DNS）是 Internet 的核心，它把 Internet 主机名解析为 IP 地址。Linux 内置了 DNS 服务器，启动 Linux 时，如果 named 启动就说明 DNS 已经开始工作。我们可以在 Xwindos 环境下用 DNS Config 工具来配置。/etc/named. conf 文件是 DNS 引导文件，在 named 进程启动时读入，是主配置文件，定义了域数据库信息的基本参数和源点，文件中包含几个域，示例如下：

```
options {                           //options 部分保护整个 DNS 服务器的全局信息。
directory "/var/named/";            //directory 语句通知 named 在配置中提及的所有文件的位置。
};
zone. "." {                         //zone "." 是缓存区。包含服务器软件使用的
    type hint;                      //许多提示，即 type hint; 语句。
    file "named. ca";
};
zone "0. 0. 127. in-addr. arpa." {  //本地回路反向解析，即 IP→主机名
    type master;
    file "0. 0. 127. 1n-addr. arpa. zone";
};
zone "www. yuwei. com" {            //网卡 eth0 上的子网地址正向解析，即主机名→IP
    type master;
    file "www. yuwei. com. zone";
}
```

3. 3 动态网页的实现

为实现动态网页，选用 PHP 脚本语言，并安装了 Mysql 数据库，用 PHP 应用程序访问 Mysql 数据库。PHP 作为一种服务器端 HTML 嵌入式脚本描述语言，其特色在于能够很方便地实现在互联网网页上对数据库的操作，而且是免费的。Mysql 是一个多用户、多线程的 SQL 数据库管理系统，它支持 Linux、Unix 等多种系统，其特点是速度快、健壮和容易使用。Apache，PHP 和 Mysql 是非常好的组合，具有安装简单，使用方便，性能稳定，速度快，成本低的特点。

3. 4 FTP 服务器

FTP（文件传输办议）提供了文件传送的基本服务。FTP 可以减少甚至消除在不同操作系统之间处理文件的不兼容性。一个 FTP 服务器进程可以同时为多个客户进程提供服务。

它所涉及到的配置文件主要为/ect 目录下的 xinetd. conf，ftpaccess，ftphosts，ftpusers 和 etc/xinetd. d 目录下的 wu－ftpd 文件。

（1）xinetd. conf 是 inetd. conf 增强版本，功能十分强大，包含对 FTP，rsh，POP3 等的配置。在 xinetd. conf 中一定要包含下面的语句，它指明了 wu－ftp 的配置文件所在位置。

includedir/etc/xinetd. d

（2）/etc/xinetd. d 目录下的 wu-ftpd 文件设置如下：

```
service ftp
{   disable = no                          //no 为打开，yes 则不打开
    socket-type = stream
    wait = no
    user = root
    server = /usr/sbin/in. ftpd
    server-args = －1－a
}
```

（3）ftpaccess 是 FTP 服务器的主要配置文件，配置信息的格式为：keyword [one or more options]。该文件包含如下几类属性：guestuser、class、loginfails、message、shutdown、password－check、limit、alias 等。

（4）/etc/ftphosts：用来控制来自各种主机的持定账号对 FTP 的访问。

（5）/etc/ftpusers：FTP 用户黑名单，为安全考虑，需要禁止某些用户使用 FTP。

3．5　E－mail 服务器

Sendmail 是 Red Hat Linux 默认安装的邮件服务器，客户和服务器间的通信协议是邮局协议（POP）和简单邮件传输协议（SMTP）。

（1）设置邮件服务器的第一步是加入邮件交换（MX）记录，它是用来标明 SMTP 邮件服务器资源的，该资源在域的 DNS 配置文件 named. conf 上设置。

（2）对配置文件进行设置。这些文件为/ect/sendmail. cf、/etc/sendmail. cw 和/etc/mail/＊。/etc/sendmail. cf 是主配置文件，控制 sendmail 运行时的配置。/etclsendmail. cw 中必须列出接收 mail 的所有主机名或域名。/etc/mail 目录下有一些配置文件，用 access 限制访问 sendmail 服务器，用 aliases 产生用户的别名，用 domaintable 映射域，用 mailtable 改变域的邮件路由，用 relay－domains 建立邮件中继。

（3）POP 服务器设置。在/etc/xinetd. d 目录下的 iPOP3 文件内容应如下：

```
service POP3
{   disable = no                          //no 为打开，yes 则不打开
  sockt type  = stream
  wait = no
  user = root
  server = /usr/sbin/ipop3d
```

4　防火墙

在 Red Hat Linux7.2 中使用 ipchains 来实现数据包过滤的功能。ipchains 是运行于主机中的数据包过滤软件，负责检查通过该主机的数据包标头（数据包有标头和数据两个部分，标头指明该数据包的源地址、目的地址和数据类型），并决定对数据包作何种处理。

ipchains 有三个内置的规则链（chains），它们决定怎样处理进、出的 IP 包：

- 流入链（IP input chains）：管理从主机一个网卡上流入的包的规则。
- 流出链（IP output chains）：管理从主机一个网卡上流出的包的规则。
- 转发链（IP forward chains）：转发经过主机的包的规则。

除此之外，可以用 ipchains 命令来创建自己命名的链。

每一种链都有自己的规则集合，定义了对各种数据包所进行的操作，每个规则都需要指定对数据包的处理方法，包括：accept（允许通过）、deny（拒绝通过）、reject（不接受且返回通知信息）、masq（IP 伪装）和 redirect（重新导向）。

配置防火墙可以通过 Xwindow 中的 firewall config 工具来进行，这个工具使用起来比较方便，也可以在文本模式下用命令来实现。

参考文献：

[1] [美] Bill Ball David Pitts 等著．马朝晖 薛静锋等译．Red Hat Linux 7 技术大全机械工业出版社．2001

[2] [美] Terry William Ogletree 著．李之棠等译 防火墙原理与实施、电子工业出版社 2001

[3] 景芳．基于 Linux 的网站解决方案．系统建设 2002 第 4 期