



Linux 系统管理专家系列

Linux

服务器配置手册

- ◆ 国内资深 Linux 系统管理员 9 年经验点滴
- ◆ 系统配置、安全防护和自动化运行配置一步到位
- ◆ Linux 系统管理员渴望已久的参考手册



北京希望电子出版社 总策划
马昕炜 主 编



科学出版社
www.sciencep.com



Linux 系统管理专家系列

Linux

服务器配置手册

- ◆ 国内资深 Linux 系统管理员 9 年经验点滴
- ◆ 系统配置、安全防护和自动化运行配置一步到位
- ◆ Linux 系统管理员渴望已久的参考手册



北京希望电子出版社 总策划
马昕炜 主 编



科学出版社
www.sciencep.com

内容简介

本书主要介绍了 RedHat Linux 系统下搭建各种服务的操作方法。

本书共由 14 章内容和一个附录组成，其中的内容包括：DNS 服务、mail 服务、Web 服务、FTP 服务、代理服务、网关服务、DHCP 服务、Samba 服务、NFS 服务、CVS 服务、VNC 服务、数据库、BBS 服务、LDAP 服务。附录部分介绍了相关系统命令。

本书的特点是结构清晰、内容丰富、并配有相应的实例。适合对 Linux 系统有一定了解，并希望熟悉各种服务配置方法的爱好者、以及 Linux 系统管理员。

需要本书或技术支持的读者，请与北京中关村 083 信箱（邮编 100080）发行部联系，电话：010-82702660 010-82702658，010-62978181（总机）转 103 或 238，传真：010-82702698，E-mail: tbd@bhp.com.cn.

图书在版编目 (CIP) 数据

Linux 服务器配置手册 / 马昕炜主编. —北京: 科学出版社, 2005.4

(Linux 系统管理专家系列)

ISBN 7-03-014928-9

I. L... II. 马... III. Linux 操作系统—技术手册
IV. TP316.89-62

中国版本图书馆 CIP 数据核字 (2005) 第 005426 号

责任编辑: 安源 / 责任校对: 娄 艳

责任印刷: 媛明 / 封面设计: 王 焯

科学出版社 出版

北京东黄城根北街 16 号
邮政编码: 100717

<http://www.sciencep.com>

北京媛明印刷厂印刷

科学出版社发行 各地新华书店经销

*

2005 年 4 月第 1 版 开本: 787×1092 1/16
2005 年 4 月第一次印刷 印张: 35 7/8
印数: 1—5000 字数: 835.8

定价: 55.00 元

目 录

第 1 章 DNS 服务.....	1	1.9.2 设置 DNS 侦听端口.....	45
1.1 DNS 原理.....	1	1.9.3 转发查询.....	46
1.2 DNS 服务器的基本配置.....	3	1.9.4 访问控制列表.....	46
1.3 DNS 服务器的安装.....	3	1.9.5 DNS 服务 chroot.....	48
1.3.1 hosts 文件.....	4	1.9.6 DNS 的负载均衡.....	51
1.3.2 host.conf 文件.....	5	1.9.7 动态 DNS.....	51
1.3.3 resolv.conf 文件.....	5	1.9.8 其他参数.....	54
1.3.4 named.conf 文件.....	7	1.10 DNS 应用举例.....	54
1.3.5 named.ca.....	9	1.10.1 /etc/hosts 文件.....	55
1.3.6 正向解析文件.....	11	1.10.2 /etc/host.conf 文件.....	55
1.3.7 反向解析文件.....	14	1.10.3 /etc/resolv.conf 文件.....	55
1.3.8 别名解析.....	15	1.10.4 /etc/named.conf 文件.....	55
1.4 DNS 服务控制.....	15	1.10.5 /var/named/named.ip 文件.....	57
1.4.1 DNS 服务的启动.....	15	1.10.6 /var/named/named	
1.4.2 DNS 服务的停止.....	15	.pip.co 文件.....	58
1.4.3 DNS 自动启动.....	16	1.10.7 /var/named.pearl.cn 文件.....	59
1.4.4 rndc 的使用.....	18	1.10.8 /etc/rndc.conf 文件.....	62
1.5 主从服务器配置.....	23	1.11 小结.....	63
1.5.1 从 DNS 服务器工作原理.....	23	第 2 章 mail 服务.....	64
1.5.2 从 DNS 服务器的配置.....	24	2.1 mail 服务原理.....	64
1.6 测试 DNS 服务器.....	26	2.2 DNS 中添加 mail 记录.....	65
1.6.1 DNS 进程检查.....	26	2.2.1 添加邮件记录.....	65
1.6.2 nslookup 的使用.....	28	2.2.2 验证 DNS 服务器设置.....	67
1.6.3 whois 的使用.....	32	2.3 SMTP 和邮件接收.....	68
1.6.4 DNS 日志.....	34	2.3.1 SMTP 协议.....	68
1.7 DNS 客户端的配置.....	36	2.3.2 接收邮件.....	70
1.7.1 Linux 客户端设置.....	36	2.4 Mail 服务器的配置.....	73
1.7.2 Windows 客户端设置.....	36	2.4.1 Mail 服务安装.....	73
1.8 DNS 服务器多域配置.....	37	2.4.2 配置 sendmail.....	73
1.8.1 多域 DNS 服务器.....	38	2.4.3 sendmail.cf 文件.....	74
1.8.2 子网域 DNS.....	41	2.4.4 hosts.allow 文件.....	83
1.8.3 划分 IP 网段的子网域.....	42	2.4.5 /etc/mail 目录下的文件.....	84
1.9 DNS 服务器特殊设置.....	44	2.4.6 邮件别名.....	87
1.9.1 设置 DNS 目录.....	44	2.5 邮件接收.....	88

2.5.1	协议安装.....	88
2.5.2	POP3 协议.....	88
2.5.3	IMPA 协议.....	89
2.6	客户端.....	90
2.6.1	Windows 用户的配置.....	90
2.6.2	Linux 用户的配置.....	94
2.7	邮件服务器的测试.....	99
2.7.1	进程检查.....	99
2.7.2	端口的测试.....	99
2.7.3	查看邮件日志.....	100
2.8	验证用户的邮件服务器.....	102
2.8.1	SASL 的安装.....	102
2.8.2	配置 sendmail.mc 文件.....	102
2.9	mail 服务命令简介.....	108
2.10	多域邮件服务器.....	111
2.10.1	多域邮件服务器的概念.....	111
2.10.2	多域邮件服务器的设置.....	111
2.11	sendmail 安全.....	112
2.11.1	relay 规则简介.....	112
2.11.2	access 文件.....	113
2.11.3	relay-domains 文件.....	114
2.11.4	sendmail.mc 文件.....	114
2.11.5	sendmail.cf 文件.....	114
2.11.6	xinetd.conf.....	115
2.11.7	服务器上的用户.....	117
2.12	邮件管理.....	117
2.12.1	查看未发送邮件.....	118
2.12.2	邮件延时.....	120
2.12.3	邮件阻塞.....	120
2.13	网页收发邮件.....	121
2.13.1	安装.....	121
2.13.2	配置.....	121
2.13.3	修改密码.....	124
2.14	应用举例.....	126
2.14.1	文件 sendmail.mc.....	126
2.14.2	文件 sendmail.cf (部分) ...	130
2.14.3	文件 access.....	131
2.14.4	文件 local-host-names.....	132
2.14.5	文件 relay-domains.....	132

2.14.6	文件 sendmail.cw.....	133
2.14.7	文件 virtusertable.....	133
2.14.8	文件 aliases (部分)	133
2.15	小结.....	133
第 3 章	Web 服务.....	134
3.1	Web 服务简介.....	134
3.2	配置 Apache.....	135
3.2.1	安装 Apache.....	135
3.2.2	控制 Apache 服务.....	135
3.2.3	配置 DNS.....	136
3.2.4	配置 httpd.conf 文件.....	136
3.3	检测 Apache 服务.....	150
3.3.1	检查进程.....	150
3.3.2	检测端口.....	150
3.4	Apache 和编程语言.....	151
3.4.1	程序的应用.....	151
3.4.2	设置目录.....	152
3.4.3	PHP.....	153
3.4.4	Perl.....	154
3.4.5	SSI.....	155
3.5	虚拟 Web 网站.....	157
3.5.1	关于 DNS.....	157
3.5.2	虚拟主机的运行原理.....	157
3.5.3	基于 IP 地址的虚拟主机.....	157
3.5.4	基于主机名的虚拟服务器.....	159
3.5.5	设置端口.....	159
3.6	Apache 代理服务.....	160
3.6.1	配置代理服务.....	160
3.6.2	配置浏览器.....	163
3.6.3	设置访问许可.....	164
3.6.4	高速缓存远程站点.....	164
3.7	Web 服务安全.....	165
3.7.1	日志分析.....	165
3.7.2	监测服务器状态.....	168
3.7.3	用户认证.....	170
3.7.4	目录权限.....	173
3.7.5	访问权限.....	173
3.7.6	错误提示页.....	174

3.7.7 使用 SSL	176	5.2 Squid 配置	284
3.8 与旧版本的区别	178	5.2.1 安装 Squid	284
3.9 Tomcat	178	5.2.2 控制 Squid 服务	285
3.9.1 安装	178	5.2.3 配置代理服务	285
3.9.2 配置 tomcat	184	5.3 检测 Squid 服务	288
3.9.3 tomcat 安全	194	5.3.1 进程检查	288
3.9.4 tomcat 和 Apache 的结合	197	5.3.2 端口检查	289
3.10 应用举例	204	5.3.3 查看日志	289
3.10.1 Apache 服务	205	5.4 Squid 优化	291
3.10.2 Tomcat 服务	236	5.5 Squid 安全	292
3.11 小结	252	5.5.1 acl 规则	292
第 4 章 FTP 服务	253	5.5.2 许可规则	293
4.1 FTP 服务	253	5.6 缓存管理	294
4.2 WU-FTPD	253	5.7 应用举例	295
4.2.1 安装	254	文件/etc/squid/squid.conf	295
4.2.2 控制 FTP 服务	254	5.8 小结	297
4.2.3 检测 FTP 服务	255	第 6 章 网关服务	298
4.2.4 配置文件 ftpaccess	258	6.1 TCP/IP 简介	298
4.2.5 WU-FTPD 工具	262	6.1.1 ISO 模型	298
4.2.6 WU-FTPD 安全	263	6.1.2 TCP/IP	299
4.3 vsftpd	265	6.1.3 TCP、UDP 协议	300
4.3.1 安装	266	6.1.4 IP 地址	300
4.3.2 控制 vsftpd 服务	266	6.1.5 MAC 地址	301
4.3.3 检测 vsftpd 服务	266	6.1.6 路由	301
4.3.4 配置文件 vsftpd.conf	266	6.2 连接 Internet	302
4.3.5 vsftpd 安全	271	6.2.1 拨号接入	302
4.3.6 FTP 命令	273	6.2.2 发送传真	312
4.4 tftp 服务	274	6.2.3 ADSL 接入	315
4.4.1 TFTP 安装	275	6.2.4 宽带接入	320
4.4.2 配置 TFTP 服务	275	6.3 路由设置	322
4.4.3 检测服务	275	6.3.1 工作原理	322
4.4.4 使用 TFTP	276	6.3.2 设置 IP 转发	323
4.5 应用举例	276	6.3.3 ipchains	324
4.5.1 WU-FTPD	276	6.3.4 iptables	328
4.5.2 vsftpd	279	6.3.5 ftp 设置	332
4.6 小结	282	6.3.6 检测设置	334
第 5 章 代理服务	283	6.4 流量控制	346
5.1 代理服务原理	283	6.4.1 安装	346

6.4.2	工作原理.....	346
6.4.3	设置流量控制.....	346
6.4.4	维护流量设置.....	349
6.5	访问内部网络.....	352
6.5.1	工作原理.....	352
6.5.2	设置.....	352
6.6	配置实例.....	353
6.6.1	文件/etc/sysconfig/network	354
6.6.2	内部网络网卡文件/etc/ sysconfig/network-scripts/ ifcfg-eth0	354
6.6.3	外部网络网卡文件/etc/ sysconfig/network-scripts/ ifcfg-eth1	354
6.6.4	防火墙脚本文件 /root/bin/fire	354
6.6.5	ADSL 接入的/etc/ sysconfig/network 文件	355
6.6.6	ADSL 外部网卡文件/etc/ sysconfig/network-scripts/ ifcfg-eth1	355
6.6.7	ADSL 接入的防火墙文件 /root/bin/fire-adsl.....	355
6.7	小结.....	356
第 7 章	DHCP 服务.....	357
7.1	DHCP 服务原理.....	357
7.2	DHCP 服务配置.....	357
7.2.1	DHCP 服务安装.....	357
7.2.2	配置 DHCP 服务.....	358
7.2.3	控制 DHCP 服务.....	360
7.2.4	检测 DHCP 服务.....	360
7.3	客户端设置.....	363
7.3.1	Windows 客户端.....	363
7.3.2	Linux 客户端.....	365
7.4	DHCP 服务特殊设置.....	366
7.4.1	多网卡 DHCP 服务器.....	366
7.4.2	分配静态 IP 地址.....	366
7.4.3	分配多网段 IP 地址.....	368

7.4.4	DHCP 服务转发代理.....	368
7.5	应用实例.....	369
7.5.1	文件/etc/dhcpd.conf.....	369
7.5.2	文件/etc/sysconfig/dhcpd.....	370
7.5.3	文件/var/lib/dhcp/dhcpd .leases (部分)	370
7.6	小结.....	371
第 8 章	Samba 服务.....	372
8.1	Samba 运行原理.....	372
8.2	安装 Samba.....	372
8.3	配置 Samba 服务.....	373
8.3.1	配置 smb.conf 文件.....	373
8.3.2	Samba 用户管理.....	379
8.4	控制 Samba 服务.....	381
8.5	检测 Samba 服务.....	382
8.5.1	检测 smb.conf 文件.....	382
8.5.2	检测服务进程.....	389
8.5.3	检测端口.....	390
8.5.4	服务日志.....	391
8.6	使用 Samba 服务.....	394
8.6.1	网上邻居.....	394
8.6.2	smbstatus.....	395
8.6.3	smbclient.....	396
8.6.4	smbmount.....	400
8.6.5	nmblookup.....	401
8.7	设置共享权限.....	403
8.8	Samba 服务安全.....	405
8.9	swat 工具.....	407
8.9.1	安装 swat.....	407
8.9.2	配置 swat.....	407
8.9.3	使用 swat.....	408
8.10	应用举例.....	410
8.10.1	应用一.....	410
8.10.2	应用二.....	423
8.11	小结.....	430
第 9 章	NFS 服务.....	431
9.1	NFS 服务简介.....	431
9.2	配置 NFS 服务.....	431

9.2.1 安装 NFS.....	431	11.3 客户端	468
9.2.2 配置服务	432	11.3.1 安装	468
9.2.3 控制 NFS 服务	432	11.3.2 连接 VNC 服务	469
9.2.4 检测 NFS 服务	433	11.4 其他设置	470
9.3 客户端	437	11.4.1 旧版本 VNC 服务	470
9.3.1 配置客户端	437	11.4.2 更改桌面环境	472
9.3.2 使用 NFS 服务	437	11.5 小结	472
9.4 设置 NFS 共享权限	439	第 12 章 数据库	473
9.5 Autofs 服务	439	12.1 数据库简介	473
9.5.1 安装 autofs	440	12.2 MySQL 数据库	473
9.5.2 配置 autofs 服务	440	12.2.1 MySQL 数据库安装	473
9.5.3 控制服务	441	12.2.2 控制数据库	474
9.5.4 检测服务	441	12.2.3 检测 MySQL 数据库	475
9.6 应用举例	443	12.2.4 管理 MySQL 数据库	476
9.6.1 服务器端	443	12.2.5 数据备份	486
9.6.2 客户端	443	12.3 Sybase 数据库	488
9.7 小结	444	12.3.1 安装数据库	488
第 10 章 CVS 服务	445	12.3.2 控制数据库服务	485
10.1 CVS 服务	445	12.3.3 检测数据库	498
10.2 配置 CVS 服务	445	12.3.4 建立数据库	500
10.2.1 安装 CVS 服务	445	12.3.5 管理数据库	506
10.2.2 配置 CVS 服务	445	12.3.6 数据备份和恢复	511
10.2.3 检测 CVS 服务	448	12.4 小结	518
10.3 配置客户端	450	第 13 章 BBS 服务	519
10.3.1 图形界面	450	13.1 介绍 BBS 服务	519
10.3.2 命令简介	452	13.2 配置 BBS 服务	519
10.4 用户权限	457	13.2.1 安装 BBS 服务程序	519
10.4.1 CVS 服务的权限管理	457	13.2.2 配置 Web 服务	520
10.4.2 通过系统设置权限	457	13.2.3 配置数据库	522
10.4.3 setfacl 命令	459	13.2.4 配置 BBS 服务	523
10.5 小结	462	13.3 使用 BBS 服务	524
第 11 章 VNC 服务	463	13.4 小结	527
11.1 VNC 服务简介	463	第 14 章 LDAP 服务	528
11.2 配置 VNC 服务端	463	14.1 LDAP 服务简介	528
11.2.1 安装 VNC 服务	463	14.1.1 目录服务	528
11.2.2 配置 VNC 服务	464	14.1.2 LDAP 服务	528
11.2.3 控制 VNC 服务	464	14.2 配置 LDAP 服务	529
11.2.4 检测 VNC 服务	465	14.2.1 安装 OPENLDAP	529

14.2.2	服务端	530	14.4	LDAP 应用举例	548
14.2.3	客户端	534	14.4.1	LDAP 服务器	548
14.2.4	检测服务	535	14.4.2	客户端配置文件	
14.3	使用 LDAP 服务	537		etc/openldap/ldap.conf	
14.3.1	添加数据	537		(同服务端在一台主机)	552
14.3.2	数据查询	540	14.5	小结	552
14.3.3	删除数据	547	附录	相关系统命令	553

第 1 章 DNS 服务

本章内容:

- 介绍 DNS 服务运行原理
- 配置 DNS 的基本方法
- 从 DNS 服务器的配置方法
- DNS 服务器的启动停止
- 检测 DNS 服务运行状态
- 不同环境下的 DNS 服务器的配置
- DNS 服务器的安全

本章主要介绍关于 DNS 服务器的配置方法,包括 DNS 的运行原理,配置方法,并介绍了一些 DNS 服务在实际运行中会遇到的不同环境,根据环境的要求对 DNS 服务器如何配置。DNS 服务器的检测,查看 DNS 服务运行情况和一些 DNS 服务使用过程中的工具。以及 DNS 服务器的其他配置参数,通过这些参数的设置,可提高 DNS 服务器的安全和运行的效率。

1.1 DNS 原理

DNS 的主要功能就是将我们熟悉的网址转换为网络上服务器熟悉的 IP 地址。将网址转换为 IP 地址,称为正向解析。将 IP 地址转换为网络地址,称为反向解析。

因此 DNS 服务器,是 Internet 网络上最重要的服务器,因为不管你架设了什么样的服务器,制作了多少精美的网站,如果想让大家共享你的劳动成果,就必须要让别人能够访问到你,而依靠 IP 地址,别人是很难记住的。所以配置 DNS,可以通过 DNS 自动完成这个复杂的过程。

DNS 的整个体系与 Linux 目录有些相似,如同一棵倒过来的树,顶级域也就是树根是“.”。例如平时我们输入的网址全名应为 `www.sohn.com.`。而所谓的“域”,就是一个范围,全球在“.”这个范围内,而这个大的范围又被分为许多小的区域,如“com.”“gov.”“org.”。如 `www.sohn.com` 网址中 `www` 为服务器的名字,而 `sohn` 为这台服务器所在的域,而 `com` 则是 `sohn` 这个域所在的域,即 `sohn` 域是 `com` 域的子域,`com` 域是 `sohn` 域的父域。`Mails.sohn.com` 是 `sohn` 域中名为 `mails` 的服务器。而 `www.along.com` 则是 `com` 域的另一个名为 `along` 域中的名为 `www` 的服务器。

注意: `www.sohn.com`, `mails.sohn.com`, `www.along.com` 这些名字所指的服务器,在实际应用中有可能不是一台服务器的名字,即一个网址对应多台服务器或多个 IP 地址。

DNS 体系结构如图 1-1 所示。

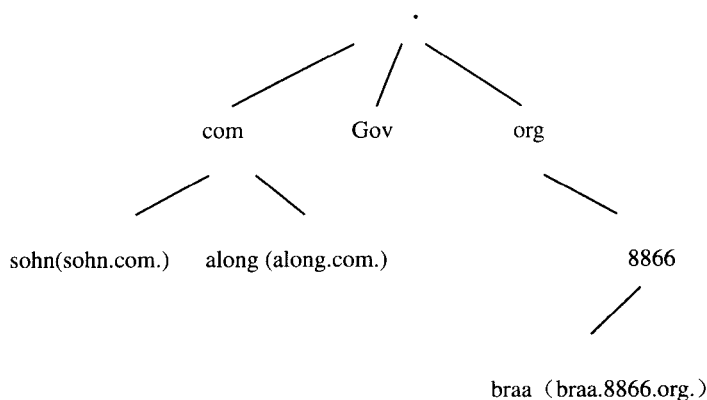


图 1-1 DNS 体系结构

首先我们在客户端输入 `www.sohn.com`，我们使用的机器会查找本机所指定的 DNS 服务器（Linux 系统下在文件 `/etc/resolv.conf` 文件中指定。），假设我们指定的 DNS 服务器是在 `braa` 这个域中的一台 DNS 服务器，通常我们指定 DNS 服务器使用 IP 地址，一般申请 ADSL 或其他接入方式时，电信工程师会告诉我们 DNS 服务器的 IP 地址，也可以到网上查找 DNS 服务器的资源。

在 `braa` 的 DNS 服务器收到 `www.sohn.com` 这个网址后，查看网址采用从右向左查看，即 `com.sohn.www`。首先在 DNS 服务器缓存中查找是否保存有这个 `www.sohn.com` 的 IP 地址。如果存在则直接将这个 IP 地址返回给我们的机器。如果不存在，`braa` 的 DNS 服务器（我们客户端指定的 DNS 服务器）会在缓存中查找 `sohn.com` 域的 DNS 服务器的 IP 地址。如果还不存在，则在缓存中继续查找是否保存 `com` 域的 DNS 服务器的 IP 地址，然后 `braa` 的 DNS 服务器再到那个 DNS 服务器上查找 `www.sohn.com` 的 IP 地址。最后将 `www.sohn.com` 的服务器的 IP 地址告诉我们的机器，机器再直接到这个 IP 地址上获取我们需要内容。通常缓存中保留的 IP 地址是以前查询过而保留下来的，但有一定的期限，过期后会被删除。

当我们的客户端所指定的 DNS 服务器在它的缓存中没有找到 `sohn` 域或 `com` 域的 DNS 服务器时，则它会直接到顶级域“.”，去查询“com.”这个域。这是因为 DNS 有个顶级服务器的列表 `/var/named/named.ca`。到某个指定的顶级 DNS 服务器查询后，顶级 DNS 服务器会告诉 `braa` 的 DNS 服务器 `com` 域的 DNS 服务器的 IP 地址，然后 `braa` 域的 DNS 服务器再到 `com` 域的 DNS 服务器上询问 `sohn` 域的 DNS 服务器的 IP 地址，从 `sohn.com` 域的 DNS 服务器得到 `www.sohn.com` 的 IP 地址，最终将这个 IP 地址返回给我们的机器。这个过程与在缓存中没有直接找到 `www.sohn.com` 地址时，需到各域的 DNS 服务器查找的过程类似，只是多了一步要到顶级域去查找 `com` 域 DNS 服务器的过程。如图 1-2 是 DNS 运行原理的基本顺序示意。

客户端指定 DNS 服务器

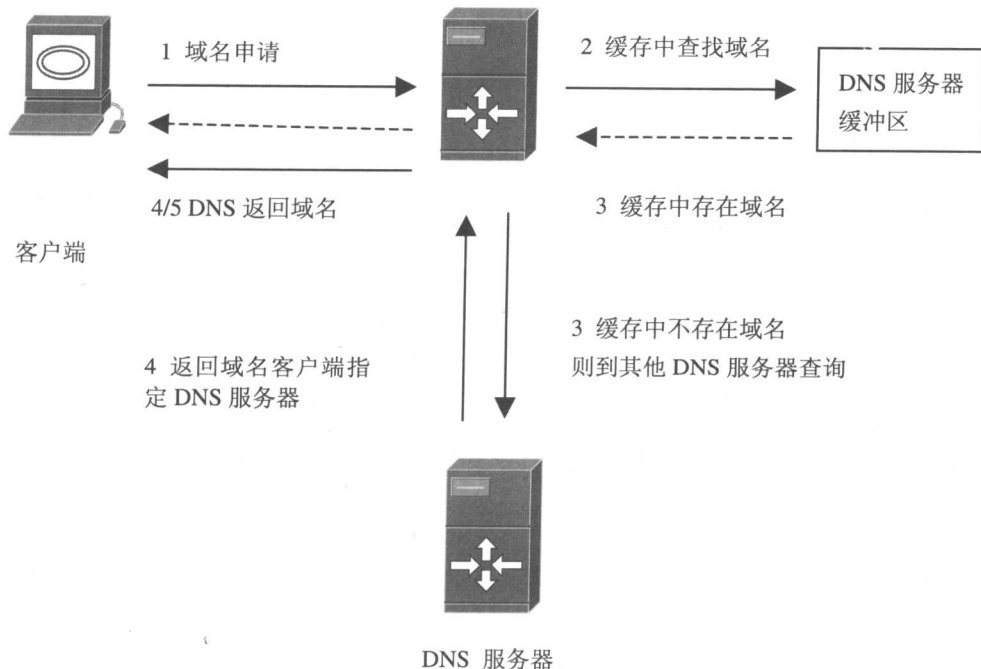


图 1-2 DNS 运行原理示意图

在实际应用中，一般先到 CNNIC 申请域名，DNS 服务器由负责服务器托管的单位来做，他们来负责你的服务器名字的解析，不过有些托管的地方要收费，而且多数默认只做单向解析，即解析从服务器名字转换到 IP 地址，不解析 IP 地址转换到服务器名字。这样做在应用上没有问题，但是不够安全，尤其是在做邮件服务器时，没有反向解析会被许多国外的邮件服务器认为是不可靠的邮件来源，邮件有可能会被拒收。所以，不论是别人还是自己做 DNS 一定要做双向解析。自己做 DNS 服务器时，要通知 CNNIC 将域名的解析指向你的 DNS 服务器的 IP 地址。

1.2 DNS 服务器的基本配置

初步介绍 DNS 服务所须的文件，每个文件的用法和格式。如何快速的建立具备基本解析功能的 DNS 服务器。

1.3 DNS 服务器的安装

DNS 服务器在 Linux 下使用的程序包名为 BIND，一般在 Linux 的安装盘中都有这个程序。可以使用命令 `rpm -q bind` 来查询本系统是否安装了这个包。

```
[root@testm conf]# rpm -q bind
```

bind-9.2.1-16

如果没有安装则将 Linux 安装盘插入光驱,用 `mount /mnt/cdrom` 命令安装光驱到系统中,用 `find /mnt/cdrom | grep bind` 查找 BIND 程序包所在路径。一般在 `/mnt/cdrom/RedHat/RPMS` 目录下。找到安装包后,使用命令 `rpm -ivh /mnt/cdrom/RedHat/RPMS/“包名”` 安装,如 `rpm -ivh /mnt/cdrom/RedHat/RPMS/bind-9.2.1-16`。

安装过程中,如果没有报错,说明 DNS 服务安装成功,为了检验安装的结果,在 `/etc` 目录下,应有 `named.conf` 文件、`rndc.conf`、`rndc.key`。目录 `/etc/init.d` 或 `/etc/rc.d/init.d` 中有 DNS 的启动脚本文件 `named`。在 `/var/named` 目录下有:

```
[root@testm conf]# ls -la /var/named
total 20
drwxr-xr-x  2 named  named    4096 Apr  1 17:12 .
drwxr-xr-x 27 root   root     4096 Sep 25 2003 ..
-rw-r--r--  1 named  named    195 Jan 25 2003 localhost.zone
-rw-r--r--  1 named  named   2499 Jan 25 2003 named.ca
-rw-r--r--  1 named  named    472 Apr  1 17:12 named.local
```

等数据库文件。

配置文件

`/etc/hosts`

`/etc/host.conf`

`/etc/resolv.conf`

`/etc/named.conf`

`/var/named` 目录下所有文件

`/etc/init.d/named`

1.3.1 hosts 文件

完成服务器名字查询功能的不光是 DNS,在没有出现 DNS 以前,网络上负责查询服务器 IP 地址的是每台机器的 `hosts` 文件,在这个文件中写入机器名和其相对应的 IP 地址,当有新机器加入网络或改动机器地址时,每台机器都要更改自己的 `hosts` 文件。在当时机器不多时,这个工作还是比较轻松的,但随着机器的增多,工作量越来越大。因此,更改了这种工作模式,采用现在的 DNS 服务。但现在 `hosts` 文件仍有它的作用。在 `/etc` 目录下的 `hosts` 文件内容如下:

```
#do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
192.168.0.1        gateway.pip.com gateway
192.168.0.6        master.pearl.net master
```

带 ‘#’ 的两行为注释,查询过程中不起作用。之后的第一行为系统安装后默认的,表示 127.0.0.1 为本机固有地址。后两行为手动添加,意思为 IP 地址为 192.168.0.1 的服务器名

字为 gateway.pip.com, 别名为 gateway。IP 地址为 192.168.0.6 的服务器名字为 master.pearl.net, 别名为 master。当输入命令 ping master 时就可 ping 通这台服务器, 如果文件中没有 master 的记录, 而 DNS 又没做解析的情况下, 则输入此命令时, 会得到找不到主机的如下提示:

```
[root@gateway etc]# ping master
ping: unknown host master
```

host 文件主要用于内部局域网, 当内部网络有些服务器是大家常访问的机器, 而输入 IP 地址又比较麻烦, 又不可能去为这些服务器申请域名, 就可以采用这种比较简单的方法, 直接把服务器名和 IP 地址写到文件中。Host 比 DNS 容易修改, 使用方便。

1.3.2 host.conf 文件

DNS 的主要配置文件在目录/etc 下, 其中 host.conf 文件指定本服务器查询名字时使用的顺序, 即/etc/目录下的 host.conf 文件是决定服务器先以哪种方式来查询名字。host.conf 文件内容如下:

```
order hosts,bind
```

order 为固定格式, 这行表示为当服务器收到查询名字的请求时, 首先查看 hosts 的文件, 如果没有找到, 再做 DNS 查询。要更改查询顺序可写为:

```
order bind,hosts
```

host.conf 文件规定的顺序很重要, 在配置 DNS 时, 不要在 hosts 文件和 DNS 中同时注册一台机器名字, 造成配置过程中出错, 难以确定问题的所在。

1.3.3 resolv.conf 文件

/etc/resolv.conf 文件定义 DNS 服务器的 IP 地址。这个文件的设置通常为客户端的配置文件, DNS 分为客户端和服务端两种模式。所谓的客户端可以理解为只提出 DNS 的查询, 本身不做 DNS 解析的设备, 例如, 我们平时使用的个人 PC 机或笔记本。而服务器则不仅做本域的机器名的查询工作, 也可以为客户端做其他域的查询工作。

做客户端时文件的格式为:

```
# MADE-BY-RP-PPPOE
nameserver 202.38.64.1
nameserver 202.106.196.115
```

第一行为注释, 无实际意义。第二行设置 IP 地址为 202.38.64.1 的服务器为本机指定的首选 DNS 服务器, 当然这台服务器一定是具备 DNS 功能的设备, 不是随便指定的。指定 IP 地址为 202.106.196.115 的 DNS 服务器为候选服务器。通常只有当首选服务器没有回应时, 才会启用候选服务器。如果你的首选 DNS 服务器没有查到你想要的机器名的 IP 地址时, 会给你一个没有找到主机的信息, 这时你的客户端会到候选服务器上去再查询一次的。通常最多只设置三台 DNS 服务器。

还可设置如下:

```
# MADE-BY-RP-PPPOE
search pip.com
nameserver 192.168.0.1
```

```
nameserver 202.38.64.1
nameserver 202.106.196.115
```

不算注释行，第一行的意思为默认的域为 `pip.com`，通常为本地域（这个域是没有申请过的，只能用来在局域网内使用）。下一行为首选的 DNS 服务器，其后依次为备选服务器。一般当存在 `search` 这行时，首选服务器为解析这个域的 DNS 服务器。`search pip.com` 这一行的主要作用是，假设我们在这个域中有一台 `www.pip.com` 的服务器。没有 `search` 这行时通常要输入完全的服务器名字，而有了这一行后，只须输入机器名就可。如 `ping www`，DNS 会自动为我们补全域名。

当配置或使用 DNS 服务器时，`resolv.conf` 文件会有影响。作为 DNS 服务器的同时，也可作为一台客户端。当做为 DNS 服务器的 `resolv.conf` 文件中的首选 DNS 解析服务器不是本机时，即将以上的配置改为：

```
search pip.com
nameserver 202.38.64.1
nameserver 192.168.0.1
nameserver 202.106.196.115
```

这时在本机发出 DNS 解析申请时，查询会到 202.38.64.1 这台机器上询问名字的解析，而此时我们询问的又是 `www.pip.com` 这种不须注册，只在内部网络使用，内部 DNS 才能解析的地址。而 202.38.64.1 做为一台 Internet 网络上的公共 DNS 服务器是不可能解析出 `www.pip.com` 这种内部地址的。而且当首选 DNS 做出应答时，我们发出申请查询地址的本机是不会再去询问第二台 DNS 服务器的，即真正能正确解析地址的 192.168.0.1 服务器。因此它会返回一条错误信息，告诉我们网址无法找到。但这并不是我们 DNS 配置错误，只是作为客户端我们的设置顺序出了问题。可更改本机的 DNS 查询顺序，或更换一台设置正确的客户端。

当 Windows 系统做为客户端时，而 Linux 做服务器端时，这条原则是不成立的。如果 Linux 做客户端，而 Windows 做 DNS 服务器时，格式如下：

```
# MADE-BY-RP-PPPOE
search pearl.net
nameserver 192.168.0.6
```

`pearl.net` 为 Windows 所在的域，192.168.0.6 为 Windows 系统的 DNS 服务器的 IP 地址。当 Linux 做客户端需要查询两个域时可写为：

```
# MADE-BY-RP-PPPOE
search pearl.net
nameserver 192.168.0.6
search pip.com
nameserver 192.168.0.1
```

`pearl.net` 为其他域，`pip.com` 为 Linux 客户端所在的域，一定要把自己所在的域放在最后。Linux 还算方便吧，说这些主要是有时做 DNS 服务器的机器在某些特定环境下也会同时做客户端。

Resolv.conf 文件的设置通常会影响到客户端的查询，对 DNS 服务器本身的设置是不会有影响的。

1.3.4 named.conf 文件

/etc/named.conf 是 BIND 的核心文件，内容如下：

```
// generated by named-bootconf.pl

options {
    directory "/var/named";           //设定 DNS 使用的文件保存的目录
    /*
     * If there is a firewall between you and nameservers you want
     * to talk to, you might need to uncomment the query-source
     * directive below. Previous versions of BIND always asked
     * questions using port 53, but BIND 8.1 uses an unprivileged
     * port by default.
     */
    // query-source address * port 53;
    listen-on port 53 {               //设定 DNS 在哪些 IP 地址上监听查询请求
        127.0.0.1;
        192.168.0.1;
    };

    forward first ;                   //设定 DNS 的转发
    forwarders {202.38.64.1; 202.96.199.133;};

};

//
// a caching only nameserver config
//
controls {                           //系统默认
    inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

zone "." IN {                         //顶级 DNS 服务器地址所在文件
    type hint;
    file "named.ca";
};

zone "localhost" IN {                //本机正向解析，系统默认
```

```

        type master;
        file "localhost.zone";
        allow-update { none; };
    };

    zone "0.0.127.in-addr.arpa" IN {           //本机反向解析，系统默认
        type master;
        file "named.local";
    };

    zone "pip.com" in {                       //本地域的正向解析，管理员输入
        type master;
        file "named.pip.com";
    };

    zone "0.168.192.in-addr.arpa" in {       //本地域的反向解析，管理员输入
        type master;
        file "named.ip";
    };

    include "/etc/rndc.key";                 //系统默认

```

在 `options {}` 中通常写入 DNS 的一些控制参数，其中 `directory "/var/named"` 指定 DNS 保存正向解析和反向解析的文件、顶级 DNS 服务器地址文件等所有非配置文件的保存目录，此参数可由管理员修改，但要把 `/var/named` 目录下的文件复制到管理员所指定的新目录中去。`options {}` 中的其他参数稍后介绍。

再下面的多是 BIND 安装后自动配置的，不用更改。重要的是要管理员输入的部分。

从

```

zone "pip.com" in {                       //本地域的正向解析，管理员输入
    type master;
    file "named.pip.com";
};

```

这部分开始是要由 DNS 管理员来输入更改了，这段主要标示正向解析部分。

```

zone "pip.com" in {

```

为标准格式，其中 `pip.com` 为管理员所需要建立的 DNS 域名。这个域的名字可以是注册过的也可以是未注册的，只要需要查询你这个域的服务器的客户能将他们的 DNS 服务器指向你的 DNS 服务器就行。如果你的域是面向整个 Internet 网络，那还是尽快去申请域名