第36章 配 置 DNS

作者：Tim Parker

本章内容包括：

- 域名服务器
- 资源记录
- 域名解析
- 配置UNIX或Linux域名服务器
- Windows与DNS

为避免记忆枯燥的网络上服务提供者主机的 IP地址，用户可以在网络中设置域名服务器，从而使用户在访问某主机时，只需敲入该主机的域名而不需敲入其 IP地址。如果给域名一定的含义，记忆域名将比记忆IP地址要容易得多。

域名系统，正如其名字所示，将整个 internet网络分割为一组域或网络，每个域又可细分为多个子域。第一组域被称之为顶级域，对于经常在网上浏览或上互联网的用户，顶级域名应该不陌生。一般情况下，顶级域包含以下七部分：

- arpa —— 特殊互联网组织
- com —— 公司、企业
- edu —— 教育组织
- gov —— 政府实体
- mil —— 军队部门
- net —— 服务提供商
- org —— 非商业组织

除了上述顶级域外，每个国家的域名空间又都分为上述的顶级域，通常用国家的简写代表国家的名字，如：.ca表示加拿大(canada)、.uk表示United Kingdom(英国)、.cn表示China(中国)。在顶级域下是单个组织一级的域 (如：sams.com及linux.org)。所有的域名均在网络信息中心(NIC)注册，每个域名都是惟一的。

36.1 域名服务器

每个域名服务器管理网络的不同区域 (或整个网络，如果网络规模较小)。由一台域名服务器管理机器的集合称为一个区 (zone)。一台域名服务器也可以管理多个区。在一个区内，通常都设有辅助或备份域名服务器，两个域名服务器 (主控域名服务器和辅助域名服务器)不断复制信息。同一个区的域名服务器使用区传输协议。

整个域名服务系统通过一组嵌套的区运作。每个域名服务器与其上级域名服务器通信。每个区至少有一台域名服务器负责区内每台机器的地址信息。每个域名服务器同时知道至少一台其他域名服务器的地址。

当某个用户的应用需要将域名解析为网域地址时，应用向解析进程发送查询信息，解析

进程再与域名服务器通信。域名服务器检查本地的表并返回与域名对应的网络地址。如果域名服务器没有所需要的信息，它将向其他域名服务器发送请求。域名服务器及解析进程都使用数据库的表并且缓存本地区内机器的信息，同时缓存区外最近的请求响应信息。

当域名服务器接收解析进程的查询请求时，域名服务器可执行多种类型的操作，所有这些操作大致可分为两类：

一种是递归解析，要求名字服务器必须访问其他域名服务器获取信息；另一种是非递归操作。在此种操作中，域名服务器返回解析请求的结果、另一个域名服务器的地址 (解析进程必须再次发送请求)或错误信息。当采用递归解析时，域名服务器在必要时请求其他域名服务器解析用户请求。远程域名服务器将返回解析结果或失败信息。 DNS规则禁止远程服务器再向其他服务器发送解析请求。

36.2 资源记录

用来解析域名的信息由域名服务器维护为一组资源记录，它是数据库中的项。资源记录 (简称为RR)以ASCII格式存储信息。用户可以非常方便地查到资源记录的格式，在此不做重复。

DNS使用的地址字段如地址资源记录类型，采用 IN-ADDR-ARPA格式。它允许由地址到域名的反向映射，同时也允许域名到地址的映射。为了更好地理解 IN-ADDR-ARPA，我们先从标准的资源记录格式开始。最简单的资源记录类型用于记录 IP地址(类型A)。下面列出了一个地址文件中的部分内容：

```
TPCI_HPWS1      IN      A       143.12.2.50
TPCI_HPWS2      IN      A       143.12.2.51
TPCI_HPWS3      IN      A       143.12.2.52
TPCI_GATEWAY    IN      A       143.12.2.100
                IN      A       144.23.56.2
MERLIN          IN      A       145.23.24.1
SMALLWOOD       IN      A       134.2.12.75
```

文件中的每一行表示一个资源记录。在上例中，所有的资源记录均采用最简单的格式：主机的域名 (别名)、主机的类别 (In表示Internet)， A表示该记录为地址资源记录，最后是Internet地址。主机TPCI_GATEWAY所对应的项包含两个IP地址，因为它是连接两个网的网关。网关在每个网中都有单独的IP地址，因此两个资源记录在同一个文件中。

这种类型的文件使域名到地址的映射变得简单。域名服务器简单查询每一行的域名，判断是否与应用请求解析的域名一致，并返回该行末尾的地址。数据库以域名为索引，因此，查询非常迅速。

由地址到域名的查询就不那么简单。如果资源记录文件很小，查询时间较短，但对于包含成千上万或百万台机器的区域，时间延迟可能很大。因为数据库以名字为索引，以地址来查询将是一个缓慢的过程。为了解决这一反向映射的问题，引入了 IN-ADDR-ARPA。IN-ADDR-ARPA采用主机地址为索引。当添加一个新的资源记录，其域名可被抽取。

IN-ADDR-ARPA采用PTR资源记录类型来指明地址所对应的域名。几乎每一个域名服务器都维护这一类指针索引。以下列出了一种地址到域名的映射文件的内容：

```
23.1.45.143.IN-ADDR-ARPA.     PTR     TPCI_HPWS_4.TPCI.COM
1.23.64.147.IN-ADDR-ARPA.     PTR     TPCI_SERVER.MERLIN.COM
3.12.6.123.IN-ADDR-ARPA.      PTR     BEAST.BEAST.COM
```

```
143.23.IN-ADDR-ARPA          PTR     MERLINGATEWAY.MERLIN.COM
```

在IN-ADDR-ARPA文件中，Internet地址被反转，以便使用。如上例所示，没有必要写出完整的IP地址，因为域名服务器将会提供足够的路由信息。

36.3 域名解析

就用户的应用而言，将域名解析为实际的网络地址比较简单。应用向域名解析者也称之为解析进程发送查询请求(解析进程有时也可能在别的机器上)。域名解析者如果可以解析该域名，将向应用返回结果。如果域名解析者不能确定网络地址，它将与域名服务器通信 (域名服务器也可能再与其他域名服务器联系)。

解析进程将会取代机器上已有的域名解析系统：如 /etc/hosts文件。取代过程对用户来说是透明的，但管理员需要知道何时使用本地域名解析系统，何时使用 DNS以便正确维护域名服务器中的表。

当解析进程从域名服务器获取了信息后，它将信息缓存在本地 Cache中，以减少对同一个域名的重复解析请求(这种情况在网络应用中经常出现)。解析进程缓存记录的时间根据资源记录中Time-to-Live字段而定，或采用系统的缺省时间。

当域名服务器不能解析某个域名时，它向解析进程返回消息，并在消息的 Authority字段填入另一台域名服务器的地址。解析进程接到消息后，向另一台域名服务器发送解析请求。解析进程也可以通过设置请求中的递归位 (RD)来要求域名服务器完成查询。域名服务器可以拒绝或接受此类请求。

解析进程可以使用UDP和TCP协议进行查询，但大部分都使用 UDP协议，因为其速度快。但对于反复查询或传输大量信息，将采用可靠性高的 TCP协议。

在预装了DNS的UNIX或Linux操作系统中，域名解析进程有多种实现方式。其中 BSD版UNIX中的解析进程功能有限，它既不提供反复查询也不支持 Cache。为了弥补这一局限，需添加伯克利Internet域名服务器(BIND)。BIND提供三种不同方式的缓存和反复查询：作为主控服务器，辅助服务器或仅作缓存服务器 (它不包含自己的数据库，只有 Cache)。在BSD系统中使用BIND允许其他进程控制域名解析的负载，该进程可以是其他主机上的进程。

36.4 配置UNIX或Linux域名服务器(DNS)

配置域名服务器需要修改或创建大量文件和数据库。这一过程非常耗时，但幸运的是每一台域名服务器仅需作一次。在大多数 DNS服务器中，这些文件及其作用如下：

- named.hosts —— 定义主机名到IP地址映射的域名。
- named.rev —— 采用IN-ADDR-ARPA实现IP地址到主机名的映射。
- named.local —— 用于解析本地驱动。
- named.ca —— 列出域名服务器。
- named.boot —— 用于设置文件和数据库的位置。

通常域名服务器都采用以上文件名，但用户也可根据需要进行修改。上述文件中最重要的是named.boot，它在系统启动时被读取，并且其中定义了其他文件的文件名及位置。因此，任何文件名的变化都必须在 named.boot中做相应的修改。为简单起见，本章使用上述约定的文件名。每个列出的文件都是一个资源记录形式的数据库。

36.4.1 添加资源记录

对于特定的服务器配置，必须使用标准的名字和网络格式，这样 DNS将使用户非常迷惑。但以简单的格式，将使用户更容易理解这些文件及资源记录的功能。

在named.hosts文件中存放SOA资源记录。分号为注解符，该资源记录采用每一行一个字段的格式，使得记录更清晰，但这不是必须的。资源记录定义了顶层域名为 tpci.com，server.tpci.com为域中的主域名服务器， root @ merlin.tpci.com为域管理员的邮件地址，其余行含义见注解。

```
tpci.com.  IN  SOA
server.tpci.com
root @ merlin.tpci.com (
2；    序列号
7200；刷新时间(2小时)
3600；重试时间(1小时)
151200；过期时间(1周)
86400)；最小TTL
```

注意，从序列号到 TTL字段包含在括号之内。这是命令的语法，必须包含括号以标明参数顺序。

除了SOA RR外， named.hosts还包含地址记录。这些记录用于从主机名到 IP地址的映射。以下列出了少量地址资源记录以说明格式：

```
artemis     IN     A     143.23.25.7
merlin      IN     A     143.23.25.9
pepper      IN     A     143.23.25.72
```

主机名并未给出域名全称，因为服务器可以推断出完整的域名。如果用户想要列出完整的域名，就必须在名称后加点号。在上例的基础上，以下给出了采用完整域名的示例：

```
artemis.tpci.com.     IN     A     143.23.25.7
merlin.tpci.com.      IN     A     143.23.25.9
pepper.tpci.com.   A     143.23.25.72
```

指针(PTR)资源记录使用IN-ADDR-ARPA完成从IP地址到域名的映射。以下仅采用一个资源记录做简单说明：

```
7.0.120.147.in-addr.arpa IN PTR merlin
```

上述记录标明主机名为merlin的机器IP地址为147.120.0.7。

域名服务器资源记录指明域名服务器对特定区的权限。名字服务器记录 (NS)被用于拥有多个子网的大型网络。其中每个子网都有其名字服务器， NS记录示例如下：

```
tpci.com   IN   NS  merlin.tpci.com
```

该记录标明tpci.com域的DNS服务器为merlin.tpci.com。如果tpci.com有多个子网，每个子网都要包含NS RR。

36.4.2 完成DNS文件

如上所述， DNS使用大量文件来存放 DNS所需的资源记录。第一个文件为 named.hosts，它包含SOA、NS和A资源记录。 named.hosts的每一项都必须从文件的第一列开始。以下是一

个named.hosts文件的示例，注解行表明记录的含义：

```
; named.hosts files
; Start Of Authority RR
tpci.com.IN
SOA merlin.tpci.com
root.merlin.tpci.com (
2  ; Serial number
7200 ; Refresh (2 hrs)
3600 ; Retry (1 hr)
151200 ; Expire (1 week)
86400 ); min TTL
;
; Name Service RRs
tpci.com    IN    NS  merlin.tpci.com
subnet1.tpci.com IN NS goofy.subnet1.tpci.com
;
; Address RRs
artemis      IN      A     143.23.25.7
merlin       IN      A     143.23.25.9
windsor      IN      A     143.23.25.12
reverie      IN      A     143.23.25.23
bigcat       IN      A     143.23.25.43
pepper       IN      A     143.23.25.72
```

文件的第一部分设置 SOA记录的各项参数：生存期、过期时间、刷新时间等。设置tpci.com域的域名服务器为merlin.tpci.com。第二部分使用名字服务器资源记录设置 tpci.com域的域名服务器为 merlin.tpci.com(与SOA中相同)。设置tpci的子网名为subnet1，该子网的域名服务器为goofy.subnet1.tpci.com。第三部分列出了一系列地址资源记录以便由域名映射为 IP地址，域中的每一台主机在这一部分都对应一项。

named.rev文件提供从IP地址到机器名的逆向映射功能，它由指针资源记录组成。其格式与named.hosts中记录的格式基本相同 (除了将域名与 IP地址交换，并且将 IP地址转换为 IN-ADDR-ARPA风格之外)。与named.hosts对应的named.rev文件如下：

```
; named.rev files
; Start Of Authority RR
23.143.in-addr.arpa IN SOA merlin.tpci.com
          root.merlin.tpci.com (
          2  ; Serial number
          7200 ; Refresh (2 hrs)
          3600 ; Retry (1 hr)
          151200 ; Expire (1 week)
          86400 ); min TTL
;
; Name Service RRs
23.143.in-addr.arpa    IN    NS  merlin.tpci.com
100.23.143.in-addr.arpa    IN NS goofy.subnet1.tpci.com
;
; Address RRs
9.25.23.143.in-addr.arpa    IN    PTR merlin
12.25.23.143.in-addr.arpa   IN    PTR windsor
```

```
23.25.23.143.in-addr.arpa  IN   PTR reverie
43.25.23.143.in-addr.arpa  IN   PTR bigcat
72.25.23.143.in-addr.arpa  IN   PTR pepper
```

网络中的每个区或子域都必须有独立的 named.rev文件。这些文件可以采用不同的文件名且放在不同的目录中。如果用户仅有一个区，只需一个 named.rev文件即可。

named.local文件包含本地驱动器的入口 (本地驱动器采用IP地址为127.0.0.0)。文件中必须包含IN-ADDR-ARPA映射到本地驱动的信息，及域信息 (因为named.rev文件中不包含 127子网)。named.local文件示例如下：

```
; named.local files
; Start Of Authority RR
0.0.127.in-addr.arpa IN
SOA merlin.tpci.com
root.merlin.tpci.com (
2  ; Serial number
7200 ; Refresh (2 hrs)
3600 ; Retry (1 hr)
151200 ; Expire (1 week)
86400 ); min TTL
;
; Name Service RR
0.0.127.in-addr.arpa   IN   NS  merlin.tpci.com
;
; Address RR
1.0.0.127.in-addr.arpa   IN   PTR localhost
```

该文件提供从名为localhost的主机到IP地址127.0.0.1的映射。

named.ca文件用于指定系统可使用的域名服务器。在 named.ca中指定的机器必须是比较稳定、不经常变化的机器。named.ca文件示例如下：

```
; named.ca
; servers for the root domain
;
.  99999999  IN   NS  ns.nic.ddn.mil.
   99999999  IN   NS  ns.nasa.gov.
   99999999  IN   NS  ns.internic.net
; servers by address
;
ns.nic.ddn.mil   99999999   IN  A  192.112.36.4
ns.nasa.gov      99999999   IN  A  192.52.195.10
ns.internic.net  99999999   IN  A  198.41.0.4
```

在上述文件中，仅指定了三个 DNS服务器。一个正常的 named.ca文件中可能仅有一个区或包含多个域名服务器，这依据具体的系统而定。用户可以通过匿名登录到 nic.ddn.mil的FTP服务器上获取/netinfo/root-servers.txt文件，该文件包含一个完整的根域名服务器列表。

这个文件可以拷贝到named.ca文件中。named.ca中指定的服务器包含两项，一项给出根域(周期)，它放在域名服务器之后；另一项给出域名服务器 IP地址。可用周期设得非常大，因为这些服务器通常认为一直可用。

named.boot文件可看作用于加载 DNS守护进程的触发器，它还指定网络中主控域名服务

器和辅助域名服务器。named.boot示例如下：

```
; named.boot
directory      /usr/lib/named
primary
tpci.com      named.hosts
primary
25.143.in-addr.arpa      named.rev
primary
0.0.127.in-addr.arpa      named.local
cache    .      named.ca
```

在文件的第一行directory关键字之后输出DNS配置文件的路径。关键字primary之后给出DNS所需的配置信息。例如：第一行设置 tpci.com的主服务器的配置文件为 named.hosts。143.25子网的IN-ADDR-ARPA信息放在文件named.rev中。本地信息放在named.local文件中。最后，服务器及名字信息放在named.ca文件中。

辅助域名服务器的配置与主控域名服务器基本相同。区别在于 named.boot文件中仅指出主服务器的名称。

36.4.3 启动DNS守护进程

配置DNS的最后一步是确保DNS守护进程named在系统启动时被加载。通常通过rc启动脚本完成上述工作。大多数 UNIX及Linux版本都已将 DNS加入到启动脚本中，通常以检测named..boot文件的形式加入。如果named.boot存在，DNS守护进程named启动。代码如下：

```
# Run DNS server if named.boot exists
if [ -f /etc/inet/named.boot -a -x /usr/sbin/in.named ]
then
   /usr/sbin/in.named
fi
```

确切的路径名及有关属性依据不同的系统而定，但通常命令都是判断 named.boot文件是否存在，若存在则启动named。

36.4.4 配置客户端

配置UNIX或Linux机器以使其可以使用主域名服务器是非常简单的。首先修改 /etc/resolv.conf文件，使其包含主域名服务器的地址，例如， resolv.conf文件可以是如下形式：

```
domain tpci.com
nameserver   143.25.0.1
nameserver   143.25.0.2
```

第一行建立域名，随后是域名服务器的IP地址。上例中指定了143.25子网中的两个域名服务器。

36.5 Windows和域名服务器

Windows NT、Windows 95和Windows 98在作DNS服务器客户方时，仅需在Network表单的DNS页中填写DNS服务器的IP地址即可。也可以同时指定多个域名服务器，在解析域名时，将依照DNS页中域名服务器的顺序依次查询。 DNS服务器既可以在用户网络中，也可以是用

户ISP的域名服务器。当然，ISP的服务器不知道用户内部网的结构。

配置基于Windows的DNS服务器必须使用额外的插件，但在纯Windows网络中，DNS并不像WINS及DHCP那样容易配置和使用。在Windows、UNIX混合的网络中，最好将DNS安装在UNIX机器上，这不但出于性能上的考虑，而且由于操作系统体系结构上的原因。要获取建立基于Windows NT的DNS服务器参见第23章。

36.6 小结

配置DNS服务器远比配置DNS客户机复杂。考虑到设置DNS服务器所带来的益处，花一定的时间及精力安装和配置DNS服务器是非常值得的。UNIX和Linux非常适合于作DNS服务器，而Windows则适于作DNS客户机。