第3章 chapter 3

DNS服务器搭建与应用

教学目标与要求

在TCP/IP网络中，只有IP地址才能唯一标识网络中的每个节点。由于计算机网络的飞速发展，如果现在还仅用IP地址标识网络上的计算机是很不现实的，因为数量繁多的IP地址难以记住。为了解决这个问题，就产生了域名系统(Domain Name System，DNS)。它是因特网的一项核心服务，可以作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问因特网，而不用记住能够被机器直接读取的IP地址。

本章将详细介绍有关DNS服务器的基本概念、域名解析系统及在Linux系统上配置使用的相关知识。通过本章的学习，读者应该做到：

- 了解DNS基本概念及域名解析过程。
- 熟悉Linux BIND服务器的常用配置。
- 掌握配置DNS服务器的方法。

教学重点与难点

DNS服务器的配置方法和具体实现过程，DHCP的工作原理及安装、配置方法。

3.1 DNS服务器简介

DNS是一种组织成为域层次结构的计算机和网络服务命名系统。DNS命名用于TCP/IP网络(如Internet)，包含从DNS域名到各种数据类型(如IP地址)的映射。

通过DNS，用户可以使用友好的名称查找计算机和服务在网络上的位置。当用户在应用程序中输入DNS名称时，DNS服务可以将此名称解析为与其相关的其他信息。例如，在TCP/IP网络中，计算机只以数字形式的IP地址在网络上与其他计算机通信，但是数字形式的IP地址却不方便用户记忆。DNS的出现提供了一种方法，将用户计算机或服务名称映射为数字地址，使用户能够使用简单好记的名称(如www.zsu.edu.cn)来定位诸如网络上的Web服务器或邮件服务器。

3.1.1 DNS简介

在一个TCP/IP架构的网络（例如因特网）环境中，DNS是一个非常重要而常用的系统。其主要功能是将易于记忆的域名（如www.zsu.edu.cn）与不易记忆的IP地址（如202.168.10.3）进行转换。而上面执行DNS服务的这台网络主机，就称为DNS服务器。通常认为DNS只是将域名转换成IP地址，然后再使用查到的IP地址连接（即“正向解析”）。事实上，将IP地址转换成域名的功能也是经常使用的，工作站会去做反向查询，找出用户是从哪个地方连线进来的（即“逆向解析”）。

早期的HOSTS文件采用集中式管理，将数据存放在一台权威的名称服务器上，由客户机进行下载。虽然这样能够保证名字与IP地址对应关系信息的唯一性，但是一旦该名称服务器发生故障，客户机将无法更新HOSTS文件，从而导致整个网络名称解析错误。

DNS对名称解析的操作进行了如下调整。

- DNS采用分散形式的数据库存储，将名称解析信息分别存储在不同的名称服务器中，形成一个分布式数据库，从而增加了名称解析的可靠性。
- DNS为层次结构，将所有名称信息组成一个名称空间（也称名字空间），并将其划分成子空间，以便提供分布式的存储。
- DNS具有备份和缓存机制，从而提高了名称解析的性能和可靠性。

3.1.2 DNS域名空间的分层结构

在域名系统中，每台计算机的域名由一系列用点分开的字母、数字段组成。完全正式域名（Full Qualified Domain Name，FQDN）在因特网的DNS域名空间中。域是其层次结构的基本单位，任何一个域最多属于一个上级域，但可以有多个下级域或没有下级域。在同一个域下不能有相同的域名或主机名，但在不同的域中可以有相同的域名或主机名。

1. 根域

在DNS域名空间中，根域（Root Domain）只有一个。它没有上级域，以圆点“.”来表示，如图3.1所示。全世界的IP地址和DNS域名空间都是由位于美国的因特网信息管理中心（Internet Network Information Center，InterNIC）负责管理或进行授权管理的。目前全世界有13台根域服务器，这些根域服务器也位于美国，并由InterNIC管理。

在根域服务器中没有保存全世界所有因特网的网址，其中只保存着顶级域的“DNS服务器-IP地址”的对应数据。

2. 顶级域

在根域之下的第一级域便是顶级域（Top-Level Domain，TLD）。它以根域为上级域，其数目有限且不能轻易变动。顶级域是由InterNIC统一管理的。在FQDN中，各级域之间都以圆点“.”分隔，顶级域位于最右边，如图3.1所示。

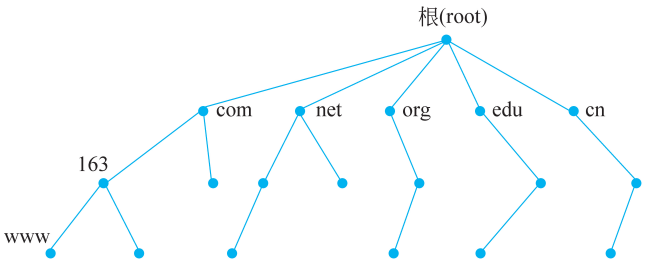

图 3.1 DNS 结构

常用的地理域和机构域有：

1）机构域

. com 商业组织	. edu 教育组织	. net 网络支持组织
. gov 政府机构	. int 国际组织	

2）地理域

. au 澳大利亚	. jp 日本	. ca 加拿大
. uk 英国	. ru 俄联邦	. kr 韩国
. it 意大利	. us 美国	. fr 法国
. ch 瑞士	. de 德国	. cn 中国
. sg 新加坡		

3. 各级子域

在 DNS 域名空间中，除了根域和顶级域之外，其他域都称为子域（Subdomain），如图 3.1 所示。

4. 反向域

为了完成反向域解析过程，需要使用另外一个概念，即反向域（in-addr.arpa）。

5. DNS 域可以包括主机和其他域（子域）

每个机构都拥有名称空间的某一部分授权，负责该部分名称空间的管理和划分，并用它来命名 DNS 域和计算机。例如，163 为 com 域的子域，其表示方法为 163.com；而 www 为 163 域中的 Web 主机，可以使用 www.163.com 表示。

3.1.3 区

区（Zone）是 DNS 名称空间的一个连续部分，它包含一组存储在 DNS 服务器上的资源记录。每个区都位于一个特殊的域节点，但区并不是域。DNS 域是名称空间的一个分区，而区一般存储在文件中的 DNS 名称空间的某一部分，可以包括多个域。一个域可以再分成几部分，每个部分或区可以由一台 DNS 服务器控制。使用区的概念，DNS 服务器可以回答关于自己区中主机的查询，以及是哪个区的授权服务器。

3.1.4 DNS 域名服务器的类型

一般情况下，DNS 服务器有如下三种类型。

（1）主服务器：每个区域中有唯一的主服务器，其中包含了授权提供服务的指定区域的数据库文件的主拷贝，此主拷贝文件包含了所有子域和主机名的资源记录。

（2）附加的辅助服务器：辅助服务器为其区域从该区域中的主 DNS 服务器上获取数据。

（3）附加的 Caching-only 服务器：与主辅助服务器不同的是，Caching-only 服务器不与任何 DNS 区域相关联，而且不包含任何活跃的数据库文件。一个 Caching-only 服务器开始时没有任何关于 DNS 域结构的信息，它必须依赖于其他 DNS 服务器得到这方面的信息。每次 Caching-only 服务器查询 DNS 服务器并得到答案时，Caching-only 服务器就将该信息存储到它的名字缓存（Name Cache）中，当另外的请求需要得到这方面的信息时，该 Caching-only 服务器就直接从高速缓存中取出答案并予以返回。一段时间之后，该 Caching-only 服务器就包含了大部分常见的请求信息。

为使 DNS 服务得到实现，必须存在一个主 DNS 服务器，而附加的辅助服务器则不是必需的。建立辅助服务器一般有下面两个好处。

（1）冗余。当主 DNS 服务器出现故障时，辅助 DNS 服务器可以完成 DNS 服务的任务。为达到最大限度的容错，主 DNS 服务器与作为备份的辅助 DNS 服务器要尽可能独立。

（2）减负。当网络较大且服务比较繁忙时，可以用辅助的 DNS 服务器来减轻对主 DNS 服务器的负担。

在下面的叙述中，除特别说明之外，DNS 服务器均指主 DNS 服务器。

3.1.5 域名解析过程

计算机在网络上进行通信时只能识别如“220.181.38.4”之类的 IP 地址，而不能识别域名。在地址栏中输入域名后，就能看到所需要的页面，这是因为 DNS 服务器自动把域名“翻译”成了相应的 IP 地址，然后调出 IP 地址所对应的网页。下面针对具体的实例讲解 DNS 的解析过程。

假设客户机使用电信 ADSL 接入 Internet，电信为其分配的 DNS 服务器地址为 202.96.128.86，那么用户访问 www.baidu.com 时，其域名解析过程如图 3.2 所示。

（1）客户机向本地域名服务器 202.96.128.86 发送解析 www.baidu.com 的请求。

（2）本地域名服务器接收到请求后，查询本地缓存。如果没有相应的 DNS 记录，本地域名服务器会将查询 www.baidu.com 的请求发送到根域名服务器。

（3）根域名服务器收到请求后，根据完全正式域名 FQDN，判断该域名属于 com 域。查询所有的 com 域 DNS 服务器的信息，并返回客户机。

（4）域名服务器 202.96.128.86 收到回应后，先保存返回的结果，再选择一台 com 域的服务器，向其提交解析域名 www.baidu.com 的请求。

（5）com 域名服务器收到请求后，判断该域名属于 baidu.com 域。通过查询本地的记录，列出管理 baidu 域的域名服务器信息，然后将查询结果返回给服务器 202.96.128.86。

（6）本地域名服务器收到回应后，先缓存返回结果，再向 baidu.com 域名服务器发出

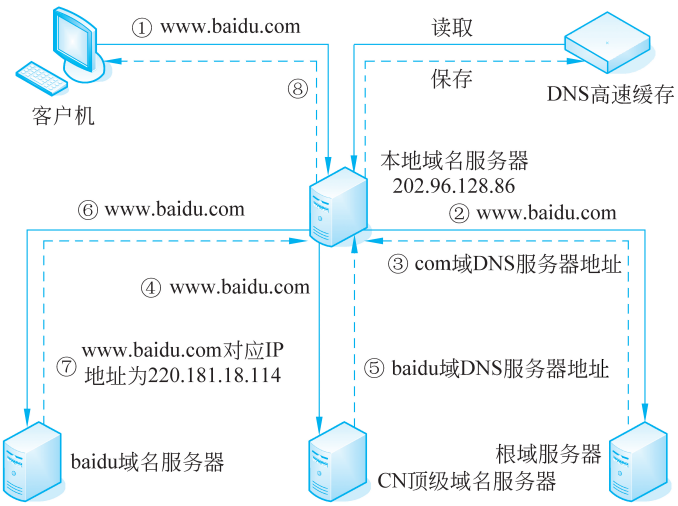

图 3.2 域名解析过程示意图

请求解析域名 www.baidu.com 的数据包。

(7) 域名服务器 baidu.com 收到请求后,查询 DNS 记录中 www 主机的信息,并将结果返回给服务器 202.96.128.86。

(8) 本地域名服务器保存查询结果到本地缓存,同时将结果返回给客户机。

3.1.6 资源记录

为了将名字解析为 IP 地址,服务器查询它们的区(又叫 DNS 数据库文件或简单数据库文件)。区中包含组成相关 DNS 域资源信息的资源记录(RR)。例如,某些资源记录把友好名字映射到 IP 地址,另一些则把 IP 地址映射到友好名字。某些资源记录不仅包括 DNS 域中服务器的信息,还可用于定义域,即指定每台服务器授权了哪些域。这些资源记录,即 SOA 和 DN 资源记录,在后面章节将会详细讲解。

1. SOA 资源记录

每个区的开始处都包含一个起始授权(Start Of Authority,SOA)记录。SOA 定义了域的全局参数,并进行整个域的管理设置。一个区域文件只允许存在唯一的 SOA 记录。

2. NS 资源记录

名称服务器(Name Server,NS)资源记录表示该区的授权服务器。它表示 SOA 资源记录中指定的该区的主服务器和辅助服务器,也表示任何授权区的服务器。每个区在区根处至少包含一个 NS 记录。

3. A 资源记录

地址(A)资源记录把 FQDN 映射到 IP 地址,因而解析器能查询 FQDN 对应的 IP 地址。

4. PTR 资源记录

相对于 A 资源记录，指针(PTR)记录把 IP 地址映射到 FQDN。

5. CNAME 资源记录

规范名字(CNAME)资源记录创建特定 FQDN 的别名。用户可以用 CNAME 记录来隐藏用户网络的实现细节，使连接的客户机无法得知这些细节。

6. MX 资源记录

邮件交换(MX)资源记录为 DNS 域名指定邮件交换服务器。邮件交换服务器是为 DNS 域名处理或转发邮件的主机。处理邮件是指把邮件投递到目的地或转交给另一个不同类型的邮件传送者。转发邮件是指把邮件发送到最终目的服务器，或使邮件经过一定时间的排队。

3.2 安装 DNS 服务

1. BIND 简介

在 Linux 中，域名服务器是由 BIND(Berkeley Internet Name Domain)软件实现的。BIND 是一个 C/S 系统，其客户端称为转换程序(resolver)，负责产生域名信息的查询，将这类信息发送给服务器端。BIND 的服务端是一个称为 named 的守护进程，负责回答转换程序的查询。

BIND 是目前最为流行的名称服务器软件，其市场占有率非常高。它主要有 3 个版本：BIND4、BIND8 和 BIND9。BIND8 已融合了许多具有稳定性、安全性的技术；而 BIND9 则增加了一些超前的理念，如支持 IPv6，公开密钥加密，支持多处理器，线程安全操作等，其基本配置与 BIND8 相同，并没有增加配置难度。

2. DNS 安装所需软件

DNS 所需要的软件包以及用途如下。

- bind-9.3.3-10.el5.i386：该包为 DNS 服务的主程序包。服务器端必须安装该软件包，后面的数字为版本号。
- bind-utils-9.3.3-10.el5.i386 ：该包为客户端工具，默认安装，用于搜索 domain name 指令。

3. DNS 的安装

Linux 的默认安装是没有安装 DNS 服务器的，可以通过以下命令检查系统是否安装了 DNS 服务器或查看已经安装了哪个版本。

```
[root@zhou~]#rpm -qa | grep bind
bind-libs-9.3.3-10.el5
bind-chroot-9.3.3-10.el5
ypbind-1.19-8.el5
bind-utils-9.3.3-10.el5
bind-9.3.3-10.el5
```

以上结果表示已安装了DNS所需的软件包。如果没有安装DNS，首先就要获得DNS服务器的安装软件。如果使用rpm包安装，则可以在Linux安装光盘中获得。

将Red Hat Enterprise Linux 5的安装盘(DVD版第一张)放入光驱，在光盘的Server目录下找到bind-9.3.3-10.el5.i386.rpm的安装包文件进行安装。安装方法同DHCP一样。

3.3 配置DNS常用服务器

安装DNS服务器后，要使其能够提供正常的服务，就必须清楚整个DNS的设定流程，以及每一步在整个流程中的作用。一个简单的DNS服务器设定流程主要分为以下3步。

① 建立主配置文件named.conf。该文件主要是设置该DNS服务器能够管理哪些区域(zone)，以及这些区域所对应的区域文件名和存放路径。

② 建立区域文件。依照named.conf文件中指定的路径建立区域文件，该文件主要记录该区域内的资源记录，如www.zsu.edu.cn对应的IP地址为202.213.202.15。

③ 重新加载配置文件或重新启动named服务，使配置生效。

为了更好地理解流程中每一步的作用，下面通过一个示例来进行讲解，如图3.3所示。

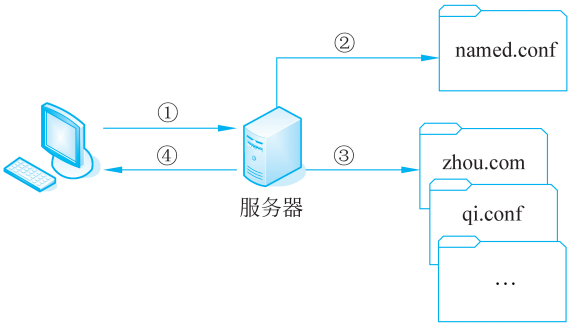

图3.3 DNS工作流程示例

(1) 客户端要获得www.zhou.com这台主机所对应的IP地址，将查询请求发送给DNS服务器。

(2) 服务器接收到请求后，查询主配置文件named.conf，看是否能够管理zhou.com区域。named.conf中记录着能够解析zhou.com区域，并提供zhou.com区域文件的所在路径及文件。

(3) 服务器根据named.conf文件中提供的路径和文件名找到zhou.com区域所对应的配置文件，并从中找到www.zhou.com主机所对应的IP地址。

(4) 将查询结果反馈给客户端，完成整个查询过程。

3.3.1 主配置文件 named.conf

安装 DNS 服务器后，要使其能够提供正常的服务，就必须对它进行配置。

named.conf 是 BIND 的核心配置文件，它包含了 BIND 的配置，但并不包括域数据。named.conf 文件定义了 DNS 服务器的工作目录所在位置，所有的区域数据文件都存放在该目录中，该文件还定义了 DNS 服务器能够管理哪些区域。如果 DNS 服务器可管理某个区域，就能够完成该区域的域名解析工作。另外，named.conf 文件还可设置是否允许客户端的查询请求等诸多功能。

下面创建 named.conf 文件。注意：如果没有安装 caching-nameserver-9.3.3-10.el5.i386.rpm 包，则需要手动建立 named.conf 文件。为了方便管理，通常把该文件建立在 /etc 目录下，如下所示。

```
[root@zhou ~]#vi /etc/named.conf
```

手动建好 named.conf 文件后，该文件是空文件，还要对其进行设置。首先对配置的框架进行介绍。

```
options
{    字段    字段值;
};
logging
{    字段    字段值;
};

view
Zone    "区域名"    {
        type    区域类型;
        file    区域文件名;
};
```

为了使 DNS 服务器定位区域文件的位置，首先需要设置 DNS 服务器工作目录。指定工作目录相当于指定 DNS 服务器根目录，后续配置文件中所出现的路径均是相对工作目录而言的，通常用于存放所有的区域文件。

设置工作目录语句的语法格式如下：

```
options
{    字段    字段值;
};
```

例如：设置 DNS 服务器的工作目录为/var/named，如下所示。

```
options
{    directory "/var/named";
};
```

directory 用于设置存储区域文件的路径，默认路径为 directory/var/named。

3.3.2 配置正向解析区域

根据前面的流程分析，在设置 DNS 的工作目录后，需要设置可管理的区域。区域信息添加完成后，DNS 服务器就能够建立与这些区域的关联。

定义区域可以使用 zone 语句，其语法格式如下。

```
zone "区域名"{
     type 区域类型;
     file "区域文件名";
};
```

说明：

(1) 区域名：是服务器要管理的区域的名称，例如 example.com。如果添加了 example.com 区域，并且该区域存在相应的资源记录，那么 DNS 服务器就可以解析该区域的 DNS 信息了。

(2) type：指定区域的类型，对于区域的管理至关重要，一共分为 6 种，分别是 Master、Slave、Stub、Forward、Hint 和 Delegation-only。就搭建一般服务而言，主要用到 master 和 hint 类型。

- master(主 DNS 服务器)：拥有区域数据文件，并对此区域提供管理数据。
- hint：根域名服务器的初始化组指定使用的线索区域 hint zone。当服务器启动时，它使用线索来查找根域名服务器，并找到最近的根域名服务器列表。如果没有指定 class IN 的线索，服务器就使用编译时默认的根服务器线索。不过，IN 的类别没有内置默认线索服务器。

(3) file：指定区域文件的名称，该文件路径为相对路径，相对于/var/name 目录而言。

下面授权一个 DNS 服务器管理 zhouqi.org 区域，并把该区域的区域文件命名为 zhouqi.org，代码如下。

1. 添加正向解析区域

使用 vi 编辑器打开 named.conf 文件。

```
[root@zhou ~]#vi /etc/named.conf
options { directory "/var/named";
};

zone "zhouqi.org" {
         type master;
```

```
        file "zhouqi.org";
};
```

其中：

- 第一个“zhouqi.org”表示服务器可以管理的区域名。
- type master 表示服务器为主 DNS 服务器。
- file“zhouqi.org”表示区域文件名称。该文件路径属于相对路径，实际路径为/var/named/zhouqi.org。

说明：配置文件中的语句必须以“;”结尾。

2. 建立正向区域文件

使用 vi 编辑器，创建正向区域文件 zhouqi.org。

```
[root@zhou ~]#vi /var/named/zhouqi.org
$TTL 86400
zhouqi.org.     IN     SOA    dns.zhouqi.org.     root.zhouqi.org (
                              20100820
                              1H
                              15M
                              1W
                              1D)

zhouqi.org.     IN     NS     dns.zhouqi.org.
dns             IN     A      192.168.1.100
aaa             IN     A      192.168.1.101
bbb             IN     A      192.168.1.102
```

3.3.3 配置反向解析区域

为了保证 zhou.com 区域服务器通信正常，必须为 zhou.com 区域设置一个反向区域，用于解析 IP 地址和域名之间的对应关系。

1. 添加反向解析区域

使用 vi 编辑器打开 named.conf 文件。

```
[root@zhou ~]#vi /etc/named.conf
```

设 zhou.com 中的服务器属于 192.168.1.0/24 网段，添加以下字段。

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192";
};
```

说明：设置反向区域时注意 zone 字段的格式，要反写 IP.in-addr.arpa。

file “1.168.192”用于配置区域文件的位置。

2. 建立反向区域文件

使用 vi 编辑器，创建反向区域文件 1.168.192，如下所示。

```
[root@zhou ~]#vi /var/named/1.168.192
$TTL 86400
@       IN    SOA    1.168.192.in-addr.arpa.      root.zhouqi.org (
                     20100820       ;serial
                     1H             ;refresh
                     15M            ;retry
                     1W             ;expire
                     1D)            ;minimun

@       IN    NS     dns.zhouqi.org.
100     IN    PTR    dns.zhouqi.org.
101     IN    PTR    aaa.zhouqi.org.
102     IN    PTR    bbb.zhouqi.org.
```

说明：

@：定义@变量的值，通常定义本区域为 zhouqi.org。

$TTL：定义资源记录在缓存中的存放时间。

3.3.4 区域文件与资源记录

DNS 服务器中存储了一个区域中包含的所有数据，保存这些数据的文件被称为区域文件，包括主机名对应的 IP 地址、刷新间隔和过期时间等。区域文件实际上是 DNS 的数据库，而资源记录就是数据库中的数据，其中包括多种记录类型，如 SOA、NA、A 记录等，这些记录统称为资源记录。如果没有资源记录，那么 DNS 服务器将无法为客户端提供域名解析服务。

一般每个区域都需要两个域文件，即正向解析区域文件和反向解析区域文件。这两种文件的结构和格式非常相似，区别是：反向解析区域文件主要建立 IP 地址映射到 DNS 域名的指针 PTR 资源记录，这点与正向区域文件恰恰相反。

如果想修改区域文件中的资源记录，可以使用 vi 命令直接编辑需要修改的区域文件。例如：

```
[root@zhou ~]#vi /etc/named.conf/zhouqi.org
```

通常，区域文件的内容需要手动制定。创建区域之后，需要向该区域添加其他的资源记录。下面介绍几个常用的重要记录的作用。

1. SOA 资源记录

SOA 资源记录为起始授权机构记录，是最重要、最常用的一种资源记录。区域以服务器授权机构的概念为基础。当 DNS 服务器配置成加载区域时，它使用 SOA 和 NS 两种资源记录来确定区域的授权属性。

SOA 资源记录总处于任何标准区域中的第一位。它表示最初创建它的 DNS 服务器或现在是该区域的主服务器的 DNS 服务器。它还用于存储影响区域更新或过期的其他属性，如版本信息和计时。这些属性会影响在该区域的域名服务器之间进行同步数据的频繁程度。

SOA 资源记录的语法格式如下：

```
区域名(当前)    记录类型    SOA    主域名服务器(FQDN)    管理员邮件地址(序列号
刷新间隔    重试间隔    过期间隔    TTL)
```

下面是 SOA 资源记录的例子。

```
zhouqi.org.    IN    SOA    dns.zhouqi.org.    root.zhouqi.org (
                            20100820    ;serial
                            10800       ;refresh
                            3600        ;retry
                            604800      ;expire
                            36000)      ;minimun
```

说明如下。

主域名服务器：区域的主 DNS 服务器 FQDN。

管理员邮件地址：管理区域负责人的电子邮件地址。在该电子邮件名称中使用英语句号“.”代替 at 符号“@”。

序列号(Serial)：该区域文件版本号。当修改数据文件里的数据时，这个版本号随之增加。每次区域改变时增加这个值非常重要，它使部分区域改动或完全修改的区域都可以在后续传输中复制到辅助 DNS 服务器上。

刷新间隔(Refresh)：以秒计算的时间。辅助 DNS 服务器请求与源服务器同步的等待时间。当刷新间隔到期时，辅助 DNS 服务器请求源服务器的 SOA 记录副本。然后，辅助 DNS 服务将源服务器的 SOA 记录的序列号与其本地 SOA 记录序列相比较。如果二者不同，则辅助 DNS 服务器从主要 DNS 服务器请求区域传输。这个域的默认时间是 900s。

重试间隔(Retry)：在辅助域名服务器刷新时无法连接到主域名服务器的情况下，辅助域名服务器等待的时间间隔，以秒为单位。

过期间隔(Expire)：以秒计算的时间，当这个时间到期时，如果辅助 DNS 服务器还无法与源服务器进行区域传输，则辅助 DNS 服务器会把它的本地数据当作不可靠数据。该默认值是 86 400s(24 小时)。

最小(Minimum，默认)：区域的默认生存时间(TTL)和缓存否定应答名称查询的最大间隔。该默认值为 3600s(1 小时)。

2. NS资源记录

NS资源记录用于指定一个区域的权威DNS服务器。在NS资源记录中列出服务器的名字，其他主机就认为它是该区域的权威服务器。这意味着，在NS资源记录中指定的任何服务器都被其他服务器当作权威的来源，并且能应答区域内所含名称的查询。

NS资源记录的语法格式如下。

```
区域名  IN  NS  完整主机名(FQDN)
```

一个NS资源记录的示例如下。

```
zhouqi.org.  IN  NS  dns.zhouqi.org
```

3. A资源记录

A资源记录是使用最为频繁的一种，通常用于将指定的主机名称解析为对应的IP地址。

A资源记录语法的格式如下。

```
完整主机名(FQDN)  IN  A IP地址
```

一个A资源记录的示例如下。

```
aaa  IN  A  192.168.1.3
```

3.4 DNS应用配置实例1

至此，本书已介绍了最常用的三种资源记录。掌握这三种资源记录的用法，可以搭建和配置一个DNS服务器，提供域名到IP地址的解析服务。

3.4.1 DNS服务器的配置与测试

下面以一个具体的配置作为实例进行讲解。

假设某单位所在的域“gztzy.org”内有三台主机，主机名分别为jwc.gztzy.org、yds.gztzy.org和cys.computer.org。其中DNS服务器的地址为192.168.1.3。三台主机的IP地址为192.168.1.4、192.168.1.5和192.168.1.6。现要求DNS服务器dns.gztzy.org可以解析三台主机名和IP地址的对应关系。

分析：根据前面的操作，首先建立主配置文件，设置可以解析的gztzy.org区域。然后建立“gztzy.org”区域文件，并在区域文件中设置SOA、NS以及A资源记录。最后配置客户端。具体步骤如下。

1. 确认或配置DNS服务器的静态IP地址

服务器的IP地址一定是静态的，使用ifconfig查看并确认。

```
[root@zhou~]#ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:A7:12:D8
          inet addr:192.168.1.3  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr:fe80::20c:29ff:fea7:12d8/64 Scope:Link
```

本例中要求DNS服务器地址为192.168.1.3，以上测试说明正好是此IP地址。

如果测试后IP地址跟本例要求不一致，就必须修改服务器的IP地址，请参考1.8.6节网卡配置文件进行操作。

配置完网卡后，必须重新禁用或启动网卡使之生效，具体操作请参考1.8.3节。

2. 建立主配置文件named.conf

使用vi命令创建named.conf。

```
[root@zhou ~]#vi /etc/named.conf
```

3. 设置named.conf文件的工作目录/var/named

添加正向gztzy.org区域和反向1.168.192区域。

```
options { directory "/var/named";
};

zone "gztzy.org" {
        type master;
        file "gztzy.org";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192";
};
```

4. 建立并配置正向区域文件gztzy.org

```
[root@zhou ~]#vi /var/named/gztzy.org
$TTL 86400
gztzy.org.      IN      SOA    dns.gztzy.org.      root.gztzy.org (
                               20100820
                               1H
                               15M
                               1W
                               1D)
```

```
gztzy.org.   IN    NS    dns.gztzy.org.
dns          IN    A     192.168.1.3
jwc          IN    A     192.168.1.4
yds          IN    A     192.168.1.5
cys          IN    A     192.168.1.6
```

说明如下。

$TTL：定义资源记录在缓存中的存放时间。

SOA：设置SOA记录，注意root表示管理员的邮件地址。应该表示为root@gztzy.org，但是这里不能使用“@”符号，因为“@”在这里表示区域，所以需要用“.”来代替，表示为“root.gztzy.org”，可以简写为“root”。

NS：设置NS资源记录。

A：设置A资源记录。

5. 建立并配置反向区域文件“1.168.192”

```
[root@zhou ~]#vi /var/named/1.168.192
$TTL 86400
@       IN    SOA    1.168.192.in-addr.arpa.      root.gztzy.org (
                     20100820
                     1H
                     15M
                     1W
                     1D)

@       IN    NS     dns.gztzy.org.
3       IN    PTR    dns.gztzy.org.
4       IN    PTR    jwc.gztzy.org.
5       IN    PTR    yds.gztzy.org.
6       IN    PRT    cys.gztzy.org.
```

说明如下。

@：表示定义@变量的值，这里是定义本区域为gztzy.org。

PTR：表示反向指针。

6. resolv.conf 文件

下面将测试DNS服务器，在Linux客户端进行，所以必须设置客户端的DNS。此例要求DNS服务器的IP地址为192.168.1.3，进行下面的修改即可。

```
[root@zhou ~]#vi /etc/resolv.conf
:generated by /sbin/dhclient-script
nameserver 192.168.1.3
```

7. 测试 DNS 服务器

在对 DNS 服务器测试之前，先重启 DNS 服务器，使修改过的配置文件生效，使用命令如下。

```
[root@zhou~]#service named restart
停止 named:                                          [确定]
启动 named:                                          [确定]
```

说明，如果启动服务器有以下提示。

```
[root@zhou~]#service named restart
Locating/var/named/chroot//etc/named.conf failed:  [失败]
```

则表示 caching-nameserver-9.3.3-10.el5.i386 包没有安装，要重新安装此包，然后再重新启动即可成功。

1）用 host 命令测试 DNS

host 是常用的测试 DNS 命令中的一个，功能相对 nslookup、dig 等命令较为简单，通常用于测试 DNS 服务器能否正常工作，如能否解析主机名与 IP 地址的对应关系等。

host 命令格式如下。

```
host   主机名
```

测试结果如下。

```
[root@zhou~]#host jwc.gztzy.org
jwc.gztzy.org has address 192.168.1.4
[root@zhou~]#host yds.gztzy.org
yds.gztzy.org has address 192.168.1.5
[root@zhou~]#host cys.gztzy.org
cys.gztzy.org has address 192.168.1.6
[root@zhou~]#host 192.168.1.4
4.1.168.192, in-addr.arpa domain name pointer jwc.gztzy.org.
[root@zhou~]#host 192.168.1.5
5.1.168.192.in-addr.arpa domain name pointer yds.gztzy.org.
[root@zhou~]#host 192.168.1.6
6.1.168.192.in-addr.arpa domain name pointer cys.gztzy.org.
[root@zhou~]#host 192.168.1.3
3.1.168.192. in-addr.arpa domain name pointer dns.gztzy.org.
```

可以看出，正向和反向都配置成功。

2）用 ping 命令测试 DNS

测试结果如下。

```
[root@zhou~]#ping dns.gztzy.org
PING dns.gztzy.org (192.168.1.3) 56(84) bytes of data.
```

```
64 bytes from dns.gztzy.org (192.168.1.3): icmp_seq=1 ttl=64 time=1.98 ms
64 bytes from dns.gztzy.org (192.168.1.3): icmp_seq=2 ttl=64 time=0.117 ms
64 bytes from dns.gztzy.org (192.168.1.3): icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from dns.gztzy.org (192.168.1.3): icmp_seq=4 ttl=64 time=0.291 ms

---- dns.gztzy.org ping statistics ----
4 packets transmitted, 4 received. 0% packet loss. time 3000 ms
rtt min/avg/max/mdev=0.091/0.620/1.982/0.790 ms
```

测试成功。

3.4.2 启动与停止 DNS 服务

下面介绍使用命令行方式和图形化方式启动、停止 DNS 服务器。

1. 使用命令行方式启动与停止 DNS 服务

启动 DNS 服务的命令为

```
[root@zhou ~]#service named start
```

停止 DNS 服务的命令为

```
[root@zhou ~]#service named stop
```

重启 DNS 服务的命令为

```
[root@zhou ~]#service named restart
```

要让 DNS 服务随系统启动而自动加载，可以执行 ntsysv 命令启动服务配置程序，找到 named 服务，按 Enter 键，即在其前面加上星号，然后单击【确定】按钮即可，如图 3.4 所示。

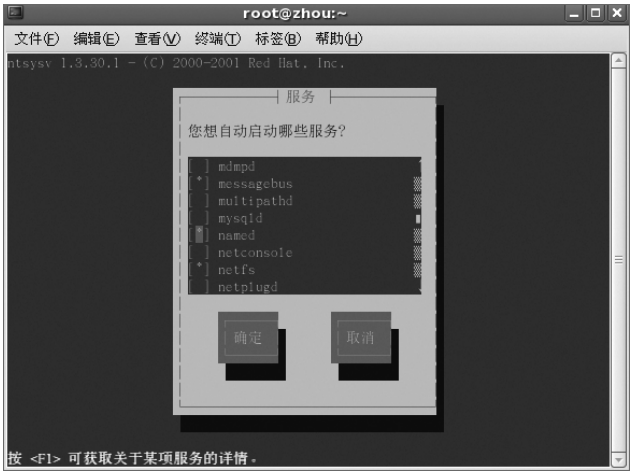

图 3.4 自动加载设置

2. 使用图形化方式启动与停止 DNS 服务

选择【系统】|【管理】|【服务器设置】|【服务】命令，弹出服务配置窗口，如图 3.5 所示。勾选【named】复选框，然后通过单击该窗口工具栏中的【开始】、【停止】或【重启】按钮操作 DNS 服务器。也可以设置系统启动时自动启动 DNS 服务器。

图 3.5 “服务配置”窗口

3.5 DNS 应用配置实例 2

1. 实例描述

假设某企业采用多个区域管理各部门的网络，产品研发部属于 development.com 域，产品销售部属于 sales.com 域，其他人员属于 free.com 域。产品研发部共有 150 人，采用的 IP 地址为 192.168.1.1～192.168.1.150。产品销售部共有 100 人，采用的 IP 地址为 192.168.2.1～192.168.2.100。其他人员共 80 人，采用的 IP 地址为 192.168.3.1～192.168.3.80。

现采用一台主机配置 DNS 服务器，其 IP 地址为 192.168.1.254。要求这台 DNS 服务器可以完成内网所有区域的正、反向解析，并且所有员工均可以访问外网地址。

2. 实训分析

本实训相对于前面讲过的 DNS 配置实例略有提高。前半部分可以依照实例 1 配置 3 个域并创建 6 个区域文件。后半部分要求所有员工均可以访问外网地址，因此还需要设置根区域，并建立根区域对应的区域文件，这样才可以访问外网地址。

（1）确认并配置 DNS 服务器 IP 地址为 192.168.1.254。

（2）建立主配置文件 named.conf。

```
[root@zhou ~]#vi /etc/named.conf
options { directory "/var/named";
};

zone"." {
        type hint;                  //设置根域
        file "named.root";          //记录全球 13 台根域名服务器的地址
};

zone "development.com" {            //设置可以解析 development.com 的区域
        type master;
        file "development.com";     //设置 development.com 区域文件
};

zone "1.168.192.in-addr.arpa" {     //设置 development.com 的反向区域
        type master;
        file "1.168.192";
};

zone "sales.com" {                  //设置可以解析 sales.com 的区域
        type master;
        file "sales.com";           //设置 sales.com 区域文件
};

zone "2.168.192.in-addr.arpa" {     //设置 sales.com 的反向区域
        type master;
        file "2.168.192";
};

zone "free.com" {                   //设置可以解析 free.com 区域
        type master;
        file "free.com";            //设置 free.com 区域文件
};

zone "3.168.192.in-addr.arpa" {     //设置 free.com 的反向区域
        type master;
        file "3.168.192";
};
```

注意 named.root 记录全球 13 台根域名服务器的地址，将该文件复制到 DNS 的工作目录(/var/named)下即可，这样它就可以正常工作了。采用这种方法不但节省时间，而且可以避免手动输入错误。

named.root 存放于/usr/share/doc/bind-9.3.3/sample/var/named/named.root 目录下。

(3) 建立 7 个区域对应的区域文件。

```
[root@zhou ~]#vi /var/named/named.root
[root@zhou ~]#vi /var/named/development.com
[root@zhou ~]#vi /var/named/sales.com
[root@zhou ~]#vi /var/named/free.com
[root@zhou ~]#vi /var/named/1.168.192
[root@zhou ~]#vi /var/named/2.168.192
[root@zhou ~]#vi /var/named/3.168.192
```

（4）分别建立7个区域文件，并添加相应的资源记录如下。

① 建立根区域文件。

```
[root@zhou ~]# cp /usr/share/doc/bind-9.3.3/sample/var/named/named.root /
var/named/
```

② 配置development.com正向解析的区域。

```
[root@zhou ~]#vi /var/named/ development.com
$TTL 86400
development.com.     IN        SOA     dns. development.com.    root (
                               20100820     ;serial
                               1H           ;refresh
                               15M          ;retry
                               1W           ;expire
                               1D)          ;minimum

development.com.     IN        NS        dns.development.com.
dns                  IN        A         192.168.1.254
depeople1            IN        A         192.168.1.1
depeople2            IN        A         192.168.1.2
…
depeople150          IN        A         192.168.1.150
```

③ 配置development.com反向解析的区域。

```
[root@zhou ~]#vi /var/named/1.168.192
$TTL 86400
@     IN    SOA   254.1.16    8.192.in-addr.arpa.   root. development.com (
                               20100820     ;serial
                               1H           ;refresh
                               15M          ;retry
                               1W           ;expire
                               1D)          ;minimum
```