项目 6 配置与管理 DNS 服务器

项目描述：

某高校组建了学校的校园网，为了使校园网中的计算机简单快捷地访问本地网络及Internet 上资源，需要在校园网中架设 DNS 服务器，用来提供域名转换成 IP 地址的功能。

在完成该项目之前，首先应当确定网络中 DNS 服务器的部署环境，明确 DNS 服务器的各种角色及其作用。

项目目标：

- 了解 DNS 服务器的作用及其在网络中的重要性
- 理解 DNS 的域名空间结构及其工作过程
- 理解并掌握缓存 DNS 服务器的配置
- 理解并掌握主 DNS 服务器的配置
- 理解并掌握辅助 DNS 服务器的配置
- 理解并掌握 DNS 客户机的配置
- 掌握 DNS 服务的测试

6.1 相关知识

DNS（Domain Name Service，域名服务）是 Internet/Intranet 中最基础也是非常重要的一项服务，它提供了网络访问中域名和 IP 地址的相互转换。

6.1.1 DNS 概述

在 TCP/IP 网络中，每台主机必须有一个唯一的 IP 地址，当某台主机要访问另外一台主机上的资源时，必须指定另一台主机的 IP 地址，通过 IP 地址找到这台主机后才能访问这台主机。但是，当网络的规模较大时，使用 IP 地址就不太方便了，所以，便出现了主机名（Host Name）与 IP 地址之间的一种对应解决方案，可以通过使用形象易记的主机名而非 IP 地址进行网络的访问，这比单纯使用 IP 地址要方便得多。其实，在这种解决方案中使用了解析的概念和原理，单独通过主机名是无法建立网络连接的，只有通过解析的过程，在主机名和 IP 地址之间建立了映射关系后，才可以通过主机名间接地通过 IP 地址建立网络连接。

主机名与 IP 地址之间的映射关系，在小型网络中多使用 hosts 文件来完成，后来，随着网络规模的增大，为了满足不同组织的要求，以实现一个可伸缩、可自定义的命名方案的需要，InterNIC 制定了一套称为域名系统（DNS）的分层名字解析方案，当 DNS 用户提出 IP 地址查

询请求时，可以由DNS服务器中的数据库提供所需的数据，完成域名和IP地址的相互转换。DNS技术目前已广泛应用于Internet中。

组成DNS系统的核心是DNS服务器，它是回答域名服务查询的计算机，它为连接Intranet和Internet的用户提供并管理DNS服务，维护DNS名字数据并处理DNS客户端主机名的查询。DNS服务器保存了包含主机名和相应IP地址的数据库。

DNS服务器分为三类：

（1）主DNS服务器（Master或Primary）。主DNS服务器负责维护所管辖域的域名服务信息。它从域管理员构造的本地磁盘文件中加载域信息，该文件（区文件）包含着该服务器具有管理权的一部分域结构的最精确信息。配置主DNS服务器需要一整套的配置文件，包括主配置文件（/etc/named.conf）、正向域的区文件、反向域的区文件、高速缓存初始化文件（/var/named/named.ca）和回送文件（/var/named/named.local）。

（2）辅助DNS服务器（Slave或Secondary）。辅助DNS服务器用于分担主DNS服务器的查询负载。区文件是从主服务器中转移出来的，并作为本地磁盘文件存储在辅助服务器中。这种转移称为“区文件转移”。在辅助DNS服务器中有一个所有域信息的完整复制，可以权威地回答对该域的查询请求。配置辅助DNS服务器不需要生成本地区文件，因为可以从主服务器下载该区文件。因而只需配置主配置文件、高速缓存文件和回送文件就可以了。

（3）唯高速缓存DNS服务器（Caching-only DNS server）。供本地网络上的客户机用来进行域名转换。它通过查询其他DNS服务器并将获得的信息存放在它的高速缓存中，为客户机查询信息提供服务。唯高速缓存DNS服务器不是权威性的服务器，因为它提供的所有信息都是间接信息。

6.1.2　DNS查询模式

按照DNS搜索区域的类型，DNS的区域分为正向搜索区域和反向搜索区域。正向搜索是DNS服务的主要功能，它根据计算机的DNS名称（域名），解析出相应的IP地址；而反向搜索是根据计算机的IP地址解析出它的DNS名称（域名）。

1．正向查询

正向查询就是根据域名，搜索出对应的IP地址。其查询方法为：当DNS客户机（也可以是DNS服务器）向首选DNS服务器发出查询请求后，如果首选DNS服务器数据库中没有与查询请求所对应的数据，则会将查询请求转发给另一台DNS服务器，依此类推，直到找到与查询请求对应的数据为止，如果最后一台DNS服务器中也没有所需的数据，则通知DNS客户机查询失败。

2．反向查询

反向查询与正向查询正好相反，它是利用IP地址查询出对应的域名。

6.1.3　DNS域名空间结构

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。例如，某台计算

机的 FQDN（Full Qualified Domain Name）为 computer.jnrp.cn，其具有的域名为 jnrp.cn；另一台计算机的 FQDN 为 www.computer.jnrp.cn，其具有的域名为 computer.jnrp.cn。域名是有层次的，域名中最重要的部分位于右边。FQDN 中最左边的部分是单台计算机的主机名或主机别名。

DNS 域名空间的分层结构如图 6-1 所示。

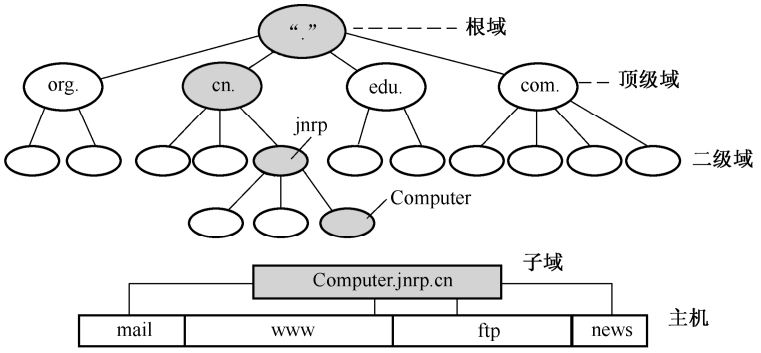

图 6-1　DNS 域名空间结构

整个 DNS 域名空间结构如同一棵倒挂的树，层次结构非常清晰。如图 6-1 所示，根域位于顶部，紧接在根域下面的是顶级域，每个顶级域又可以进一步划分为不同的二级域，二级域再划分出子域，子域下面可以是主机也可以再划分子域，直到最后的主机。在 Internet 中的域是由 InterNIC 负责管理的，域名的服务则由 DNS 来实现。

6.1.4　DNS 域名解析过程

DNS 解析过程如图 6-2 所示。

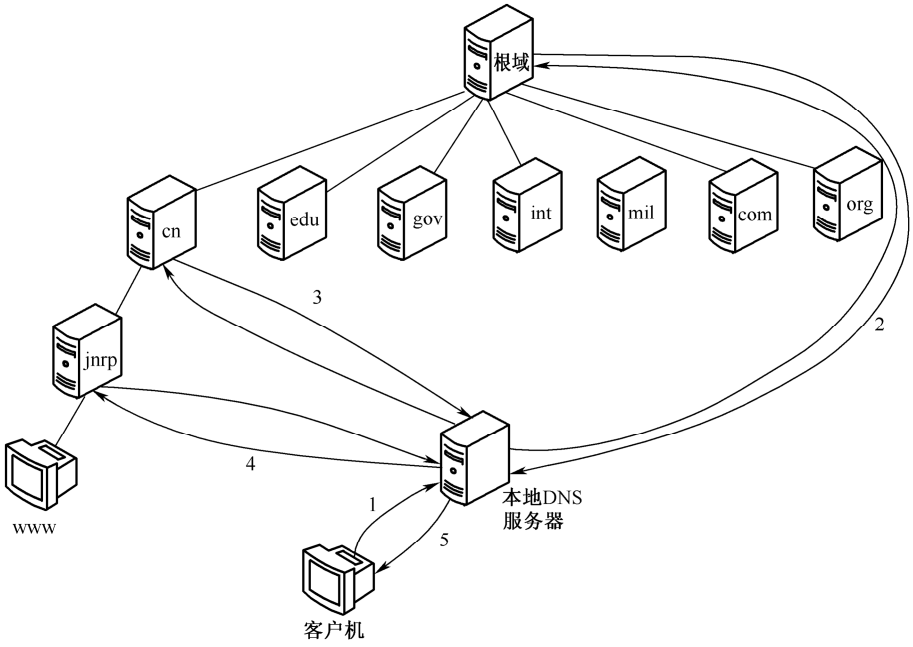

图 6-2　DNS 域名解析过程

（1）客户机提出域名解析请求，并将该请求发送给本地的域名服务器。

（2）当本地的域名服务器收到请求后，就先查询本地的缓存，如果有该记录项，则本地的域名服务器就直接把查询的结果返回。

（3）如果本地的缓存中没有该记录，则本地域名服务器就直接把请求发给根域名服务器，然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址。

（4）本地服务器再向上一步返回的域名服务器发送请求，然后接受请求的服务器查询自己的缓存，如果没有该记录，则返回相关的下级域名服务器的地址。

（5）重复步骤（4），直到找到正确的记录。

（6）本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时还将结果返回给客户机。

6.1.5　DNS 常见资源记录

从 DNS 服务器返回的查询结果可以分为两类：权威的（authoritative）和非权威的（non-authoritative）。所谓权威的查询结果，是指该查询结果是从被授权管理该区域的域名服务器的数据库中查询而来的。所谓非权威的查询结果，是指该查询结果来源于非授权的域名服务器，是该域名服务器通过查询其他域名服务器而不是本地数据库得来的。

在能够返回权威查询结果的域名服务器中存在一个本地数据库，该数据库中存储与域名解析相关的条目，这些条目称为 DNS 资源记录。

资源记录的内容通常包括 5 项，基本格式如下：

```
Domain        TTL        Class        Record Type        Record Data
```

各项的含义如表 6-1 所示。

表 6-1　资源记录条目中各项含义

项目	含义
域名（Domain）	拥有该资源记录的 DNS 域名
存活期（TTL）	该记录的有效时间长度
类别（Class）	说明网络类型，目前大部分资源记录采用“IN”，表示 Internet
记录类型（Record Type）	说明该资源记录的类型，常见资源记录类型如表 6-2 所示
记录数据（Record Data）	说明和该资源记录有关的信息，通常是解析结果，该数据格式和记录类型有关

表 6-2　DNS 资源记录类型

资源记录类型	说明
A	主机资源记录，建立域名到 IP 地址的映射
CNAME	别名资源记录，为其他资源记录指定名称的替补
SOA	起始授权机构
NS	名称服务器，指定授权的名称服务器
PTR	指针资源记录，用来实现反向查询，建立 IP 地址到域名的映射
MX	邮件交换记录，指定用来交换或者转发邮件信息的服务器
HINFO	主机信息记录，指明 CPU 与 OS

例如为了能够解析 www.jnrp.cn 这个域名对应的 IP 地址，需要在 jnrp.cn 所在的域名服务器中添加如下条目：

```
www.jnrp.cn.        IN      A       192.168.0.1
```

或者：

```
www                 IN      A       192.168.0.1
```

6.1.6 /etc/hosts 文件

hosts 文件是 Linux 系统中一个负责 IP 地址与域名快速解析的文件，以 ASCII 格式保存在 /etc 目录下，文件名为“hosts”。hosts 文件包含了 IP 地址和主机名之间的映射，还包括主机名的别名。在没有域名服务器的情况下，系统上的所有网络程序都通过查询该文件来解析对应于某个主机名的 IP 地址，否则就需要使用 DNS 服务程序来解决。通常可以将常用的域名和 IP 地址映射加入到 hosts 文件中，以实现快速方便的访问。hosts 文件的格式如下：

```
IP 地址      主机名/域名
```

【例 6-1】假设要添加域名为 www.jnrp.cn，IP 地址为 192.168.0.1；域名为 computer.jnrp.cn，IP 地址为 192.168.21.1。则可在 hosts 文件中添加如下记录。

```
www.jnrp.cn         192.168.0.1
computer.jnrp.cn    192.168.21.1
```

6.1.7 DNS 规划与域名申请

在建立 DNS 服务之前，进行 DNS 规划是非常必要的。

1．DNS 的域名空间规划

决定如何使用 DNS 命名，以及通过使用 DNS 要达到什么目的。要在 Internet 上使用自己的 DNS，公司必须先向一个授权的 DNS 域名注册颁发机构申请并注册一个二级域名，注册并获得至少一个可在 Internet 上有效使用的 IP 地址。这项业务通常可由 ISP 代理。

2．DNS 服务器的规划

确定网络中需要的 DNS 服务器的数量及其各自的作用，根据通信负载、复制和容错问题，确定在网络上放置 DNS 服务器的位置。对于大多数安装配置来说，为了实现容错，至少应该对每个 DNS 区域使用两台服务器。DNS 被设计成每个区域有两台服务器，一个是主服务器，另一个是备份或辅助服务器。在单个子网环境中的小型局域网上仅使用一台服务器时，可以配置该服务器扮演区域的主服务器和辅助服务器两种角色。

3．申请域名

同时，为了将企业网络与 Internet 很好地整合在一起，实现局域网与 Internet 的相互通信，建议向域名服务商（如万网 http://www.net.cn 和新网 http://www.xinnet.com）申请合法的域名。然后设置相应的域名解析。

提示：若要实现其他网络服务（如 Web 服务、E-mail 服务等），DNS 服务是必不可少的。

没有 DNS 服务，就无法将域名解析为 IP 地址，客户端也就无法享受相应的网络服务。若要实现服务器的 Internet 发布，就必须申请合法的 DNS 域名。

6.2　项目设计及准备

6.2.1　项目设计

为了保证校园网中的计算机能够安全可靠地通过域名访问本地网络以及 Internet 资源，需要在网络中部署主 DNS 服务器、辅助 DNS 服务器、缓存 DNS 服务器。

6.2.2　项目准备

（1）安装 Linux 企业服务器版，用作 DHCP 服务器。
（2）安装有 Windows XP 操作系统的计算机 1 台，用来部署 DNS 客户端。
（3）安装有 Linux 操作系统的计算机 1 台，用来部署 DNS 客户端。
（4）确定每台计算机的角色，并规划每台计算机的 IP 地址及计算机名。
（5）或者用 VMware 虚拟机软件部署实验环境。

DNS 服务器的 IP 地址必须是静态的。

6.3　项目实施

6.3.1　任务 1：安装 DNS 服务

Linux 下架设 DNS 服务器通常使用 BIND（Berkeley Internet Name Domain Service）程序来实现，其守护进程是 named。

1．认识 BIND

BIND 是一款实现 DNS 服务器的开放源码软件。BIND 原本是美国 DARPA 资助伯克利大学（Berkeley）开设的一个研究生课题，后来经过多年的变化发展，已经成为世界上使用最为广泛的 DNS 服务器软件，目前 Internet 上绝大多数的 DNS 服务器都是用 BIND 来架设的。

BIND 经历了第 4 版、第 8 版和最新的第 9 版，第 9 版修正了以前版本的许多错误，并提升了执行时的效能，BIND 能够运行在当前大多数的操作系统平台之上。目前 BIND 软件由因特网软件联台会（Internet Software Consortium，ISC）这个非赢利性机构负责开发和维护。

2．安装 BIND 软件包

BIND 包含以下几个软件包：

- bind：DNS 服务器软件包。
- bind-utils：DNS 测试工具，包括 dig、host 与 nslookup 等。
- bind-chroot：使 BIND 运行在指定的目录中的安全增强工具。
- caching-nameserver：高速缓存 DNS 服务器的基本配置文件，建议一定安装。

要安装 DNS 服务，可将 Red Hat Enterprise Linux 4.0 第 4 张安装盘放入光驱，加载光驱后使用命令“rpm -ivh /media/cdrom/RedHat/RPMS/bind-9.2.4-2.i386.rpm”可以安装 bind 软件包。其命令执行结果如下：

```
[root@RHEL4 RPMS]# rpm -ivh /media/cdrom/RedHat/RPMS/bind-9.2.4-2.i386.rpm
warning: /media/cdrom/RedHat/RPMS/bind-9.2.4-2.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
        package bind-9.2.4-2 is already installed
```

3．安装 chroot 软件包

chroot 是 Change Root 的缩写，它可以改变程序运行时所参考的“/”根目录位置，即将某个特定的子目录作为程序的虚拟“/”根目录。chroot 对程序运行时可以使用的系统资源、用户权限和所在目录进行严格控制，程序只在这个虚拟的根目录具有权限，一旦跳出该目录就无任何权限了。举个简单的例子，使用过 FTP 的读者都知道，用户登录到 FTP 服务器时，看到的根目录并不是服务器上真正的根目录，而是它的主目录。用户不能访问除主目录外的任何资源，用户的任何操作仅对自己的主目录有效，不会影响系统和其他用户的文件，chroot 的作用也是类似的。

对于网络管理员而言，可以使用 chroot 技术增强 DNS 服务的安全性。将 Red Hat Enterprise Linux 4.0 第 4 张安装盘放入光驱，加载光驱后使用命令“rpm -ivh /media/cdrom/RedHat/RPMS/bind-chroot-9.2.4-2.i386.rpm”可以安装 chroot 软件包。其命令执行结果如下：

```
[root@RHEL4 RPMS]# rpm -ivh /media/cdrom/RedHat/RPMS/bind-chroot-9.2.4-2.i386.rpm
warning: /media/cdrom/RedHat/RPMS/bind-chroot-9.2.4-2.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...                ########################################### [100%]
package bind-chroot-9.2.4-2 is already installed
```

使用了 chroot 后，由于 BIND 程序的虚拟目录是/var/named/chroot，所以 DNS 服务器的配置文件、区域数据文件和配置文件内的语句，都是相对这个虚拟目录而言的。如/etc/named.conf 文件的真正路径是/var/named/chroot/etc/named.conf，/var/named 目录的真正路径是/var/named/chroot/var/named。

4．配置 BIND 配置文件

建立 DNS 服务器过程中，通常用到以下 BIND 配置文件，如表 6-3 所示。

（1）/etc/named.conf。BIND 默认主配置文件是/etc/named.conf。该文件的每一行都以分号作为结束符，行注释可使用“#”或者“//”。对多行文字的注释采用/*…..*/。该文件的主要

内容如下：

表 6-3　BIND 配置文件

配置文件	说明
/etc/named.conf	BIND 的主配置文件
/var/named/named.ca	指向根域名服务器的指示文件
/var/named/localhost.zone	用于 localhost 到本地回环地址的解析
/var/named/named.local	用于本地回环地址到 localhost 的解析
/var/named/domainname.zone	用户自己建立的 DNS 区域的数据库文件

```
[root@RHEL4 ~]# cat /etc/named.conf
//定义全局配置语句
options {
//定义服务器区域配置文件的存放目录
directory "/var/named";
        };
// 以下内容声明一个控制通道，用于 rndc 实用程序控制 named 守护进程
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

//zone 用于声明一个区，以下部分定义根域的区声明
zone "." IN {
        type hint;
        file "named.ca";
};

//定义本地回环地址的正向解析区声明
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

//定义本地回环地址的反向解析区声明
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
//定义包含文件，即将/etc/rndc.key 文件包含进当前配置文件
include "/etc/rndc.key";
```

说明：

① options 配置段。该配置段属于全局性的设置，常用配置项命令及功能如下：

- directory：用于指定 named 守护进程的工作目录，各区域正反向搜索解析文件和 DNS

根服务器地址列表文件（named.ca）应放在该配置项指定的目录中。

- pid-file：指定创建用于保存 named 守护进程号的文件名及路径。守护进程号文件一般保存在/var/run 目录中，BIND 软件包安装时在/var/run 目录下创建了一个 named 目录，因此，可将进程号文件保存在该目录中，相应的配置命令为：“pid-file "/ var / run / named / named.pid";”。
- statistics-file：用于指定记录状态信息的文件的位置。若将其保存在与进程号文件相同的位置，相应的配置命令为“statistics-file "/var/ run/ named/ named.stats";”。
- allow-recursion{}：指定允许查询该 DNS 服务器的 IP 地址或网络。在{}中可指定允许查询的 IP 地址或网络地址列表，地址间用分号分隔。若不配置该项，则默认所有主机均可以查询。allow-query{}与此功能相同。另外，还可使用地址匹配符来表达允许的主机。比如，any 可匹配所有的 IP 地址，none 不匹配任何 IP 地址，localhost 匹配本地主机使用的所有 IP 地址，localnets 匹配同本地主机相连的网络中的所有主机。比如若仅允许 127.0.0.1 和 192.168.1.0/24 网段的主机查询该 DNS 服务器，则命令为：allow-recursion{127.0.0.1;192.168.1.0/24;} 或表达式为：allow-query{127.0.0.1;192.168.1.0/24;}。
- transfer-format：用于控制在发送的每个信息中包含一个资源记录，还是包含多个资源记录。若每个信息包中包含多个资源记录，则效率更高，但只有 8.1 或以上版本的 BIND 域名服务器才支持，默认为 one-answer。

  每个信息包含多个资源记录的配置命令为“transfer-format many-answers;”。

  每个信息包含一个资源记录的配置命令为“transfer-format one-answer;”。
- listen-on：设置 named 守护进程监听的 IP 地址和端口。若未指定，默认监听 DNS 服务器的所有 IP 地址的 53 号端口。当服务器安装有多块网卡，有多个 IP 地址时，可通过该配置命令指定所要监听的 IP 地址。对于只有一个地址的服务器，不必设置。若要设置 DNS 服务器监听 192.168.1.2 这个 IP 地址，端口使用标准的 5353 号，则配置命令为“listen-on 5353{192.168.1.2;};”。
- forwarders{}：用于定义 DNS 转发器。当设置了转发器后，所有非本域的和在缓存中无法找到的域名查询，可由指定的 DNS 转发器来完成解析工作并做缓存。forward 用于指定转发方式，仅在 forwarders 转发器列表不为空时有效，其用法为：“forward first | only ; ”。forward first 为默认方式，DNS 服务器会将用户的域名查询请求，先转发给 forwarders 设置的转发器，由转发器来完成域名的解析工作，若指定的转发器无法完成解析或无响应，则再由 DNS 服务器自身来完成域名的解析。若设置为“forward only;”，则 DNS 服务器仅将用户的域名查询请求，转发给转发器，若指定的转发器无法完成域名解析或无响应，DNS 服务器自身也不会试着对其进行域名解析。例如，某地区的 DNS 服务器为 61.128.192.68 和 61.128.128.68，若要将其设置为 DNS 服务器的转发器，则配置命令为：

```
options{
forwarders {61.128.192.68;61.128.128.68;};
forward first;
};
```

② controls 声明段。BIND 软件包提供了一个 rndc 工具。通过该工具，使用命令行参数可

实现本地或远程管理 named 守护进程，为了使 rndc 能够连接 named 守护进程，在 named.conf 配置文件中必须添加 controls 声明段，用于指定控制通道，以允许管理员在本地执行 rndc 命令，实现 named 进程的管理。在进行身份验证时所需的密钥信息，默认存放在/etc/rndc.key 文件中，因此在 named.conf 配置文件的末尾，使用“include "/etc/rndc.key";”语句将其包含了进来。

③ Zone 区域声明：

- 主域名服务器的正向解析区域声明格式为：

```
zone   "区域名称" IN {
       type master ;
       file   "实现正向解析的区域文件名";
       allow-update {none;};
};
```

- 从域名服务器的正向解析区域声明格式为：

```
zone   "区域名称" IN {
       type slave ;
       file   "实现正向解析的区域文件名";
       masters {主域名服务器的 IP 地址;};
};
```

反向解析区域的声明格式与正向相同，只是 file 所指定要读的文件不同，另外就是区域的名称不同。若要反向解析 x.y.z 网段的主机，则反向解析的区域名称应设置为：z.y.x.in-addr.arpa。

（2）根区域文件/var/named/named.ca。/var/named/named.ca 是一个非常重要的文件，该文件包含了 Internet 的顶级域名服务器的名字和地址。利用该文件可以让 DNS 服务器找到根 DNS 服务器，并初始化 DNS 的缓冲区。当 DNS 服务器接到客户端主机的查询请求时，如果在 Cache 中找不到相应的数据，就会通过根服务器进行逐级查询。/var/named/named.ca 文件的主要内容如下：

```
[root@RHEL4 ~]# cat /var/named/named.ca
; formerly NS.INTERNIC.NET
;
.                        3600000   IN   NS     A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000        A      198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000        NS     B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000        A      192.228.79.201
;
; formerly C.PSI.NET
;
.                        3600000        NS     C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000        A      192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                        3600000        NS     D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000        A      128.8.10.90
;
```

```
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
;
; operated by VeriSign, Inc.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
;
; operated by RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
;
; operated by ICANN
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000      A     198.32.64.12
;
; operated by WIDE
;
.                       3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000      A     202.12.27.33
; End of File
```

说明：

- 以“;”开始的行都是注释行。

- 其他每两行都和某个域名服务器有关，分别是NS和A资源记录。
- 行“. 3600000 IN NS A.ROOT-SERVERS.NET.”的含义是：“.”表示根域；3600000是存活期；IN是资源记录的网络类型，表示Internet类型；NS是资源记录类型；“A.ROOT-SERVERS.NET.”是主机域名。
- 行“A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4”的含义是：“A.ROOT-SERVERS.NET.”是主机名；3600000是存活期；A是资源记录类型；最后对应的是IP地址。
- 其他各行的含义与上面两项基本相同。

由于named.ca文件经常会随着根服务器的变化而发生变化，所以建议最好从国际互联网络信息中心（InterNIC）的FTP服务器下载最新的版本，下载地址为：ftp://ftp.internic.net/domain/。文件名为named.root。

（3）/var/named/localhost.zone。该文件是主机名localhost到本地回环地址127.0.0.1的正向解析文件。该文件不需要修改，可以直接使用。文件内容如下：

```
[root@RHEL4 ~]# cat /var/named/localhost.zone
$TTL    86400
@               IN SOA  @       root  (
                                        42              ; serial  (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                IN NS           @
                IN A            127.0.0.1
```

（4）/var/named/named.local。该文件是本地回环地址127.0.0.1到主机名localhost的反向解析文件。文件内容如下：

```
[root@RHEL4 ~]# cat /var/named/named.local
$TTL    86400
@       IN      SOA     localhost. root.localhost.  (
                                        1997022700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
        IN      NS      localhost.
1       IN      PTR     localhost.
[root@RHEL4 ~]#
```

6.3.2 任务2：配置DNS服务器

本节将结合具体实例介绍缓存DNS、主DNS、辅助DNS等各种DNS服务器的配置。

1．缓存DNS服务器的配置

Red Hat Linux默认的DNS配置文件提供了缓存DNS服务器的配置。缓存DNS服务器上

只运行域名服务软件，没有域名数据库文件。当客户机试图从该服务器解析域名时，缓存 DNS 服务器从其他某个域名服务器上查询得到结果，并将结果存放在高速缓存中。在一定时间内有客户机查询相同的域名时，缓存 DNS 服务器直接利用缓存中的数据响应客户端的解析请求。

系统只要安装了 caching-nameserver 软件包，并启动 DNS 服务就已经成功配置了高速缓存 DNS 服务器。启动 named 软件包的方法如下：

```
[root@RHEL4 RPMS]# service named start
//或者按以下方法也可以启动 named 进程
[root@RHEL4 RPMS]#/etc/rc.d/init.d/named start
//可以利用以下命令查看 named 进程的监听端口
[root@RHEL4 RPMS]#/netstat –ln | grep named
```

在设置缓存 DNS 服务器时，通常设置域名转发器。方法为在/etc/named.conf 主配置文件的 options 中使用 forwarders 语句即可。

2．配置主 DNS 服务器

下面以建立一个主区域 jnrp. cn 为例，讲解 DNS 主服务器的配置。

【例 6-2】某校园网要架设一台 DNS 服务器负责 jnrp.cn 域的域名解析工作。DNS 服务器的 FQDN 为 dns.jnrp.cn，IP 地址为 192.168.1.2。要求为以下域名实现正反向域名解析服务：

```
dns.jnrp.cn                          192.168.1.2
mail.jnrp.cn      MX 记录            192.168.0.3
slave.jnrp.cn                        192.168.0.4
forward.jnrp.cn        ←→            192.168.0.6
www.jnrp.cn                          192.168.0.5
computer.jnrp.cn                     192.168.22.98
ftp.jnrp.cn                          192.168.0.11
stu.jnrp.cn                          192.168.21.22
```

另外为 www.jnrp.cn 设置别名为 web.jnrp.cn。

```
//1．编辑 DNS 服务器的主配置文件，添加如下区域声明
[root@RHEL4 ~]#vi /etc/named.conf
zone "jnrp.cn" IN {
        type master;
        file "jnrp.cn.zone";
};
zone "168.192.in-addr.arpa" IN {
        type master;
        file "192.168.zone";
};

//2．在/var/named/chroot/var/named 目录下，创建 jnrp.cn.zone 正向区域文件
[root@RHEL4 ~]# vi /var/named/chroot/var/named/jnrp.cn.zone
$TTL    86400
@               IN SOA   dns.jnrp.cn. mail.jnrp.cn.(
                                        2007100101      ; serial
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D              ; minimum
```

```
)

@                IN NS              dns.jnrp.cn.
@                IN MX      10      mail.jnrp.cn.

dns              IN A               192.168.1.2
mail             IN A               192.168.0.3
slave            IN A               192.168.0.4
www              IN A               192.168.0.5
forward          IN A               192.168.0.6
computer         IN A               192.168.22.98
ftp              IN A               192.168.0.11
stu              IN A               192.168.21.22
web              IN CNAME           www.jnrp.cn.

//3. 在/var/named/chroot/var/named 目录下，创建 192.168.zone 反向区域文件
[root@RHEL4 ~]# vi    /var/named/chroot/var/named/192.168.zone
$TTL      86400
@                IN SOA    dns.jnrp.cn. mail.jnrp.cn. (
                                    2007100101          ; serial

                                          3H                ; refresh
                                          15M               ; retry
                                          1W                ; expiry
                                          1D                 ; minimum
)

@                IN NS              dns.jnrp.cn.
@                IN MX      10      mail.jnrp.cn.

2.1              IN PTR             dns.jnrp.cn.
3.0              IN PTR             mail.jnrp.cn.
4.0              IN PTR             slave.jnrp.cn.
5.0              IN PTR             www.jnrp.cn.
6.0              IN PTR             forward.jnrp.cn.
98.22            IN PTR             computer.jnrp.cn.
11.0             IN PTR             ftp.jnrp.cn.
22.21            IN PTR             stu.jnrp.cn.

//4. 重新启动 DNS 服务
[root@RHEL4 ~]# service named restart
或者
[root@RHEL4 ~]# service named reload
```

说明：

（1）正反向区域文件的名称一定要与/etc/named.conf 文件中 zone 区域声明中指定的文件名一致。

（2）正反向区域文件的所有记录行都要顶头写，前面不要留有空格。否则会导致 DNS

服务不能正常工作。

（3）第一个有效行为 SOA 资源记录。该记录的格式如下：

```
@                IN SOA   origin. Contact.（
                                    2007100101        ; serial （d. adams）
                                    3H                ; refresh
                                    15M               ; retry
                                    1W                ; expiry
                                    1D                ; TTL
）
```

- @是该域的替代符，例如 jnrp.cn.zone 文件中的@代表 jnrp.cn。
- IN 表示网络类型。
- SOA 表示资源记录类型。
- origin 表示该域的主域名服务器的 FQDN，用“.”结尾表示这是个绝对名称。例如 jnrp.cn.zone 文件中的 origin 为 dns.jnrp.cn.。
- contact 表示该域的管理员的电子邮件地址。它是正常 Email 地址的变通，将@变为“.”。例如 jnrp.cn.zone 文件中的 contact 为 mail.jnrp.cn.。
- serial 为该文件的版本号，该数据是辅助域名服务器和主域名服务器进行时间同步的，每次修改数据库文件后，都应更新该序列号。习惯上用“yyyymmddnn”，即年月日后加两位数字，表示一日之中第几次修改。
- refresh 为更新时间间隔。辅助 DNS 服务器根据此时间间隔周期性地检查主 DNS 服务器的序列号是否改变，如果改变则更新自己的数据库文件。
- retry 为重试时间间隔。当辅助 DNS 服务器没有能够从主 DNS 服务器更新数据库文件时，在定义的重试时间间隔后重新尝试。
- expiry 为过期时间。如果辅助 DNS 服务器在所定义的时间间隔内没有能够与主 DNS 服务器或另一台 DNS 服务器取得联系，则该辅助 DNS 服务器上的数据库文件被认为无效，不再响应查询请求。
- TTL 为最小时间间隔。对于没有特别指定存活周期的资源记录，默认取 TTL 的值为 1 天。

①行“@ IN NS dns.jnrp.cn.”说明该域的域名服务器，至少应该定义一个。

②行“@ IN MX 10 mail.jnrp.cn.”用于定义邮件交换器，其中 10 表示优先级别，数字越小，优先级别越高。

③类似于行“www IN A 192.168.0.5”是一系列的主机资源记录，表示主机名和 IP 地址的对应关系。

④行“web IN CNAME www.jnrp.cn.”定义的是别名资源记录，表示 web.jnrp.cn.是 www.jnrp.cn.的别名。

⑤类似于行“98.22 IN PTR computer.jnrp.cn.”是指针资源记录，表示 IP 地址与主机名称的对应关系。其中 PTR 使用相对域名，如“98.22”，表示“98.22.168.192.in-addr.arpa”，它表示 IP 地址为 192.168.22.98。

3．配置辅助 DNS 服务器

配置辅助域名服务器相对简单，只需在要配置辅助域名服务器的计算机上对

/etc/named.conf 主配置文件进行修改，无需配置区数据库文件，区数据库文件将从主域名服务器上自动获得。

需要注意的是，不能在同一台计算机上同时配置同一个域的主域名服务器和辅助域名服务器。

【例 6-3】为例 6-2 的 DNS 服务器配置 jnrp.cn 域及其反向区域的辅助域名服务器。辅助域名服务器的 FQDN 为 slave.jnrp.cn，IP 地址为 192.168.0.4。

```
//1．在 192.168.0.4 上编辑 DNS 服务器的主配置文件，添加如下区域声明
[root@RHEL4 ~]#vi /etc/named.conf
zone "jnrp.cn" IN {
        type slave;
        file "jnrp.cn.zone";
        masters { 192.168.1.2; };
};
zone "168.192.in-addr.arpa" IN {
        type slave;
        file "192.168.zone";
masters { 192.168.1.2; };
};
//2．在 192.168.1.2 的主 DNS 服务器上编辑主配置文件，在 options 中添加如下语句
[root@RHEL4 ~]#vi /etc/named.conf

    allow-transfer {   192.168.0.4;   };
//3. 重新启动 DNS 服务
[root@RHEL4 ~]# service named restart
或者
[root@RHEL4 ~]# service named reload
```

说明：只有在主域名服务器允许当前可以进行区域传输的情况下，辅助域名服务器才能进行区域复制操作。例如上例中，只有在 192.168.1.2 主域名服务器的 options 声明中添加“allow-transfer { 192.168.0.4; };”语句，辅助域名服务器才能够从主域名服务器进行区域复制。

4．使用直接域名解析

许多用户有直接使用域名访问 Web 网站的习惯，即在浏览器中不输入主机名 www，而直接使用如 http://baidu.com 或 http://google.com 来访问，如图 6-3 所示。

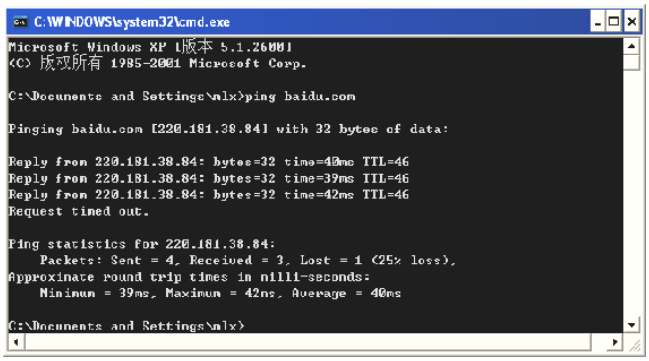

图 6-3　直接域名解析

然而，并不是所有的 Web 网站都支持这种访问方式，只有 DNS 服务器能直接解析域名的网站才可以。DNS 服务器默认只能解析完全规范域名（FQDN），不能直接将域名解析成 IP 地址。为了方便用户访问，可以在 DNS 服务器的区域文件加入下面一条特殊的主机资源记录，以便实现直接域名解析功能。

```
jnrp.cn.      IN      A      192.168.0.5
```

或者

```
.             IN      A      192.168.0.5
```

设置好后，用户只要访问 jnrp.cn，DNS 服务器就会将其直接解析成 IP 地址 192.168.0.5。

5．使用泛域名解析

泛域名是指一个域名下的所有主机和子域名都被解析到同一个 IP 地址上，如使用“ping rhel4.china.com”和“ping linden.china.com”命令，DNS 服务器的解析结果是一样的。即域名 rhel4.china.com 和 linden.china.com 域名对应的 IP 地址是相同的，如图 6-4 所示。

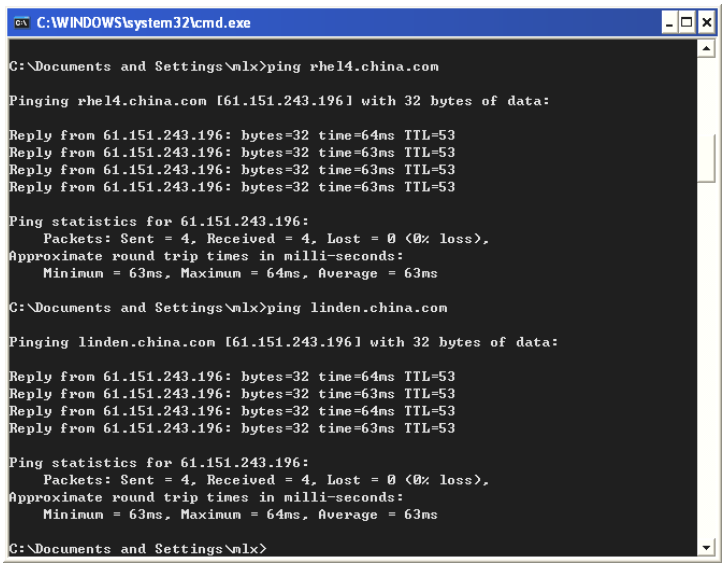

图 6-4　泛域名解析

可以在 DNS 服务器的区域文件的末尾加入下面一条特殊的主机资源记录，以实现泛域名解析功能。

```
*.jnrp.cn.    IN      A      192.168.0.5
```

或者

```
*             IN      A      192.168.0.5
```

6.3.3　任务 3：配置 DNS 客户端

DNS 客户端的配置非常简单，假设本地首选 DNS 服务器的 IP 地址为 192.168.1.2，备用 DNS 服务器的 IP 地址为 192.168.0.9，DNS 客户端的设置如下所示：

- Windows 客户端：打开“Internet 协议（TCP/IP）”属性对话框，在如图 6-5 所示的对话框中输入首选和备用 DNS 服务器的 IP 地址即可。

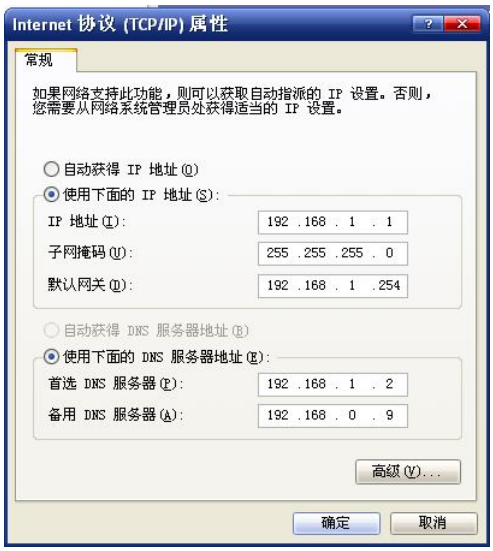

图 6-5　Windows 系统中 DNS 客户端配置

- Linux 客户端：在 Linux 系统中可以通过修改/etc/resolv.conf 文件来设置 DNS 客户端。如下所示：

```
[root@RHEL4 RPMS]# vi /etc/resolv.conf
    nameserver 192.168.1.2
    nameserver 192.168.0.9
    search   jnrp.cn
```

其中 nameserver 指明域名服务器的 IP 地址，可以设置多个 DNS 服务器，查询时按照文件中指定的顺序进行域名解析，只有当第一个 DNS 服务器没有响应时才向下面的 DNS 服务器发出域名解析请求。search 用于指明域名搜索顺序，当查询没有域名后缀的主机名时，将会自动附加由 search 指定的域名。

在 Linux 系统的图形界面下也可以利用网络配置工具（可以利用 system-config-network 命令打开）进行设置。

6.3.4　任务 4：测试 DNS

BIND 软件包提供了三个 DNS 测试工具：nslookup、dig 和 host。其中 dig 和 host 是命令行工具，而 nslookup 既可以使用命令行模式也可以使用交互模式。

1．nslookup 命令

下面举例说明 nslookup 命令的使用方法。

```
//运行 nslookup 命令
[root@RHEL4 ~]# nslookup
//正向查询，查询域名 www.jnrp.cn 所对应的 IP 地址
> www.jnrp.cn
Server:          192.168.1.2
Address:         192.168.1.2#53
```

```
Name:     www.jnrp.cn
Address: 192.168.0.5
//反向查询，查询 IP 地址 192.168.1.2 所对应的域名
> 192.168.1.2
Server:              192.168.1.2
Address:             192.168.1.2#53

2.1.168.192.in-addr.arpa          name = dns.jnrp.cn.
//显示当前设置的所有值
> set all
Default server: 192.168.1.2
Address: 192.168.1.2#53
Default server: 192.168.0.1
Address: 192.168.0.1#53
Default server: 192.168.0.5
Address: 192.168.0.5#53

Set options:
  novc                  nodebug             nod2
  search                recurse
  timeout = 0           retry = 2           port = 53
  querytype = A         class = IN
  srchlist =
//查询 jnrp.cn 域的 NS 资源记录配置
> set type=NS     //此行中 type 的取值还可以为 SOA、MX、CNAME、A、PTR 以及 any 等
> jnrp.cn
Server:              192.168.1.2
Address:             192.168.1.2#53
jnrp.cn nameserver = dns.jnrp.cn.
```

2．dig 命令

dig（domain information groper）是一个灵活的命令行方式的域名查询工具，常用于从域名服务器获取特定的信息。例如，通过 dig 命令查看域名 www.jnrp.cn 的信息。

```
[root@RHEL4 ~]# dig www.jnrp.cn

; <<>> DiG 9.2.4 <<>> www.jnrp.cn
;; global options:   printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59656
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;www.jnrp.cn.                    IN      A

;; ANSWER SECTION:
www.jnrp.cn.            86400   IN      A       192.168.0.5
```

```
;; AUTHORITY SECTION:
jnrp.cn.                86400   IN      NS      dns.jnrp.cn.

;; ADDITIONAL SECTION:
dns.jnrp.cn.            86400   IN      A       192.168.1.2

;; Query time: 38 msec
;; SERVER: 192.168.1.2#53（192.168.1.2）
;; WHEN: Sat Sep 29 20:22:48 2007
;; MSG SIZE  rcvd: 79
[root@RHEL4 ~]#
```

3．host 命令

host 命令用来做简单的主机名的信息查询，在缺省情况下，host 只在主机名和 IP 地址之间进行转换。下面是一些常见的 host 命令的使用方法。

```
//正向查询主机地址
[root@RHEL4 ~]# host dns.jnrp.cn
//反向查询 IP 地址对应的域名
[root@RHEL4 ~]# host 192.168.22.98
//查询不同类型的资源记录配置，-t 参数后可以为 SOA、MX、CNAME、A、PTR
[root@RHEL4 ~]# host -t NS jnrp.cn
//列出整个 jnrp.cn 域的信息
[root@RHEL4 ~]# host -l jnrp.cn 192.168.1.2
//列出与指定的主机资源记录相关的详细信息
[root@RHEL4 ~]# host -a computer.jnrp.cn
```

4．检查 DNS 服务器配置中的常见错误

- 配置文件名写错。在这种情况下，运行 nslookup 命令不会出现命令提示符“>”。
- 主机域名后面没有小点“.”。这是最常犯的错误。
- /etc/resolv.conf 文件中的域名服务器的 IP 地址不正确。在这种情况下，nslookup 命令不出现命令提示符。
- 回送地址的数据库文件有问题。同样 nslookup 命令不出现命令提示符。
- 在 /etc/named.conf 文件中的 zone 区域声明中定义的文件名与 /var/named/chroot/var/named 目录下的区域数据库文件名不一致。

6.4　练习题

1．在 Linux 环境下，能实现域名解析的功能软件模块是（　）。

A．apache　　B．dhcpd　　C．BIND　　D．SQUID

2．www.jnrp.edu.cn 是 Internet 中主机的（　）。

A．用户名　　B．密码　　C．别名　　D．IP 地址

E．FQDN

3．在 DNS 服务器配置文件中 A 类资源记录是什么意思？（　）

A．官方信息　　B．IP 地址到名字的映射

C．名字到 IP 地址的映射　　D．一个 name server 的规范

4．在 Linux DNS 系统中，根服务器提示文件是（　）。

A．/etc/named.ca　　B．/var/named/named.ca

C．/var/named/named.local　　D．/etc/named.local

5．DNS 指针记录的标志是（　）。

A．A　　B．PTR　　C．CNAME　　D．NS

6．DNS 服务使用的端口是（　）。

A．TCP 53　　B．UDP 53　　C．TCP 54　　D．UDP 54

7．以下哪个命令可以测试 DNS 服务器的工作情况。（　）

A．ig　　B．host

C．nslookup　　D．named-checkzone

8．下列哪个命令可以启动 DNS 服务？（　）

A．service named start　　B．/etc/init.d/named start

C．service dns start　　D．/etc/init.d/dns　start

9．指定域名服务器位置的文件是（　）。

A．/etc/hosts　　B．/etc/networks

C．/etc/resolv.conf　　D．/.profile

10．主域名服务器在 DNS 配置文件/etc/named.conf 中由 zone 语句中的“type master;”来定义。这种说法（　）。

A．正确　　B．错误

6.5　实训 配置与管理 DNS 服务器

一、实训目的

掌握 Linux 下主 DNS、缓存 DNS 服务器和辅助 DNS 服务器的配置与调试方法。

二、实训环境

在 VMware 虚拟机中启动 3 台 Linux 服务器，IP 地址分别为 192.168.203.1、192.168.203.2 和 192.168.203.3。并且要求此 3 台服务器已安装了 DNS 服务所对应的软件包。

三、实训内容

（1）配置主域名服务器：在 IP 地址为 192.168.203.1 的服务器上，配置主域名服务器来负责区域“mlx.com”的解析工作，同时负责对应的反向查找区域。

- 在/etc/named.conf 主配置文件中添加如下内容：

```
zone "mlx.com" {
type master;
file "mlx.com.zone";
};
zone "203.168.192.in-addr.arpa" {
type master;
```

```
file "192.168.203.zone";
};
```

- 在/var/named/chroot/var/named 目录下创建区域文件“mlx.com.zone”，内容如下：

```
$TTL 1D
@   IN   SOA   www.mlx.com.   mail.mlx.com.  (
                    2007101100
                    3H
                    15M
                    1W
                    1D
                   )
@     IN     NS    www.mlx.com.
@     IN    MX    10    www.mlx.com.

www          IN       A        192.168.203.1
mail          IN       A      192.168.203.1
forward     IN       A      192.168.203.2
slave         IN       A      192.168.203.3
ftp           IN    A      192.168.203.101
www1       IN    CNAME    www.mlx.com.
www2       IN    CNAME    www.mlx.com.
www3       IN    CNAME    www.mlx.com.
```

- 在/var/named/chroot/var/named 目录下创建区域文件 192.168.203.zone，内容如下：

```
$TTL 1D
@   IN   SOA   www.mlx.com.   mail.mlx.com.  (
2007101100
                              3H
                              15M
                              1W
                              1D
)
@     IN     NS    www.mlx.com.
@     IN     MX    10    www.mlx.com.
1       IN     PTR     www.mlx.com.
1       IN     PTR     mail.mlx.com.
2       IN     PTR     forward.mlx.com.
3       IN     PTR     slave.mlx.com.
101    IN     PTR     ftp.mlx.com.
```

- 重新启动域名服务器。
- 测试域名服务器，并记录观测到的数据。

（2）配置缓存域名服务器：在 IP 地址为 192.168.203.2 的 Linux 系统上配置缓存域名服务器。

- 在/etc/named.conf 中的“option”区域添加类似下面的内容：

  forwarders {192.168.0.9; };

  forward only
- 启动 named 服务。

- 测试配置。

（3）配置辅助域名服务器：在 IP 地址为 192.168.203.3 的 Linux 系统上配置 mlx.com 区域和 203.168.192.in-addr.arpa 区域的辅助域名服务器。

- 在/etc/named.conf 文件中添加如下行：

```
zone “mlx.com” IN {
type slave;
masters { 192.168.203.1; };
file “slave-mlx.com.zone”;
 };

zone “203.168.192.in-addr.arpa” IN {
type slave;
masters { 192.168.203.1; };
file “slave-192.168.203.zone”;
};
```

- 重新启动 named 服务。
- 检查在/var/named/chroot/var/named 目录下是否自动生成了 slave-mlx.com.zone 和 slave-192.168.203.zone 文件。

四、实训报告

按要求完成实训报告。