# BIND9 VIEW 功能实现 DNS 智能解析

**编辑：LinuxPad　　日期：2011/10/3**

本人系 LINUX 爱好者，关注开源、网络安全、自动化运维
BLOG:linuxpad.blog.chinaunix.net　　E-Mail:linuxpad.cn@gmail.com
QQ 交流群：161230409　　欢迎加群交流　共同探讨 LINUX 技术

DNS 智能解析简单的来说就是根据 DNS 服务器根据客户端请求 IP 的不同来给客户端返回不同的服务器地址，比如说电信用户访问 www.linuxpad.cn 的时候 DNS 服务器会返回给用户电信服务器，网通用户访问 www.linuxpad.cn 的时候 DNS 服务器会返回给用户网通服务器，这样就解决了南北用户访问过慢或电信用户访问网通服务器过慢的问题，国内著名的 DNSpod 实现的也是这样的一个功能，而 BIND9 自带的 VIEW 视图功能就可以完全实现这个功能。VIEW 视图可以说是 BIND9 一个最强大的功能之一，他可以完全按照你要求来实现 DNS 服务器对不同 IP、不同网段的智能解析工作。本文以 centos5.6 i386 系统及系统自带的 BIND9 和 Webmin 为例讲述 BIND9 的安装以及 VIEW 视图的配置功能。Webmin 是一个图形化的服务器管理工具，由于 DNS 配置文件比较复杂，所以建议采用这款图形化配置工作来进行 DNS 配置。

阅读本文你需要了解一些 DNS 基础，如知道为什么会有 DNS，什么是 A 记录、CNAME 记录、DNS 的正向解析/逆向解析，本文不会涉及这些基础知识。

本文采用 VMware 虚拟机来模拟 DNS 服务器，虚拟机须配置双网卡来模拟 DNS 对两个不同的网段做出不同的解析，其中一块网卡配置为 Bridged 模式，直接连接到局域网内网(192.168.0.0/24)上，另一块网卡配置为 host-only，仅与本机进行通信(192.168.136.0/24)。

IP 配置如下：

本地：物理网卡（本地连接）192.168.0.100/24，DNS 为 192.168.0.101

虚拟网卡（VMware Network Adapter VMnet1）192.168.136.1/24，

DNS 为 192.168.136.128

虚拟机：eth0(Bridged) 192.168.0.101/24

eth1(host-only)192.168.136.128/24

DNS 配置：以 www.linuxpad.cn 为例，如果客户端为 192.168.0.0/24 段，则将

www.linuxpad.cn 解析到 192.168.0.200；如果客户端为 192.168.136.0/24 段，则将 www.linuxpad.cn 解析到 192.168.136.200。

测试方案：先禁用本地连接，使用 nslookup 工具查看 www.linuxpad.cn，返回 192.168.136.128 则正确；再禁用虚拟网卡，使用 nslookup 工具查看 www.linuxpad.cn，返回 192.168.0.101 则正确。

# 1. 安装 bind

我们需要安装以下 rpm 包：

bind　　DNS 服务器主程序

bind-libs　程序库

bind-utils 客户端命令工具

bind-chroot chroot 运行模式

bind 的 chroot 功能是一个很有用的安全设置，使 bind 可以在一个 chroot 的模式下运行. 也就是说,bind 运行时的/(根)目录,并不是系统真正的/(根)目录,只是系统中的一个子目录而已.这样做的目的是为了提高安全性.因为在 chroot 的模式下,bind 可以访问的范围仅限于这个子目录的范围里,无法进一步提升,进入到系统的其他目录中。

使用 yum install 命令来安装，

```
[root@localhost soft]# yum install bind
[root@localhost soft]# yum install bind-libs
[root@localhost soft]# yum install bind-utils
[root@localhost soft]# yum install bind-chroot
```

使用以下命令查看 rpm 包是否正确安装

```
[root@localhost soft]# rpm -qa | grep bind
ypbind-1.19-12.el5
kdebindings-3.5.4-6.el5
bind-chroot-9.3.6-16.P1.el5
bind-utils-9.3.6-16.P1.el5
bind-9.3.6-16.P1.el5
```

bind-libs-9.3.6-16.P1.el5

如果安装正确，你会看到我们所安装的 rpm 包。

设置 DNS 服务开机自启动

[root@localhost soft]# chkconfig named on

启动命令为：

[root@localhost soft]# service ntamed start

## 2. 安装 webmin

webmin 是一个可视化的 linux 服务器管理工具，可以帮助我们实现很多功能，从官方网站 http://www.webmin.com/下载 webmin 的最新 rpm 包，目前最新的为 1.560，下载后安装

[root@localhost soft]# rpm -ivh webmin-1.560-1.noarch.rpm

warning: webmin-1.560-1.noarch.rpm: Header V3 DSA signature: NOKEY, key ID 11f63c51

Preparing... ########################################### [100%]

Operating system is CentOS Linux

1:webmin ########################################### [100%]

Webmin install complete. You can now login to http://localhost.localdomain:10000/

as root with your root password.

安装完成之后，默认的访问端口是 10000，默认用户名位 root，密码为系统 root 密码。访问时请确认系统防火墙已经开放 10000 端口。启动命令为

[root@localhost soft]# service webmin start

访问界面如下图 1/图 2：


图 1

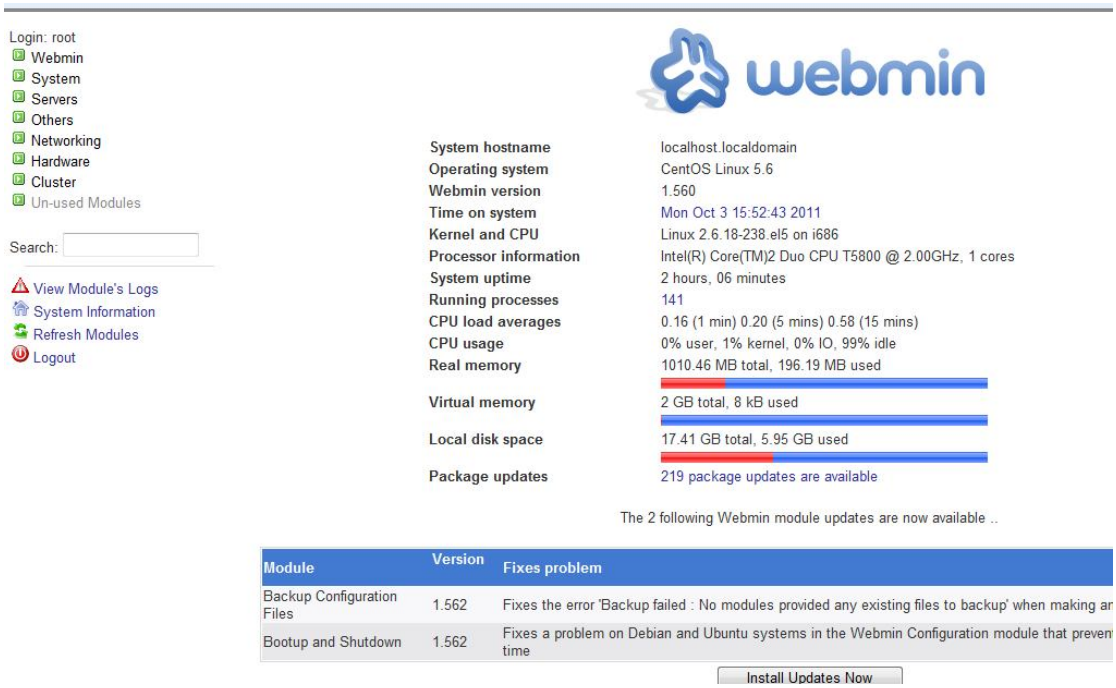


图 2

更改界面语言，选择 WebMin 下的 Change Language and Theme，在语言栏选择”Simplified Chinese(ZH_CN.UTF-8)”。

# 3. 配置 DNS

### a. 启动 DNS 服务器

打开 Webmin 界面，选择 Servers 下的 BIND DNS Server，点击创建配置文件并启动 dns 服务器，这里只是内网测试，所以只选择第一个即可，如果你的 DNS 用与外网解析，请选择第二个，如图 3。


图 3

启动成功后会自动跳转至 DNS 配置页面，如图 4。


图 4

图中标出的即是我们需要使用的功能。

创建新的主区域：创建一个新的 DNS 配置文件，有正向和逆向之分，稍后介绍；

创建新的视图：这就是我们实现 DNS 智能解析的视图功能。

**b．创建视图**

由于我们需要对两个不同的 IP 段来实现分别解析，因此我们这里需要创建两个不同的视图。需要注意的是，一旦创建了视图，所有的域名记录（创建的主区域）都必须属于某个视图，不允许没有视图的主区域存在。创建过程如图 5/图 6

这里创建两个视图分别为：

名称：view_192.168.0.0　对 192.168.0.0/24 的客户端请求进行解析

名称：view_192.168.136.0 对 192.168.136.0/24 的客户端请求进行解析

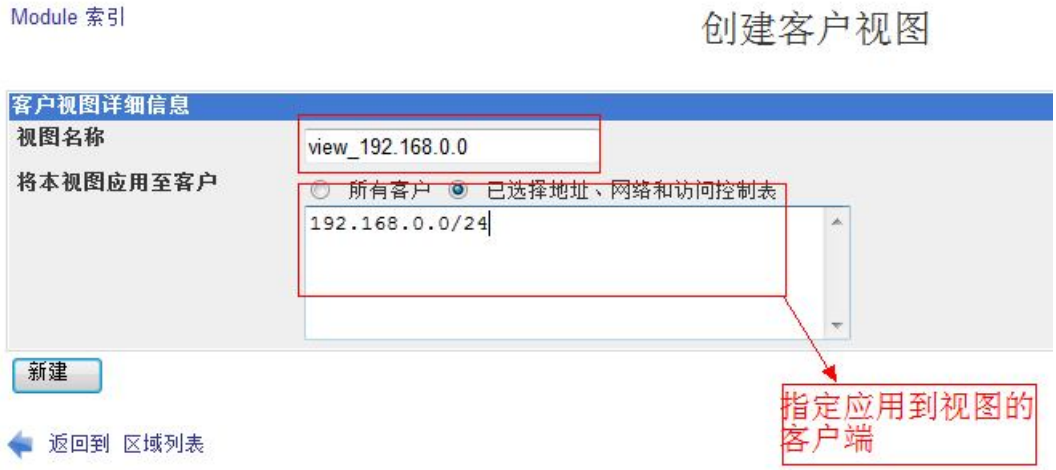


图 5

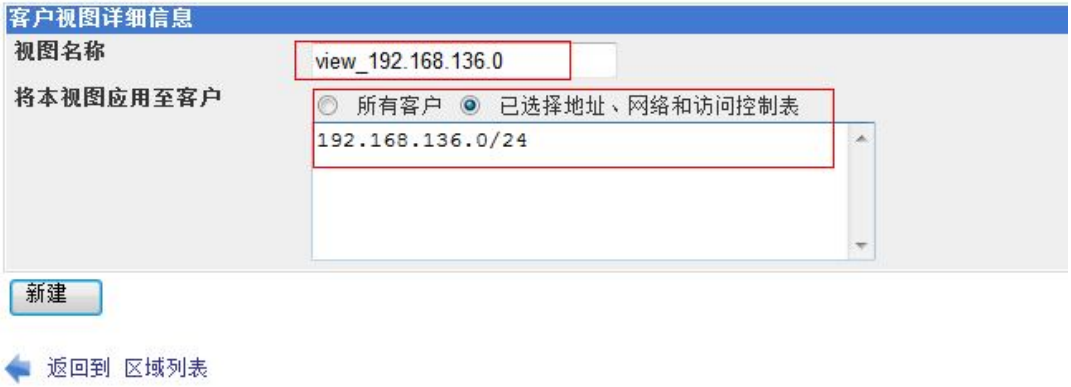


图 6

**c. 创建正向主区域**

创建主区域就相当于创建每个域名在 DNS 上的配置文件，以 linuxpad.cn 为例，我们需要首先在 DNS 服务器上创建一个将 linuxpad.cn 解析到 192.168.0.200 的主记录（先不考虑 192.168.136.0 段，只介绍主区域的创建方法），这个记录我们称之为正向记录，即域名到 IP；然后需要再创建一个将 192.168.0.200 解析到 linuxpad.cn 的主记录，这个记录我们称之为逆向记录，即 IP 到域名。这样一个域名的配置文件就成功了。

对于属于同一段 IP 的服务器来说，每个域名必须创建一个正向主区域，但是所有域名可以共用一个逆向主区域。

我们点击图 4 上的 创建新的主区域，创建过程如图 7

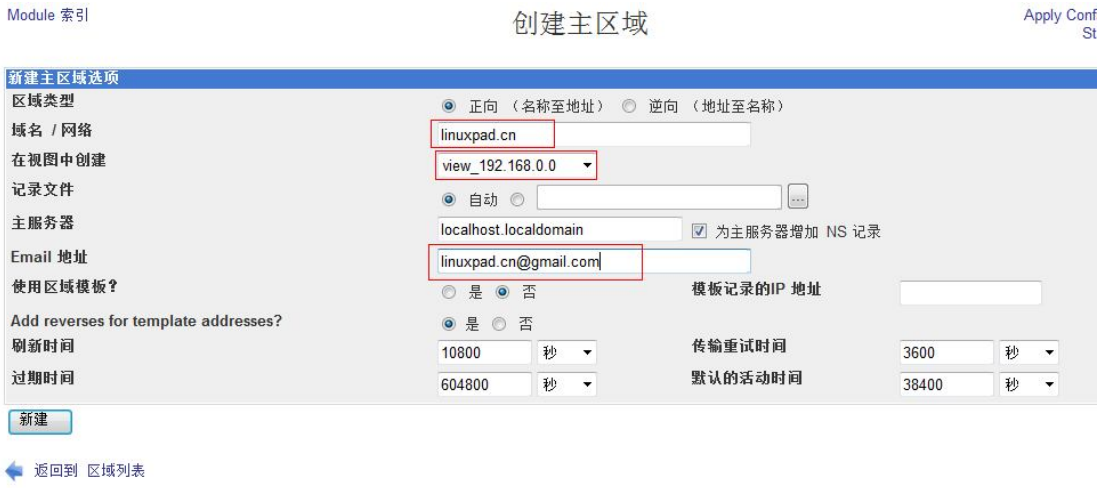


图 7

区域类型选择”正向”，域名/网络填写域名”linuxpad.cn”,在视图创建选择此主区域所属的视图，这里选择”view_192.168.0.0”,E-mail 地址须写上，否则会报错。

点击创建如果没有错误即创建成功，会自动跳转到编辑主区域的界面，这里我们为”linuxpad.cn”这个区域来添加 A 记录。选择”地址”选项(地址选项就相当于 A 记录)，如图 8


图 8

在名称中填写二级域名，在地址中填写域名所对应的服务器地址，这里名称填写”@”，即表示 linuxpad.cn，没有二级域名，当然你也可以填写 www/ftp/mail 之类的，如图 9

值得一提的是这里可以配置泛域名解析，即在名称处填写”*”，这样所有在地址列表中没有的名称全部会匹配到名称”*”所对应的 IP 地址，如 aaa.linuxpad.cn，aaa 这个名称不存在于地址记录中，则 aaa.linuxpad.cn 就会匹配名称为”*”的这个地址记录，注意这条规则的位置，请确认”*”规则位于最末尾，否则位于”*”之后的地址记录将得不到解析。


图 9

**d. 创建逆向主区域**

我们在上一步创建了 linuxpad.cn 正向解析，但是 DNS 解析只有正向是不行的，还必须有逆向解析，即将 IP 解析为域名，只有这样服务器才能将数据通过对应的域名返回给客户端。创建逆向主区域过程如图 10

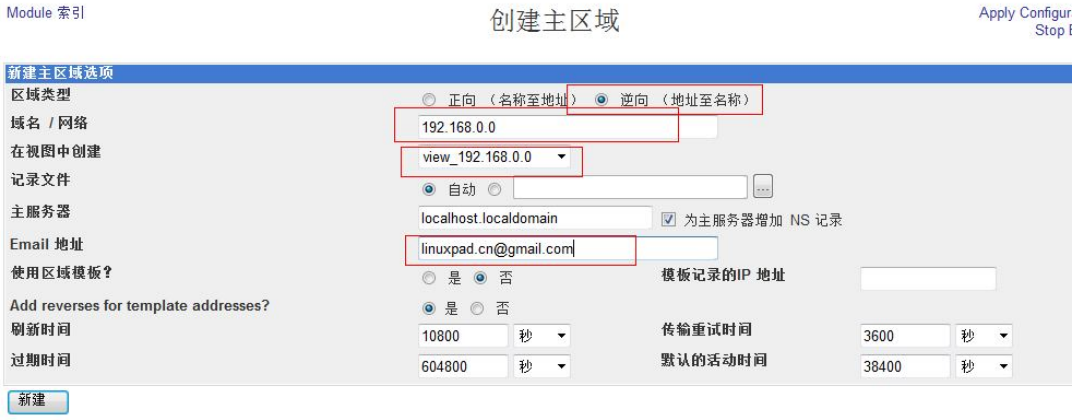


图 10

区域类型选择”逆向”，域名/网络填写”192.168.0.0”，在视图中创建选择”view_192.168.0.0”，同样填入 E-mail，然后点击创建，创建成功后会自动跳转到编辑主区域的界面。

接下来，选择”逆向地址”，进行逆向地址的创建，如图 11/图 12。


图 11

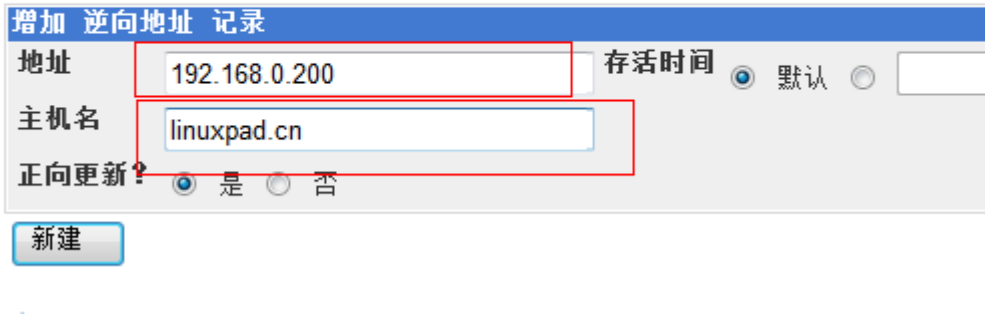


图 12

在地址中填写服务 IP 地址，主机名中填写 IP 所对应的域名。

到此刻为止 linuxpad.cn 的解析就完全创建成功了，我们的 DNS 服务器就能解析 linuxpad.cn 这个域名了。但是不要着急，我们来完成最后一步的配置。

**e．另一个视图中域名解析的配置**

在上面的创建主区域的时候，”在视图中创建”这个选项，我们选择的是 view_192.168.0.0，这样的话，我们所创建的 linuxpad.cn 这个域名解析只能对 192.168.0.0/24 这个段内的客户进行解析，如果我使用 192.168.136.0 段对 linuxpad.cn 进行访问的时候 DNS 就找不到服务器了，因为我们还没有在 view_192.168.136.0 这个视图中添加规则呢。

按照上一步，我们再来创建两个规则，区域类型为”正向”，域名/网络为 linuxpad.cn，视图属于”view_192.168.136.0”，在”linuxpad.cn”主区域添加地址，名称为”@”，地址为”192.168.136.200”，这里有人会疑惑主区域的名称 linuxpad.cn 不是与上一步的重复了，不冲突嘛，实际上是不冲突的，在不同的视图中可以存在同名的主区域，但是在相同的视图中

不能存在同名的主区域。

我们再创建一个逆向的主区域，区域类型为逆向，域名/网络为”192.168.136.0”， 视图属于”view_192.168.136.0”。在”192.168.136.0”主区域添加逆向地址，地址为”192.168.136.200”，主机名为”linuxpad.cn”。

这样我们就完成了所有的 DNS 配置工作。

创建完成之后，返回到区域列表，我们发现配置完成之后主界面会显示出大概的配置信息。如图 13。


图 13

## 4. 测试

配置完成后，首先我们须重启 DNS 服务，你可以通过 Webmin 图像界面来应用配置(Apply Configuraion)，如图 14，也可以通过服务器使用命令 service named restart 来重启 DNS 服务。

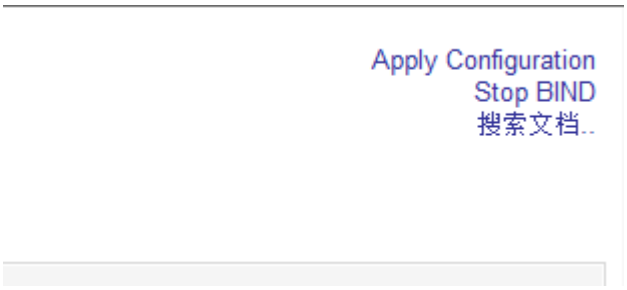


图 14

测试 192.168.0.0 段：

禁用虚拟网卡，以本地连接的 192.168.0.0/24 段来测试。如图 15/图 16

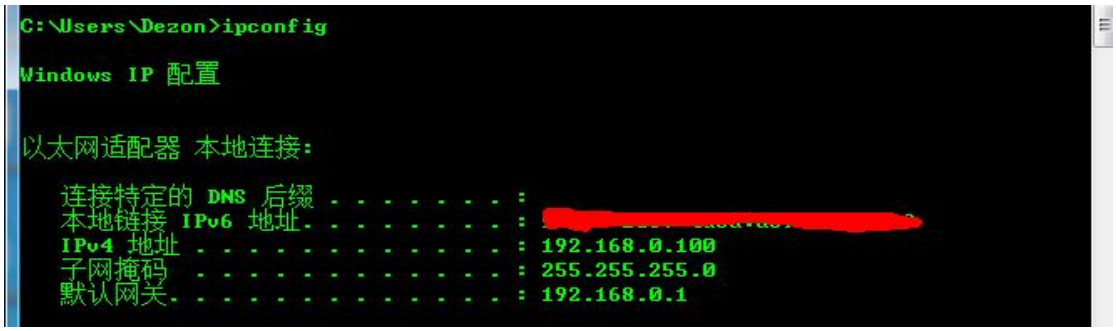


图 15


图 16

禁用本地连接，以虚拟网卡的 192.168.136.0/24 段来测试。如图 17/图 18

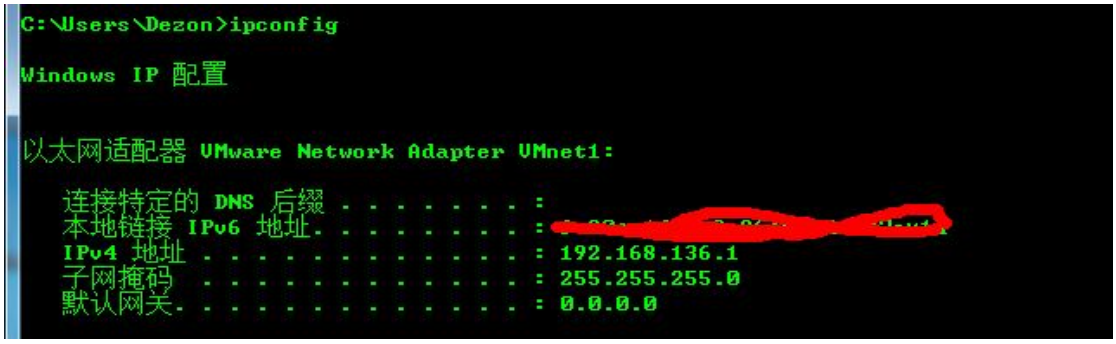


图 17

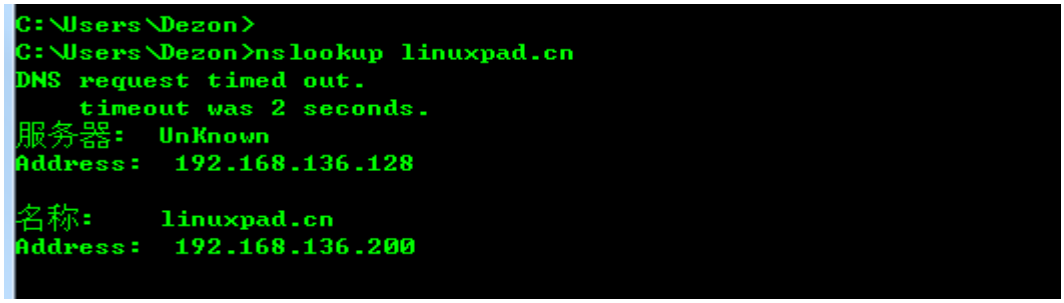


图 18

这样就利用 BIND9 的 VIEW 视图功能完美的解决了 DNS 智能解析的问题。

## 延伸：

1、 这个实验中我们完成了 DNS 服务器对不同网段的 IP 进行智能解析，这在内网和外网同时访问公司网站是很有效的，我们只需要在公司 DNS 服务器上配置双网卡，判断如果请求 IP 是外网则返回外网地址，如果请求 IP 是内网则返回内网地址，有效的解决了公司内部电脑访问公司网站速度过慢的问题（因为常规情况下，内部电脑访问网站需要先经过互联网 DNS 服务器进行解析，然后再将服务器返回的数据通过外网返回给内网用户，等于在外面绕了一大圈）。

2、 如何让电信用户解析到电信服务器，网通用户解析到网通服务器。

这个可以在 DNS 服务器上创建两个视图，一个电信视图一个网通视图，并且把电信和网通的 IP 分别写到两个视图内（电信和网通的 IP 列表以及南方和北方的 IP 列表这个网上都可以查到），然后再针对不同的客户端分别在两个视图内实现 DNS 智能解析。