**DNS分离解析和智能解析**

# 1、构建DNS域名服务器的分离解析

DNS分离解析域名服务器概述

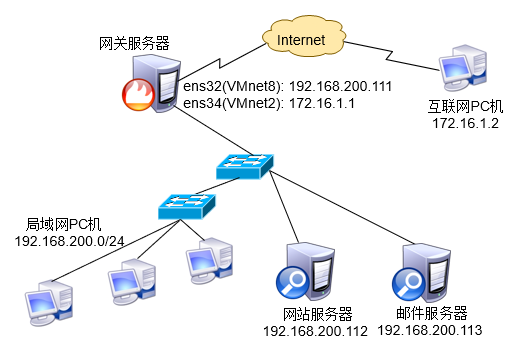
DNS分离解析域名服务器实际也是主域名DNS服务器，这里所说的分离解析（Split DNS），主要是指根据不同来源的客户端请求，提供不同的域名解析记录。来自不同地址的客户机请求解析同一域名时，为其提供不同的解析结果。

分离解析案例：

如下图所示：Benet工作室的DNS域名服务器架设在公司网关服务器中，网关服务器拥有两个网卡，ens32（或ens33）（VMnet8）的IP地址为192.168.200.111属于公司的内网通信网络；网卡ens34（或ens37）（Vmnet2）的IP地址为172.16.1.1属于公司的公网通信网络。公司注册的域名有网站服务器：[www.benet.com](http://www.crushlinux.com)。

案例需求：

* 来自Internet的客户机解析[www.benet.com](http://www.crushlinux.com和mail.crushlinux.com) 域名时考虑服务器的安全性，需解析为公司的公网地址172.16.1.1。使其通过公司的网关服务器转发后访问网站。
* 来自公司局域网中的客户机解析[www.benet.com](http://www.crushlinux.com和mail.crushlinux.com) 域名时考虑到用户访问速度解析为服务器局域网地址192.168.200.112。使其通过公司局域网直接访问相应服务器。
* 客户机切换网络模式，模拟内网与公网地址进行解析测试。



1.1、前期环境准备

**[root@localhost ~]# ip a | grep ens**

**2: ens32: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000**

**inet 192.168.200.111/24 brd 192.168.200.255 scope global ens32**

**3: ens34: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000**

**inet 172.16.1.1/24 brd 172.16.1.255 scope global ens34**

**[root@localhost ~]# systemctl stop firewalld**

**[root@localhost ~]# iptables -F**

**[root@localhost ~]# setenforce 0**

**setenforce: SELinux is disabled**

**[root@localhost ~]# yum -y install bind**

1.2、修改/etc/named.conf主配置文件中为不同网络的客户机地址准备不同的zone区域设置，各自使用独立的数据文件

**[root@localhost ~]# vim /etc/named.conf**

**options {**

**directory "/var/named";**

**};**

**view "LAN" {**

**match-clients { 192.168.200.0/24; }; //匹配局域网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.lan";**

**};**

**};**

**view "WAN" {**

**match-clients { any; }; //匹配互联网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.wan";**

**};**

**};**

1.3、分别建立不同的区域数据文件

**[root@localhost ~]# cd /var/named/**

**[root@localhost named]# vim benet.zheng.lan**

**$TTL 86400**

**@ IN SOA benet.com. admin.benet.com. (**

**2019011001**

**3H**

**15M**

**1W**

**1D**

**)**

**IN NS www.benet.com.**

**www IN A 192.168.200.111**

**[root@localhost named]# vim benet.zheng.wan**

**$TTL 86400**

**@ IN SOA benet.com. admin.benet.com. (**

**2019011001**

**3H**

**15M**

**1W**

**1D**

**)**

**IN NS www.benet.com.**

**www IN A 172.16.1.1**

**[root@localhost named]# chgrp named benet.zheng.\***

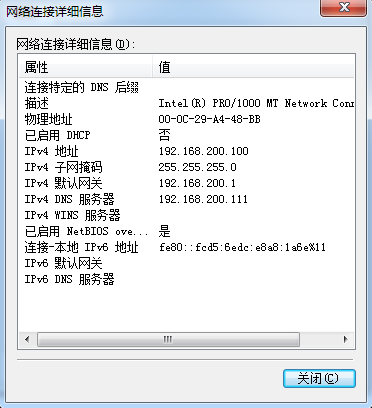
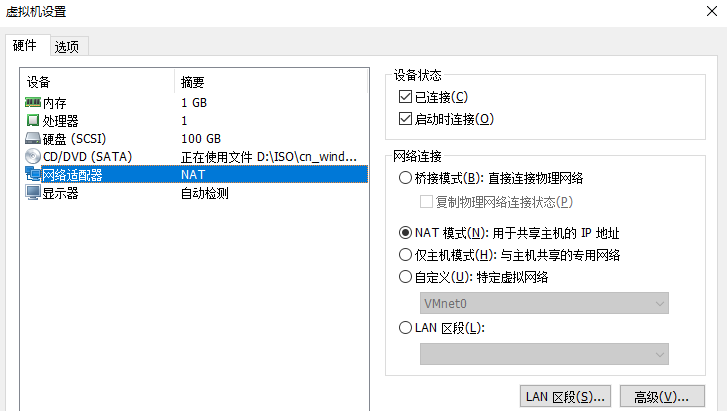
**[root@localhost named]# ls -l benet.zheng.\***

**-rw-r--r-- 1 root named 229 1月 10 23:51 benet.zheng.lan**

**-rw-r--r-- 1 root named 214 1月 10 23:52 benet.zheng.wan**

**[root@localhost named]# systemctl restart named**

1.4、客户机设置网络模式为VMnet8，DNS服务器指向为192.168.200.111，解析测试



**C:\Users\Benet>nslookup www.benet.com**

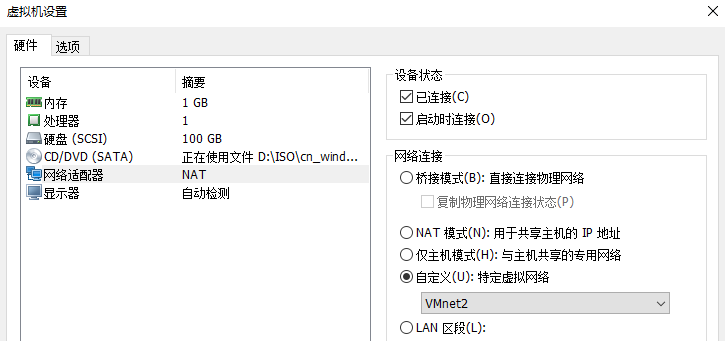
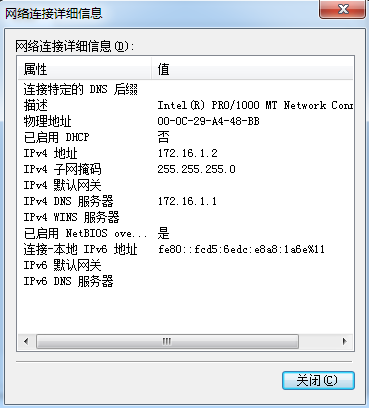
**服务器: UnKnown**

**Address: 192.168.200.111**

**名称: www.benet.com**

**Address: 192.168.200.111**

1.5、客户机设置网络模式为VMnet2，DNS服务器指向为172.16.1.1，解析测试

**C:\Users\Benet>nslookup www.benet.com**

**服务器: UnKnown**

**Address: 172.16.1.1**

**名称: www.benet.com**

**Address: 172.16.1.1**

**C:\Users\Benet>nslookup mail.benet.com**

**服务器: UnKnown**

**Address: 172.16.1.1**

**名称: mail.benet.com**

**Address: 172.16.1.1**

# 2、DNS view的多种应用方式

2.1、match-clients直接指定地址

**[root@localhost ~]# vim /etc/named.conf**

**options {**

**directory "/var/named";**

**};**

**view "LAN" {**

**match-clients { 192.168.200.0/24; }; //匹配局域网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.lan";**

**};**

**};**

**view "WAN" {**

**match-clients { any; }; //匹配互联网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.wan";**

**};**

**};**

2.2、基于acl访问控制列表

**[root@localhost ~]# vim /etc/named.conf**

**options {**

**directory "/var/named";**

**};**

**acl lan { 192.168.200.0/24; }; //定义访问控制列表**

**acl wan { any; };**

**view "LAN" {**

**match-clients { lan; }; //匹配局域网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.lan";**

**};**

**};**

**view "WAN" {**

**match-clients { wan; }; //匹配互联网的客户端**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.wan";**

**};**

**};**

2.3、基于访问控制文件

**[root@localhost ~]# cat /var/named/lan.txt**

**acl lan {**

**192.168.200.0/24;**

**};**

**[root@localhost ~]# cat /var/named/wan.txt**

**acl wan {**

**any;**

**};**

**[root@localhost ~]# vim /etc/named.conf**

**[root@localhost ~]# cat /etc/named.conf**

**options {**

**directory "/var/named";**

**};**

**include "/var/named/lan.txt";**

**include "/var/named/wan.txt";**

**view "LAN" {**

**match-clients { lan; };**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.lan";**

**};**

**};**

**view "WAN" {**

**match-clients { wan; };**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.wan";**

**};**

**};**

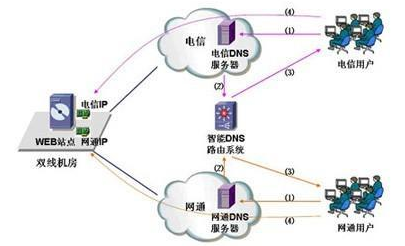
# 3、构建智能DNS域名解析服务器

随着原中国电信集团按南北地域分家,新的中国电信和网通集团随即成立,互联网的骨干网也被一分为二了，北有[网通](https://baike.baidu.com/item/%E7%BD%91%E9%80%9A/350790)、南有电信。从此，细心的网民可以发现,有些经常访问的网站速度一下子慢了下来，有时候还有访问不到的情况出现。例如北方地区的网络用户访问中国网通的服务器会非常快，而访问中国电信的服务器时，感觉非常慢。这种现象不仅影响了网站的访问量,更严重的是它直接影响了一些[经营性网站](https://baike.baidu.com/item/%E7%BB%8F%E8%90%A5%E6%80%A7%E7%BD%91%E7%AB%99/5971261)的经济效益。据分析,产生这个问题的根本原因是中国电信分家之后，电信与网通之间的互连存在问题。虽然[信息产业部](https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E4%BA%A7%E4%B8%9A%E9%83%A8/2212317)已经在规划南北互通计划，但在今后相当长的一段时期内,南北方网互连的问题还会长期存在。

智能DNS解析是针对电信和网通互联互通不畅的问题推出的一种DNS解决方案。

智能DNS域名解析服务器能自动判断访问者的IP地址并根据IP地址所属的运营商不同可为其解析出对应运营商服务器的IP地址，使网通用户访问到网通服务器，电信用户访问到电信服务器，而不需要用户进行选择。避免用户访问跨运营商导致用户访问速度缓慢。

例如一个企业网站站点带宽租用了三个运营商的带宽：电信、网通、移动，同样有三个来自不同运营商网络的访问用户，那电信用户访问企业网站时，智能DNS会进行自动判断，根据IP来源运营商，为其解析为电信运营商IP地址，使用户访问同运营商服务器；其他运营商的用户访问的也同理，如下图所示。



智能DNS策略解析还可以实现就近访问机制。有些用户在国外和国内都放置了服务器，使用我们的DNS策略解析服务可以让国外的网络用户访问你国外的服务器，国内的用户访问国内的服务器，从而使国内外的用户都能迅速的访问到你的服务器。

智能DNS作用

* 双线路的机房：服务本身有两个IP，一个电信IP，一个网通IP或者其他线路。
* 镜象网站：在网通及电信的机房放置多个相同的镜象站点， 让不同的地方客户访问不同的站点。
* [负载均衡](https://baike.baidu.com/item/%E8%B4%9F%E8%BD%BD%E5%9D%87%E8%A1%A1)：对于流量比较大的网站，可以把流量分配到几台不同的服务器上，以提高网站速度。
* 个性化站点服务：比如通过IP表的重新定义， 让国外的客户自动访问英文版的网站； 让国内的客户自动访问中文版的网站。
* CDN(内容分发网络)加速器：通过与squid、Nginx、Varnish等WEB缓存软件结合实现CDN加速器。
* 防止DDOS（分布式拒绝服务）攻击：通过多个线路分散攻击流量，从而达到抵挡DDOS攻击。

CDN加速基础原理

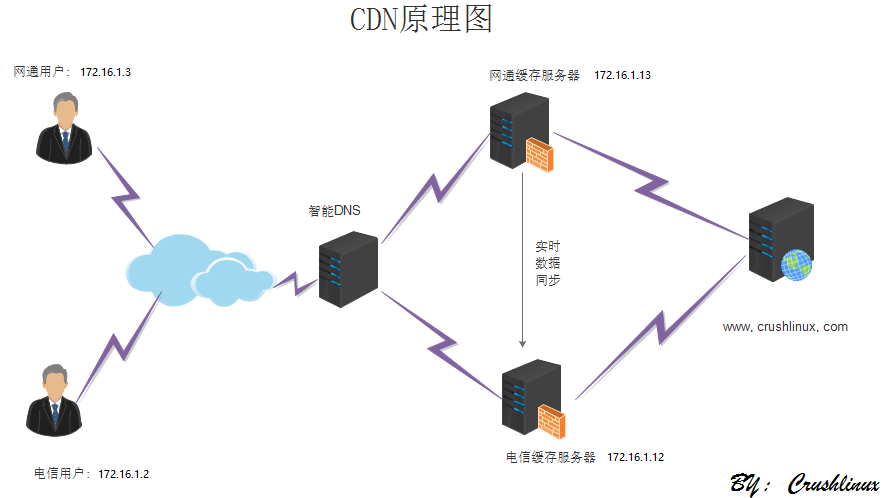


智能DNS域名服务器案例：

如下图所示：Benet工作室的DNS域名服务器架设在公司网关服务器中，网关服务器拥有两个网卡，ens32（VMnet8）的IP地址为192.168.200.111属于公司的内网通信网络；网卡ens34（Vmnet2）的IP地址为172.16.1.1（VMnet2）属于公司的公网通信网络。公司注册的域名有网站服务器：[www.benet.com](http://www.crushlinux.com)。

案例需求：

* 来自Internet的电信客户机解析[www.benet.com](http://www.crushlinux.com和mail.crushlinux.com) 域名时需解析为电信地址172.16.1.12。
* 来自Internet的网通客户机解析[www.benet.com](http://www.crushlinux.com和mail.crushlinux.com) 域名时需解析为网通地址172.16.1.13。
* 客户机切换IP地址模拟电信与网通运营商进行解析测试。



3.1、前期环境准备

**[root@localhost ~]# ip a | grep ens**

**2: ens32: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000**

**inet 192.168.200.111/24 brd 192.168.200.255 scope global ens32**

**3: ens34: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc pfifo\_fast state UP group default qlen 1000**

**inet 172.16.1.1/24 brd 172.16.1.255 scope global ens34**

**[root@localhost ~]# systemctl stop firewalld**

**[root@localhost ~]# iptables -F**

**[root@localhost ~]# setenforce 0**

**setenforce: SELinux is disabled**

**[root@localhost ~]# yum -y install bind**

3.2、修改/etc/named.conf主配置文件中为不同运营商的客户机地址准备不同的zone区域设置，各自使用独立的数据文件

**[root@localhost ~]# cat /var/named/wangtong.txt**

**acl wangtong {**

**172.16.1.3;**

**};**

**[root@localhost ~]# cat /var/named/dianxin.txt**

**acl dianxin {**

**172.16.1.2;**

**};**

**[root@localhost ~]# cat /etc/named.conf**

**options {**

**directory "/var/named";**

**};**

**include "/var/named/dianxin.txt";**

**include "/var/named/wangtong.txt";**

**view "dianxin" {**

**match-clients { dianxin; };**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.dianxin";**

**};**

**};**

**view "wangtong" {**

**match-clients { wangtong; };**

**zone "benet.com" IN {**

**type master;**

**file "benet.zheng.wangtong";**

**};**

**};**

3.3、分别建立不同的区域数据文件

**[root@localhost ~]# cd /var/named/**

**[root@localhost ~]# cat /var/named/benet.zheng.dianxin**

**$TTL 86400**

**@ IN SOA benet.com. admin.benet.com. (**

**2019011001**

**3H**

**15M**

**1W**

**1D**

**)**

**IN www ns.benet.com.**

**www IN A 172.16.1.12**

**[root@localhost ~]# cat /var/named/benet.zheng.wangtong**

**$TTL 86400**

**@ IN SOA benet.com. admin.benet.com. (**

**2019011001**

**3H**

**15M**

**1W**

**1D**

**)**

**IN NS www.benet.com.**

**www IN A 172.16.1.13**

**[root@localhost named]# chgrp named benet.zheng.\***

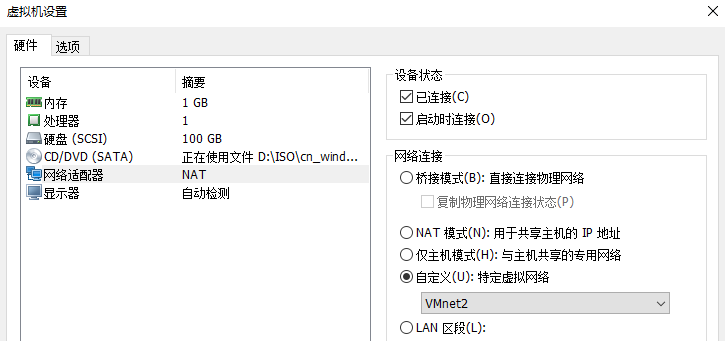
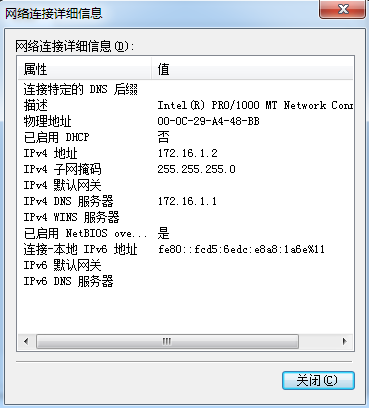
**[root@localhost named]# ls -l benet.zheng.\***

**-rw-r--r-- 1 root named 229 1月 10 23:51 benet.zheng.lan**

**-rw-r--r-- 1 root named 214 1月 10 23:52 benet.zheng.wan**

**[root@localhost named]# systemctl restart named**

3.4、客户机设置网络模式为VMnet2，IP地址为172.16.1.2模拟电信用户，解析测试

**C:\Users\Benet>nslookup www.benet.com**

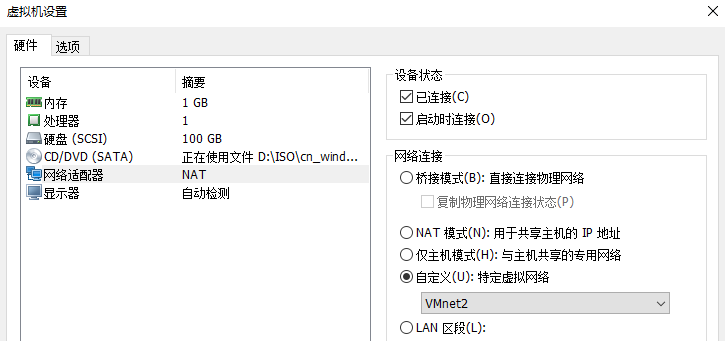
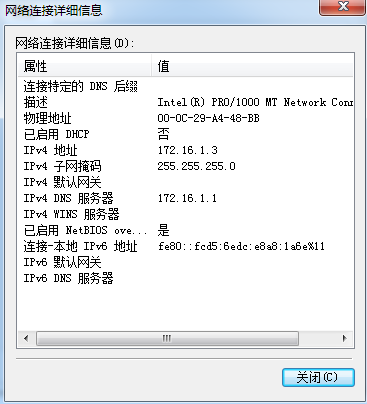
**服务器: UnKnown**

**Address: 172.16.1.1**

**名称: www.benet.com**

**Address: 172.16.1.12**

3.5、客户机设置网络模式为VMnet2，IP地址为172.16.1.3模拟网通用户，解析测试

**C:\Users\Benet>nslookup www.benet.com**

**服务器: UnKnown**

**Address: 172.16.1.1**

**名称: www.benet.com**

**Address: 172.16.1.13**