DNS Servers Configuration and Management Research Based on Red Hat Linux Platforms

Mo yuqing, Peng Liling, Yang li

Hunan College of Information, Changsha Hunan,410200

Keywords: DNS,primary DNS servers,auxiliary DNS servers,client host,IP address

Abstract. Domain name resolution is a core service of Internet, DNS servers's security and stability is essential. Red Hat Linux operating system can be applied as a DNS servers, which is an open-source and free operating system with security and stability. It is worthy of study and discussion on how to configure the primary DNS servers and secondary DNS servers on this platform in order to achieve domain name resolution of an unit or company.

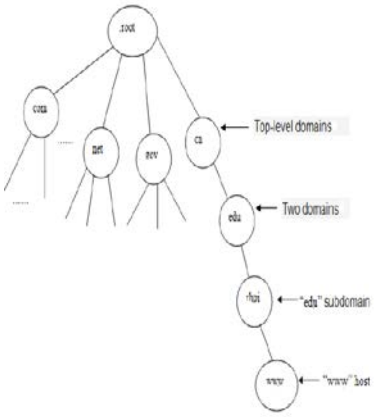
1 Introduction

In the internet, domain name is commonly used to access the web pages.In order to achieve to access web pages with domain name, firstly we must realize the mapping from domain name to IP address. At present, the common DNS operating systems have Windows and Linux. As an open-source and free operating system, Red Hat Linux operating system is applied more widely in server field, and it’s functions are more perfect. We can configure primary DNS domain name servers and secondary DNS servers on the Red Hat Linux operating system to ensure the security and stability of the domain name system and to realize the domain management of units and enterprises. [1]

2 Overview of DNS Domain Name Resolution System

2.1. Concept of DNS domain name resolution

An agency, called inerNIC, is responsible for the structure of IP address range in the world, and is responsible for allocating domain structure on Internet[2]. Domain Name System uses an inverted tree structure, the top layer is root domain, the root domain DNS servers only handles resolution requests from top-level domain name DNS servers;Layer 2 is top-level domain, such as com、org、gov、 net and country code;Layer 3 is a second- level domain under the top-level domain; Layer 4 is a sub-domain under the second-level domain, sub-domain can be also divided into sub-domains; Layer 5 is the host, WWW usually stands for WEB servers,FTP for FTP servers,SMTP for e-mail sending servers,and POP for e-mail receiving servers.As shown in "Figure 1":



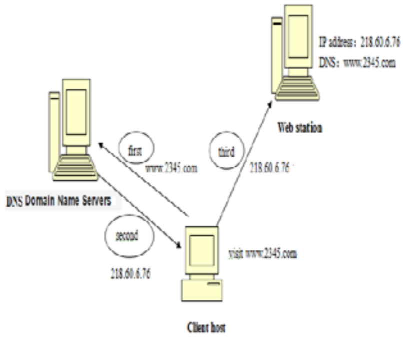


Figure 1.DNS domain name space structure   Figure 2.DNS domain name resolution principle

DNS is the abbreviation for Domain Name System or Domain Name Service, which is a core service of the Internet. It is a distributed database which can make domain names and IP addresses mapped to each other, can make people more conveniently access to web pages without having to remember the IP number that can be read directly by machines. It will be done by domain name resolution server[3].

2.2.DNS domain name resolution principle

DNS servers is a server which preserves domain names of all hosts in the network and their corresponding IP addresses and converts domain name into IP address. The parser resolves the domain name from the client into it's corresponding IP address (domain name -> IP),then the client accesses Web pages by parsing out the IP. it can also resolve IP addresses into domain names (IP-> domain name) [4].

DNS name resolution principle is shown in "Figure 2".The client host enters www.2345.com in the IE address bar to visit web station whose IP address is 218.60.6.76. The first step :The client host will send www.2345.com to DNS domain name servers. The second step: DNS servers will return the corresponding IP address 218.60.6.76 of www.2345.com to IE browser after resolution. The third step: The client host visits the web station whose IP address is 218.60.6.76.

3. Resolution process of DNS servers

3.1 DNS file

DNS can achieve a positive resolution and reverse resolution. Positive resolution is to convert the domain name into an IP address, and reverse resolution is to convert an IP address to the domain name. In small networks we usually use /etc/hosts file to resolve. The domain name and IP to be resolved is written directly to the file, and we can manually add or delete file contents. It is generally confined to resolution from domain name to IP address; In large networks, in order to meet the requirements of different organizations and achieve a scalable, customizable naming scheme, database files of DNS domain name servers are established[5].

3.2 DNS resolution process

DNS client host sends a request for resolution of www.163.com. The resolution process of DNS servers is shown in "Figure 3".

①DNS client host sends a request for resolution of www.163.com to the local DNS servers, and the local DNS servers does not find resolution result and then the request is sent to the root domain (ROOT) DNS servers.

②Root domain DNS In the "root hints" tabs (There are 13 root domain name servers. 1 main root servers, placed in the United States and the remaining 12 are secondary root servers, nine in the United States, one in the United Kingdom ,one in Sweden ,one in Japan. All root servers are managed by ICANN Internet Corporation for Assigned Names and Numbers) manages the address resolution of .com、.Net、.Org and other top-level domain name, the analytical results (such as server's IP address of .Com domain) is returned to the local DNS servers after receiving the request.

③After having obtained query results, the local DNS servers then t sends a request to the DNS servers of .com domain for further inquiries asking for DNS servers's IP address of 163.com.

④.Com domain returns the analytical results (DNS servers's IP address of 163.com) to the local DNS servers.

⑤After having got the query results, the local DNS servers then sends a request to the DNS servers of 163.com domain for inquiring the detailed host IP address of www.163.com.

⑥DNS servers of 163.com returns the resolved host IP address 172.16.64.11 to the local DNS servers.

⑦After getting the final query result, the Local DNS servers returns the host IP address 172.16.64.11 to the client host.

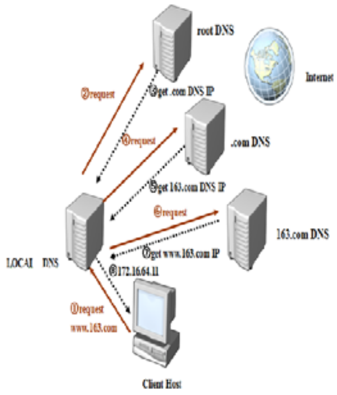


Figure 3.DNS resolution process

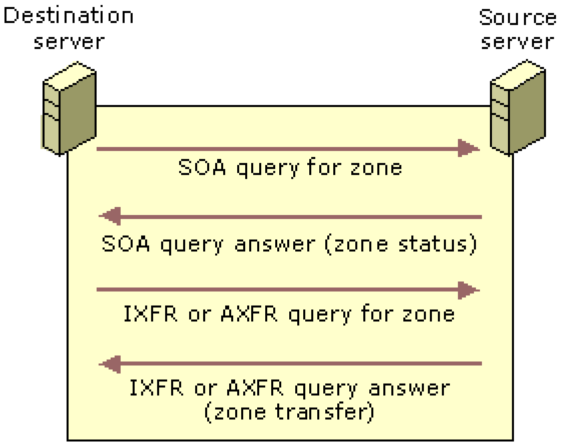

Destination server
Source server
SOA query for zone
SOA query answer (zone status)
IXFR or AXFR query for zone
IXFR or AXFR query answer (zone transfer)

Figure 4. Zone transfer process

4 Configuration and Management of DNS Servers

DNS server resolve domain names within the region. The main types of servers include primary DNS severs and secondary DNS server, and each undertakes different tasks.

4.1.security policy of DNS server

Red Hat Linux operating system with powerful networking functions in the server space has been widely used. DNS resolution server built on Red Hat Linux operating system platform, the focus from the three aspects of the firewall, SELinux, package installationthe safety considerations.

(1)The firewall settings

Firewalls are used to control who can connect to the DNS server. For those respond only to internal users query a DNS server, firewall configuration settings to prevent external host connection DNS server.

The important thing is that the firewall policy settings prevent internal users from using the DNS protocol to connect an external DNS server.

Linux kernel supports IP packet filtering, so no need to add additional software you can build packet filtering firewall, Ipchains package on the Linux platform is a powerful packet filtering policy management software for setting a reliable firewall system.

(2)SELinux

SELinux stands for Security-Enhanced Linux, which is by the U.S. National Security Agency NSA developed access control system, it is possible to ensure the security of Linux systems. SELinux Add two kernel components in Linux,one is the security server, to achieve the strategies Encapsulation, and provide a common interface; Another is access vector cache module.SELinux security server implements a hybrid security policy, including the TE, RBAC and optional multi-level security controls[11].

SELinux provides a secure server with the matching security policy configuration language, which is used to configure the security server security policy described[6].

SELinux can control access to a thorough, able to process given only minimal privileges, to prevent privilege escalation etc.

Turn off SELinux of common methods:

①No need to restart the linux operating systems:

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

②Need to restart the Linux operating system method:

vi/etc/selinux/config change the SELINUX = enforcing to SELINUX = disabled

(3)Bind-chroot package

Red Hat Linux system to build a DNS server is typically implemented using the bind process.Bind is the Berkeley Internet Name Domain Service shorthand, it is by the University of California, Berkeley, developed and maintained, it is the world's most widely used open source DNS server software that supports linux platform and windows platform.When configured DNS server, and then bind the packageis installed,again install the bind-choot package to a disguised root for bind,system see a "/var/ named/chroot" enhanced path, this time as long as the DNS zone files and configuration files put the enhancement of the path, you can improve the security of DNS servers.

4.2.Area Transmission

Secondary DNS server enables DNS, it is mainly to get the primary DNS server zone files through regional transmission information.Secondary DNS server synchronized with the primary DNS server, mainly by area transmission to achieve.

(1) Occurs Zone transfer

Area Transmission generally occurs between the primary and secondary DNS servers.The primary DNS server is authorized specific domain and DNS zone file with rewritable, set the refresh time in the file to be updated.Secondary DNS server receives these read-only copy of zone files from the main DNS server.Secondary DNS server is used to improve the response performance of DNS queries from the inside or the Internet.Area transmission occurs with the first part of the set of the primary DNS server zone files several times closely related. When the refresh interval expires of the area, a zone transfer automatically;when it changes the notification area of the primary DNS server to the secondary DNS server;When the DNS Server service starts on the secondary DNS server for the zone.

(2) Transmission principle of Area

Zone transfer is always on the secondary DNS server area begins, and as a regional source configuration is sent to the primary DNS server.When the primary DNS server receives the request of area, it can be a secondary server to answer some or all of the transfer area.Zone transfer between servers are sequentially,as shown in Figure 4,This process depends on the Area in the past over whether to copy and change, depending on whether or area in the implementation of the new changes in the initial replication.

In Figure 4, the secondary DNS server request (target area server) and the source server (primary DNS server) performed in the following order.

①During performing the new configuration, the secondary DNS server (the target server) to the primary DNS server (configured as a Area source) sends (AXFR) initial request of"all areas".Primary (source) DNS server responds, and this area is completely transferred to the secondary (target) DNS server.

②The region send a message to request transmission of the target server,it was along the transmission the start of authority (SOA) the resource record in the "Serial Number" (serial) field established by version.SOA also contains a state in seconds refresh interval (default is 900 seconds, or 15 minutes), pointed out that once a target server should use the source server when the request to renew the area.

③When the refresh interval expires, the secondary (target) DNS server using SOA query to request renewal of this area from the master (source) DNS server.

④Primary (source) DNS server response SOA record query.

⑤The response includes the region in the primary (source) DNS server sequence number of the current state (serial).

⑥Auxiliary (target) DNS server checks the response of the SOA record serial numbers and determine how to renew the area.If the sequence number in the SOA response (serial) whose value is equal to the current local sequence number, then the conclusion of the area are the same in both the server and does not require the transmission region.Then, the secondary (target) DNS server to reset its refresh interval to renew the area based on SOA response from the primary (source) DNS server in the field value.If the sequence number in the SOA response than its current local serial number is higher, you can determine this area has been updated and need to transfer.

If this secondary (target) DNS server to infer that this area has changed, then it will IXFR query is sent to the primary (source) DNS servers, including local value recorded in current SOA serial number of this region.

Primary (source) DNS server responds by incrementing the transmission area or completely transmitted.

If the primary (source) DNS server resource records that have been modified to maintain the latest incremental change in the history of the region to support the incremental transmission, then it may make answering incremental zone transfer (IXFR) through this area[13].

If the primary (source) DNS server does not support incremental transmission or no change in the region's history, it may make the response completely (AXFR) transfer to other regions through.

4.3.Build a primary DNS domain name server

In the Internet,the primary DNS server is unique, it manages the authoritative DNS records.Primary DNS server needs to be set locally managed regional database files[12].

Database files are generally two types of files, that is the main configuration file and zone files.The main configuration file is named "/var/named/chroot/etc/ named.conf", it is mainly set up where the zone file access path and file name setting area.If there is a secondary DNS name resolution server connection, it should be set to allow zone transfers, and specify the IP address of the secondary DNS server.It is the full path to the zone file "/var/named/chroot/var/named/zone file name."Its content is generally consists of two parts: one part is SOA, this section contains the serial number of zone transfers and the primary DNS server is refresh and Retry and maturity and other time settings; partly to resolve domain names into IP addresses .

Primary DNS server hosts throughout the region to resolve the domain name, DNS built on Red Hat Linux operating system platform, mainly to complete the three-step operation.The first step to complete bind and bind-chroot package is installed, the second step is completed on the "... /named.conf" main configuration file and zone file editing, the third step to open named services.

4.4.Set up a secondary DNS server

When the primary DNS failure,or DNS manage a large area, in order to reduce the load master DNS resolution, you can configure the appropriate number of secondary DNS,use the secondary DNS name resolution to undertake the same task.

Secondary DNS server, the main function is to provide a backup, often the primary DNS server to provide services at the same time, for the client, the primary, secondary DNS servers provide the same functionality.But the secondary DNS server address resolution records are not their own decisions, it is able to resolve the domain name is determined by the primary DNS server.Its database files generally have the main configuration file and zone files on the secondary DNS server is generally not edit zone files, zone files are obtained by synchronizing the primary DNS server, along with the changes in the zone file and change the primary DNS server. And the primary DNS server to synchronize updates.

Secondary DNS server needs to be done to build three steps, the first step to complete the installation bind and bind-chroot package; Step edit the main configuration file ". .. / named.conf", set the area to save the file path; third step open the named service.In the second step does not need to edit the zone file, the file is the primary DNS zone transfers by automatically synchronizing to get[1].

4.5.Test

In the primary DNS and secondary DNS server set up after a good, in order to verify the correctness of the server's database files, DNS servers can achieve the correct domain name resolution, to be tested by the client computer.The client can be of various types of operating systems, commonly used windows and linux operating systems.

In order not to affect the client's test, first turn off the main DNS and secondary DNS server firewall.

(1)client computer of Red Hat Linux operating system

Linux operating system as the client computer, the first to use the ping command to check whether is capable of.

The linux operating system with the DNS server. Then linux network settings, the eth0 network card DNS settings first primary DNS server IP address, and the second set to the IP address of the secondary DNS DNS server.Restart network services (service network restart), last used command in a terminal window to test, enter the domain name to parse the command line, if you find the corresponding IP address, indicating successful domain name resolution.

(2)client of windows operating system

Windows operating system as the client computer, the first to use the ping command to check whether the client computer with the DNS server can ping.Windows operating system set the preferred DNS as the primary DNS server IP address in the TCP/IP protocol, the alternate DNS settings for the secondary DNS server IP address.Finally, use the command to test in DOS command window.

(3)Test Command

Linux operating system client DNS name resolution test commonly used commands are host、nslookup、dig.

①host command format:

```
host [-a] [FQDN] [server]
host -l [domain] [server]
```

Parameter Description:

-a:the representative of the host lists all the relevant information, including IP, TTL etc.

-l: If you followed that domain settings allow allow-transfer, then list all the host name of the domain that corresponds to data management.

server: This parameter can be omitted, while in linux, when you want to take advantage of a host of non /etc/ resolv.conf to query corresponds to the host name and ip, you can take this argument.

②dig command format:

```
dig [@server] [FQDN] [type]
```

Parameter Description:

@server: In the linux operating system is not in /etc/resolv.conf as dns host, you can enter other ip in this.

type: A default query records, other records can be written here, such as: MX, NS etc.

③nslookup command format:

```
nslookup [FQDN] [server]
```

After nslookup can be directly coupled to query the host name or ip, [server], but omitted. You can not add any host name or ip behind nslookup, enter nslookup query capabilities.nslookup query function which can enter additional parameters for specific queries, such as: set type = any / / list all the information

set type = mx / / mx lists related information

In windows and linux operating systems commonly used nslookup command to test DNS.often after dos command window or terminal window, enter the nslookup command directly hit the Enter key to enter the domain name resolution.If the client is configured correctly, DNS servers named service opens successfully, the> prompt, enter the full domain name to be resolved, we can resolve the IP address corresponding to the domain name.

5 Configuration Practice of DNS Servers

5.1.Project Requirements

In order to provide domain name resolution services ,now we are required to build a primary DNS server and secondary DNS servers within enterprise. DNS servers manage the domain name resolution of rhlx.com. the domain name of the primary DNS servers is dns.rhlx.com and its IP address is 192.168.1.2.The IP address of the secondary DNS servers is 192.168.1.3. you are required to resolve the following domain names:Finance Department(cw.rhlx.com:192.168.1.11),Sales Department (xs.rhlx.com:192.168.1.12),Manager Department (jl.rhlx.com:192.168.1.13),OA System(oa.rhlx.com:192.168.1.13).Take Red Hat Linux 5.5 platform for example to complete the configuration of DNS servers by the following procedures.

5.2.Configuration of Primary DNS servers

There are three main steps to complete the configuration of the primary DNS servers.The first step is to install bind package and bind-chroot package (bind-chroot package may not be installed);The second step is to edit the main configuration file named.conf and its corresponding zone files and to resolve the required domain names;The third step is to open named services.

(1)Installation packages

Install the service package bind-*. rpm and bind-chroot-*. rpm package enhancing the security of DNS database file.

①Use the find command to find the two packages above.

```
[root@localhost ~]# find / -name bind-*
…
  /media/RHEL_5.5 i386 DVD/Server/bind-9.3.6-4.P1.el5_4.2.i386.rpm
…
[root@localhost ~]#find/-name bind-chroot-*
…
/media/RHEL_5.5 i386 DVD/Server/bind-chroot-9.3.6-4.P1.el5_4.2.i386.rpm
...
```

"/ media/RHEL_5.5 i386 DVD / Server /"found is the path to the package.

②Use RPM Installation package

Install bind package.The path is marked with double quotes because there are spaces in the full path of the package.

```
 [root@localhost ~]#rpm -ivh "/media/RHEL_5.5 i386 DVD/Server/bind-9.3.6-4.P1.el5_4.2.i386.rpm"
```

Install bind-chroot package.The path is marked with double quotes because there are spaces in the full path of the package.

```
 [root@localhost ~]#rpm -ivh "/media/RHEL_5.5 i386 DVD/Server/bind-chroot-9.3.6-4.P1.el5_4.2.i386.rpm"
```

(2) Edit the main configuration file and zone files

①Edit the main configuration file

After installation of bind-chroot package is completed,the system appears enhanced path /var/named/chroot,You can put the main configuration file and zone files under this path, edit the main configuration file "/var/named/chroot/etc/named.conf" under this path,and establish positive zone rhlx.com,If you want to create multiple zones,you can use more than one zone,Reverse zone will not be descripted here because the way is the same.Open the main configuration file,"vi /var/named/chroot/etc/named.conf" by VI editor.Edit content as follows:

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


};
zone "rhlx.com" in {
    type master;
    file "rhlx.com.zone";
};
```

②Edit zone files

According to the zone file name "rhlx.com.zone" of positive zone "rhlx.com" determined by the primary configuration file, edit the zone file(vi /var/named/chroot/var/named/rhlx.com.zone) by VI editor. Edit zone file " rhlx.com.zone" of positive zone " rhlx.com" as follows:

```
 $TTL 86400
@  IN SOA  dns.rhlx.com. mail.rhlx.com.(
                42        ; serial
10800      ; refresh (3 hours)
900        ; retry (15 minutes)
604800     ; expire (1 week)
86400      ; minimum (1 day)
  )
NS      dns.rhlx.com.
MX  10  mail.rhlx.com.
cw  A       192.168.1.11
dns A       192.168.1.2
jl  A      192.168.1.13
oa  A      192.168.1.13
xs  A      192.168.1.12
```

③Open the Services

"Named"is the corresponding service name of DNS service. Open the named service After the main configuration file and zone file are edited without error.Use the service command to open service (that is "service named start").The main configuration file and zone file are properly configured.the service is turned on, otherwise to check the correctness of the main configuration file or zone file with hints.

```
[root@localhost ~]# service names start
open named                    [ok]
```

5.3. Configuration of secondary DNS servers

After the configuration of primary DNS servers is completed,you can configure the secondary DNS servers as required. Configuration of secondary DNS servers includes three steps:The first step is to install package "bind" and package "bind-chroot" (bind-chroot package may not be installed);The second step is to edit the main configuration file "named.conf" on secondary DNS servers and modify the main configuration file named.conf on the primary DNS servers;The third step is to open "named" service on secondary DNS servers and restart the named service on the primary DNS servers.

(1) Edit the main configuration file

Install package "bind" and package "bind-chroot" on the secondary DNS servers. Installation method is just the same with primary DNS server, so it will not be introduced here.Open the main configuration file "vi/var/named/chroot/etc/named.conf" and edit content as follows:

```
 options{
   directory "/var/named";
};
zone "rhlx.com" in {
    type  slave;
    file "slaves/rhlx.com.zone";
    masters{192.168.1.2;};     //192.168.1.2 is the IP address of the primary DNS server
};
```

Modify the main configuration file on the primary DNS server and open the main configuration file "vi /var/named/chroot/etc/named.conf".Just add the following content in the options section,and other parts will not be changed.

```
options{
  directory "/var/named";
allow-transfer{192.168.1.3;};  //192.168.1.3 is the IP address of the secondary DNS servers
};
```

(2)Open the named service

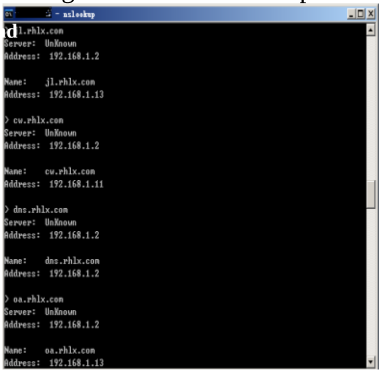
Start service with service command on the secondary DNS servers (that is “service named start”).Restart named service on the primary DNS servers(that is “service named restart”). On the secondary DNS servers, the primary DNS server will transfer zone files to directory “/var/named/chroot/var/named /slaves” on the secondary DNS servers through the zone transfer,and the file name is the same on the primary DNS server.

5.4. DNS test

Client computers can be Windows and Linux operating system.DNS servers named service after opening, the client host should be able to correctly resolve the domain name, the servers will be the first to use the command "iptables -F" to close the firewall.

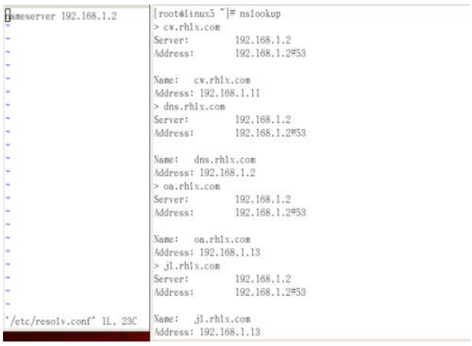
(1)the windows operating system as the client computer

When a client computer uses Windows operating system, select IP address(192.168.1.2) of the primary DNS servers or IP address(192.168.1.3) of the secondary DNS servers when setting TCP/IP protocol for local connections, and then use “nslookup” to test the domain name of domain zone file in the DOS command line window. Getting the IP address corresponding to the domain name proves the success of DNS server configuration.As shown in figure 5.



```
> jl.rhlx.com
Server:  UnKnown
Address:  192.168.1.2

Name:    jl.rhlx.com
Address:  192.168.1.13

> cw.rhlx.com
Server:  UnKnown
Address:  192.168.1.2

Name:    cw.rhlx.com
Address:  192.168.1.11

> dns.rhlx.com
Server:  UnKnown
Address:  192.168.1.2

Name:    dns.rhlx.com
Address:  192.168.1.2

> oa.rhlx.com
Server:  UnKnown
Address:  192.168.1.2

Name:    oa.rhlx.com
Address:  192.168.1.13
```

Figure 5.Windows test client



```
nameserver 192.168.1.2
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/resolv.conf" 1L, 23C
```

```
[root@linux5 ~]# nslookup
> cw.rhlx.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   cw.rhlx.com
Address: 192.168.1.11
> dns.rhlx.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   dns.rhlx.com
Address: 192.168.1.2
> oa.rhlx.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   oa.rhlx.com
Address: 192.168.1.13
> jl.rhlx.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   jl.rhlx.com
Address: 192.168.1.13
```

Figure 6.Linux test client

(2)Linux operating system as the client computer

When the client uses Linux operating system, edit the etho NIC ,set IP address(192.168.1.2) of the primary DNS servers or IP address(192.168.1.3) of the secondary DNS servers as the IP address of DNS,and then enter “nslookup” to test in the terminal window. Obtaining the IP address corresponding to the domain name indicates a successful configuration of DNS servers.As shown in figure 6.

6 Conclusion

Red Hat Linux operating system is developed on the basis of the unix operating system and its security and stability is unquestioned. Red Hat Linux operating system has been widely applied in servers field, and it is often used as a DNS domain name servers[8].The configuration of a primary DNS server mainly includes the installation of packages and the edition of the main configuration file and zone files. The configuration of a secondary DNS server mainly includes the installation of packages and the edition of the main configuration file. zone files are obtained by primary DNS servers and update with primary DNS servers.Secondary DNS is mainly used in some large companies with a wide geographical distribution and a lot of subsidiaries. Set secondary DNS servers in different areas to reduce the heavy load on the primary DNS servers,and when the primary DNS server is attacked or fails,the secondary DNS servers can also play the role of resolution[9].

Acknowledgements

Mo Yuqing(1977.9-),female,Yingshan Sichuan,China,Senior Technician, Master, research direction: Computer Software and Applications

Peng Liling (1977.12-),female,Shaoyang Hunan, China,lecturer,master,research direction:Applied English

C.Yang Li (1979.6-), female, Changsha Hunan, China, lecturer, master, research direction: Computer Software

References

[1] Sun Lina;Kong Linghong;Yang Yun,etc. Linux network operating system training (2nd edition) [M]. Chinese Railway Publishing House.2012 May:151-174

[2] Zhang Xinchang;Li Xiaodong;Yan Baoping. For more information adapt registered address RPSL query expansion [J].Computer Application Research.2008.7:2132-2134

[3] Zhi Weiyan; Anlei Hu; Wei Wang.BOTNET DOMAIN NAME DETECTION BASED ON DNS TRAFFIC FEATURES.Proceedings of 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems.2012.10

[4] D.Dagon.Botnet Detection and Response-The Network is the Infection. Proceedings of the 2005 Workshop of DNS Operations Analysis and Research Center.2005

[5] Wang Zhong;Ouyang Shoucheng;Rensu Ping;Huang Zhonghui.LINUX system security. Sichuan Provincial Institute of Communications 2002 Annual Conference Proceedings [C]. 2002.12

[6] Ma Yichao;Yang Xiaobin.Red Hat Enterprise Linux Network Services Security Research[J].Computer Security.2009.6:8-10

[7] Song Guozhu;Chen Junjie.Design and implementation of intelligent DNS system based on Mysql database[J].Computer Engineering and Design.2009.12:5771-5773 +5777

[8] Zhao Yanbo;Ma Jie;Kang Wei. Research and Implementation WAN environment remotely deployed applications[J].Computer Engineering.2007.8:240-242 +245

[9] Peng Yong;Fan Yuejun;Chen Dongqing;CHENG Xueqi.Based Transparent Proxy Domain Name System Hazard Analysis and Defense Strategies[J].Journal of Tsinghua University (Natural Science).2011.10:1318-1322 +1328

[10]Yang Ke;Chen Jihao;Lu Chun;Li Li.DNS system Research and implementation of intelligent based on Linux.Information Security and Communications Privacy[J].2011.10:72-75

[11]Tang Lin.Research of Linux and SELinux.The Second Asia-Pacific Symposium on Information Theory[C].2011.11

[12]TAN Ming-jia.Application analysis of DNS technology.Computer Engineering and Design[J].2004.4:596-598

[13]Luo Jieyun;He Minwei.DNS security protocol analysis.Applications of The Computer Systems[J].2004.1:36-38+35