DNS 实验

一 实验目的

1. 掌握 DNS 的报文格式
2. 掌握 DNS 协议的工作原理
3. 理解简单的本地 DNS 服务器的配置流程

二 预备知识

1. 资源记录

DNS 服务器中存储了资源记录(Resource Record)，RR 提供了主机名到 IP 地址的映射。资源记录的定义格式：

Name [TTL] IN RR_Type Value

其中,Name 和 Value 的值取决于记录类型 RR_Type。常用的记录类型有：A、AAAA、SOA、NS、PTR、CNAME、MX。起始授权记录 SOA（Start Of Authority）表示一个授权区的开始；NS（Name Server）表示该记录存储了该域内的 DNS 服务器相关信息；A（Address）表示存储的是域内主机名对应的 ip 地址；CNAME（Canonical Name）记录为主机的规范名起了一个别名；MX（Mail Exchanger）记录了邮件服务器的域名及主机名相关信息……

2. DNS 报文格式

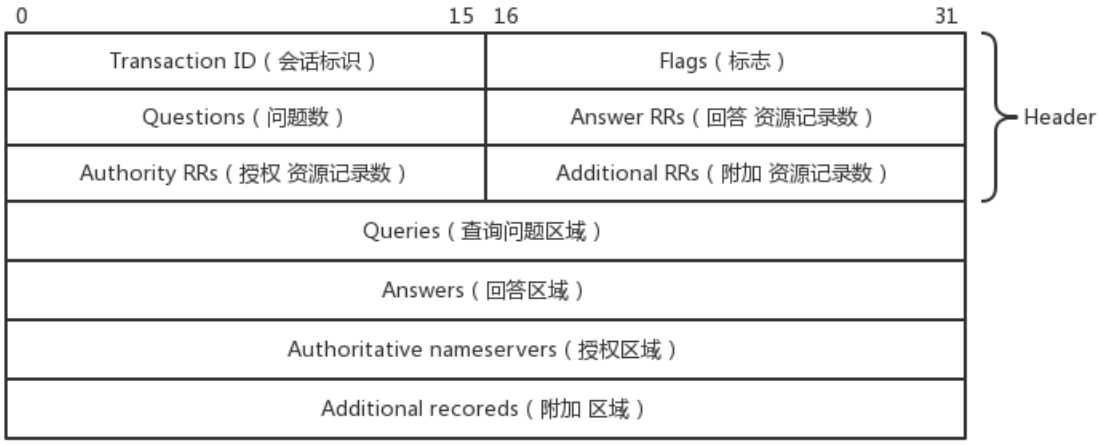


图 1

3. BIND

BIND（Berkeley Internet Name Domain）是目前使用最广泛的 DNS 服务器软件，支持现今绝大多数的操作系统（Linux，UNIX，Mac，Windows）。Linux 版本中，BIND 配置信息主要保存在“**/etc/named.conf**”(主配置文件)和“**/var/named/xxx.xxx.zone**“(dns 资源记录配置文件)中。

三 实验环境

右上角选择”**DNS**”，网络拓扑图如图 2 所示，两台主机所在子网网段为“**10.10.10.0/24**

“，其中一台主机为 Centos 7 系统（IP：**10.10.10.4**），用于搭建一个本地 DNS 服务器；另一台主机为 WinXp 系统（IP：**10.10.10.14**），用于测试 DNS 服务器和分析 DNS 数据报。（注：子网网段、IP 地址等信息会因具体的实验环境而不同。）

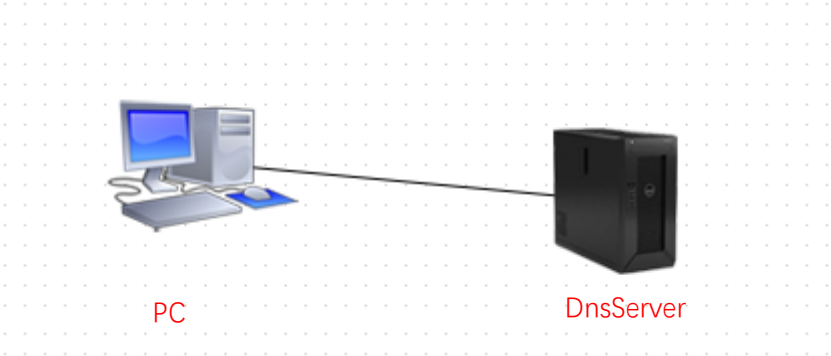


图 2

四 实验步骤

1. 配置 DNS 服务器

1）修改 BIND 主配置文件“**/etc/named.conf**“配置子网信息，更改 options---listen-on port 53 参数为 DNS 服务器地址。同时配置 options---allow-query 参数为实验环境中的子网网段。

```
options {
        listen-on port 53 { 10.10.10.14; };
//      listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { 10.10.10.0/24; };
```

2）在域名配置文件“**/etc/named.rfc1912.zones**“的最后面添加域名”**test.com**”。

```
zone "test.com" IN {
        type master;
        file "test.com.zone";
};
```

3）在”**/var/named**”文件夹下创建”**test.com.zone**”文件并添加资源记录。

```
$TTL 1D
$ORIGIN test.com.
@       IN SOA  test.com. root(
                                        0       ; serial
                                        1H      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      dnsserver
dnsserver       IN      A       10.10.10.14
www     IN      A       10.10.10.14
web     IN      CNAME   www
```

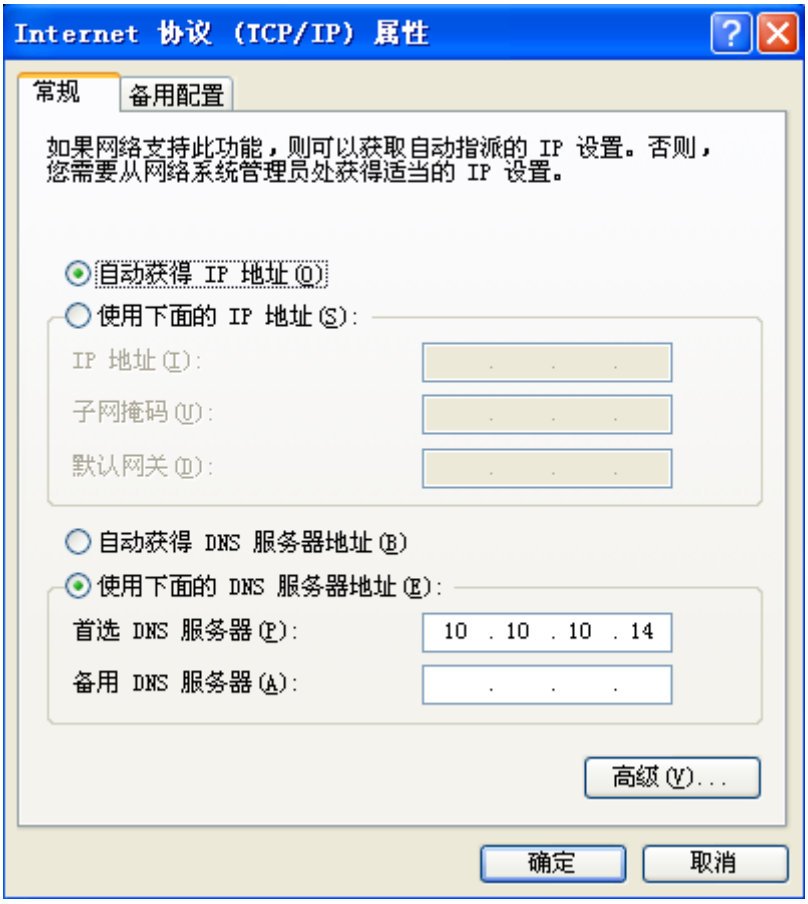
4) 改变"test.com.zone"文件的属主为 **named**，修改其权限为 **640**。

```
[root@dnsserver named]# chown named /var/named/test.com.zone
[root@dnsserver named]# chmod 640 /var/named/test.com.zone
```

5) 重启 BIND 服务：**systemctl restart named.service**

2. 测试 DNS 服务器

1）在 PC 主机中配置 DNS 服务器地址：开始---控制面板---运行---输入"ncpa.cpl"---本地连接（右键选择属性）---双击"Internet 协议(TCP/IP)"---更改服务器地址---确定---确定(本地连接属性窗口)。注意最后点击"本地连接 属性"窗口的确定按钮后配置才会生效。



2）打开"命令提示符"窗口，运行"**ipconfig /flushdns**"清空本地 dns 缓存记录，输入"**ipconfig /displaydns**"发现当前并没有与域名"xxx.test.com"对应的资源记录。

```
C:\Documents and Settings\admin>ipconfig /displaydns

Windows IP Configuration

        1.0.0.127.in-addr.arpa
        ----------------------------------------
        Record Name . . . . . : 1.0.0.127.in-addr.arpa.
        Record Type . . . . . : 12
        Time To Live  . . . . : 308494
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        PTR Record  . . . . . : localhost


        localhost
        ----------------------------------------
        Record Name . . . . . : localhost
        Record Type . . . . . : 1
        Time To Live  . . . . : 308494
        Data Length . . . . . : 4
        Section . . . . . . . : Answer
        A (Host) Record . . . : 127.0.0.1
```

打开 Wireshak 开始抓包，接着我们运行“**ping www.test.com**”，发现可以与 IP 地址为“**10.10.10.14**”的主机进行通信：

```
C:\Documents and Settings\admin>ping www.test.com

Pinging www.test.com [10.10.10.14] with 32 bytes of data:

Reply from 10.10.10.14: bytes=32 time<1ms TTL=64
Reply from 10.10.10.14: bytes=32 time<1ms TTL=64
Reply from 10.10.10.14: bytes=32 time<1ms TTL=64
Reply from 10.10.10.14: bytes=32 time<1ms TTL=64
```

再次运行“ipconfig /displaydns“查看本机 dns 缓存记录：

```
www.test.com
----------------------------------------
Record Name . . . . . : www.test.com
Record Type . . . . . : 1
Time To Live  . . . . : 86086
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 10.10.10.14


Record Name . . . . . : dnsserver.test.com
Record Type . . . . . : 1
Time To Live  . . . . : 86086
Data Length . . . . . : 4
Section . . . . . . . : Additional
A (Host) Record . . . : 10.10.10.14
```

很显然，PC 通过 DNS 服务器获取到了域“**www.test.com**”所对应的资源记录，同时还多出了“**dnsserver.test.com**”的资源记录，那么这是如何发生的呢？

3. 分析 DNS 工作原理

分析上述步骤中 Wireshark 所捕获的数据包我们会发现两条 DNS 报文：

```
992.259031000   10.10.10.4      10.10.10.14     DNS      72 Standard query 0xeae9  A www.test.com
992.259538000   10.10.10.14     10.10.10.4      DNS     128 Standard query response 0xeae9  A 10.10.10.14
```

其中一条是 PC 发往 DnsServer 的 DNS 请求报文，一条是 DnsServer 对 PC 的响应报文。首先查看请求报文的详细信息：

```
⊟ Domain Name System (query)
    [Response In: 65]
    Transaction ID: 0xeae9
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊟ www.test.com: type A, class IN
        Name: www.test.com
        Type: A (Host address)
        Class: IN (0x0001)
```

结合 DNS 报文结构分析发现，Questions 字段指明了请求的资源记录的数量为 1，Queries 字段包含着正在进行的查询信息，包含了主机名（Name）、资源记录类型（Type）。但是请求报文中并不包含 Answers、Authoritative nameservers 和 Additional records 等字段。

接下来我们查看响应报文的详细信息：

```
⊞ Flags: 0x8580 Standard query response, No error
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
⊞ Queries
⊟ Answers
  ⊟ www.test.com: type A, class IN, addr 10.10.10.14
      Name: www.test.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 1 day
      Data length: 4
      Addr: 10.10.10.14 (10.10.10.14)
⊟ Authoritative nameservers
  ⊟ test.com: type NS, class IN, ns dnsserver.test.com
      Name: test.com
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 1 day
      Data length: 12
      Name Server: dnsserver.test.com
⊟ Additional records
  ⊟ dnsserver.test.com: type A, class IN, addr 10.10.10.14
      Name: dnsserver.test.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 1 day
      Data length: 4
      Addr: 10.10.10.14 (10.10.10.14)
```

响应报文在 Answers 字段中给出了“www.test.com”对应的 IP 地址、TTL 等信息。除此之外，Authoritative nameservers 字段给出了我们在 DnsServer 中设置的权威服务器的记录；Additional records 包含了其他有帮助的记录。

五 思考

本实验简单配置了一个本地 DNS 服务器并利用其进行域名解析。然而，我们实际生活中使用的 DNS 其实是由大量的以层次结构组织起来的 DNS 服务器所构成的，请结合本章实验自行设计一个具有层次性结构的 DNS 域名系统。