

一、域名系统概述

域名系统DNS(Domain Name System)是因特网使用的命名系统，用来把便于人们使用的机器名字转换成为IP地址。域名系统其实就是名字系统。为什么不叫“名字”而叫“域名”呢？这是因为在这种因特网的命名系统中使用了许多的“域(domain)”，因此就出现了“域名”这个名词。“域名系统”明确地指明这种系统是应用在因特网中。

二、常见的资源记录类型

资源记录类型

A记录：地址记录(Address)

解释

将域名FQND (Fully Qualified Domain Name：全限定域名) 映射到IP正向解析。

，优先级相同时，表示轮循，可以达到负载均衡的目的，但需要服务商支持。

CNAME记录：别名记录，正式名记录(Canonical Name)

A记录优先于CNAME记录

。即如果一个主机地址同时存在A记录和CNAME记录，则CNAME记录不生效。

NS记录：域名服务记录(Name Service)

解析服务器记录。

用来表明由哪台服务器对该域名进行解析

。这
里的NS记录只对子域名生效

。

。

	NS记录优先于A记录 。即，如果一个主机地址同时存在NS记录和A记录，则A记录不生效。这里的NS记录只对子域名生效。
MX记录：邮件交换器(Mail Exchanger)	邮件交换器记录，用于告知邮件服务器进程将邮件发送到指定的另一台邮件服务器。
	，优先级相同时，表示轮循 ，可以达到负载均衡的目的，但需要服务商支持。
SOA记录：起始授权记录(Start Of Authority)	指出当前区域内谁是主DNS服务器
AAAA记录：(Ipv6)地址记录(Address)	把域名解析成IPv6地址。(FQDN->IPv6)；一个ipv4是32位，假设用A表示，那么128位长度的IPv6就用AAAA来表示。这个一个比较特殊。从IP到FQDN的解析。
PTR记录：指针(Pointer)，反向解析	

三、IP地址分类

类别	解释
A类IP地址	一个A类IP地址由1字节的网络地址和3字节主机地址组成，网络地址的最高位必须是“0”，地址范围从1.0.0.0~126.0.0.0 。可用的A类网络有126个，每个网络能容纳1亿多个主机。
B类IP地址	一个B类IP地址由2个字节的网络地址和2个字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从128.0.0.0~191.255.255.255

C类IP地址

。可用的B类网络有16382个，每个网络能容纳6万多个主机。

一个C类IP地址由3字节的网络地址和1字节的主机地址组成，网络地址的最高位必须是“110”

。范围从

192.0.0.0~

223.255.255.255

。C类网络可达209万余个，每个网络能容纳254个主机。

D类地址用于多点广播 (Multicast)

D类IP地址第一个字节以“11110”开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播 (Multicast) 中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。224.0.0.0到239.255.255.255用于多点广播。

E类

E类IP地址以“111110”开始，为将来使用保留。240.0.0.0到255.255.255.254，255.255.255.255用于广播地址。全零 (“0 . 0 . 0 . 0”) 地址对应于当前主机。全“1”的IP地址 (“255 . 255 . 255 . 255”) 是当前子网的广播地址

注意：数字0和 127不作为A类地址，数字127保留给内部回送函数，而数字0则表示该地址是本地宿主机，不能传送。

四、DNS查询常用工具使用 (dig、nslookup)

4.1、dig简单使用

4.1.1、简介

dig

是一个在类Unix命令行模式下查询DNS包括NS记录，A记录，MX记录等相关信息的工具。

4.1.2、dig 命令默认的输出信息可以分为 5 个部分。

- 第一部分显示 dig 命令的版本和输入的参数。
- 第二部分显示服务返回的一些技术详情，比较重要的是 status。如果 status 的值为 NOERROR 则说明本次查询成功结束。
- 第三部分中的 "QUESTION SECTION" 显示我们要查询的域名。
- 第四部分的 "ANSWER SECTION" 是查询到的结果。
- 第五部分则是本次查询的一些统计信息，比如用了多长时间，查询了哪个 DNS 服务器，在什么时间进行的查询等等。

4.1.2、简单使用

1) 查询CName记录

```
$ dig qq.com CNAME
```

2) 从指定的 DNS 服务器上查询

```
$ dig qq.com CNAME @8.8.8.8
```

如果不指定 DNS 服务器，dig 会依次使用 /etc/resolv.conf 里的地址作为 DNS 服务器

3) 控制显示结果，只显示DNS解析处理的ip地址

```
$ dig +short qq.com
```

4) 跟踪整个查询过程

```
$ dig +trace qq.com
```

5) 查询域的MX记录

```
$ dig qq.com MX
```

6) 查询域的TTL记录

```
$ dig qq.com TTL
```

7) 仅查询答案部分

```
$ dig qq.com +nocomments +noquestion +noauthority +noadditio
```

```
nal +nostats
```

8) 反向查询

```
dig -x 8.8.8.8 +short
```

4.2、nslookup

4.2.1、简介

nslookup

用于查询DNS的记录，查询域名解析是否正常，在网络故障时用来诊断网络问题

4.2.2、简单使用

1) 直接查询

```
?????nslookup domain[dns-server]
```

```
$ nslookup www.163.com
```

2) 查询其它记录 (以CNAME为例，查询其它记录也一样)

```
?????nslookup -qt=type domain[dns-server]type:      A -->????
      AAAA    -->????      AFSDB Andrew    -->?????????????      ATMA
-->ATM????      CNAME    -->????      HINHO    -->?????????????CPU????
??           ISDN    -->??????ISDN??      MB    -->?????????????      MG
-->??????      MINFO    -->????????????????      MR    -->?????????      MX
-->????????      NS    --> ?????????      PTR    ->?????      RP    -
->??????      RT    -->????????      SRV    -->TCP?????????      TXT    --
>????????????      X25    -->??????X.25?????
```

```
$ nslookup -qt=CNAME www.163.com
```

五、域名到IP地址的解析过程

linux DNS解析优先级配置

```
$ grep -C3 hosts /etc/nsswitch.conf
```

```
[root@Centos8-bridge-168-0-113 ~]# getent ahosts `hostname`
120.240.95.33 STREAM Centos8-bridge-168-0-113
120.240.95.33 DGRAM
120.240.95.33 RAW
[root@Centos8-bridge-168-0-113 ~]# ping `hostname`
```

最好在/etc/hosts文件中配置hostname跟本机ip映射

```
命令提示符
Wireless LAN adapter WLAN:
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wireless-AC 9560 160MHz
Physical Address. . . . . : 08-71-90-18-0E-C0
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::55bf:3028:e51c:4e0%22 (Preferred)
IPv4 Address. . . . . : 192.168.0.108 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 2021年7月6日 22:18:22
Lease Expires . . . . . : 2021年7月7日 23:52:53
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 168325520
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-22-83-3F-08-71-90-18-0E-C0
DNS Servers . . . . . : 192.168.0.1
                        8.8.8.8
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter 蓝牙网络连接:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : 08-71-90-18-0E-C4
```

在Linux下可以通过/etc/resolv.conf如下方式查询配置的DNS Server，如下图所示：