ＤＮＳ常用指令：

DIG(Domain Information Groper): 如dig 99yx.com，dig 99yx.com +trace，dig @ns1.dnsv3.com 99yx.com

Whois 99yx.com

Nslookup：在linux和windows都是默认安装的指令，用于检查域名，如：nslookup 99yx.com

Host：Linux常用指令，如：host -v 99yx.com

[root@host70-154 ~]# dig p.99yx.com

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> p.99yx.com

;; global options: printcmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4683

;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 2, ADDITIONAL: 6

;; QUESTION SECTION:

;p.99yx.com. IN A

;; ANSWER SECTION:

p.99yx.com. 5 IN A 222.187.220.138

p.99yx.com. 5 IN A 222.187.222.62

p.99yx.com. 5 IN A 218.93.205.145

;; AUTHORITY SECTION:

99yx.com. 250 IN NS ns2.dnsv3.com.

99yx.com. 250 IN NS ns1.dnsv3.com.

;; ADDITIONAL SECTION:

ns1.dnsv3.com. 87079 IN A 119.167.195.10

ns1.dnsv3.com. 87079 IN A 183.60.59.231

ns2.dnsv3.com. 87023 IN A 115.236.151.139

ns2.dnsv3.com. 87023 IN A 180.153.162.152

;; Query time: 45 msec

;; SERVER: 219.141.136.10#53(219.141.136.10)

;; WHEN: Wed Feb 29 22:25:02 2012

;; MSG SIZE rcvd: 214

QUESTION SECTION：查询的内容

ANSWER SECTION：相应的内容，一般会得到至少一条A记录，否则就还没定义

AUTHORITY SECTION：授权信息

ADDITIONAL SECTION：每个授权服务器的IP地址

SERVER：查询的dns服务器，可能会被缓存

[root@localhost ~]# nslookup s1.long.uu1758.com

Server: 211.155.23.88

Address: 211.155.23.88#53

Non-authoritative answer:

s1.long.uu1758.com canonical name = cls.long.my9yu.com.

Name: cls.long.my9yu.com

Address: 59.34.148.135

Name: cls.long.my9yu.com

Address: 115.238.54.189

Name: cls.long.my9yu.com

Address: 116.28.65.208

Linux域名配置： /etc/resolv.conf

[root@localhost ~]# less /etc/resolv.conf

nameserver 211.155.23.88

nameserver 211.155.27.88

DNS查询有两种方式：递归 和 迭代。DNS客户端设置使用的DNS服务器一般都是递归服务器，它负责全权处理客户端的DNS查询请求，直到返回最终结果。而DNS服务器之间一般采用迭代查询方式。以查询 zh.wikipedia.org 为例：

* 客户端发送查询报文"query zh.wikipedia.org"至DNS服务器，DNS服务器首先检查自身缓存，如果存在记录则直接返回结果。
* 如果记录老化或不存在，
  + - 1. 则DNS服务器向根域名服务器发送查询报文"query zh.wikipedia.org"，根域名服务器返回 .org 域的权威域名服务器地址。
      2. DNS服务器向 .org 域的权威域名服务器发送查询报文"query zh.wikipedia.org"，得到 .wikipedia.org 域的权威域名服务器地址。

**[权威域名服务器地址]，域名的销售服务商为基准。**

* + - 1. DNS服务器向 .wikipedia.org 域的权威域名服务器发送查询报文"query zh.wikipedia.org"，得到主机 zh 的A记录，存入自身缓存并返回给客户端。

Whois

一个域名的所有者可以通过查询WHOIS数据库而被找到；对于大多数根域名服务器， 基本的WHOIS由ICANN维护，而WHOIS的细节则由控制那个域的**域注册机构维护**。 对于240多个国家代码顶级域名(ccTLDs)，通常由该域名权威注册机构负责维护WHOIS。例如中国互联网络信息中心(China Internet Network Information Center)负责 .CN 域名的WHOIS维护，香港互联网注册管理有限公司(Hong Kong Internet Registration Corporation Limited) 负责 .HK 域名的WHOIS维护，台湾网络资讯中心 (Taiwan Network Information Center) 负责 .TW 域名的WHOIS维护。

DNS缓存：

Win下面

查看缓存：Ipconfig /displaydns

清楚缓存：Ipconfig /flushdns

WHOIS通常使用TCP协议43埠。每个域名或IP的WHOIS信息由对应的管理机构保存，例如，以.com结尾的域名的WHOIS信息由.com域名运营商VeriSign管理，中国国家顶级域名.cn域名由CNNIC管理。

根服务器最新地址：

<ftp://ftp.internic.net/domain/named.root>  
a.root-servers.net.--> m.root-servers.net.

顶级域TLD(Top Level Domain)

a.gtld-servers.net.

10个在美国,2个在欧洲,1个在日本.

主根服务器（A）美国1个，设置在弗吉尼亚州的杜勒斯；辅根服务器（B至M）美国9个，瑞典、荷兰、日本各1个。另外借由任播（Anycast）技术，部份根域名服务器在全球设有多个镜像点（mirror），因此可以抵抗针对其所进行的分散式阻断服务攻击（DDoS）。

GFW域名劫持  
  
从2002年左右开始，中国大陆的网络安全单位开始采用域名劫持（域名污染）技术，使用思科（Cisco）提供的路由器IDS监测系统来进行域名劫持，防止了一般民众访问被过滤的网站，2002年Google被封锁期间其域名就被劫持到百度。中国部分ISP也会通过此技术插入广告。  
  
对于含有多个IP地址或经常变更IP地址逃避封锁的域名，防火长城通常会使用此方法进行封锁。具体方法是当用户向DNS服务器提交域名请求时，DNS返回虚假（或不解析）的IP地址。  
  
全球一共有13组根域名服务器（Root Server），目前中国大陆有F、I這2个根域DNS镜像[7]，但现在均已因为多次DNS污染外国网络，威胁互联网安全和自由而被断开与国际互联网的连接。  
  
2010年3月，当美国和智利的用户试图访问热门社交网站如facebook.com、youtube.com和twitter.com等域名，他们的域名查询请求转交给中国控制的DNS根服务器处理，由于这些网站在中国被封锁，结果用户收到了错误的DNS信息，这意味着防火长城的DNS域名污染域名劫持已影响国际互联网。  
  
同年4月8日，中国大陆一个小型ISP的错误路由数据，经过中国电信的二次传播，扩散到了整个互联网，波及到了AT&T、Level3、Deutsche Telekom、Qwest Communications和Telefonica等多个国家的大型ISP。  
  
最后中国的根域名服务器被断开与国际互联网的连接。

2010年百度域名被劫持事件发生于2010年1月12日。当天，中国大陆最大中文搜索引擎公司百度被自称是伊朗网军（Iranian Cyber Army）的黑客组织入侵，导致网民无法正常登陆百度网站达8小时[1]。此次是百度成立以来最严重的服务器故障事件，且此事件造成百度直接损失超过700万人民币[2]。



电信ADSL劫持