



# DNS体系之\_\_基础

2017-07-18 ©mospan



## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## œ DNS是什么？

- ø 因特尔域名系统
- ø 提供域名到IP地址的映射，或反之
- ø 是分布式、C/S结构的服务
- ø 主要定义在RFC1034/1035上



## œ 为什么需要DNS?

- ø IP地址难以记忆与理解
- ø 邮件投递需要寻址 (MX)
- ø 域身份鉴定 (DomainKey, SPF)
- ø 负载均衡(轮询、最小连接)
- ø CDN、GSLB



## œ 什么是域(zone)与域名(domain)?

- ø “.”是域，是所有其他域的起始点
- ø 宇宙大爆炸：混沌初开，乾坤乃定





## œ 什么是域(zone)与域名(Domain)?

- ø com.、com.cn.、cn、net.是域
- ø mospan.cn.、mospx.com.也是域
- ø blog.mospan.cn.、www.mospx.com.是域名
- ø domain = host(主机名) + zone
- ø 标准的域名与主机名，只包括字母、数字、短横线和点
- ø 域名的最大长度为255个字符，单个label最大为63个字符



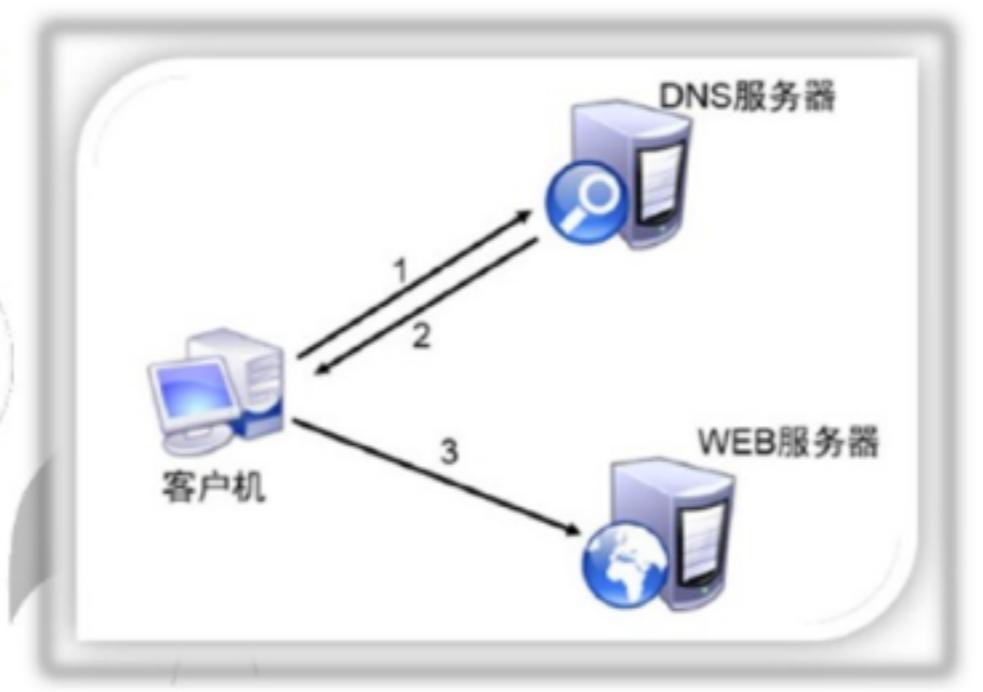
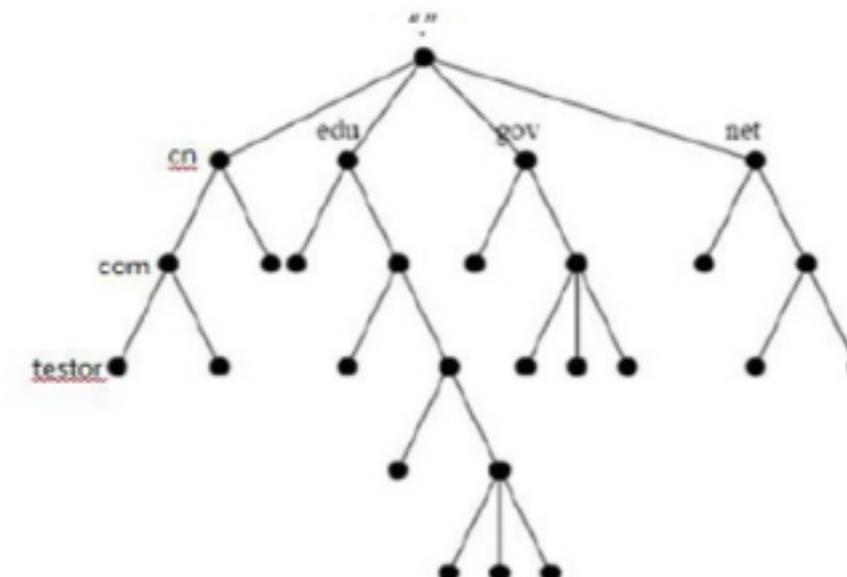
## ① DNS基本概念

### DNS基本概念

#### DNS组成

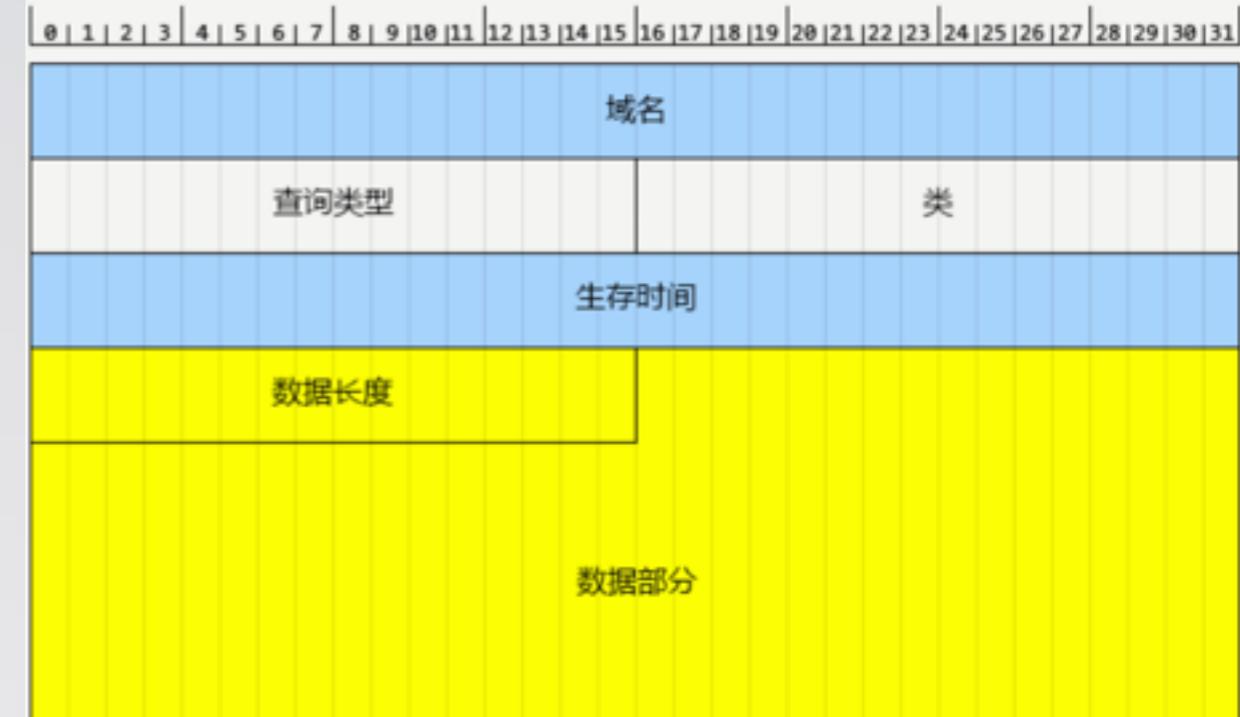
- 域名空间和资源记录，域名空间是一个树状结构，资源记录是与名字相关的一些数据
- 名字服务器，分缓存和授权服务器两类。

Resolver是向名字服务器提出查询请求  
并将结果返回给客户的程序





## œ DNS报文格式



```

Domain Name System (query)
[Response In: 6]
Transaction ID: 0xd6a9
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.baidu.com: type A, class IN
  Name: www.baidu.com
  [Name Length: 13]
  [Label Count: 3]
  Type: A (Host Address) (1)
  Class: IN (0x0001)

0000 00 88 2a e8 35 eb 08 00 27 fe a1 c2 08 00 45 00
0010 00 3b 23 48 00 00 80 11 00 00 c0 a8 58 69 ca 60
0020 80 56 04 02 00 35 00 27 04 f6 d6 a9 01 00 00 01
0030 00 00 00 00 00 03 77 77 77 05 62 61 69 64 75
0040 03 63 6f 6d 00 00 01 00 01

```

**Answers**  
 www.baidu.com: type CNAME, class IN, cname www.a.shifen.com  
 Name: www.baidu.com  
 Type: CNAME (Canonical NAME for an alias) (5)  
 Class: IN (0x0001)  
 Time to live: 600  
 Data length: 15  
 CNAME: www.a.shifen.com  
 www.a.shifen.com: type A, class IN, addr 14.215.177.38  
 Name: www.a.shifen.com  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 600  
 Data length: 4  
 Address: 14.215.177.38 (14.215.177.38)  
 www.a.shifen.com: type A, class IN, addr 14.215.177.37  
 Name: www.a.shifen.com  
 Type: A (Host Address) (1)  
 Class: IN (0x0001)  
 Time to live: 600  
 Data length: 4  
 Address: 14.215.177.37 (14.215.177.37)



## œ DNS RR(资源记录集)

```
root@bj94:~# dig +nocmd qint.cdn.clouddn.com +noall +answer
qint.cdn.clouddn.com. 586 IN CNAME tiny.china.qiniu.qnydns.net.
tiny.china.qiniu.qnydns.net. 3586 IN CNAME all.lv2.qnydns.net.
all.lv2.qnydns.net. 125 IN A 220.194.102.111
all.lv2.qnydns.net. 125 IN A 220.194.102.112
```

domain	ttl	class	type	rdata
--------	-----	-------	------	-------

ø domain: 最大长度为255个字符, 以点(.)进行分割

ø ttl: 缓存生存时间(单位: 秒), 4个字节

ø type: 常用有A、CNAME、MX、TXT等

详见: <https://ephem.me/2016/dns-rr/>



## œ ends-client-subnet

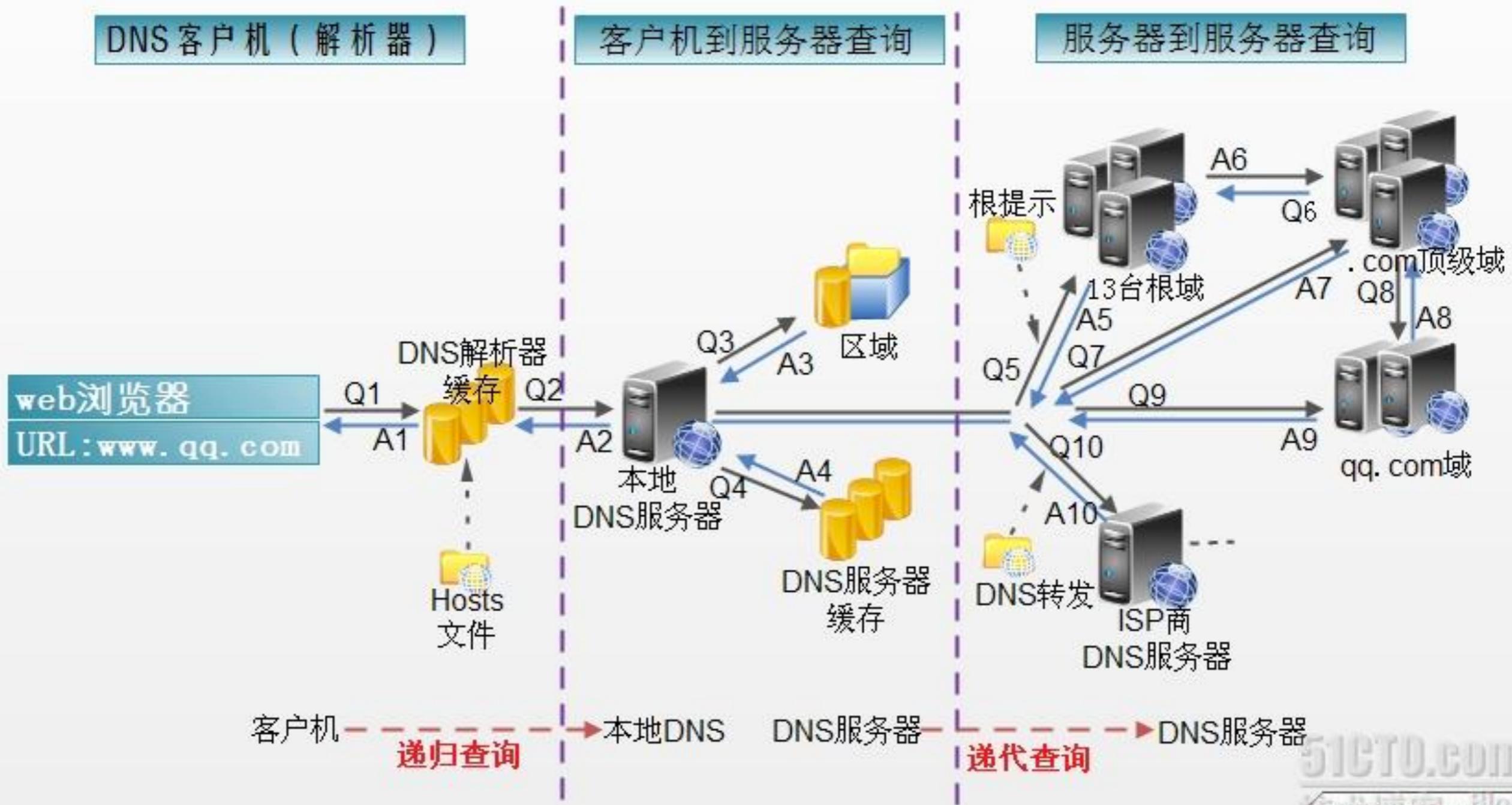
```
▼ Domain Name System (query)
  [Response In: 2177]
  Transaction ID: 0x5334
  ▶ Flags: 0x0120 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 1
  ▶ Queries
  ▼ Additional records
    ▶ <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    ▶ Z: 0x0000
      0... .... .... .... = DO bit: Cannot handle
      .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 11
    ▶ Option: CSUBNET - Client subnet
      Option Code: CSUBNET - Client subnet (8)
      Option Length: 7
      Option Data: 00011800780000
      Family: IPv4 (1)
      Source Netmask: 24
      Scope Netmask: 0
      Client Subnet: 120.0.0.0
  ▶ Answers
    ▶ www.zhxfei.com: type A, class IN, addr 10.0.0.1
      Name: www.zhxfei.com
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 86400
      Data length: 4
      Address: 10.0.0.1
  ▶ Authoritative nameservers
  ▶ Additional records
    ▶ ns.zhxfei.com: type A, class IN, addr 172.16.130.129
    ▶ <Root>: type OPT
      Name: <Root>
      Type: OPT (41)
      UDP payload size: 4096
      Higher bits in extended RCODE: 0x00
      EDNS0 version: 0
    ▶ Z: 0x0000
      0... .... .... .... = DO bit: Cannot handle DNSSEC
      .000 0000 0000 0000 = Reserved: 0x0000
      Data length: 11
    ▶ Option: CSUBNET - Client subnet
      Option Code: CSUBNET - Client subnet (8)
      Option Length: 7
      Option Data: 00011818780000
      Family: IPv4 (1)
      Source Netmask: 24
      Scope Netmask: 24
      Client Subnet: 120.0.0.0
```

详见：<http://www.cnblogs.com/cobbliu/p/3188632.html>



# œ DNS解析过程

DNS的查询过程





## œ DNS组织机构

### ø ICANN(互联网名称与数字地址分配机构)

- ø IP地址分配
- ø 协议标识符的指派
- ø 通用顶级域名 (gTLD) 管理
- ø 国家和地区顶级域名 (ccTLD) 系统的管理
- ø 根服务器系统的管理





## œ DNS组织机构

ø Registry: 注册局。

ø 维护区数据、委托注册机构提供注册服务。(**CNNIC**)

ø Registrar: 注册机构。

ø 代表注册局提供注册服务。(万网、新网)

ø Registrant: 域名所有者。

ø 托管机构: 为域名所有者提供域名托管服务。(**dnsPod、XNS**)



## œ DNS组织机构

### ø 根服务器。

- ø 全球有13个根服务器，每个根服务器由不同的机构管理，每个服务器都有若干的镜像，使用anycast技术提供就近访问。
- ø 大部分服务器在美国，北京和香港有根的镜像服务器。
- ø 根区的内容由ICANN管理，除了现有的TLD，ICANN已经开放了顶级域的注册。



## œ DNS组织机构

ø 全球有13台根服务器(242节点)。

∂ a.root-servers.net. ~m.root-servers.net.。

∂ 美国10台

  β A(Verisign, 6); B(ISI, 1)

  β C(Cogent, 6); B(UMD, 1)

  β E(NASA, 1); B(ISC, 49)

  β G(DOD, 6); H(US Army, 2)

  β J(Verisign, 70); H(ICANN, 39)

∂ 欧洲2台

  β J(RIPE NCC, 18); H(SE, 33)

∂ 日本1台

  β M(WIDE, 6)



## œ DNS组织机构

### ø 根服务器分布。





## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## œ DNS服务器组成

### ø 域名注册服务器

ø 代表注册局提供注册服务。(万网、新网)

### ø 递归DNS服务器

ø 包含ISPDNS、public DNS、自建本地DNS。

### ø 授权DNS服务器

ø 包含根DNS服务器、各级授权DNS。



## œ 域名注册服务器

### ø 域名怎么得来?

ø 需到域名注册商网站上注册申请。(万网、新网)

### ø 域名注册协议

ø RRP协议(RFC2832)、EPP协议(RFC3731)

### ø 域名状态

**Active:** 正常状态  
**Server Hold:** 注册局暂停，域名没有解析，可以续费；  
**Server Update prohibited:** 注册局禁止更新，不能修改，可以续费；  
**Server Transfer prohibited:** 注册局禁止转移，不能转移注册商；  
**Server Delete prohibited:** 注册局禁止删除；  
**Server Renew prohibited:** 注册局禁止续费；  
**Client Hold:** 注册商暂停，域名没有解析，可以续费；  
**Client Update prohibited:** 注册商禁止更新，不能修改，可以续费；  
**Client Transfer prohibited:** 注册商禁止转移，不能转移注册商；  
**Client Delete prohibited:** 注册商禁止删除；  
**Client Renew prohibited:** 注册商禁止续费；  
**Redemptionperiod:** 偿还期，域名过期后由注册商申请删除域名，域名进入偿还期，偿还期 30天内不能正常使用，但可以交纳赎回费用恢复  
**Pendingdelete:** 域名30天偿还期后进入5天的删除期，删除期不允许其他人注册，此状态表明域名即将被删除释放。  
**Pending Transfe:** 域名处理于转移状态。

详见：[https://help.aliyun.com/knowledge\\_detail/35793.html](https://help.aliyun.com/knowledge_detail/35793.html)



## ø whois服务器

### ø whois是什么？

ø 谁是（Who is）这个域名或IP地址的负责人与注册信息？

### ø whois查询

```
root@bj94:~# whois mospan.cn
Domain Name: mospan.cn
ROID: 20160116s10001s81249326-cn
Domain Status: ok
Registrant ID: hc3268400991209
Registrant: 莫
Registrant Contact Email: mospan.cn@163.com
Sponsoring Registrar: 阿里云计算有限公司（万网）
Name Server: lv3ns1.ffdns.net
Name Server: lv3ns2.ffdns.net
Name Server: lv3ns3.ffdns.net
Name Server: lv3ns4.ffdns.net
Registration Time: 2016-01-16 13:35:49
Expiration Time: 2018-01-16 13:35:49
DNSSEC: unsigned
root@bj94:~#
```

```
# start
NetRange:      8.8.8.0 - 8.8.8.255
CIDR:          8.8.8.0/24
NetName:        LVLT-GOGL-8-8-8
NetHandle:     NET-8-8-8-8-1
Parent:         LVLT-ORG-8-8 (NET-8-8-8-1)
NetType:        Reallocated
OriginAS:
Organization:   Google Inc. (GOGL)
RegDate:       2014-03-14
Updated:        2014-03-14
Ref:           https://whois.arin.net/rest/net/NET-8-8-8-1

OrgName:        Google Inc.
OrgId:          GOGL
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:    94043
Country:        US
RegDate:       2000-03-30
Updated:        2017-01-28
Ref:           https://whois.arin.net/rest/org/GOGL
```

### ø 用途

ø 判断域名是否接管、到期等



## œ DNS服务器组成

### ø 递归DNS服务器

- ø 主要功能有缓存、递归、转发、ACL、广告植入
- ø 缓存设计要点：大容量，高命中，老化回收，预取、请求合并
- ø 递归设计要点：多递归关联递归、超时处理、状态处理、递归合并
- ø ISPDNS优点：距离近响应快、调度准确
- ø PUBDNS优点：支持EDNS0、BGP-anycast、防劫持



## œ DNS服务器组成

### ø 权威DNS服务器

- ø 主要功能有常规记录、301/302/LINK跳转、subzone、域名绑定
- ø 设计要点：解析精准、生效快体验好、稳定高性能，安全易运维
- ø 调优点：节点本地覆盖、协议标准可兼容



## ① DNS服务器组成

### Ø 注册权威DNS服务器

### Ø 配置胶水记录

注册新的DNS

\*填写DNS名字: ns301 mophya.com  
例如: ns1.xinnetdns.com

\*ip地址: 121 . 15 . 220 . 16  
例如: 202.108.32.110

### Ø 检查注册信息(<http://www.internic.net/whois.html>)

Whois Search Results

Search again (.aero, .arpa, .asia, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, or .travel):  
**ns301.qnydns.net**

Domain (ex. internic.net)  
 Registrar (ex. ABC Registrar, Inc.)  
 Nameserver (ex. ns.example.com or 192.0.2.53)

Submit

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

Server Name: NS301.QNYDNS.NET  
IP Address: 121.15.220.16  
Registrar: BIZCN.COM, INC.  
Whois Server: whois.bizcn.com  
Referral URL: <http://www.bizcn.com>



# DNS组成



## œ DNS服务器组成

### ø 权威DNS效果

### ø 全网性能

运营商	监测点数	DNS时间(秒)				
		均值	最好		最差	
dr...监测一天	104778	0.131	四川省-中国移动	0.000	江苏省-中国移动	0.955
牛ns监测一天	104958	0.107	福建省-长城宽带	0.009	辽宁省-中国电信	0.593
...x...监测一天	104763	0.139	福建省-长城宽带	0.000	广东省-长城宽带	0.891

### ø 全网可用性

省份	dr...监测一天			牛ns监测一天			...x...监测一天		
	DNS时间(秒)	可用性(%)	监测点数	DNS时间(秒)	可用性(%)	监测点数	DNS时间(秒)	可用性(%)	监测点数
平均/汇总	0.131	83.61	104778	0.107	99.78	104958	0.139	85.92	104763
排除点数	0			0			0		



## œ DNS服务器组成

### ø 权威DNS服务器托管域名

### ø 注册商处修改NS

修改域名DNS

使用新网DNS提供解析服务（注：新网每组DNS服务器都具有同等效能）  
 使用非新网DNS（注：最少配置两个DNS服务器名称以保证域名能够正常解析，DNS服务器名称不分先后，请输入有效的DNS服务器名称。）

主DNS: ns301.qnydns.net

辅DNS: ns302.qnydns.net

DNS3: ns303.qnydns.net

DNS4: ns304.qnydns.net

### ø 配置解析记录并检查解析结果

```
[root@jumpbox:~$ dig +nocmd www.mophya.com @ns301.qnydns.net +noall +answer +authority
www.mophya.com.      600    IN     A      3.3.3.3
www.mophya.com.      600    IN     A      4.4.4.4
www.mophya.com.      600    IN     A      1.1.1.1
www.mophya.com.      600    IN     A      2.2.2.2
mophya.com.          3600   IN     NS     ns302.qnydns.net.
mophya.com.          3600   IN     NS     ns303.qnydns.net.
mophya.com.          3600   IN     NS     ns304.qnydns.net.
mophya.com.          3600   IN     NS     ns301.qnydns.net.
```



## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## œ 递归DNS

### ø DNS劫持

∂ 取得服务器或域名的控制权进行记录篡改

### ø 缓存投毒

∂ 传统方式污染Answer区 (防范：ID与源端口随机)

∂ Kaminsky方式污染Authority区

### ø 0X20技术

∂ 请求域名随机大小写(现实中还需配合白名单)



## œ 授权DNS

### ø 系统漏洞

∂ 例如前年的TKEY攻击

### ø DDOS攻击

∂ 主机耗尽型(虚假源、随机域名、泛域名攻击)

∂ 带宽耗尽型(反射攻击)

### ø 根服务器安全

∂ 使用不同的解析软件

∂ 镜像节点多



## œ查看全球正发生攻击



<http://map.norsecorp.com/>



## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## œ DNS与CDN

### ø CDN利用DNS的CNAME记录

```
moshengping@jumpbox:~$ dig +nocmd ni.ppsrc.com +noall +answer
ni.ppsrc.com.      526   IN    CNAME  iduzk3v.qiniudns.com.
iduzk3v.qiniudns.com. 526   IN    CNAME  tiny.china.qiniu.qnydns.net.
tiny.china.qiniu.qnydns.net. 1779 IN    CNAME  all.lv2.qnydns.net.
all.lv2.qnydns.net.   65    IN    A     183.136.218.207
all.lv2.qnydns.net.   65    IN    A     183.131.87.16
all.lv2.qnydns.net.   65    IN    A     183.131.87.17
all.lv2.qnydns.net.   65    IN    A     183.136.218.206
```

### ø CDN利用DNS的A记录、负载均衡

### ø CDN利用DNS的edns-client-subnet

### ø CDN的DNS调度占比90%+



## ➤ 目录

1

### DNS常识

2

### DNS组成

3

### DNS安全

4

### DNS与CDN

5

### DNS未来



## œ DNS未来

### ø DNS缓存刷新

◊ 都是我的错， 请你❤上我

### ø DNSSEC发展

◊ 天下熙熙 皆为利来 天下壤壤 皆为利往

### ø DNS与区块链

◊ 合久必分， 分久必合

### ø DNS会消亡么？

◊ 物壮则老， 是谓不道， 不道早已



谢谢欣赏！

