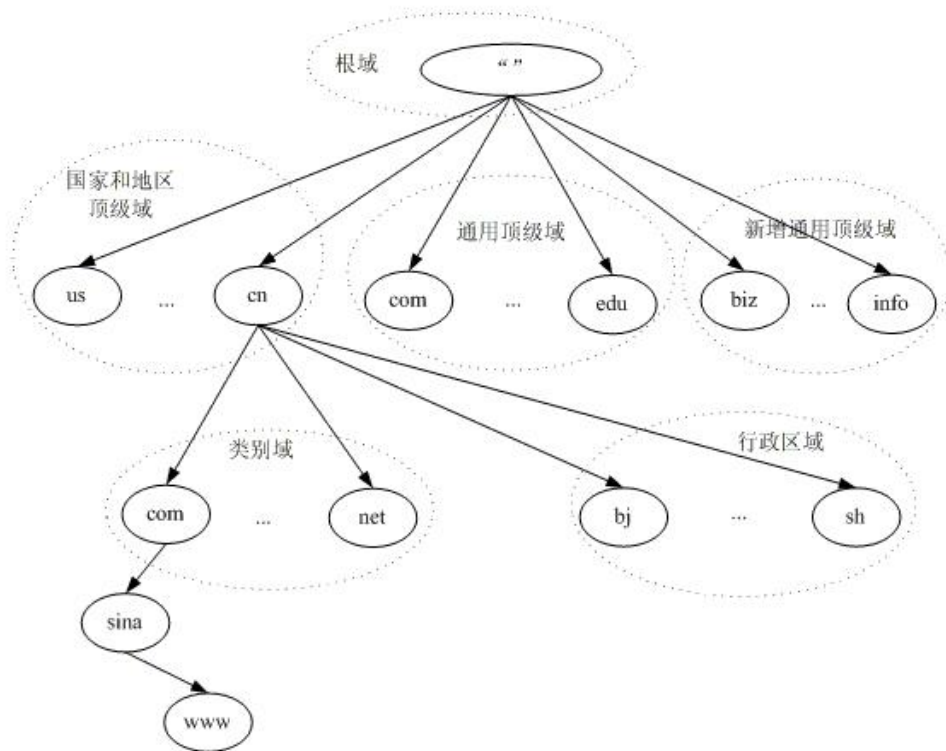


DDNS

1. DNS 原理

DNS 最核心的工作就是域名解析，也就是把计算机名翻译成 IP 地址

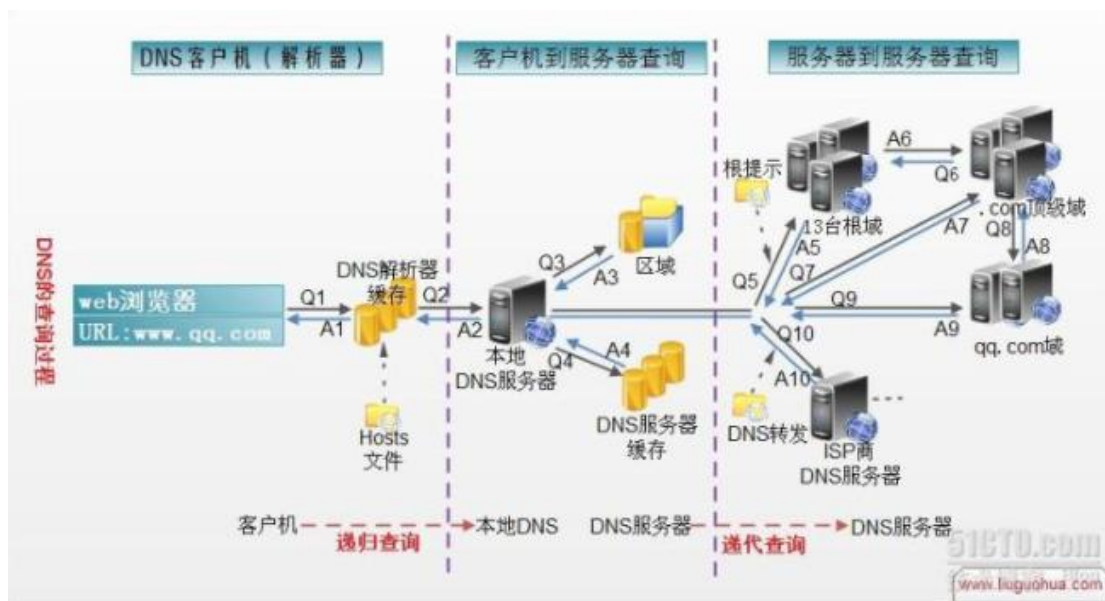
(1) DNS 采用的是分布式解决方案



(2) DNS 查询类型

递归查询：一次查询就得到最终的结果，通常是客户端与本地 DNS 服务器之间会使用递归查询

迭代查询：有可能发生多次请求，且每次得到的结果有可能只是参考答案，通常是 DNS 服务器直接会使用迭代查询



步骤解析

- (1) 本地发起请求后,先查询本机 DNS 缓存和本地 host 文件是否又域名对应的 IP 地址。查询本地缓存命令 `ipconfig /displaydns`。清除 DNS 缓存命令 `ipconfig /flushdns`。本地 host 文件路径 `C:\Windows\System32\drivers\etc`
- (2) 本地没有发现缓存, 然后向本机 DNS 服务器发送请求, 服务器收到请求后查询是否又对应的记录, 如果没有的话, 就会向 13 台根域名服务器发送请求。本机 DNS 服务器就是电脑上获取到的 DNS
- (3) 根域名服务器收到请求后, 查询出顶级域名所在的服务器, 然后告诉本机顶级域名服务器的 IP 地址

本机继续查询该 IP 地址, 以此类推最终查询出 IP 地址

2. 域名的组成

主机名.次级域名.顶级域名.根域名

主机域名: 用户自定义, 一般为 `www`。又称三级域名

次级域名: 用户注册

顶级域名: `.com .net .cn`

根域名: 根域名都是统一的, 所有在常见的链接中都是隐藏了的。世界上存在 13 台根服务器, 从 `A.ROOT-SERVERS.NET` 一直带 `M.ROOT-SERVERS.NET`

3. DNS 报文分析

(1) DNS 请求报文

Domain Name System (query)

[Response In: 62]

Transaction ID: 0xc6f8

Flags: 0x0100 Standard query

- 0... .. = Response: Message is a query
- .000 0... .. = Opcode: Standard query (0)
-0. = Truncated: Message is not truncated
-1 = Recursion desired: Do query recursively
-0.. = Z: reserved (0)
-0 = Non-authenticated data: Unacceptable

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)

(2) DNS 回答报文

Domain Name System (response)

[Request In: 13]

[Time: 0.041360000 seconds]

Transaction ID: 0xc718

Flags: 0x8180 Standard query response, No error

- 1... .. = Response: Message is a response
- .000 0... .. = Opcode: Standard query (0)
-0. = Authoritative: Server is not an authority for domain
-0. = Truncated: Message is not truncated
-1 = Recursion desired: Do query recursively
-1... .. = Recursion available: Server can do recursive queries
-0.. = Z: reserved (0)
-0. = Answer authenticated: Answer/authority portion was not authenticated by the server
-0 = Non-authenticated data: Unacceptable
-0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 3

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)

Answers

- www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
- www.a.shifen.com: type A, class IN, addr 180.97.33.107
 - Name: www.a.shifen.com
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)
 - Time to live: 34
 - Data length: 4
 - Address: 180.97.33.107
- www.a.shifen.com: type A, class IN, addr 180.97.33.108

(3) 报文解析（首部区域）

- ① QR(1 比特): 查询/响应的标志位, 1 为响应, 0 为查询

- ② **opcode(4 比特)**: 定义查询或响应的类型(若为 0 则表示是标准的, 若为 1 则是反向的 (用 IP 查询域名))。
- ③ **AA(1 比特)**: 授权回答的标志位。该位在响应报文中有效, 1 表示名字服务器是权限服务器, 指出给出应答的服务器是查询域名的授权解析服务器
- ④ **TC(1 比特)**: 截断标志位。1 表示响应已超过 512 字节并已被截断
- ⑤ **RD(1 比特)**: 该位为 1 表示客户端希望得到递归回答
- ⑥ **RA(1 比特)**: 1 为应答服务器支持递归查询 (根服务器不支持递归)
- ⑦ **zero(3 比特)**: 保留字段
- ⑧ **rcode(4 比特)**: 返回码, 表示响应的差错状态, 通常为 0 和 3, 各取值含义如下:
 - 1) 0 无差错
 - 2) 1 格式差错 - 服务器不能理解请求的报文
 - 3) 2 问题在域名服务器上 - 因为服务器的原因导致没办法处理这个请求
 - 4) 3 域参照问题 - 只有对授权域名解析服务器有意义, 指出解析的域名不存在
 - 5) 5 请求被服务器拒绝

(2) 报文解析 (回答区域)

包含正在进行的查询信息。包含查询名(被查询主机名字的名字字段)、查询类型、

查询类

- ① 查询类型
- ② 通常查询类型为 A(由名字获得 IP 地址)或者 PTR(获得 IP 地址对应的域名)

③ 查询类：通常为 1，指 Internet 数据

④ 额外还有生存时间：用于指示该记录的稳定程度，极为稳定的信息会被分配一个很大的值(如 86400，一天的秒数)。该字段表示资源记录的生命周期(以秒为单位)

4. DDNS 原理

- (1) 基本原理：将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候，客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务程序负责提供 DNS 服务并实现动态域名解析。就是说 DDNS 捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样域名就可以始终解析到非固定 IP 的服务器上，互联网用户通过本地的域名服务器获得网站域名的 IP 地址，从而可以访问网站的服务
- (2) 设备：DDNS 客户端（路由器或者开启了 DDNS 服务的 PC），DDNS 服务器（花生壳）
- (3) 设备功能：客户端负责动态更新域名和 IP 地址对应关系，服务器负责通知 DNS 服务器动态更新域名和 IP 地址之间的对应关系
- (4) 注：开启 DDNS 服务只是针对公网 IP，也就是说公网 IP 变化了之后，DDNS 服务器才会更新 IP 与域名的对应关系。开启了 DDNS 后，如果 web 服务是在内网中，则还需要增加端口转发功能才能正常使用 DDNS 服务
- (5) DDNS 服务商：提供公网 DDNS 服务，其中包括响应服务器和 DNS 服务器。响应服务器负责接收 DDNS 客户端的请求解析动态域名，DNS 服务器提供 DNS 服务

扩展

获取当前 IP 地址是否发生变化的方式有两个：定期轮询和异步实现（当 IP 发生变化时主动上报）

异步实现时，当 IP 发生变化，客户端将发送指令，删除旧的 IP 与域名的对应关系，然后增加新的 IP 与域名的关系