

DNS原理图解

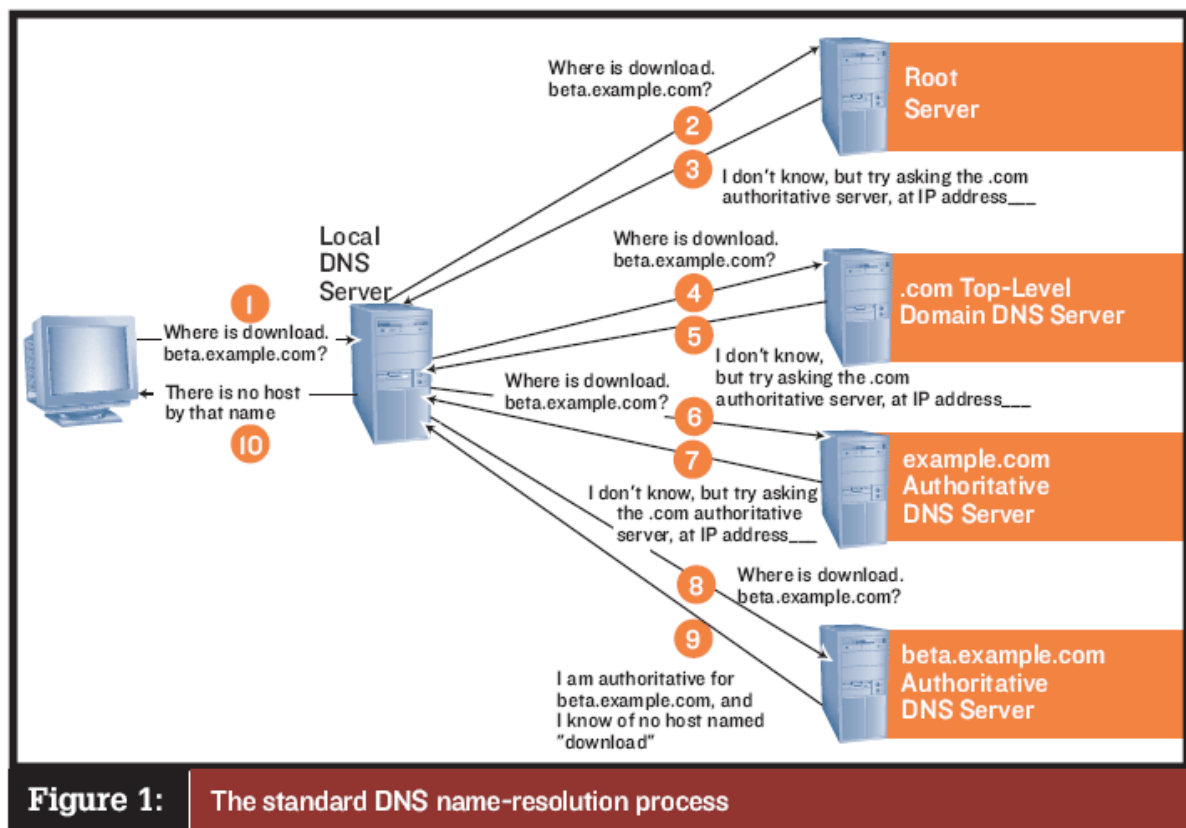
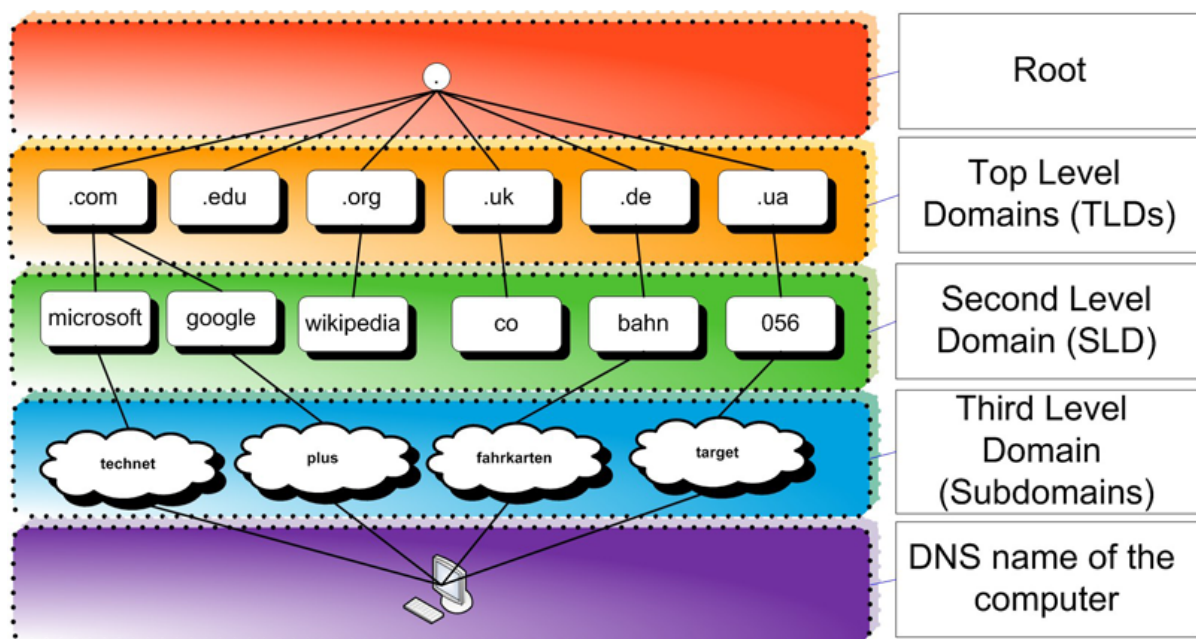


Figure 1: The standard DNS name-resolution process

DNS(Domain Name System),网域名称系统，是互联网上基础性的服务。DNS将域名和网络服务器的IP地址相互映射，并将这些数据保存至DNS服务器。两台主机的通信事实上是依赖于IP地址，而不是域名，IP地址非常不方便于人类记忆，域名的产生，极大的方便了访问互联网。

相关概念

域名的组织结构



域名采用层次化结构进行组织，如上图。每个点代表一个层次，例如 `www.xuejinwei.com`。最后面的“.”代表**根域**，常常省略。`.com`是顶级域。`xuejinwei.com`是二级域。

子域是一个相对概念，是更大网域的一部分。例如 `xuejinwei.com` 是 `.com` 的子域，`www.xuejinwei.com` 是 `xuejinwei.com` 的子域，子域也是一个网域。

DNS查询方式

递归查询：客户端向本地DNS服务器发出请求后，一直处于等待状态，直到本地名称服务器返回查询结果。以 `www.xuejiwnei.com` 为例叙述递归查询过程。当客户端向本地名称服务器发出请求后，本地名称服务器查询本机缓存，如果有记录，则直接返回；如果没有，则本地DNS服务器以客户端的角色将查询请求发给根名称服务器，根名称服务器通过查询返回给本地DNS服务器 `.com` 顶级名称服务器的IP地址；本地DNS服务器收到 `.com` 顶级名称服务器的IP地址后继续向 `.com` 顶级名称服务器发出请求，顶级名称服务器收到请求后查询缓存，如果有记录则直接返回本地DNS服务器，如果没有，则返回 `xuejinwe.com` 二级名称服务器的IP地址；本地名称服务器继续发出请求，二级名称服务器同样查找缓存，返回 `www.xuejinwei.com` 的IP地址。

迭代查询：客户端和本地DNS服务器的查询方式就属于迭代查询，客户端发出查询请求后，处于等待状态，直到本地DNS服务器返回确定回复或否定答复。

DNS服务器类型

1. **主域名服务器(primary name server)**。从域管理员构造的本地磁盘文件中加载域信息，该文件（区域文件）包含着该服务器具有管理权的一部分域结构的最精确信息。主服务器是一种权威性服务器，因为它以绝对的权威去回答对其管辖域的任何查询。
2. **从域名服务器(secondary name server)**。它可从主服务器中复制一整套域信息。区文件是从主服务器中复制出来的，并作为本地磁盘文件存储在辅助服务器中。这种复制称为"区域文件复制"。在辅助域名服务器中有一个所有域信息的完整拷贝，可以有权权威地回答对该域的查询。因此，辅助域名服务器也称作权威性服务器。配置辅助域名服务器不需要生成本地区文件，因为可以从主服务器中下载该区文件。
3. **缓存名称服务器(caching-only server)**。可运行域名服务器软件，但是没有域名数据库软件。它从某个远程服务器取得域名服务器查询的结果，一旦取得一个，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。高速缓存服务器不是权威性服务器，因为它提供的所有信息都是间接信息。当 BIND 被配置为缓存服务器的时候，它只会回应已缓存的请求，并将所有其他的请求转发到上游的 DNS 服务器。缓存名称服务器只需要 `cache` 这个zone file文件即可。
4. **转发名称服务器(forwarding DNS)**。转发域名服务器需要指定上层DNS服务器作为转发目标，转发名称服务器甚至不需要 `cache` 这个zone file文件，全部查询都交给上层DNS服务器进行查询。

解析类型

正向解析：通过域名查找IP的过程

反向解析：通过IP查找域名的过程

FQDN

(Fully Qualified Domain Name)完全合格域名/全称域名，唯一地标识在 DNS 分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。

DNS资源记录类型

DNS服务器数据库中每一个条目都是一个资源记录（Resource Record，RR）。资源记录格式中的域名可以写成FQDN格式，也可以写成主机名，写成主机名格式时，会自动补上区域名称，@表示区域名称。

1. SOA` (Start of Authority)，SOA名叫起始授权机构记录，SOA记录说明了在众多NS记录里那一台才是主要的服务器。

```
1 #格式
2 ZONE_NAME      IN   SOA FQDN      admin_mailbox  (
3     sereial number
4     refresh
5     retry
6     exprise
7     na ttl )
8 #示例
9 @    600 IN   SOA dns.xuejinwei.com.
      jinweiayy.gmail.com (
10     2017021701
11     1H
12     2M
13     1W
14     1D )
```

sereial number：序列号。从DNS服务器通过此序列号传送区域数据文件

refresh：刷新时间。从DNS服务器多久检查一次主服务器的区域文件

retry: 重试时间。如果从DNS服务器连接主DNS服务器连接失败多久重新连接

expire: 过期时间。如果从DNS服务器重试超过这个时间, 则放弃连接主DNS服务器

negative answer TTL: 否定答复的TTL

注意: ZONE_NAME为区域名称, 例如: xuejinwei.com., 通常可以简写为@符号; 时间单位: 默认是秒。M是分钟、H是小时、D是天; SOA必须是区域数据库文件的第一条记录; 邮箱中出现@符号换成. 符号; 可以使用宏定义例如: `$TTL 600` 表示默认的TTL值。

2.NS (Name Server), 域名服务器记录, 用来指定该域名由哪个DNS服务器来进行解析。NS记录必须要有一条A记录, 指明DNS服务器的IP地址。NS记录可以写多条。

```
1 #示例
2 @ 600 IN NS dns.xuejinwei.com.
```

3..A记录也称为主机记录。将域名指向一个IPv4地址, 一个域名可以创建多个不同的IPv4地址。

```
1 #示例
2 www IN A xxx.xxx.xxx.xxx
```

4.AAAA记录将DNS域名指向一个IPv6的IP地址。

5.MX (Mail exchanger), 邮件服务记录。

```
1 #示例
2 xuejinwei.com. 600 IN MX 10 mail.xuejinwei.com.
3 mail.xuejinwei.com. 600 IN MX xxx.xxx.xxx.xxx
```

6.PTR, 通常出现在反向解析文件中。逆向的主机地址, 即主机地址要反过来写。例如, 完全格式为: `7.100.16.172.in-addr.arpa.`

参考

维基百科-域名: <https://zh.wikipedia.org/wiki/%E5%9F%9F%E5%90%8D>

DNS 的 SOA 记录简介:http://www.sigma.me/2011/01/01/about_dns_soa.html