10-1 加餐 - DNS 与 ICMP

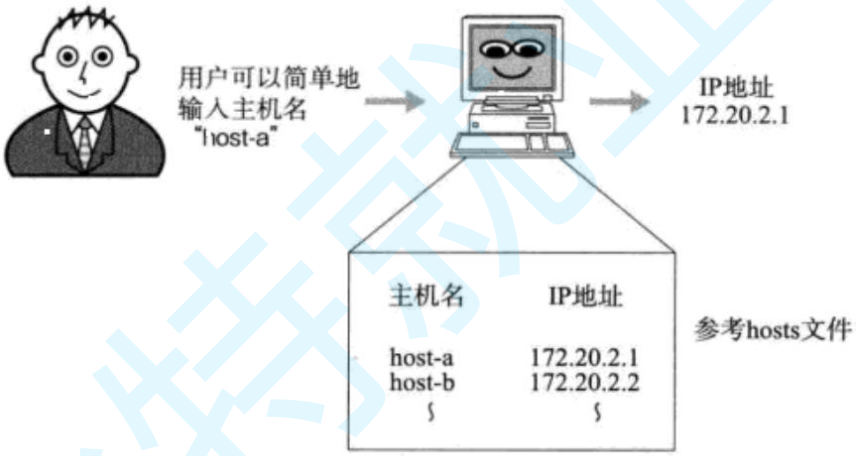
DNS(Domain Name System)快速了解

DNS 是一整套从域名映射到 IP 的系统

DNS 背景

TCP/IP 中使用 IP 地址和端口号来确定网络上的一台主机的一个程序. 但是 IP 地址不方便记忆.

于是人们发明了一种叫主机名的东西, 是一个字符串, 并且使用 hosts 文件来描述主机名和 IP 地址的关系.



最初, 通过互连网信息中心(SRI-NIC)来管理这个 hosts 文件的.

- 如果一个新计算机要接入网络, 或者某个计算机 IP 变更, 都需要到信息中心申请变更 hosts 文件.
- 其他计算机也需要定期下载更新新版本的 hosts 文件才能正确上网.

这样就太麻烦了, 于是产生了 DNS 系统.

- 一个组织的系统管理机构, 维护系统内的每个主机的 IP 和主机名的对应关系.
- 如果新计算机接入网络, 将这个信息注册到数据库中;
- 用户输入域名的时候, 会自动查询 DNS 服务器, 由 DNS 服务器检索数据库, 得

> 到对应的 IP 地址.

至今, 我们的计算机上仍然保留了 hosts 文件. 在域名解析的过程中仍然会优先查找 hosts 文件的内容.

```
C
cat /etc/hosts
```

域名简介

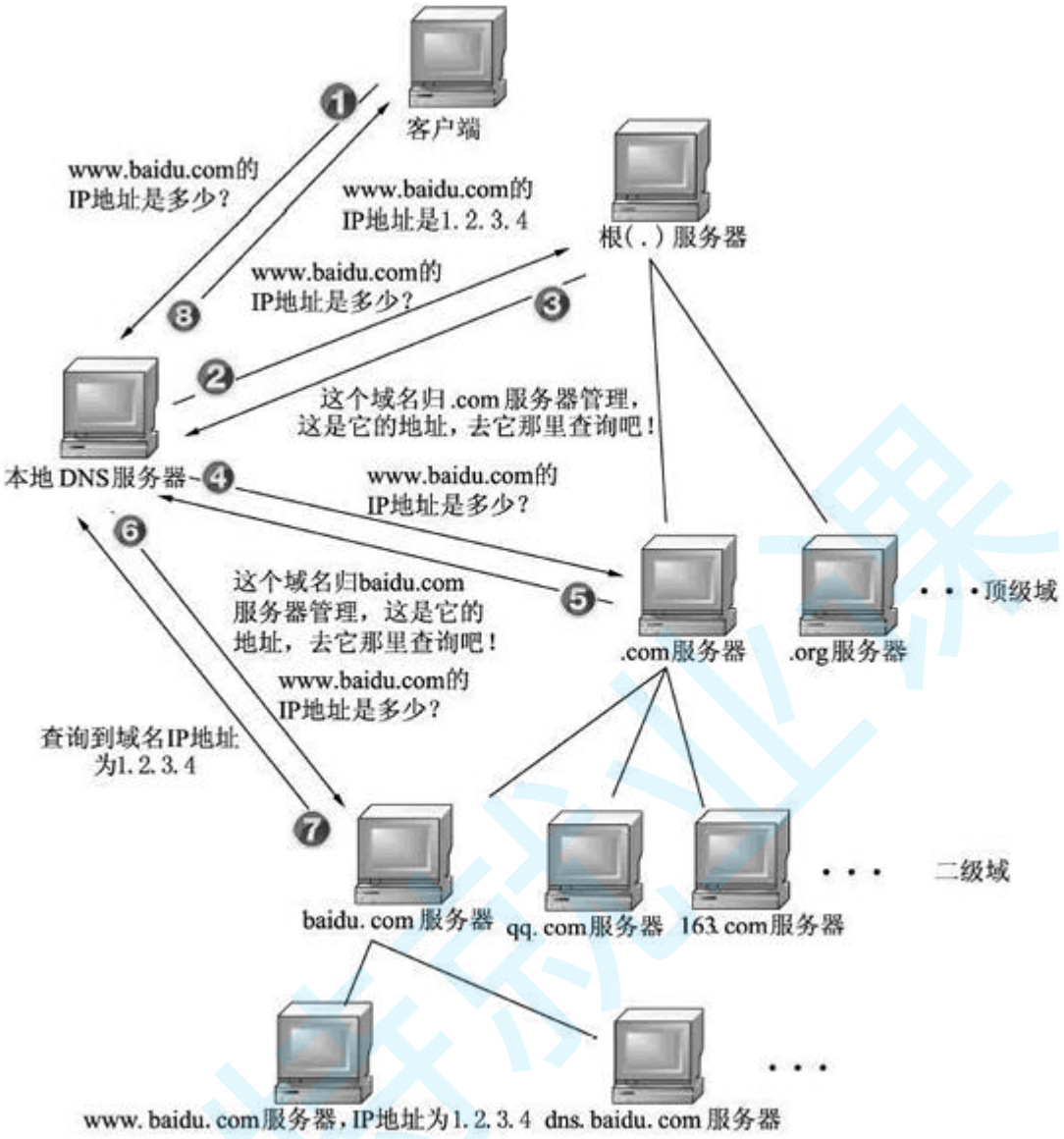
主域名是用来识别主机名称和主机所属的组织机构的一种分层结构的名称.

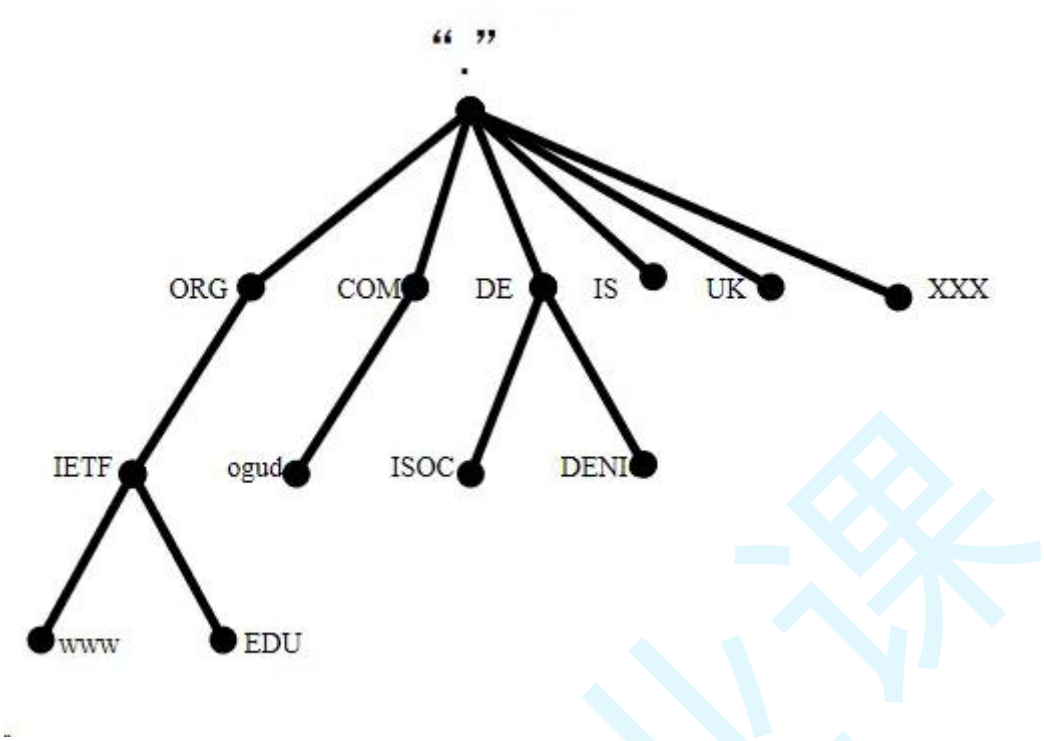
```
C
www.baidu.com
```

域名使用 . 连接

> - com: 一级域名. 表示这是一个企业域名. 同级的还有 "net"(网络提供商), "org"(非盈利组织) 等.
> - baidu: 二级域名, 公司名.
> - www: 只是一种习惯用法. 之前人们在使用域名时, 往往命名成类似于 ftp.xxx.xxx/www.xxx.xxx 这样的格 式, 来表示主机支持的协议.

域名解析过程(选学)


客户端
www.baidu.com的
IP地址是多少？
www.baidu.com的
IP地址是1.2.3.4
根(.)服务器
www.baidu.com的
IP地址是多少？
这个域名归.com服务器管理，
这是它的地址，去它那里查询吧！
本地DNS服务器
www.baidu.com的
IP地址是多少？
这个域名归baidu.com
服务器管理，这是它的
地址，去它那里查询吧！
.com服务器
.org服务器
顶级域
www.baidu.com的
IP地址是多少？
查询到域名IP地址
为1.2.3.4
baidu.com服务器
qq.com服务器
163.com服务器
二级域
www.baidu.com服务器，IP地址为1.2.3.4
dns.baidu.com服务器



如上图所示，域名结构是树状结构，树的最顶端代表根服务器，根的下一层就是由我们所熟知的.com、.net、.cn 等通用域和.cn、.uk 等国家域组成，称为顶级域。网上注册的域名基本都是二级域名，比如 http://baidu.com、http://taobao.com 等等二级域名，它们基本上是归企业和运维人员管理。接下来是三级或者四级域名，这里不多赘述

使用 dig 工具分析 DNS 过程

安装 dig 工具

```
C
yum install bind-utils
```

之后就可以使用 dig 指令查看域名解析过程了.

```
C
dig www.baidu.com
```

结果形如

```
C
; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<>> www.baidu.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41628
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.baidu.com.          IN A
;; ANSWER SECTION:
www.baidu.com.       1057   IN   CNAME   www.a.shifen.com.
www.a.shifen.com.    40   IN   A   115.239.210.27
www.a.shifen.com.    40   IN   A   115.239.211.112

;; Query time: 0 msec
;; SERVER: 100.100.2.136#53(100.100.2.136)
;; WHEN: Wed Sep 26 00:05:25 CST 2018
;; MSG SIZE rcvd: 90
```

结果解释

1. 开头位置是 dig 指令的版本号
2. 第二部分是服务器返回的详情, 重要的是 status 参数, NOERROR 表示查询成功
3. QUESTION SECTION 表示要查询的域名是什么
4. ANSWER SECTION 表示查询结果是什么. 这个结果先将 www.baidu.com 查询成了 www.a.shifen.com, 再将 www.a.shifen.com 查询成了两个 ip 地址.
5. 最下面是一些结果统计, 包含查询时间和 DNS 服务器的地址等.

更多 dig 的使用方法, 参见

https://www.imooc.com/article/26971?block_id=tuijian_wz

关于 DNS 缓存:

- 在 Windows 系统中, 可以使用 `ipconfig /displaydns` 命令来查看系统级别的 DNS 缓存
- 浏览器的缓存, 大家可以自行搜索一下, 看看能不能找到

浏览器中输入 url 后, 发生的事情. (作业)

这是一个经典的面试题. 没有固定答案, 越详细越好. 可以参考:

浏览器中输入 url 后发生的事情

ICMP 协议快速了解

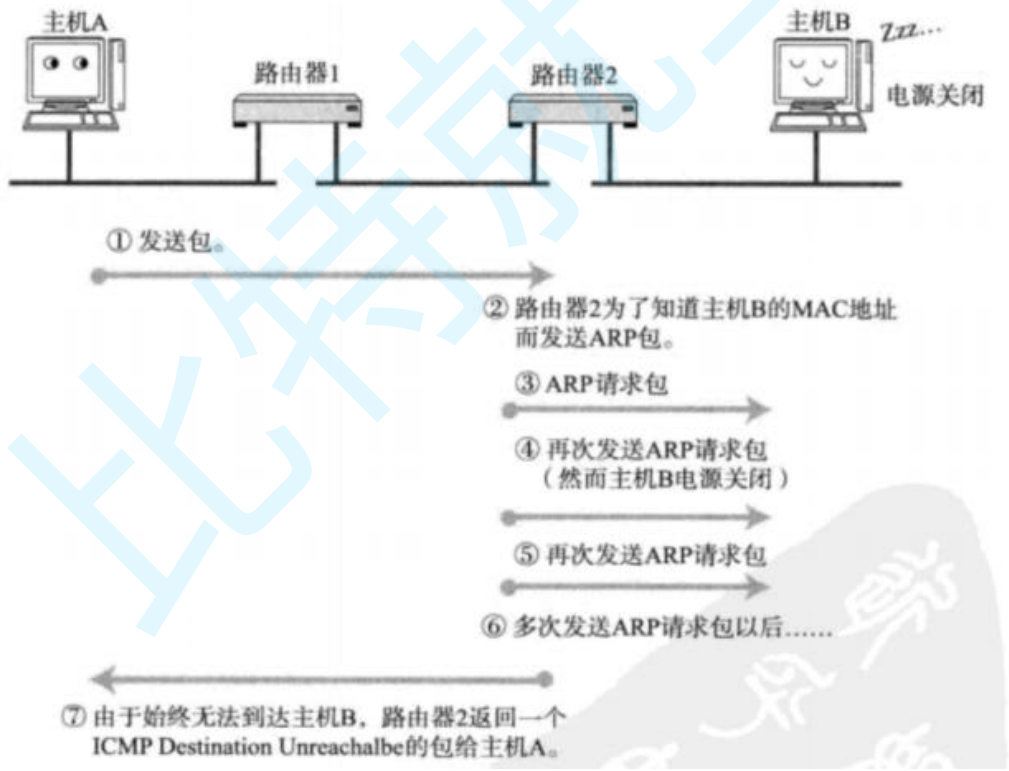
ICMP 协议是一个 **网络层协议**

一个新搭建好的网络, 往往需要先进行一个简单的测试, 来验证网络是否畅通; 但是 IP 协议并不提供可靠传输. 如果丢包了, IP 协议并不能通知传输层是否丢包以及丢包的原因.

ICMP 功能

ICMP 正是提供这种功能的协议; ICMP 主要功能包括:

- 确认 IP 包是否成功到达目标地址.
- 通知在发送过程中 IP 包被丢弃的原因.
- ICMP 也是基于 IP 协议工作的. 但是它并不是传输层的功能, 因此人们仍然把它归结为网络层协议;
- ICMP 只能搭配 IPv4 使用. 如果是 IPv6 的情况下, 需要使用 ICMPv6;



ICMP 的报文格式 (选学)

关于报文格式, 我们并不打算重点关注, 大家稍微有个了解即可.

ICMP 大概分为两类报文:

- 一类是通知出错原因
- 一类是用于诊断查询

类型（十进制数）	内　　容
0	回送应答（Echo Reply）
3	目标不可达（Destination Unreachable）
4	原点抑制（Source Quench）
5	重定向或改变路由（Redirect）
8	回送请求（Echo Request）
9	路由器公告（Router Advertisement）
10	路由器请求（Router Solicitation）
11	超时（Time Exceeded）
17	地址子网请求（Address Mask Request）
18	地址子网应答（Address Mask Reply）

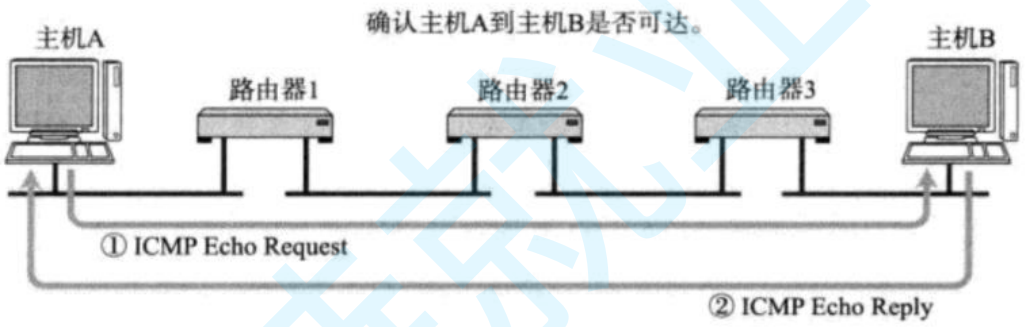
ping 命令

```
C:\Users\HGtz>ping www.baidu.com

正在 Ping www.a.shifen.com [61.135.169.121] 具有 32 字节的数据:
来自 61.135.169.121 的回复: 字节=32 时间=61ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=28ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=66ms TTL=52
来自 61.135.169.121 的回复: 字节=32 时间=44ms TTL=52

61.135.169.121 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 28ms, 最长 = 66ms, 平均 = 49ms
```

- 注意, 此处 ping 的是域名, 而不是 url! 一个域名可以通过 DNS 解析成 IP 地址.
- ping 命令不光能验证网络的连通性, 同时也会统计响应时间和 TTL(IP 包中的 Time To Live, 生存周期).
- ping 命令会先发送一个 ICMP Echo Request 给对端;
- 对端接收到之后, 会返回一个 ICMP Echo Reply;



一个值得注意的坑

有些面试官可能会问: telnet 是 23 端口, ssh 是 22 端口, 那么 ping 是什么端口?

千万注意!!! 这是面试官的圈套

ping 命令基于 ICMP, 是在网络层. 而端口号, 是传输层的内容. 在 ICMP 中根本就不关注端口号这样的信息.

traceroute 命令

也是基于 ICMP 协议实现, 能够打印出可执行程序主机, 一直到目标主机之前经历多少路由器.

```
[tangzhong@tz ~]$ traceroute www.baidu.com
traceroute to www.baidu.com (61.135.169.121), 30 hops max, 60 byte packets
 1  * * *
 2  10.254.1.13 (10.254.1.13)  24.307 ms  32.617 ms  32.634 ms
 3  10.254.1.69 (10.254.1.69)  32.600 ms  32.512 ms  39.239 ms
 4  10.254.1.53 (10.254.1.53)  32.475 ms  32.459 ms  32.402 ms
 5  123.139.1.193 (123.139.1.193)  32.355 ms  32.325 ms  32.307 ms
 6  221.11.0.1 (221.11.0.1)  32.301 ms  23.785 ms  28.480 ms
 7  221.11.0.97 (221.11.0.97)  61.396 ms 221.11.0.85 (221.11.0.85)  56.582 ms  63.129 ms
 8  219.158.112.17 (219.158.112.17)  53.336 ms 219.158.112.21 (219.158.112.21)  53.269 ms  53.194 ms
 9  124.65.194.158 (124.65.194.158)  53.178 ms  53.149 ms  53.598 ms
10  124.65.58.54 (124.65.58.54)  56.066 ms 124.65.58.62 (124.65.58.62)  47.815 ms 124.65.59.114 (124.65.59.114)
38.873 ms
11  202.106.48.18 (202.106.48.18)  53.095 ms 61.49.168.110 (61.49.168.110)  57.682 ms 123.125.248.98 (123.125.248
.98)  46.452 ms
12  * * *
13  * * *
```

附录：

- 关于域名，我提问 AI 的问题列表，非技术问题，但是有助于理解域名解析: https://yiyan.baidu.com/share/YAWkPiO7ER