

# DNS与ICMP

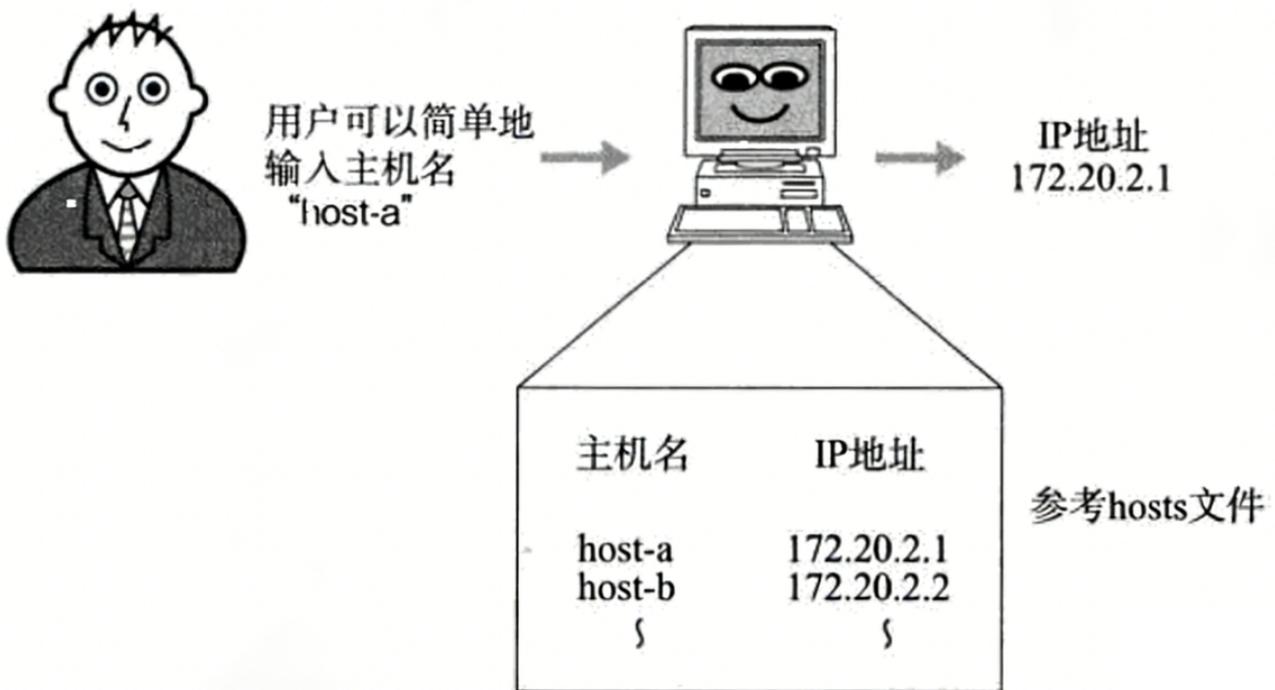
## DNS(Domain Name System)快速了解

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.

```
代码块 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。

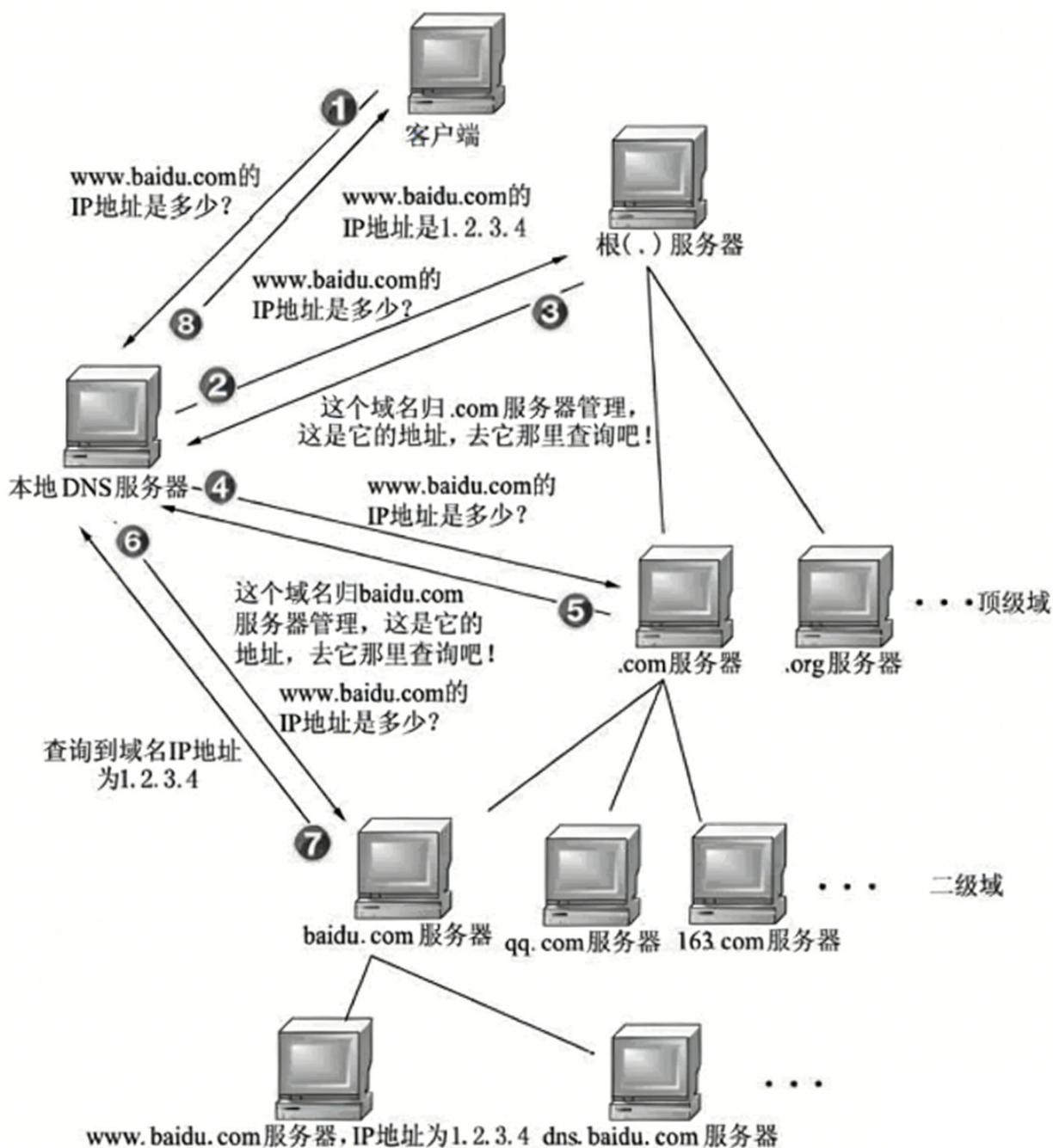
```
代码块
```

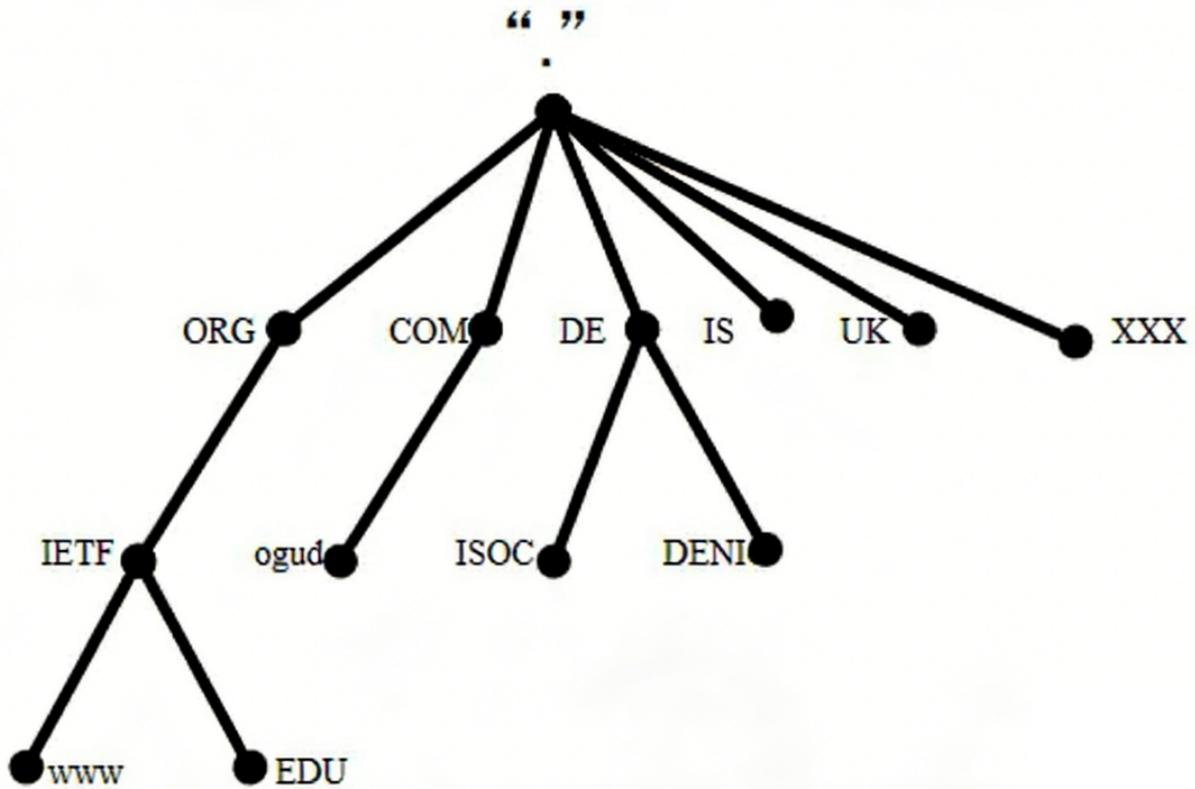
```
1 www.baidu.com
```

### 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)





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

代码块

```
1 yum install bind-utils
```

之后就可以使用 dig 指令查看域名解析过程了。

代码块

```
1 dig www.baidu.com
```

结果形如

代码块

```
1 ; <<> DiG 9.9.4-RedHat-9.9.4-61.el7_5.1 <<> www.baidu.com
2 ;; global options: +cmd
3 ;; Got answer:
4 ;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 41628
5 ;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
6
7 ;; QUESTION SECTION:
8 ;www.baidu.com. IN A
9 ;; ANSWER SECTION:
10 www.baidu.com. 1057 IN CNAME www.a.shifen.com. www.a.shifen.com.
11     40 IN A 115.239.210.27
12 www.a.shifen.com. 40 IN A 115.239.211.112
13
14 ;; Query time: 0 msec
15 ;; SERVER: 100.100.2.136#53(100.100.2.136)
16 ;; WHEN: Wed Sep 26 00:05:25 CST 2018
17 ;; 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](http://www.baidu.com) 查询成了 [www.a.shifen.com](http://www.a.shifen.com), 再将 [www.a.shifen.com](http://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](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

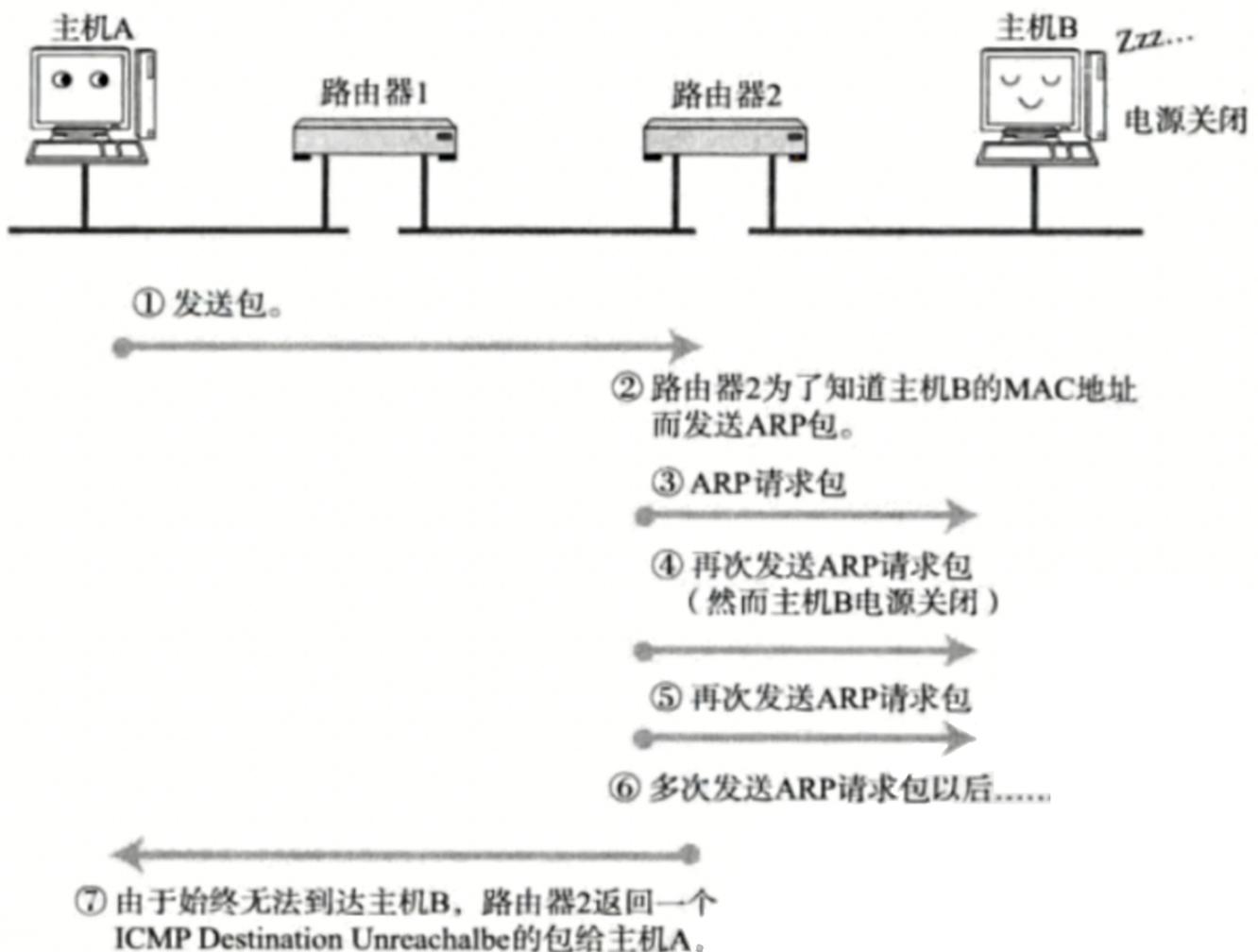
ICMP协议是一个 **网络层协议**

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.

0                      7                      15                      31

类型	代码	校验和
不同类型和代码有不同的内容		

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
```

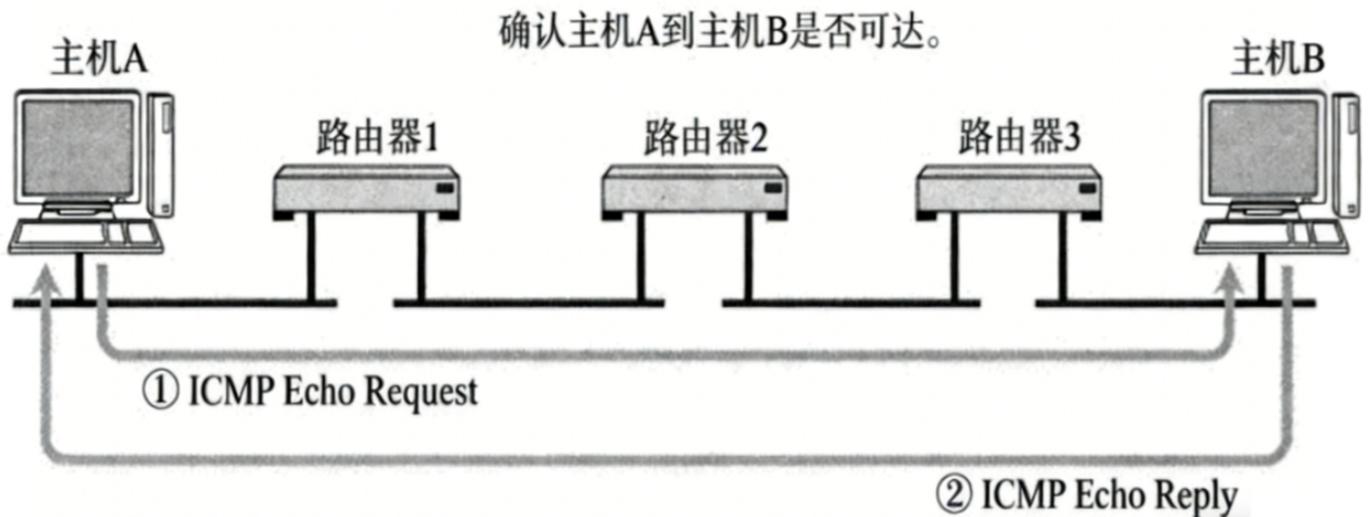
```
61.135.169.121 的 Ping 统计信息:
```

```
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.

## 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://yiyi.baidu.com/share/YAWkPiOTER>