是你的山楂 2020-12-07 540 阅读12分钟 关注

最近读完了 《图解http》，总体感觉比较通俗易懂，作为http的入门教程还不错；以前脑子里一些零散的http知识，通过读本书能有一个比较系统的认识，推荐大家读一下，如果时间不够，也可以读此文。以下是正文：

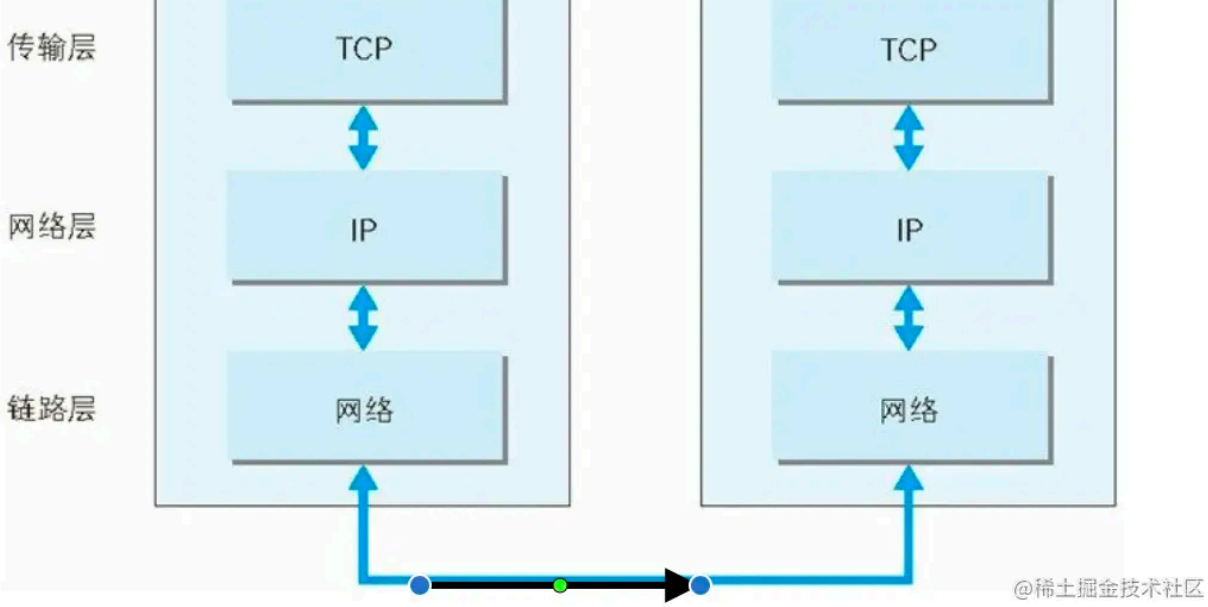
首先，Http是TCP/IP协议族的子集。

TCP/IP协议族

分层的TCP/IP协议

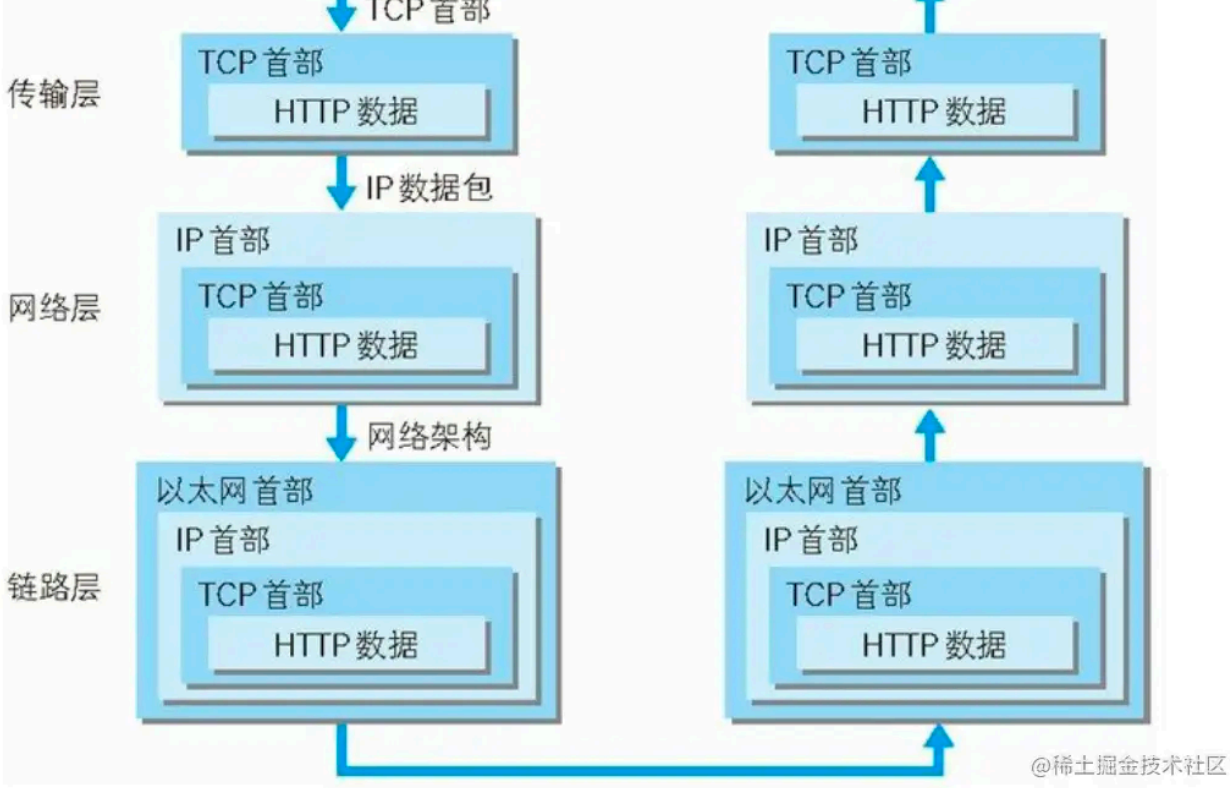
既然Http是TCP/IP协议族的子集，那么我们先认识一下它。TCP/IP协议族，互联网相关联的协议集合起来总称为 TCP/IP。TCP/IP协议最重要的是分层，从上到下分为：

- 应用层: 决定了向用户提供应用服务时通信的活动。FTP、DNS、HTTP都位于这层。
- 传输层： 网络链接中两台计算机之间的数据传输。
- 网络层： 规划数据包（网络中最小的数据流）的传输路径。
- 数据链路层: 网络链接中的硬件部分，如网线、网卡、光纤等。 分层可以让网络通信中各个部分解耦合，每一层只需专注自己的事情即可。
  利用 TCP/IP 协议族进行网络通信时，会通过分层顺序与对方进行通信。发送端从应用层往下走，接收端则往应用层往上走。



举个🌰：小明在网页输入一个url、按下回车即发起了一个客户端向服务端请求网页数据的**应用层**http请求；接着，为了传输方便，在**传输层**（TCP协议）把从应用层处收到的数据（HTTP请求报文）进行分割，并在各个报文上标记序号及端口号后转发给网络层；在**网络层**（IP协议），增加MAC地址（通信目的地，一条完整的网络通信链路中会有多个MAC中转站）后转发给**数据链路层**； 接受端的服务器在数据链路层获取到请求数据，从下到上依次往上传输，一直传输到应用层，服务端才算接受到了此次通信。

发送端在层与层之间传输数据时，每经过一层时必定会被打上一个该 层所属的首部信息。反之，接收端在层与层传输数据时，每经过一层 时会把对应的首部消去。

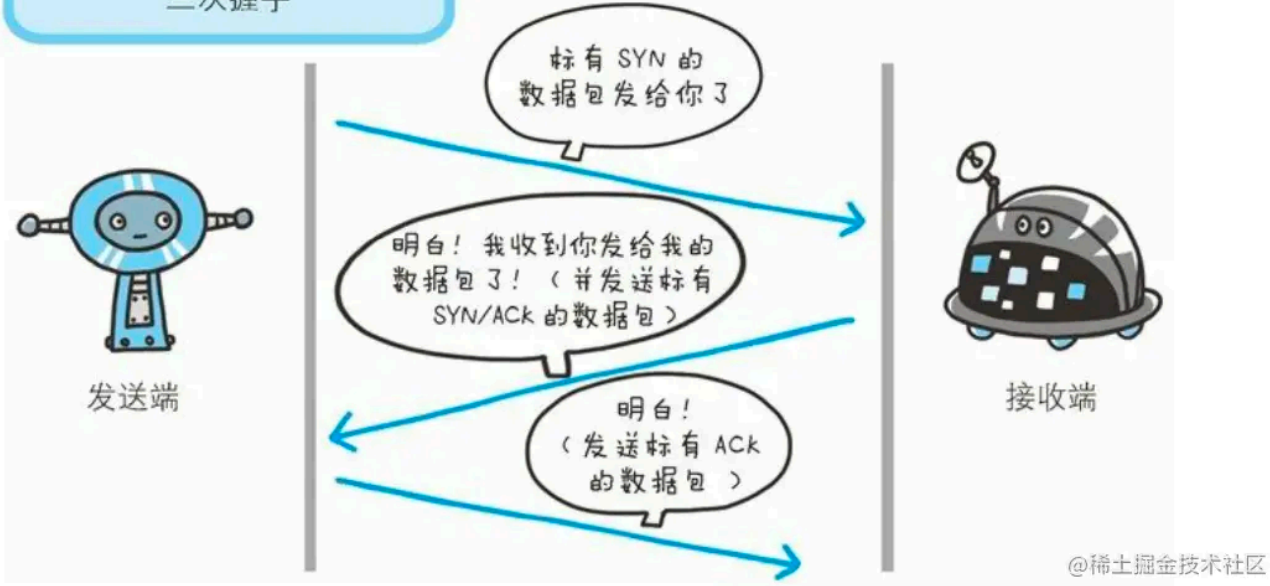


网络传输中的协议

负责传输的IP协议

IP（INternet Protocol）网际协议位于*网络层*，作用是将各种数据包传送给对方。为了保证将协议传到对方，有两个重要的因素：IP地址和MAC(Media Access Control Address)地址。IP地址指明了节点被分配到的地址，MAC地址指的是网卡所属的固定地址。

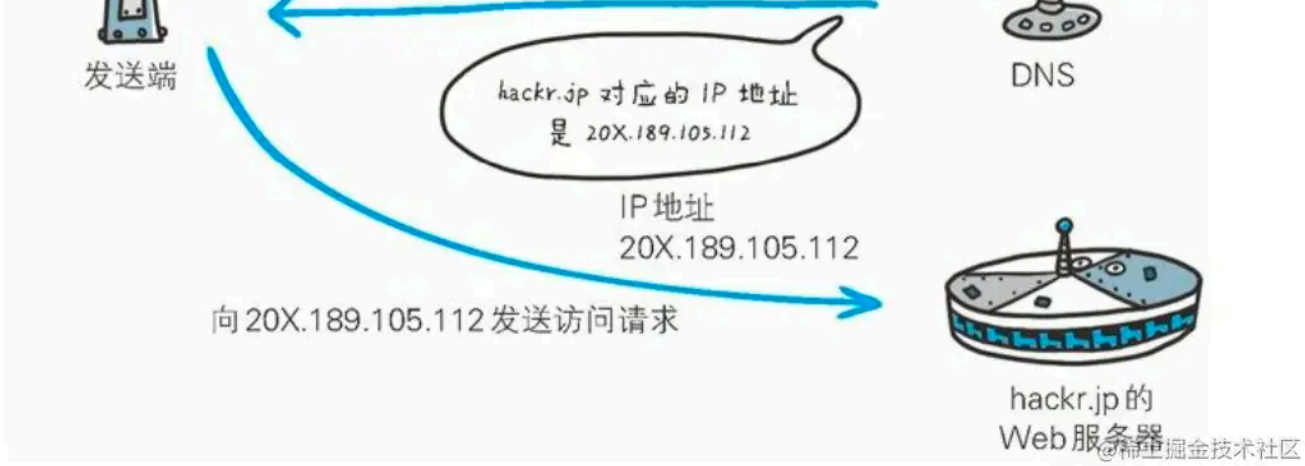
```
1  IP 间的通信依赖 MAC 地址。在网络上，通信的双方在同一局域网 (LAN)内的情况是很少的，通常是经过多台计算机
```

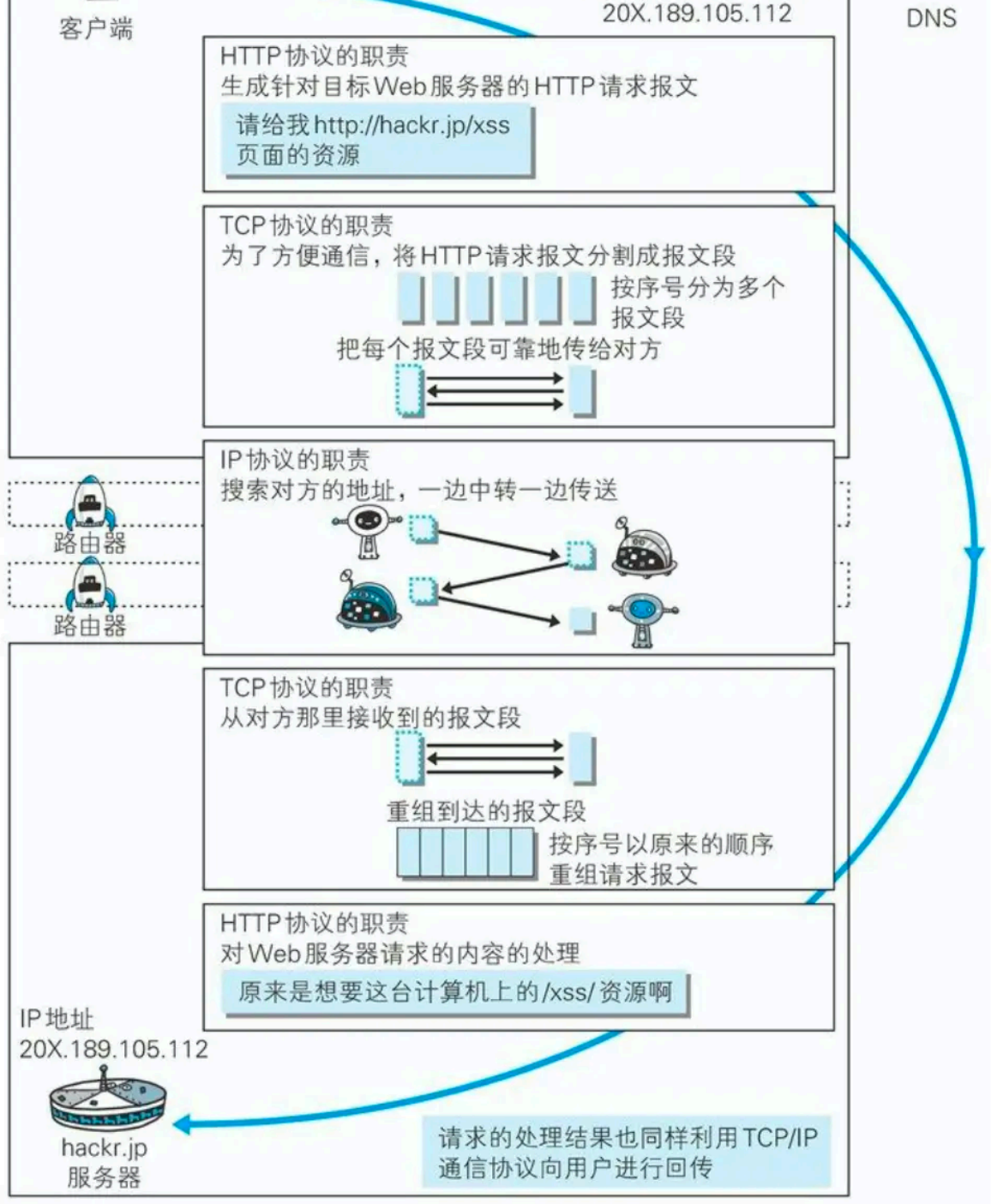


负责域名解析的DNS协议

DNS(Domain Name System)服务是和 HTTP 协议一样位于**应用层**的协议。它提供域名到 IP 地址之间的解析服务。用户通常使用主机名或域名来访问对方的计算机，而不是直接通过 IP 地址访问,因为域名更符合人类的记忆习惯。

三个协议在过程的作用

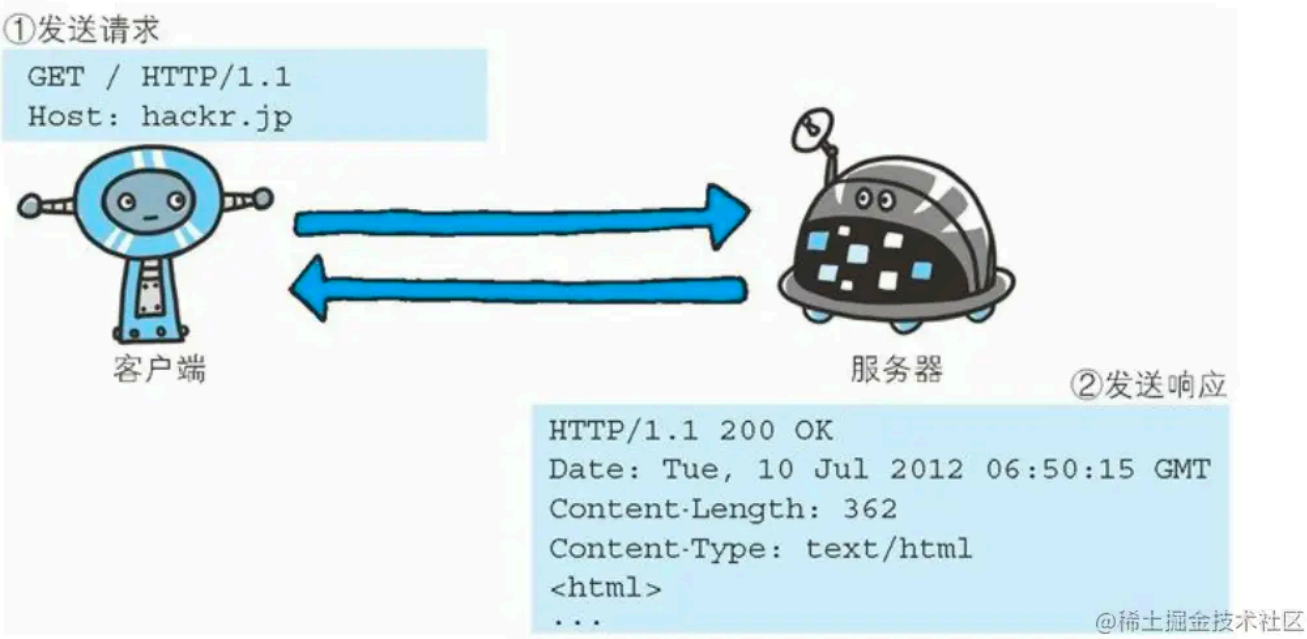




URI和URL

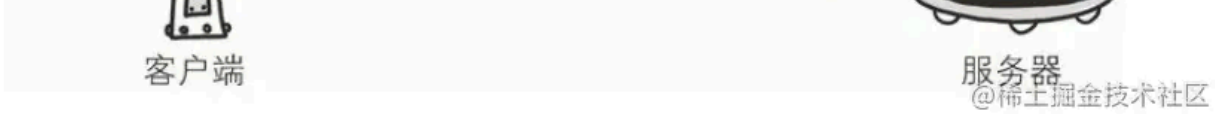
Http协议用于客户端和服务端之前的通信

请求访问文本或图像等资源的一端称为客户端，而提供资源响应的一端称为服务器端。在两台计算机之间使用 HTTP 协议通信时，在一条通信线路上必定有 一端是客户端，另一端则是服务器端。HTTP 协议规定，请求从客户端发出，最后服务器端响应该请求并返回。



Http是不保存状态的协议

HTTP 是一种不保存状态，即无状态(stateless)协议。HTTP 协议自 身不对请求和响应之间的通信状态进行保存。



通过请求URI定位资源

HTTP 协议使用 URI 定位互联网上的资源，在互联网上任意位置的资源都能访问到。

通过请求方法（GET/POST）告知服务器请求的意图

- GET 方法用来请求访问已被 URI 识别的资源。
- POST 方法用来传输实体的主体。鉴于 HTTP/1.1 的 PUT 方法自身不带验证机制，任何人都可以 上传文件 , 存在安全性问题，因此一般的 Web 网站不使用该方法。适合需要需要把某些信息主动告诉服务端。
- HEAD 方法和 GET 方法一样，只是不返回报文主体部分。用于确认 URI 的有效性及资源更新的日期时间等。

方法	说明	支持的 HTTP 协议版本
GET	获取资源	1.0、1.1
POST	传输实体主体	1.0、1.1
PUT	传输文件	1.0、1.1
HEAD	获得报文首部	1.0、1.1
DELETE	删除文件	1.0、1.1
OPTIONS	询问支持的方法	1.1
TRACE	追踪路径	1.1
CONNECT	要求用隧道协议连接代理	1.1
LINK	建立和资源之间的联系	1.0
UNLINE	断开连接关系	1.0

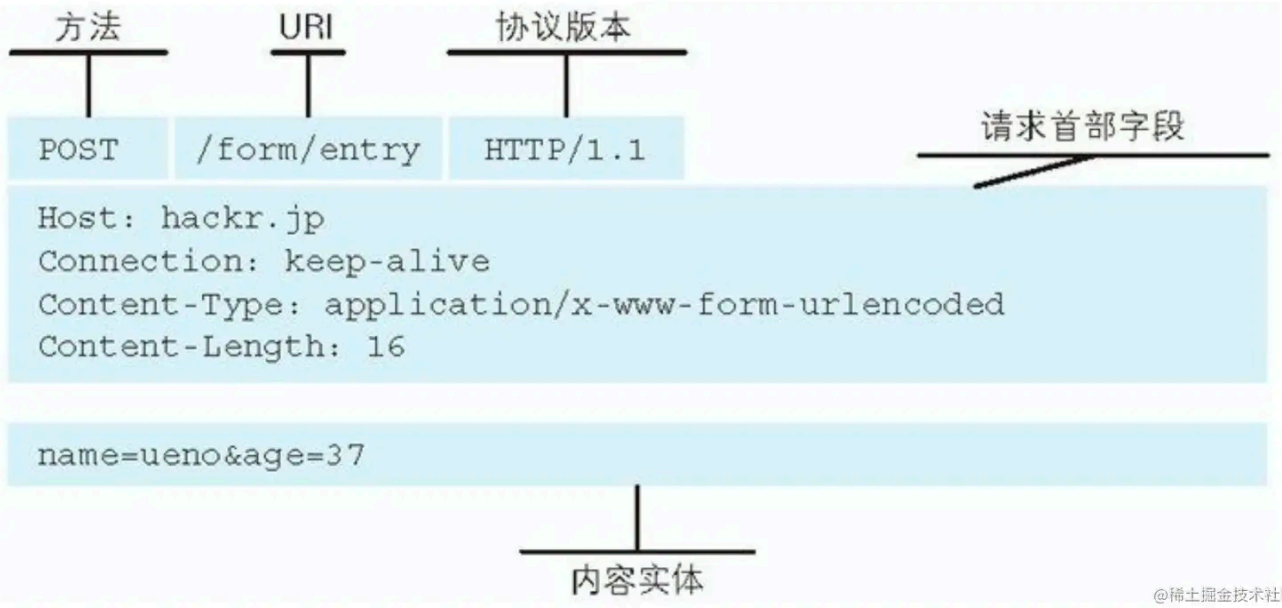
HTTP 是无状态协议，它不对之前发生过的请求和响应的状态进行管 理。也就是说，无法根据之前的状态进行本次的请求处理。 Cookie 技术通过在请求和响应报文中写入 Cookie 信息来控制客户端的状态。 更多关于cookie,简短清晰的教程

Http报文

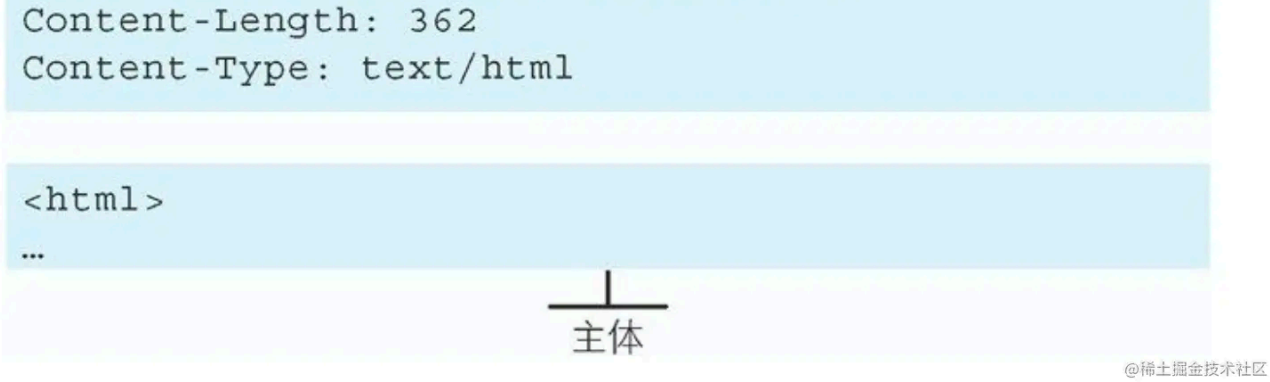
用于 HTTP 协议交互的信息被称为 HTTP 报文。请求端(客户端)的 HTTP 报文叫做请求报文，响应端(服务器端)的叫做响应报文。 HTTP 报文本身是由多行数据构成的字符串文本。

请求报文

请求报文由 1.请求方法 2.请求url 3.协议版本 4.可选的请求首部（包括通用首部——即请求和响应通用的首部、请求首部、实体首部） 5. 内容实体 构成的。



响应报文



Http状态码

2xx 表明请求被正常处理了

- 200 表示从客户端发来的请求在服务器端被正常处理了
- 204 表示从客户端发来的请求在服务器端被正常处理了
- 206 表示客户端进行了范围请求，而服务器成功执行了这部分的 GET 请求。响应报文中包含由 Content-Range 指定范围的实体内容。

3xx 重定向

- 301 永久重定向。表示请求的资源已经被新分配了uri，之后的请求都会去请求最新的uri
- 302 临时重定向。表示请求的资源已被分配了新的 URI，希望用户(本次)能使用新的 URI 访问。302禁止将post变为get，但实际运用上通常会将post转为get。
- 303 临时重定向，且应该用GET访问。
- 304 启用缓存。虽然304在3xx中，但是跟重定向毫无关系。表示请求带着条件（如If-Match，If-Modified- Since，If-None-Match，If-Range，If-Unmodified-Since ）请求,但不满足条件可启用缓存这种情况。
- 307 临时重定向，不会从 POST 变成 GET。

- 501 服务端bug
- 503 表明服务器处于超负载或者正在停机维护，暂时不能处理请求。 状态码和状况的不一致不少返回的状态码响应都是错误的，但是用户可能察觉不到这点。 比如 `Web` 应用程序内部发生错误，状态码依然返回 `200 OK`，这种 情况也经常遇到。

与Http协作的web服务器

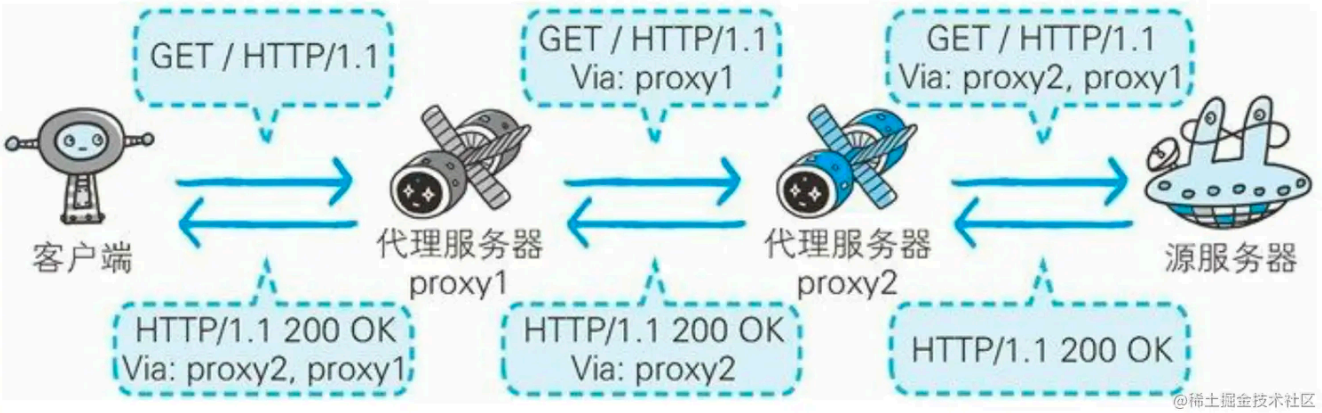
单台虚拟主机可以实现多个域名

单台虚拟主机可以托管多个域名，我们用DNS域名解析后，实际访问的是IP地址，单台主机的IP地址是相同的。

通信数据转发程序

代理

代理是一种有转发功能的应用程序，它扮演了位于服务器和客户 端“中间人”的角色，接收由客户端发送的请求并转发给服务器，同时 也接收服务器返回的响应并转发给客户端。



代理不改变请求 URI，会直接发送给前方持有资源的源服务器，可级联多台代理服务器。转发时，需要附加 Via 首部字段以标记出经过的主机信息。 使用代理服务器的目的有:

网关是转发其他服务器通信数据的服务器，接收从客户端发送来的请求时，它就像自己拥有资源的源服务器一样对请求进行处理。有时客户端可能都不会察觉，自己的通信目标是一个网关。

网关能使通信线路上的服务器由 HTTP 请求转化为其他协议通信。

利用网关能提高通信的安全性，因为可以在客户端与网关之间的通信线路上加密以确保连接的安全。比如，网关可以连接数据库，使用 SQL 语句查询数据。

HTTP+ 加密 + 认证 + 完整性保护 =HTTPS

- 经常会在Web登录和购物车结算时使用https。
- 使用https时，url前会有一把小锁的标记（不同浏览器会有差异）
- 通常，http直接和tcp通信。当使用ssl时，则先和ssl通信，ssl再和tcp通信。简而言之，https就是身披ssl壳的http。在采用 SSL 后，HTTP 就拥有了 HTTPS 的加密、证书和完整性保护 这些功能。
- https要比http慢2-100倍。一是指通信慢；另外由于大量消耗CPU 及内存等资源，导致处理

web攻击

主动攻击

主动攻击是指攻击者通过直接访问Web应用，把攻击代码传入的攻击模式，攻击者需要能够访问到web服务器的资源。如SQL注入攻击和OS命令注入攻击。

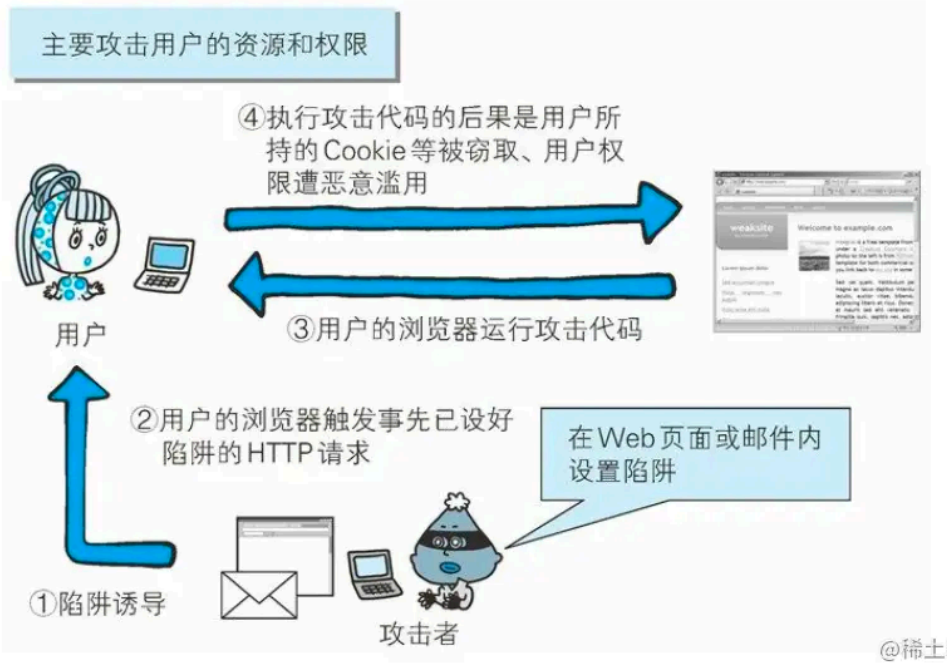
SQL 注入(SQL Injection) 是指针对 Web 应用使用的数据库，通 过运行非法的 SQL 而产生的攻击。该安全隐患有可能引发极大 的威胁，有时会直接导致个人信息及机密信息的泄露。

OS 命令注入攻击(OS Command Injection) 是指通过 Web 应用，执行 非法的操作系统命令达到攻击的目的。只要在能调用 Shell 函数的地 方就有存在被攻击的风险。

被动攻击

被动攻击是指不直接对web应用进行攻击，而是利用全套策略诱使用户触发陷阱。如跨站脚本攻击（Cross-Site Scripting XSS）和站点请求伪造。

利用被动攻击，可发起对原本从互联网上无法直接访问的企业内网等网络的攻击。只要用户踏入攻击者预先设好的陷阱，在用能够访问到的网络范围内，即使是企业内网也同样会受到攻击。



XSS 是攻击者利用预先设置的陷阱触发的被动攻击 跨站脚本攻击属于被动攻击模式，因此攻击者会事先布置好用于 攻击的陷阱。

- 利用虚假输入表单骗取用户个人信息

评论 1

登录 / 注册 即可发布评论!

最热 最新

woow_wu7 LV.4 神居岛 @马林佛多

是你的滴滴

3年前 点赞 评论 ···

目录 收起

TCP/IP协议族

- 分层的TCP/IP协议
- 网络传输中的协议
  - 负责传输的IP协议
  - 确保可靠性的TCP协议
  - 负责域名解析的DNS协议
  - 三个协议在过程的作用
- URI和URL

简单的http协议

- 请求报文
- 响应报文

Http状态码

- 2xx 表明请求被正常处理了
- 3xx 重定向
- 4xx 客户端错误
- 5xx 服务器本身发生错误

与Http协作的web服务器

- 单台虚拟主机可以实现多个域名
- 通信数据转发程序
  - 代理
  - 网关

HTTP+ 加密 + 认证 + 完整性保护 =HTTPS

- 为什么不一直使用 HTTPS

web攻击

- 主动攻击
- 被动攻击

为你推荐

图解HTTP常见知识点总结

疫情快滚蛋吧　3年前　301　2　评论　HTTP　后端

网络协议—七/五层模型、三次握手和四次挥手原理详解、UDP/TCP、TCP可靠传输

sober_1128　3年前　788　1　评论　网络协议

《图解HTTP》读书笔记

RCui　3年前　152　点赞　评论　JavaScript　HTTP

HTTP 协议详解

亦黑迷失　3年前　808　3　评论　HTTP　前端

前端网络知识点总结

蜡笔韭菜　3年前　803　11　评论　前端

图解tcp/ip中ip协议及相关技术 小结

海娩　3年前　1.2k　11　4　TCP/IP

1.8万字深入学习HTTP

ffiyu　3年前　791　11　评论　HTTP

前端需要具备的http知识（http1.0=>http1.1=>http2.0）

佩子　2年前　722　3　评论　前端　HTTP

通过TCP/IP了解HTTP（四）

独树一帜　3年前　271　2　评论　TCP/IP　后端

有毒的水母 7月前 243 1 评论 网络协议 后端

学好 TCP/IP 基础

wentianyang 3年前 569 3 评论 HTTP

【计算机网络】前端应该知道的计算机网络知识点

DarkHorse 1年前 779 28 2 前端 后端 面试

TCP vs UDP：揭秘可靠性与效率之争

努力的小雨 10月前 159 2 评论 后端 面试 网络协议