面经预热-Day8（计网专题）

1、HTTPS的工作原理？（HTTPS是如何建立连接的）

1. 首先，客户端向服务器端发送请求报文，请求与服务端建立连接
2. 服务端产生一堆公私钥，然后将自己的公钥发给CA机构，CA机构也有一对公私钥，然后CA机构使用自己的私钥将服务端发送过来的公钥进行加密，产生一个CA数字整数
3. 服务端响应客户端的请求，将CA机构生成的数字证书发送给客户端
4. 客户端将服务端发送过来的数字证书进行解析（因为浏览器产商跟CA机构有合作，所以浏览器中已经保存了大部分的CA机构的密钥，用于对服务端发送过来的数字证书进行解密），验证这个数字证书是否合法，如果不合法，会发送一个警告。如果合法，取出服务端生成的公钥。
5. 客户端取出公钥并生成一个随机码Key（其实就是对称加密中的密钥）
6. 客户端将加密后的随机码key发送给服务端，作为接下来的对称加密的密钥
7. 服务端接收到随机码key后，使用自己的私钥对它进行解密，然后获得到随机码key
8. 服务端使用随机码key对传输的数据进行加密，在传输加密后的内容给客户端
9. 客户端使用自己生成的随机码key解密服务端发送过来的数据，之后，客户端和服务端通过对称加密传输数据，随机码key作为传输的密钥

2、HTTPS与HTTP的区别

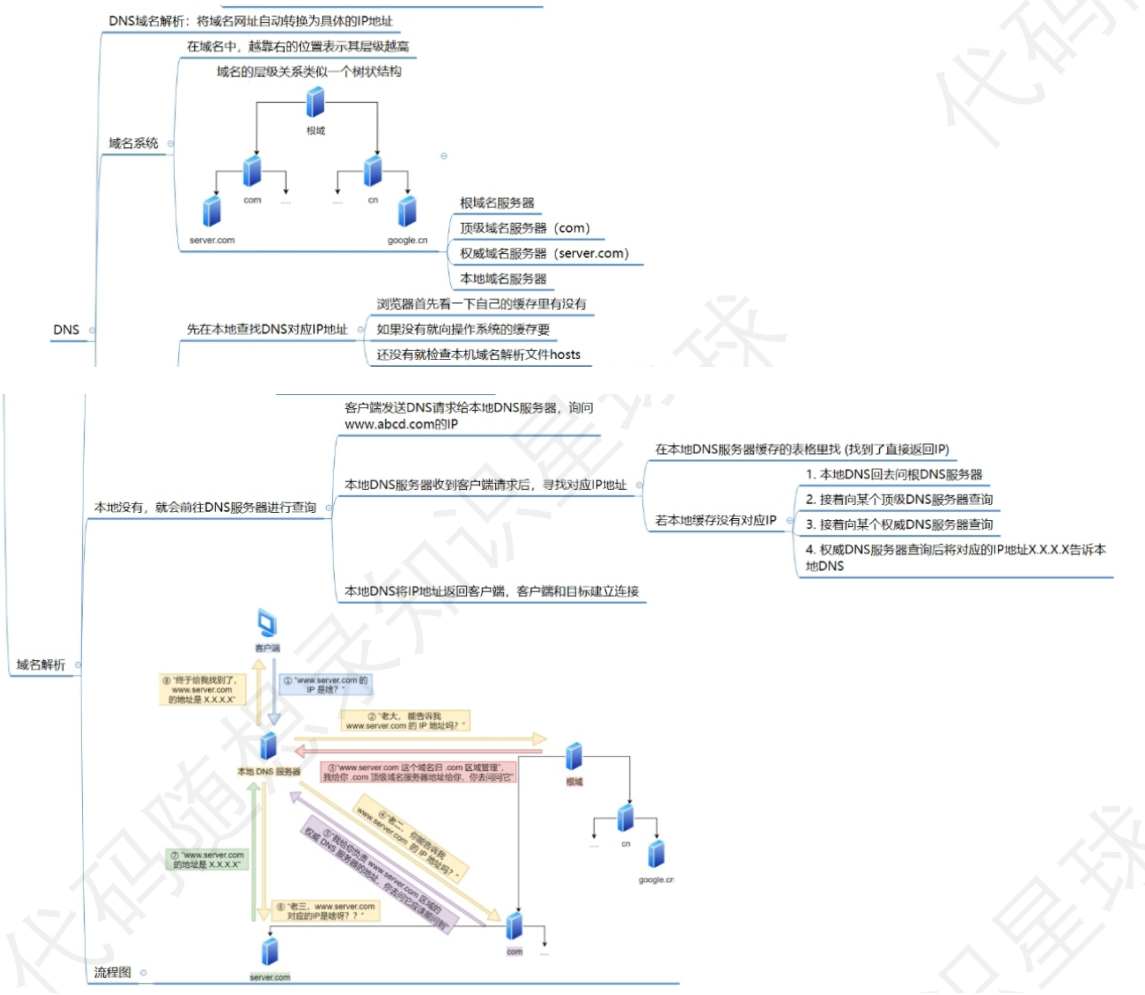
- HTTP是明文传输，而HTTPS通过`SSL/TLS`进行了加密
- HTTP的端口号是80，HTTPS是443
- HTTPS需要到`CA`申请证书
- HTTP的连接简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比HTTP协议安全

3、DNS是什么？查询过程是怎么样的?

DNS (Domain Name System) 域名管理系统，是当用户使用浏览器访问网址之后，使用的第一个重要协议。DNS 要解决的是域名和IP 地址的映射问题。

- 1.首先用户在浏览器输入URL地址后，会先查询浏览器缓存是否有该域名对应的IP地址。
- 2.如果浏览器缓存中没有，会去计算机本地的Host文件中查询是否有对应的缓存。
- 3.如果Host文件中也没有则会向本地的DNS解析器 (通常由你的互联网服务提供商 (ISP) 提供)发送一个DNS查询请求。
- 4.如果本地DNS解析器没有缓存该域名的解析记录，它会向根DNS服务器发出查询请求。根DNS服务器并不负责解析域名，但它能告诉本地DNS解析器应该向哪个顶级域 (.com/.net/.org)的DNS服务器继续查询。

- 5本地DNS解析器接着向指定的顶级域DNS服务器发出查询请求。顶级域DNS服务器也不负责具体的域名解析，但它能告诉本地DNS解析器应该前往哪个权威DNS服务器查询下一步的信息。
- 6.本地DNS解析器最后向权威DNS服务器发送查询请求。 权威DNS服务器是负责存储特定域名和IP地址映射的服务器。当权威DNS服务器收到查询请求时，它会查找"example.com"域名对应的IP地址，并将结果返回给本地DNS解析器。
- 7.本地DNS解析器将收到的IP地址返回给浏览器，并且还会将域名解析结果缓存在本地，以便下次访问时更快地响应



4、HTTP多个TCP连接怎么实现?

多个TCP连接是依靠某些服务器对 `Connection:Keep-alive` 的 `Header` 进行了支持。简而言之，完成这个HTTP请求之后，不要断开HTTP请求使用的TCP连接。这样的好处是连接可以被重新使用，之后发送 HTTP 请求的时候不需要建立TCP连接，以及如果维持连接，那么SSL的开销也可以避免。

5、TCP连接如何确保可靠性

TCP连接确保可靠性方法如下:

1.数据块大小控制:应用数据被分割成TCP认为最合适发送的数据块，再传输给网络层，数据块被称为报文段或段。

2.序列号: TCP给每个数据包指定序列号，接收方根据序列号对数据包进行排序，并根据序列号对数据包去重

3.校验和: TCP将保持它首部和数据的校验和。这是一个端到端的检验和，目的是检测数据在传输过程中的任何变化。如果收到报文的检验和有差错，TCP将丢弃这个报文段和不确认收到此报文段。

4.流量控制: TCP连接的每一方都有固定大小的缓冲空间，TCP的接收端只允许发送端发送接收端缓冲区能接纳的数据。当接收方来不及处理发送方的数据，能提示发送方降低发送的速率，防止包丢失。TCP利用滑动窗口实现流量控制。

5.拥塞控制:当网络拥塞时，减少数据的发送。

6.确认应答: 通过 AR 协议实现。基本原理是每发完一个分组就停止发送，等待对方确认。如果没收到确认，会重发数据包，直到确认后再发下一个分组。

7.超时重传: 当TCP发出一个数据段后，它启动一个定时器，等待目的端确认收到这个报文段。如果不能及时收到一个确认，将重发这个报文段。