大家好，上一小节我们介绍了一些基础的网络协议和面试中的高频考点。本节我们继续介绍基础网络协议相关知识点，主要知识点包括HTTP和HTTPS相关协议，路由汇聚以及子网掩码的求法等。 6

（1）HTTP和HTTPS的区别有哪些？（掌握）

答：HTTP和HTTPS的主要区别可以总结如下：

- HTTP是超文本传输协议，数据明文传输；HTTPS在HTTP的基础上加入了SSL协议，实现数据的加密传输；
- HTTPS需要区申请证书，一般是收费的；
- HTTP默认使用80端口，HTTPS默认使用443端口

解析：

这是一网络协议的基础题目，请大家务必掌握。在这里我们一起更加详细的进行学习吧。既然HTTPS = HTTP + SSL，那么我们先来看何为HTTP协议吧。

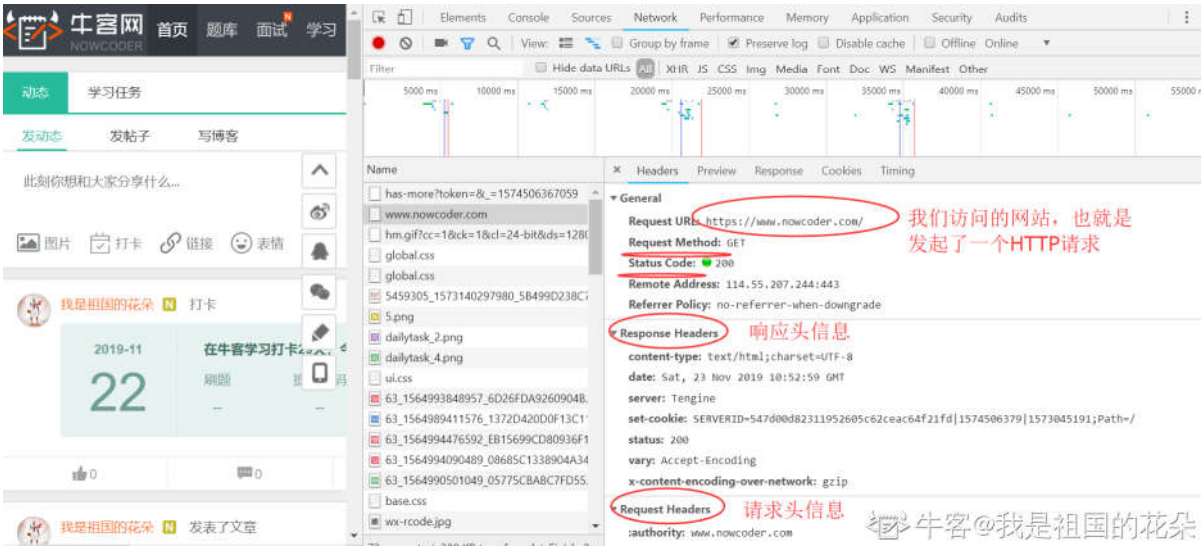
HTTP协议：

HTTP是超文本传输协议，是一种无状态的协议，是常见的一种应用层协议。HTTP是一个通信规则，规定了客户端发送给服务器的内容格式，也规定了服务器发送给客户端的内容格式。

HTTP请求信息：HTTP请求头中可以看到当前请求支持的语言，压缩格式，编码格式以及何种类型的返回文件，Connection以及Cookie，Content-Type等信息。

HTTP返回信息：HTTP返回信息中包括响应协议，HTTP Code以及Content-Type，时间和Cookie等信息。

（HTTP请求和返回的具体信息，大家可以任意打开一个网址，F12查看每一个具体的HTTP请求的请求和返回信息）



面试官：“HTTP请求中的Get和Post方法有哪些区别？”

- Get一般用来从服务器上查询获取资源；Post一般用来更新服务器上的资源；
- Get方法将参数直接拼接在了URL后边，明文显示，可以通过浏览器地址栏直接访问；
- Post请求用于提交表单，数据不是明文的，安全性更高；
- Get请求有长度限制，Post请求没有

面试官：“常见的HTTP Code有哪些？”

- 1xx（临时响应）
- 2xx（成功）
- 3xx（重定向）：表示要完成请求需要进一步操作
- 4xx（错误）：表示请求可能出错，妨碍了服务器的处理
- 5xx（服务器错误）：表示服务器在尝试处理请求时发生内部错误

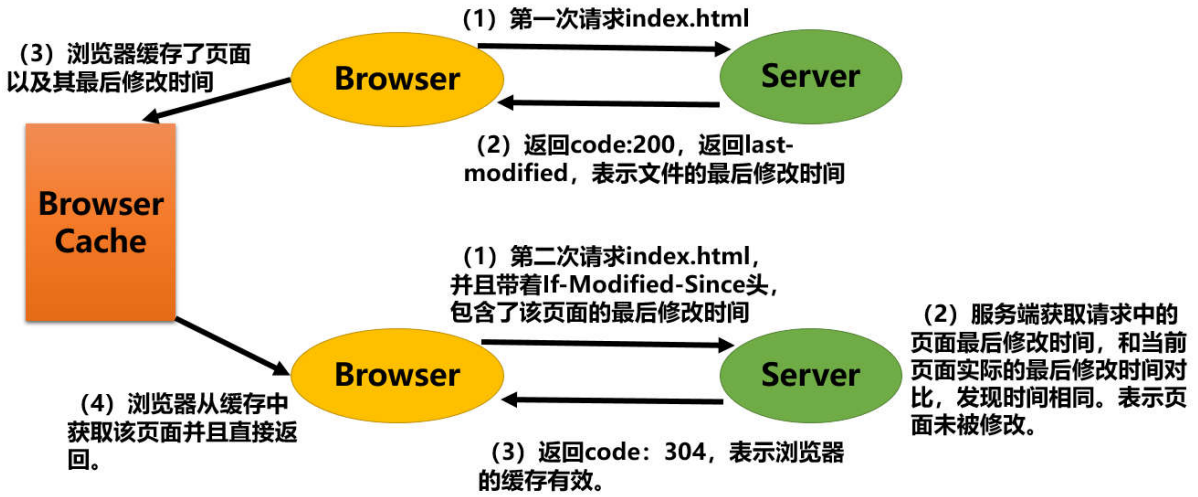
接着，我们可以给出具体的状态码。

常见HTTP协议的状态码：

- 200（成功）
- 302 （重定向）：请求重定向到指定网页
- 304（未修改）：自从上次请求后，请求的网页未修改过。服务器返回此响应时，不会返回网页内容
- 401（未授权）：请求要求身份验证
- 403（禁止）：服务器拒绝请求（比如死循环了，一直访问）
- 404（未找到）：服务器找不到请求的网页
- 405 （方法禁用）:Post请求当成了Get请求直接访问
- 500 （服务器内部错误）：有bug导致程序嗝屁了
- 502 （错误网关）：服务器从上游接到了无效响应

- 504 （网关超时）：nginx请求超时，请求一直没有返回

这里简单阐述304的含义，304表示上次请求结束到现在，目标网页内容未改变，客户端可以直接显示上次的内容。通过客户端和服务端之间的一个Last-Modified来判断。如下所示：



HTTP Code 返回304的示意图：

前面我们说到了HTTP是一种无状态的协议，也就是说每一次请求都是一个独立的会话，那么**会话状态（比如说用户的登录状态）该如何保持呢?**

面试官：“cookie和session有了解吗？“

HTTP协议是一种无状态的协议，我们可以使用cookie和session来保持会话状态。用户发起请求，服务端收到请求处理后可以生成一个sessionId，并且将sessionId存入cookie中返回给客户端，将session的内容存储在服务器上。在下一次的请求中，客户端带着cookie来请求服务器，服务端从cookie中取出sessionId，实现了用户会话状态的保持。

这样做有一个缺点就是将一些东西存在了服务器上，在用户量较大的情况下，服务器容量会不足。实际情况中，经常是将所需要的会话状态，比如说登录态直接存入cookie并且返回给客户端，下次请求时，服务端直接取出cookie中的信息和参数信息进行比较，保持HTTP会话状态。

总结：session保存在服务端。cookie保存在客户端,并且cookie有大小限制。

基本了解了HTTP协议之后，我们再来简单看下何为SSL协议吧~

SSL协议：

HTTPS协议在HTTP的基础上加入了SSL（安全套接字层）协议，SSL逐渐演变为了TLS协议，但是业界习惯仍然称其为SSL协议。

SSL协议在传输控制层的基础上建立了安全的连接，它作为一种通用可靠的安全解决方案，可与多种应用层协议结合使用，实现应用数据的安全传输。SSL协议分为**记录协议，握手协议，警告协议和密码规范改变协议**：

记录协议：接收上层协议或下层协议的消息并进行一系列的处理，然后再将处理后的消息继续向下或向上传递。主要包括对消息进行加解密，压缩解压缩，分段或者重组等操作。

握手协议：建立在三次握手之后，为通信双方确立安全连接所需要的安全参数，通常也会在此阶段对通信双方身份的真实性进行验证。

警告协议：无论是在握手阶段还是在对应用层数据的传输阶段，都有可能出现差错。警告协议规定了在SSL协议工作过程中可能出现的差错、错误的严重等级以及相应的处理方式。

密码规范改变协议：在SSL握手刚开始的时候，加密参数还没确定，消息都是明文传送的。双方协商好加密参数之后，在发送握手结束消息之前，需要发送一个密码规范改变消息（Change Cipher Message）来通知对方随后的消息都使用刚刚协商好的加密算法和加密密钥进行加密。

（2）HTTP1.0，HTTP1.1以及HTTP2.0协议的区别：

答：主要区别和特点可以概括如下：

- **HTTP1.0：**

HTTP1.0是一种无状态，无连接的协议。浏览器的每次请求都需要与服务器建立一个TCP连接，服务器处理完成后立即断开TCP连接（无连接），服务器不跟踪每个客户端也不记录过去的请求（无状态）。也就是默认使用Connection: close

- **HTTP1.1：**

HTTP/1.1中默认使用Connection: keep-alive，避免了连接建立和释放的开销。但服务器必须按照客户端请求的先后顺序依次回送相应的结果，以保证客户端能够区分出每次请求的响应内容。通过Content-Length字段来判断当前请求的数据是否已经全部接收。不允许同时存在两个并行的响应。

- **HTTP2.0：**

HTTP2.0协议新增了二进制分帧，多路复用，头部压缩和服务器推送等功能，进一步提高了传输效率。

接下来，我们再来介绍**路由汇聚和子网掩码**相关的知识点吧，这块知识点常见于笔试题目中，要求我们计算出正确的答案。

（3）路由汇聚：

答：路由汇聚是指把一组路由汇聚为一个单个的路由广播。路由汇聚优点是可以缩小网络上的路由表的尺寸。

算法实现：

- 将各子网地址的网段以二进制写出。
- 比较，从第1位比特开始进行比较，将从开始不相同的比特到末尾位填充为0。由此得到的地址为汇总后的网段的网络地址，其网络位为连续的相同的比特的位数。

6

举例：

假设下面有4个网络:

```
172.18.129.0/24
172.18.130.0/24
172.18.132.0/24
172.18.133.0/24
```

这四个进行路由汇聚,那么能覆盖这四个网络的汇总地址是:**172.18.128.0/21**

具体计算方式如下：

- 129的二进制代码是10000001
- 130的二进制代码是10000010
- 132的二进制代码是10000100
- 133的二进制代码是10000101

这四个数的前五位相同都是10000，所以加上前面的172.18这两部分相同的位数，网络号就是**8+8+5=21**。而10000000的十进制数是128，所以，路由汇聚的IP地址就是172.18.128.0。所以最终答案就是172.18.128.0/21

（4）子网掩码的求法：

答：笔试中关于子网掩码的求法一般考察下边的两种。

根据划分的子网数：

算法实现：在求子网掩码之前必须先搞清楚要划分的子网数目，以及每个子网内的所需主机数目。

- 将子网数目转化为二进制来表示
- 取得该二进制的位数，为 N
- 取得该IP地址的类子网掩码，将其主机地址部分的前N位置1 即得出该IP地址划分子网的子网掩码。

举例：

如欲将B类IP地址168.195.0.0划分成27个子网，则其子网掩码为**255.255.248.0**

- 27=11011
- 该二进制为五位数，N = 5
- 将B类地址的子网掩码255.255.0.0的主机地址前5位置1（B类地址的主机位包括后两个字节，所以这里要把第三个字节的前5位置1），得到 **255.255.248.0**

6

根据每个子网中的主机数：

算法实现：利用主机数来计算。

- 将主机数目转化为二进制来表示
- 如果主机数小于或等于254（注意去掉保留的两个IP地址），则取得该主机的二进制位数，为N，这里肯定N<8。如果大于254，则 N>8，这就是说主机地址将占据不止8位。
- 使用255.255.255.255来将该类IP地址的主机地址位数全部置1，然后从后向前的将N位全部置为 0，即为子网掩码值。

举例：

如欲将B类IP地址168.195.0.0划分成若干子网，每个子网内有主机700台，则其子网掩码为：**255.255.252.0**

- 700=1010111100
- 该二进制为十位数，N = 10
- 将该B类地址的子网掩码255.255.0.0的主机地址全部置1，得到255.255.255.255
- 然后再从后向前将后10位置0,即为： 11111111.11111111.11111100.00000000
- 即255.255.252.0。

总结：

本小节中，我们主要介绍了HTTP和HTTPS等相关知识点。在文章的最后，对于路由汇聚以及子网掩码的求法也做了简单的介绍，希望大家可以有效理解和掌握。下一小节中，我们将介绍关于Web安全的常见攻击方式，主要包括XSS攻击和CSRF攻击等。

限于作者水平，文章中难免会有不妥之处。大家在学习过程中遇到我没有表达清楚或者表述有误的地方，欢迎随时在文章下边指出，我会及时关注，随时改正。另外，大家有任何话题都可以在下边留言，我们一起交流探讨。

讨论 评论

刘畅201904211606816 1#

打卡

发表于 2020-01-08 21:47:53 赞(0) 回复(0)

柳杰201905011049420 2#

502错误网关什么意思

发表于 2020-02-04 18:24:50 赞(0) 回复(0)

牧水s

打卡

发表于 2020-02-14 18:19:42 赞(0) 回复(0)

星如月勿忘初心 4#

打卡

发表于 2020-02-21 22:47:34 赞(0) 回复(0)

中都 5#

面试吉比特的时候就问了我http请求头响应头的知识，还有https，我的理解，服务器用明文的方式给客户端发送自己的公钥，客户端收到公钥之后，会生成一把密钥(对称加密用的)，然后用服务器的公钥对这把密钥进行加密，之后再把密钥传输给服务器，服务器收到之后进行解密，最后服务器就可以安全着得到这把密钥了，而客户端也有同样一把密钥，他们就可以进行对称加密了（对象加密效率高）。（这中间为了保证这个公钥是服务端的需要服务端提供CA证书和数字签名，否则会有中间人劫持的情况出现）；

发表于 2020-04-21 11:05:10 赞(0) 回复(0)

Shawn_Liu 6#

05/05打卡

发表于 2020-05-09 10:20:23 赞(0) 回复(0)