1. get和post分别是什么？区别？

**1. ​GET**

* ​**用途**: 用于从服务器获取数据。
* ​**数据传输方式**: 数据通过 URL 的查询字符串（Query String）传递。
  + 例如：https://example.com/search?q=keyword
* ​**特点**:
  + 数据附加在 URL 后面，因此长度有限（通常受浏览器和服务器限制）。
  + 数据是公开的，会显示在浏览器地址栏中，不适合传输敏感信息。
  + 可以被缓存，可以被收藏为书签。
  + 是幂等的（多次请求相同 URL 的结果相同）。
* ​**适用场景**: 获取资源，如加载网页、搜索、查询数据等。

**2. ​POST**

* ​**用途**: 用于向服务器提交数据。
* ​**数据传输方式**: 数据通过请求体（Request Body）传递，不会显示在 URL 中。
* ​**特点**:
  + 数据长度没有明确限制（受服务器配置影响）。
  + 数据不会显示在 URL 中，适合传输敏感信息（如密码、文件等）。
  + 不会被缓存，也不能被收藏为书签。
  + 不是幂等的（多次提交可能会产生不同的结果，例如多次提交表单可能会创建多个资源）。
* ​**适用场景**: 提交表单、上传文件、创建或更新资源等。

**1. 数据传输效率**

* ​**GET**: 更高效。
  + 数据通过 URL 的查询字符串传递，请求体为空，因此请求头和数据包更小，传输速度更快。
  + 适合传输少量数据（如搜索关键字、分页参数等）。
* ​**POST**: 相对较低效。
  + 数据通过请求体传递，请求头和数据包更大，传输速度较慢。
  + 适合传输大量数据（如表单、文件等）。

**2. 服务器处理效率**

* ​**GET**: 更高效。
  + 通常用于获取数据，服务器只需读取数据并返回，处理逻辑简单。
  + 由于是幂等的，可以缓存结果，减少服务器重复处理的压力。
* ​**POST**: 相对较低效。
  + 通常用于提交数据，服务器需要处理数据（如验证、存储、更新等），处理逻辑更复杂。
  + 由于不是幂等的，无法缓存结果，每次请求都需要重新处理。

**3. 网络缓存效率**

* ​**GET**: 更高效。
  + 可以被浏览器和代理服务器缓存，重复请求时可以直接从缓存中获取结果，减少网络传输和服务器负载。
* ​**POST**: 无法缓存。
  + 每次请求都需要重新发送数据并处理，无法利用缓存机制。

**4. 安全性**

* ​**GET**: 较低效（在安全性方面）。
  + 数据通过 URL 传递，容易被记录在浏览器历史、服务器日志或代理服务器中，存在安全隐患。
* ​**POST**: 更高效（在安全性方面）。
  + 数据通过请求体传递，不会显示在 URL 中，适合传输敏感信息。

1. http和https的区别

HTTP（HyperText Transfer Protocol）和HTTPS（HyperText Transfer Protocol Secure）是用于在客户端和服务器之间传输数据的协议。它们之间的主要区别在于安全性、端口号、证书等方面。以下是HTTP和HTTPS的主要区别：

**1. ​安全性**

* ​**HTTP**：HTTP是明文传输协议，数据在客户端和服务器之间传输时没有加密，容易被中间人攻击（Man-in-the-Middle Attack）窃取或篡改数据。
* ​**HTTPS**：HTTPS在HTTP的基础上加入了SSL/TLS加密协议，数据在传输过程中是加密的，确保了数据的机密性、完整性和身份认证，防止数据被窃取或篡改。

**2. ​端口号**

* ​**HTTP**：默认使用端口80。
* ​**HTTPS**：默认使用端口443。

**3. ​证书**

* ​**HTTP**：不需要证书，数据以明文形式传输。
* ​**HTTPS**：需要SSL/TLS证书来验证服务器的身份，并建立加密连接。证书由受信任的证书颁发机构（CA）签发，确保客户端与合法的服务器通信。

**4. ​性能**

* ​**HTTP**：由于没有加密和解密的过程，HTTP的传输速度通常比HTTPS快。
* ​**HTTPS**：由于需要进行加密和解密操作，HTTPS的传输速度相对较慢，但随着硬件和协议的优化，这种差距已经逐渐缩小。

**5. ​SEO（搜索引擎优化）​**

* ​**HTTP**：搜索引擎对HTTP网站的排名较低，尤其是涉及用户隐私和数据安全的网站。
* ​**HTTPS**：搜索引擎（如Google）对HTTPS网站给予更高的排名权重，HTTPS已成为SEO的重要因素之一。

**6. ​浏览器标识**

* ​**HTTP**：在浏览器地址栏中显示为http://，通常不会有任何安全标识。
* ​**HTTPS**：在浏览器地址栏中显示为https://，并且通常会有一个锁形图标，表示连接是安全的。

**7. ​应用场景**

* ​**HTTP**：适用于不涉及敏感数据的场景，如新闻网站、博客等。
* ​**HTTPS**：适用于涉及敏感数据的场景，如电子商务、在线支付、用户登录等。

**8. ​协议层**

* ​**HTTP**：工作在应用层，直接传输数据。
* ​**HTTPS**：在HTTP和TCP之间加入了SSL/TLS层，负责加密和解密数据。

**总结：**

HTTPS是HTTP的安全版本，通过加密和身份验证机制，确保了数据的安全性和完整性。随着网络安全意识的提高，越来越多的网站已经转向使用HTTPS，以保护用户隐私和数据安全。

1. http协议和socket区别，哪个协议更加高效