跨域请求和Ajax会带来安全隐患，主要是CSRF（Cross-site Request Forgery）跨站请求伪造。

为此，CORS产生了。

CORS分为简单请求和非简单请求

一、简单请求

必须满足：请求方式只能是GET、POST、HEAD

请求头只能包括 Accept Accept-Language Last-Event-ID Content-Language

Content-Type

Content-Type只能是：application/x-www-urlencoded ，multipart/form-data text/plain

浏览器发现是跨域请求，会自动处理。(推测是查看Referer和Host字段，或者浏览器查看当前页面的域和要请求的域)。浏览器会自动添加Origin字段，表明这是一个跨域请求。当服务器接收到这请求后，查看Access-Control-Allow-Origin和Access-Control-Allow-Method。

如果请求成功，当然是200 OK，不允许你请求的话返回403 Forbidden

二、非简单请求

1.预先请求

当不符合简单请求时，浏览器会先发送一个OPTION请求，用来和服务器协商是否可以发送实际的跨域请求。

这时候的请求报文中除了Origin字段，还有关键的Access-Control-Request-Method和Access-Control-Request-Headers。

服务器接收到预请求后，设置Access-Control-Allow-Origin、Access-Control-Allow-Method、Access-Control-Allow-Headers头部与浏览器沟通来判断是否允许这个请求。

如果预请求失败403，则不会再发送真正的跨域请求，节省了带宽。

带认证的请求：

默认不带cookie等凭证。但是将XMLHttpRequest对象的withCredentials设置为true，服务器设置Access-Control-Allow-Credentials为true就可以携带cookie等凭证。

请求报文

Origin

Access-Control-Request-Method

Access-Control-Request-Headers

响应报文

Access-Control-Allow-Origin

Access-Control-Allow-Methods

Access-Control-Allow-Credentials

Access-Control-Allow-Headers //预请求中

告诉浏览器在发送实际的跨域请求时，可以支持的请求头，可以是\*或者列表等等

Access-Control-Expose-Headers

指定浏览器可以获得的响应字段，除了默认的几个字段，浏览器在跨域请求时，其他字段是获得不到的。

Access-Control-Max-Age

服务器通过这个告诉浏览器，将预请求返回的结果缓存的时间。在缓存时间内，浏览器会使用缓存的预先结果判断是否还要发送跨域请求。