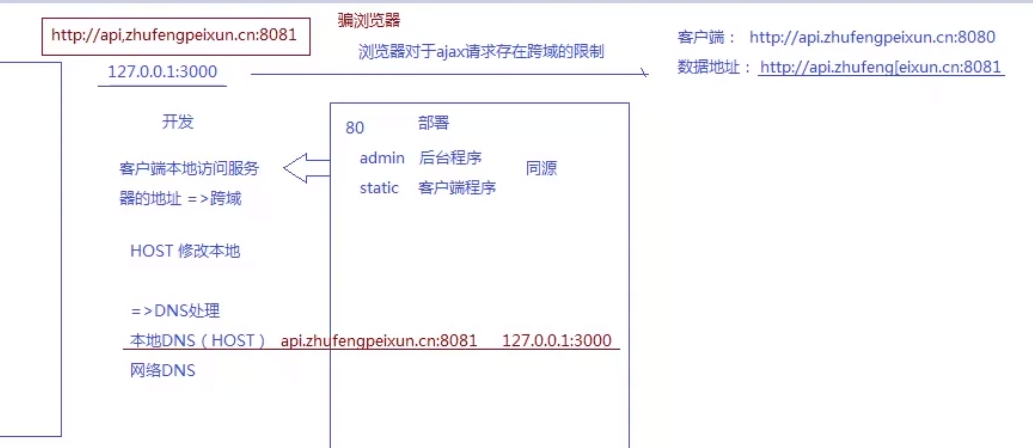
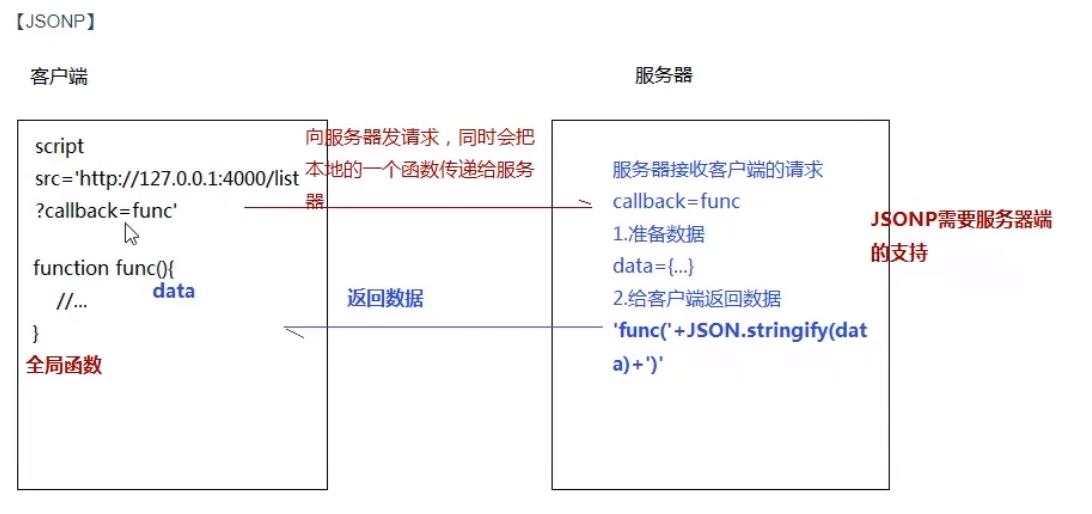
服务器与服务器不存在跨域

修改本地host

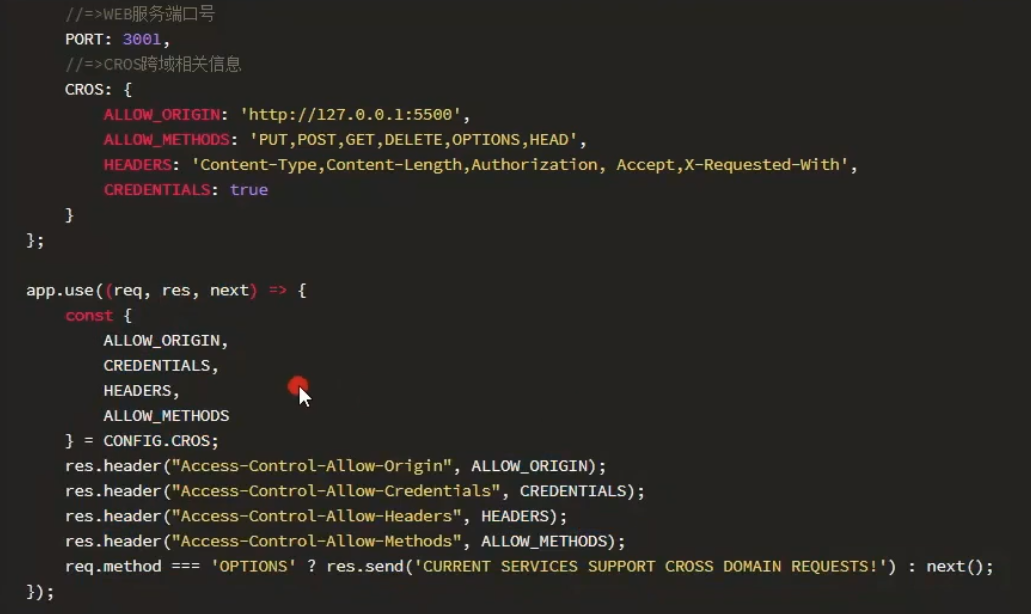


JSONP【只有get请求，不安全】



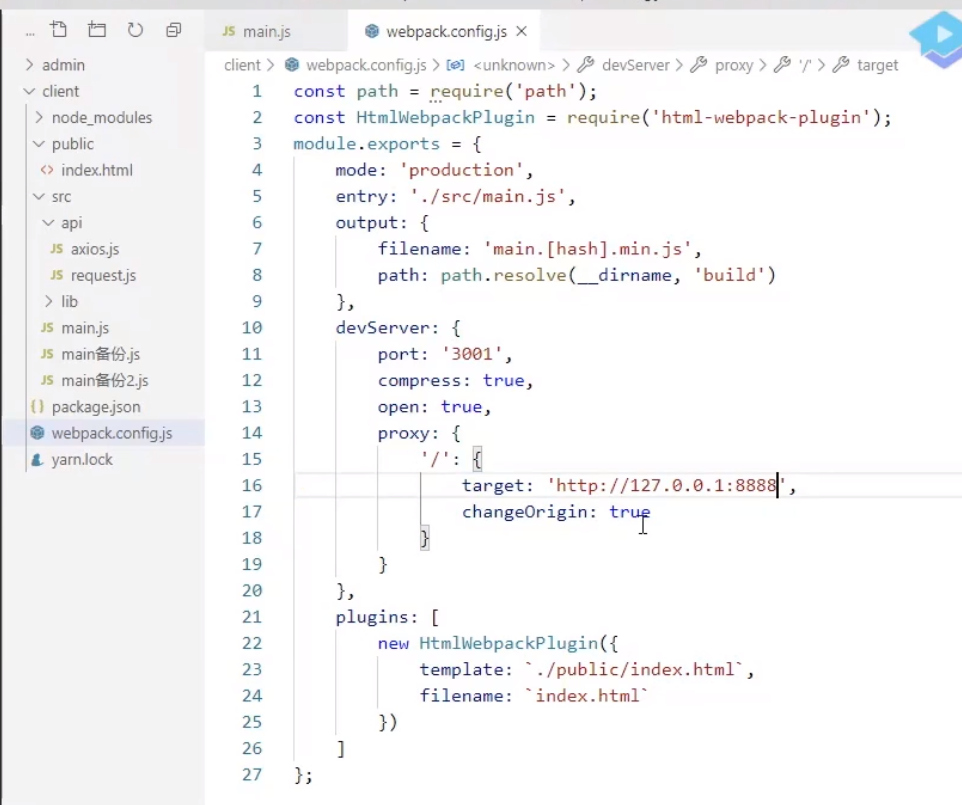
CORS【服务器和客户端约定header头就行 但是Access-Control-Allow-Origin: [http://api.bob.com](http://api.bob.com/) 或者\* 只有这俩种写法 也就只能接收一个源当接收\*的时候不能接收cookie】

细节：如果Origin指定的源，不在许可范围内，服务器会返回一个正常的HTTP回应。浏览器发现，这个回应的头信息没有包含Access-Control-Allow-Origin字段（详见下文），就知道出错了，从而抛出一个错误，被XMLHttpRequest的onerror回调函数捕获。注意，这种错误无法通过状态码识别，因为HTTP回应的状态码有可能是200。



PROXY

1. web端自带的代理 ：如vue react等 webpack-dev-server起一个web服务；



1. nginx的反向代理

