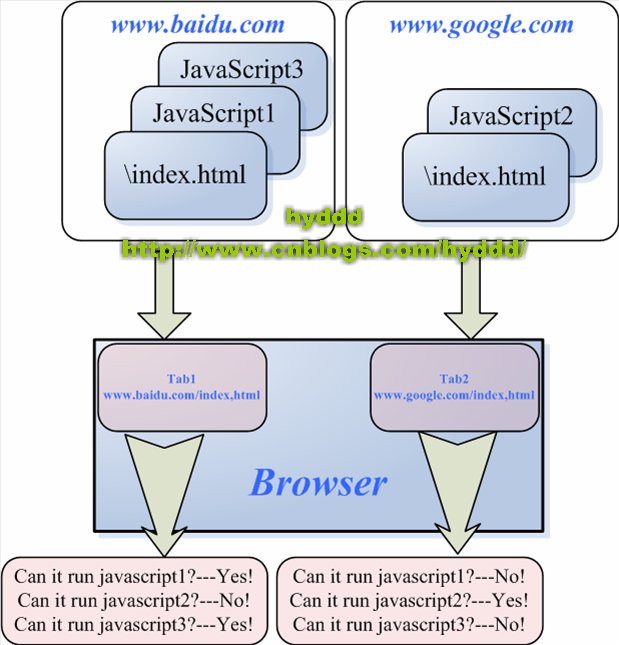
[Selenium私房菜系列7 -- 深入了解Selenium RC工作原理(2)](http://www.cnblogs.com/hyddd/archive/2009/05/30/1492289.html)

    继续前一篇的问题，为什么Selenium RC中的Selenium Server需要以这种代理服务器的形式存在?其实，这和浏览器的“同源策略”(The Same Origin Policy)有关。

**一.什么是同源策略**

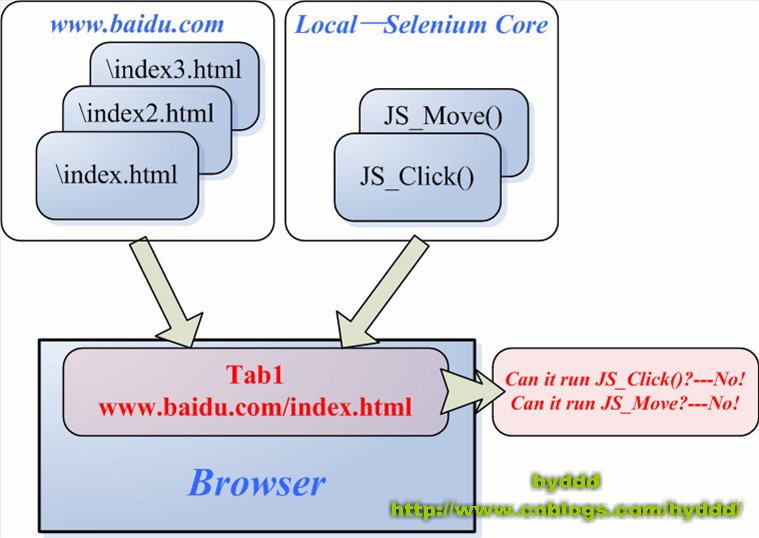
**同源策略**，它是由Netscape提出的一个著名的安全策略，现在所有的可支持javascript的浏览器都会使用这个策略。

**为什么需要同源策略**，这里举个例子：  
    假设现在没有同源策略，会发生什么事情呢？大家知道，JavaScript可以做很多东西，比如：读取/修改网页中某个值。恩，你现在打开了浏览器，在一个tab窗口中打开了银行网站，在另外一个tab窗口中打开了一个恶意网站，而那个恶意网站挂了一个的专门修改银行信息的JavaScript，当你访问这个恶意网站并且执行它JavaScript时，你的银行页面就会被这个JavaScript修改，后果会非常严重！而同源策略就为了防止这种事情发生，看下图：



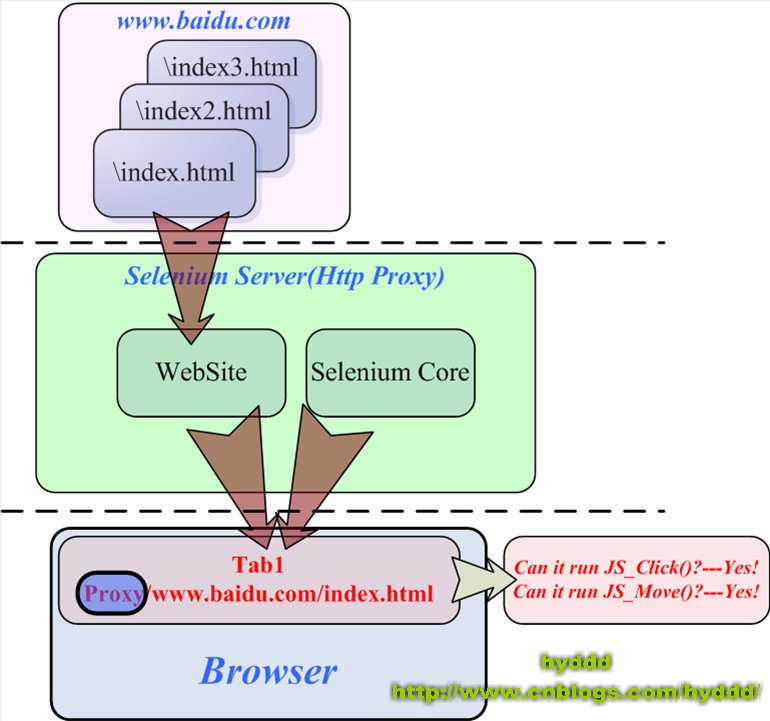
比如说，浏览器的两个tab页中分别打开了[http://](http://www.baidu.com/index.html)[www.baidu.com](http://www.baidu.com/)/index.html和http://[www.google.com](http://www.google.com/)/index.html，其中，JavaScript1和JavaScript3是属于百度的脚本，而JavaScript2是属于谷歌的脚本，当浏览器的tab1要运行一个脚本时，便会进行同源检查，只有和[www.baidu.com](http://www.baidu.com/)同源的脚本才能被执行，所谓**同源**，就是指域名、协议、端口相同。所以，tab1只能执行JavaScript1和JavaScript3脚本，而JavaScript2不能执行，从而防止其他网页对本网页的非法篡改。

**二.Selenium Server为什么以这种代理服务器的形式存在**  
    上面说了同源策略，那同源策略的Selenium Server有什么关系呢？？呵呵，上一篇说过，Selenium Core是一堆JS函数的集合，它是我们操作浏览器的基础。当存在同源策略时，便出现一些问题，看下图：



因为Selenium Core的JS脚本的“源”是localhost，所以浏览器会阻止Selenium Core的JS脚本在测试页面上执行，这就是为什么在本系列第一篇中说，如果只使用Selenium Core进行测试，需要把Selenium Core安装到远程服务器上。

    为了解决上面这个问题，Selenium RC中的Selenium Server就以代理服务器的形式出现了，下图说明它是如何借助代理的身份蒙骗浏览器的:>

[](http://images.cnblogs.com/cnblogs_com/hyddd/WindowsLiveWriter/Selenium7SeleniumRC2_CC96/3_2.jpg)

Selenium Server以代理的形式存在，通过修改WebSite的源信息，从而达到欺骗浏览器的目的，就这样，Selenium RC就轻松绕过了同源策略。在上图中，浏览器会认为WebSite和Selenium Core来自同一个“源”----代理服务器！