**HTTP Session**

一、淺析

HTTP協議(http://www.w3.org/Protocols/)是“一次性單向”協議。服務端不能主動連接客戶端，只能被動等待並答复客戶端請求。客戶端連接服務端，發出一個HTTP Request，服務端處理請求，並且返回一個HTTP Response給客戶端，本次HTTP Request-Response Cycle結束。HTTP協議並不支持服務端保存客戶端的狀態信息。於是Web Server中引入了session的概念，用來保存客戶端的狀態信息。

假設Web Server是商場的存包處，HTTP Request是顧客，第一次到存包處，管理員把顧客的物品存放在某一個櫃子裡面(櫃子就相當於Session)，然後把號碼牌交給顧客，作為取包憑證(號碼牌就是Session ID)。顧客(HTTP Request)下一次來時，要把號碼牌(Session ID)交給存包處(Web Server)的管理員。管理員根據號碼牌(Session ID)找到相應的櫃子(Session)，根據顧客(HTTP Request)的請求，Web Server可以取出、更換、添加櫃子(Session)中的物品，Web Server也可以讓顧客(HTTP Request)的號碼牌和號碼牌對應的櫃子(Session)失效。顧客(HTTP Request)的忘性很大，管理員在顧客回去的時候(HTTP Response)都要重新提醒顧客記住自己的號碼牌(Session ID)。顧客(HTTP Request)下次來的時候，就又帶著號碼牌回來了。Session ID實際上是在客戶和服務端間通過HTTP Request和HTTP Response傳遞。號碼牌(Session ID)必須包含在HTTP Request裡面。HTTP Request的具體格式，參見HTTP協議(http://www.w3.org/Protocols/)。

在Java Web Server(即Servlet/JSP Server)中，Session ID用jsessionid表示(請參見Servlet規範)。

HTTP Request一般由3部分組成：

(1) Request Line。這一行由HTTP Method(如GET或POST)、URL、和HTTP版本號組成。例如，GET http://www.w3.org/pub/WWW/TheProject.html HTTP/1.1

GET http://www.google.com/search?q=Tomcat HTTP/1.1

POST http://www.google.com/search HTTP/1.1

GET http://www.somsite.com/menu.do;jsessionid=1001 HTTP/1.1

(2) Request Headers。定義了重要的頭部信息，如瀏覽器的種類，語言，類型。Request Headers中還可包括Cookie的定義。例如：

User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)

Accept-Language: en-us

Cookie: jsessionid=1001

(3) Message Body。如果HTTP Method是GET，Message Body為空。如果HTTP Method是POST，說明這HTTP Request是submit一個HTML Form的結果，那Message Body為HTML Form裡面定義的Input屬性。例如，

user=guest

password=guest

jsessionid=1001

如果把HTML Form元素的Method屬性改為GET。Message Body為空，所有的Input屬性都會加在URL的後面。瀏覽器的URL地址欄中會看到這些屬性，類似於http://www.somesite/login.do?user=guest&password=guest&jsessionid=1001

從理論上來說，這3個部分(Request URL，Cookie Header, Message Body)都可以用來存放Session ID。由於Message Body方法必須需要一個包含Session ID的HTML Form，所以這種方法不通用。一般用來實現Session的方法有兩種：

1. URL重寫。Web Server返回Response時，檢查頁面中所有的URL，包括所有的連接，和HTML Form的Action屬性，在URL後面加上“;jsessionid=XXX”。下一次，用戶訪問這個頁面中的URL。jsessionid就會傳回到Web Server。
2. Cookie。如果客戶端支持Cookie，Web Server在返回Response時，在Response的Header部分，加入一個“set-cookie: jsessionid=XXXX”header屬性，把jsessionid放在Cookie里傳到客戶端。客戶端會把Cookie存放在本地文件裡，下次訪問Web Server的時候，再把Cookie的信息放到HTTP Request的“Cookie”header屬性裡面，這樣jsessionid就隨著HTTP Request返回給Web Server。

**cookie和session機制之間的區別與聯繫**

cookie機制採用在客戶端保持狀態的方案。它是在用戶端的會話狀態的存貯機制，需要用戶打開客戶端的cookie支持。cookie是為了解決HTTP協議無狀態的缺陷。session機制是在客戶端與服務器之間保持狀態的解決方案。採用服務器端保持狀態的方案在客戶端也要保存一個標識，所以session機制需藉助cookie機制來達到保存標識的目的。而session提供了方便管理全局變量的方式。

session針對每一個用戶，變量的值保存在服務器上，用一個sessionID來區分是哪個用戶session變量，這個值是通過用戶的瀏覽器在訪問時返回給服務器，當客戶禁用cookie時，這個值也可能設置為由get來返回給服務器。

就安全性來說：當你訪問一個使用session的站點，同時在自己機子上建立一個cookie，建議在服務器端的SESSION機制更安全些。因為它不會任意讀取客戶存儲的信息。正統的cookie分發是通過擴展HTTP協議來實現的，服務器通過在HTTP的響應頭中加上一行特殊的指示以提示瀏覽器按照指示生成相應的cookie。從網絡服務器觀點看所有HTTP請求都獨立於先前請求。每個HTTP響應完全依賴於相應請求中包含的信息狀態管理機制克服了HTTP的一些限制並允許網絡客戶端及服務器端維護請求間的關係。在這種關係維持的期間叫做會話(session)。Cookies是服務器在本地機器上存儲的小段文本並隨每一個請求發送至同一個服務器。網絡服務器用HTTP頭向客戶端發送cookies，在客戶終端，瀏覽器解析這些cookies並將它們保存為一個本地文件，它會自動將同一服務器的任何請求縛上這些cookies。

**理解session機制**

session機制是服務器端的機制，服務器用類似於散列表的結構保存信息。當程序為客戶端的請求創建一個session時，服務器先檢查客戶端的請求裡是否包含session標識(session id)，如果已包含，則此客戶已端創建session，服務器就按照session id把session檢索出來使用(如檢索不到，可能會新建一個)，如果客戶端請求不包含session id，則為客戶端創建session並生成與此session相關聯的session id，session id的值是一個不重複，又不易被找到規律仿造的字符串，這個session id將被在本次響應中返回給客戶端保存。保存session id的方式可採用cookie，這樣在交互過程中瀏覽器可自動的按照規則把這個標識發揮給服務器。一般cookie的名字都是類似於JSESSIONID。如weblogic對於web應用程序生成的cookie，JSESSIONID=ByOK3vjFD75aPnrF7C2HmdnV6QZcEbzWoWiBYEnLerjQ99zWpBng!-145788764。由於cookie可被人為禁止，要有其他機制在cookie被禁止時仍能夠把session id傳遞回服務器。常被用的技術叫做URL重寫，把session id直接加在URL路徑後，附加方式是作為URL路徑的附加​​信息，表現形式為*http://.../xxx;jsessionid= By…64*。另一種是作為查詢字符串加在URL後面，表現形式為*http://...../xxx?jsessionid=By...64*。這兩種方式對於用戶來說是沒有區別的，只是服務器在解析時處理的方式不同，第一種方式有利於把session id的信息和正常程序參數區分開來。為了在整個交互過程中始終保持狀態，在每個客戶端可能請求的路徑後面都包含這個session id。

session機制常聽到誤解“只要關閉瀏覽器，session就消失”。想像會員卡的例子，除非顧客主動對店家提出銷卡，否則店家不會輕易刪除顧客資料。session也一樣，除非程序通知服務器刪除一個session，否則服務器會一直保留，程序一般都是在用戶做log off時發指令去刪除session。然而瀏覽器從來不會主動在關閉前通知服務器它將要關閉，因此服務器不會有機會知道瀏覽器已關閉，之所以有這種錯覺，是大部分session機制都使用會話cookie來保存session id，而關閉瀏覽器後這個session id就消失了，再次連接服務器時也無法找到原來的session。如果服務器設置的cookie被保存到硬盤上，或者使用某種手段改寫瀏覽器發出的HTTP請求頭，把原來的session id發送給服務器，則再次打開瀏覽器仍然能夠找到原來的session。由於關閉瀏覽器不會導致session被刪除，迫使服務器為session設置了一個失效時間，當距離客戶端上一次使用session的時間超過這個失效時間時，服務器就認為客戶端已停止活動，會刪除session以節省存儲空間。

**由JSESSIONID談cookie與SESSION的區別和聯繫**

HTTP是無狀態的協議，客戶每次讀取web頁面時，服務器都打開新的會話，而服務器也不會自動維護客戶的上下文信息，要怎麼實現網上商店中的購物車呢，session是保存上下文信息的機制，它是針對每一個用戶的，變量的值保存在服務器端，通過SessionID來區分不同的客戶，session是以cookie或URL重寫為基礎的，默認使用cookie來實現，系統會創造一個名為JSESSIONID的輸出cookie，叫做session cookie，以區別persistent cookies，也就是通常所說的cookie，session cookie存儲於瀏覽器內存中，不是寫到硬盤上，通常是看不到JSESSIONID的，但是當我們把瀏覽器的cookie禁止後，web服務器會採用URL重寫的方式傳遞Sessionid，就可以在地址欄看到sessionid=KWJHUG6JJM65HS2K6之類的字符串。

明白了原理，我們就可以很容易的分辨出persistent cookies和session cookie的區別了，session cookie針對某一次會話而言，會話結束session cookie也就隨著消失了，而persistent cookie是存在於客戶端硬盤上的一段文本(通常是加密的)，而且可能會遭到cookie欺騙以及針對cookie的跨站腳本攻擊，自然不如session cookie安全了。

通常session cookie是不能跨窗口使用的，當你新開了一個瀏覽器窗口進入相同頁面時，系統會賦予你一個新的sessionid，這樣信息共享的目的就達不到了，此時可以把sessionid保存在persistent cookie中，然後在新窗口中讀出來，就可以得到上一個窗口SessionID了，通過session cookie和persistent cookie的結合實現了跨窗口的session tracking(會話跟踪)。