HTTP State Management using Cookies

.....All you need to know about HTTP cookies.....

Tharuja Sandeepanie Feb 21, 2020 · 5 min read

What are HTTP Cookies..?

As you all know, HTTP is a stateless protocol which means that the client-server connection is lost once the transaction ends between them. So, HTTP server does not save details about each client. Hence, server can not decide whether a request came from a client who has requested before or from a new one.

Cookie is used as a stolution for this problem. It is a small piece of data sent from server and stored on client's computer by the web browser when a client sends a request to a particular server. It is reliable mechanism to remember stateful information since HTTP is stateless.

HTTP cookie is a combination of following components.

- Name
- Value
- Attributes- Domain, Path, Expires, Max-Age, HttpOnly, Secure

A) The **Domain** and **Path** attributes are the scope of the cookie. They define to which website the cookie belongs to. If a cookie's Domain and Path attributes are not specified by the server, they default to the domain and path of the resource that was requested. So that, the cookie will only be sent only for that domain and path (also known as a host-only cookie). If domain and path are specified, all sub domains and sub directories are also included.

B) The **Expires** attribute defines a specific date and time for when the browser should delete the cookie. The date and time are specified in the form "Wdy, DD Mon YYYY HH:MM:SS GMT" format according to the RfC -6265 specification. Alternatively, the **Max-Age** attribute sets the cookie's expiration using seconds, relative to the creation time of the cookie. If any of these two are not specified, it will be a session cookie.

C) The **HttpOnly** attribute tells browser to send cookies only to HTTP (and HTTPS) requests.

D) The **Secure** attribute tells browsers to use cookies only via secure/encrypted connections (HTTPS)

State management using Cookies...

> *Cookies use two HTTP headers: **Set-Cookie** and **Cookie**.*

When receiving an HTTP request, a server can send cookies using the “Set-Cookie” header in an HTTP response and send to the user. When sending multiple cookies server must use separate Set-Cookie headers for each cookie.

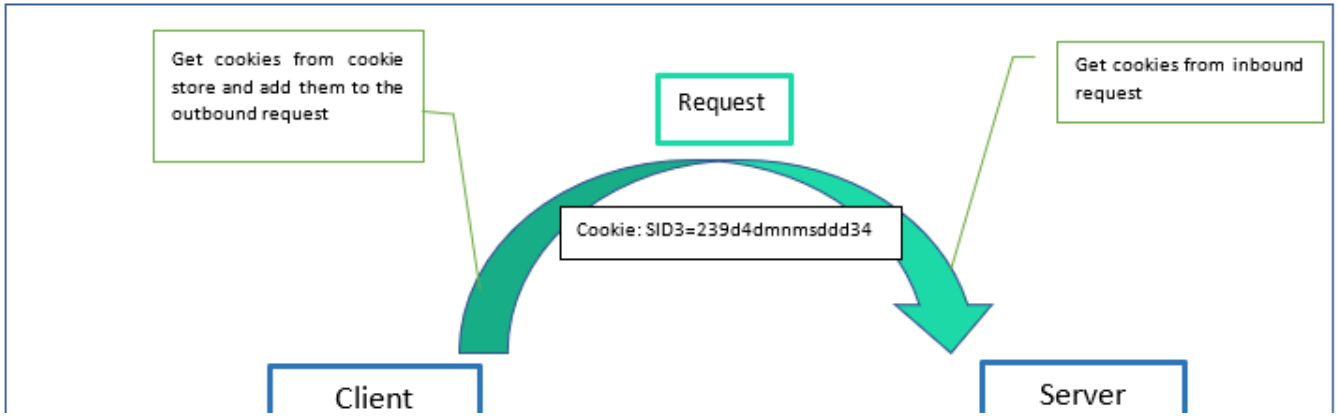
```
HTTP/1.0 200 OK
Content-type: text/html
Set-Cookie: theme=light
Set-Cookie: lang=eng; Expires=Wed, 09 Jun 2021 10:18:14 GMT
```

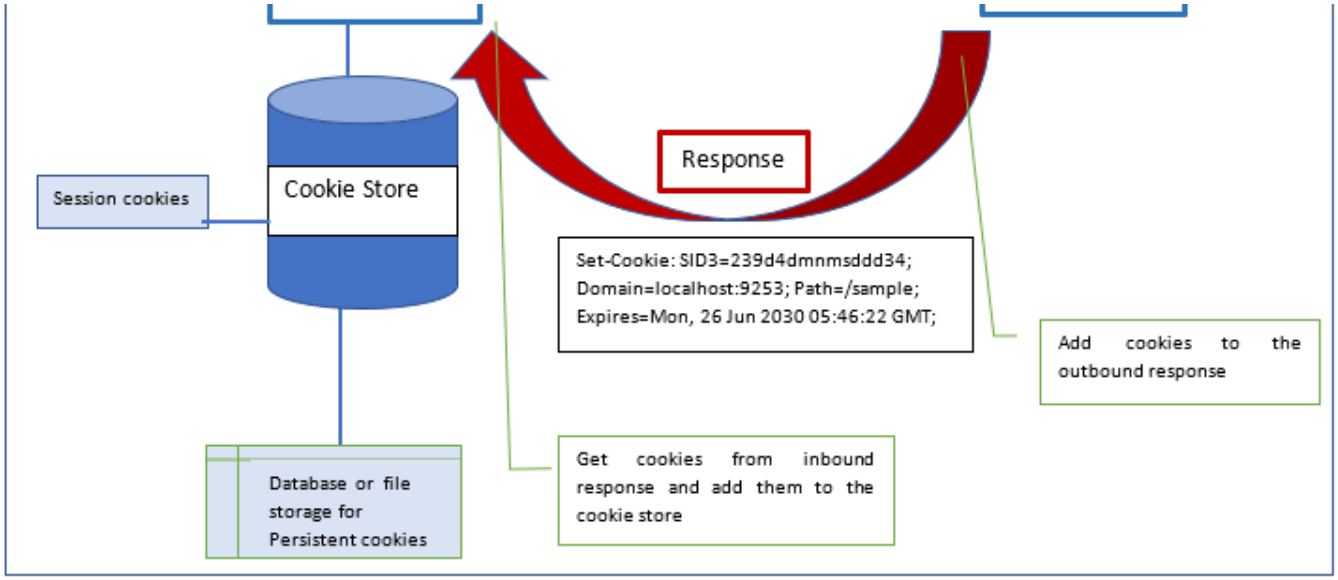
These cookies are stored by the browser temporarily or persistently in client’s cookie store, and then relevant cookies are sent with each subsequent requests to that particular server inside a “Cookie” HTTP header.

```
GET /spec.html HTTP/1.1
Host: www.sample.com
Cookie: theme=light; lang=eng
```

Through this way, server can get to know that this request is sent by a client who has previously requested to this server. The server can add new cookies, modify existing cookies, or remove cookies of the client by including more Set-Cookie headers in the response.

If the server wants to modify the value of an existing cookie , server can send the modified cookie under a Set-Cookie header in the response to a page request. Then browser replaces the old cookie with the new cookie. According to the RfC -6265 specification , two cookies are considered as similar cookies if both have same name,same domain and same path values.





Over all process of HTTP cookies

Types of cookies

1. **Session cookie** — It exists only in temporary memory while a user is visiting a website. Once the user closes the web browser, these cookies are removed by the browser. They do not have an expiration date value, which signals the browser that they are session cookies.
2. **Persistent cookie** — A persistent cookie expires at a specific date or after a specific length of time. During that time period, this cookie will be sent to the server every time the user visits the website that it belongs to. These cookies are stored in the client's cookie store using a database or in a file system for the specified time duration.

3. **Secure cookie** — A secure cookie is sent only to a server with an encrypted request over the HTTPS protocol.
4. **HTTP-only cookie** — Cookies with HttpOnly attribute are sent only with HTTP requests.
5. **Third-party cookie**- They are cookies that are set by a website other than the one client is currently visiting. When rendering an HTML document, a user agent often requests resources from other servers (such as advertising networks). These third-party servers can use cookies to track the user even if the user never visits the server directly. For example, if a user visits a site that contains content from a third party and then later visits another site that contains content from the same third party, the third party can track the user between the two sites.

Purpose of cookies

When a user visits a website for several times, the server will consider each and every request as unique. To uniquely remember a user, the server sends the cookies along with the response which is saved in user's local machine. Then next time user hits the same server, he will get a response which matches with his preferences such that server can recognize him.

Cookies are mainly used for three purposes:
A) Session management — Logins, shopping carts or anything else the server should remember.

B) Personalization — User preferences, themes, language, country and other settings.

C) Tracking — Recording and analyzing user behavior.

Removing cookies

If server wants to remove a cookie, server must returns that cookie with a past expiration date. This will signal to the browser that the cookie should be removed. Session cookies must be removed after the browser is closed and all expired persistent cookies must be removed by web browser from the cookie store if, at any time, an expired cookie exists in the cookie store.

> *Note:- This article is based on the rules in RfC-6265 specification..*

Http Cookie