David M. Kristol
Bell Laboratories, Lucent Technologies

HTTP Proxy State Management Mechanism

Status of this Memo

This is author’s draft 1.3.

1. ABSTRACT

This document specifies a way to create a stateful session, using HTTP requests and responses, between an HTTP proxy server and its client. It describes two new headers, `Pcookie` and `Set-Pcookie`, which carry state information between participating HTTP proxy servers and their clients.

2. INTRODUCTION

RFC 2109 defines an HTTP State Management Mechanism that applies between user agents and origin servers. That is, it is end-to-end. Occasions arise, however, where it is useful for an HTTP proxy server and its client (which could be a user agent or another proxy server) to share state. That is, the proxy server has state information about its relationship with the client that it wants the client to remember and to return with each request. Examples include identity or preference information. This specification defines such a mechanism, which is modeled after the end-to-end mechanism.

3. TERMINOLOGY

The terms *user agent*, *client*, *server*, *proxy*, and *origin server* have the same meaning as in the HTTP/1.1 specification [RFC 2068].

Host name (HN) means either the host domain name (HDN) or the numeric Internet Protocol (IP) address of a host. The fully qualified domain name is preferred; use of numeric IP addresses is strongly discouraged.

The term *proxy-host* refers to the proxy, both host name and port, that receives a request, and *request-URI* refers to the `abs_path` portion of the `absoluteURI` (`http_URL`) of the HTTP request line.

To maintain parallel terminology with the HTTP State Management Mechanism, I will use the term *Pcookie* to refer to the state information that passes between a proxy server and client, and that gets stored by the client.

4. STATE AND SESSIONS

This document describes a way to create stateful sessions with HTTP requests and responses. Currently, HTTP proxy servers respond to each client request without relating that request to previous or subsequent requests; this state management mechanism allows clients and proxy servers that wish to exchange state information to place HTTP requests and responses within a larger context, which I term a ‘‘proxy session.’’

5. DESCRIPTION

I describe here a way for a proxy server to send state information to its client, and for the client to return the state information to the proxy server. The goal is to have a minimal impact on HTTP clients and proxy servers.

5.1 Syntax: General

The two state management headers, `Set-Pcookie` and `Pcookie`, have common syntactic properties involving attribute-value pairs. The following grammar uses the notation, and tokens `DIGIT` (decimal digits), `token` (informally, a sequence of non-special, non-white space characters), and `http_URL` from the HTTP/1.1 specification [RFC 2068] to describe their syntax.

```
av-pairs    =    av-pair *(";" av-pair)
av-pair     =    attr ["=" value]        ; optional value
attr        =    token
value       =    token | quoted-string
```

Attributes (names) (attr) are case-insensitive. White space is permitted between tokens. Note that while the above syntax description shows `value` as optional, most attrs require them.

NOTE: The syntax above allows whitespace between the attribute and the = sign.

5.2 Proxy Server Role

5.2.1 General The proxy server initiates a session, if it so desires. To do so, it returns an extra response header to the client, `Set-Pcookie.` (The details follow later.)

A client returns a `Pcookie` request header (see below) to the proxy server if it chooses to continue a session. The proxy server may ignore it or use it to determine the current state of the session. It may send back to the client a `Set-Pcookie` response header with the same or different information, or it may send no `Set-Pcookie` header at all. The origin server effectively ends a session by sending the client a `Set-Pcookie` header with `Max-Age=0`.

Proxy servers may return `Set-Pcookie` response headers with any response. Clients should send `Pcookie` request headers, subject to other rules detailed below, with every request.

5.2.2 `Set-Pcookie` *Syntax* The syntax for the `Set-Pcookie` response header is

```
set-pcookie-hdr =    "Set-Pcookie:" 1#set-pcookie
set-pcookie     =    NAME "=" VALUE *(";" set-pcookie-av)
NAME            =    attr
VALUE           =    value
set-pcookie-av  =    "CommentURL" "=" <"> http_URL <">
                |    "Max-Age" "=" value
                |    "Persist" "=" value
                |    "Version" "=" 1*DIGIT
```

Informally, the `Set-Pcookie` response header comprises the token `Set-Pcookie:`, followed by a comma-separated list of one or more Pcookies. Each Pcookie begins with a *NAME=VALUE* pair, followed by zero or more semi-colon-separated attribute-value pairs. The syntax for attribute-value pairs was shown earlier. The specific attributes and the semantics of their values follows. The *NAME=VALUE* attribute-value pair must come first in each Pcookie. The others, if present, can occur in any order. If an attribute appears more than once in a set-pcookie, only the value associated with the first appearance of the attribute shall be used; subsequent values after the first must be ignored.

The *NAME* of a Pcookie may be the same as one of the attributes in this specification. However, because the Pcookie's *NAME* must come first in a `Set-Pcookie` response header, the *NAME* and its *VALUE* cannot be confused with an attribute-value pair.

NAME=VALUE

> **Required**. The name of the state information (''Pcookie'') is *NAME*, and its value is *VALUE*.
>
> The *VALUE* is opaque to the client and may be anything the proxy server chooses to send, possibly in a server-selected printable ASCII encoding. ''Opaque'' implies that the content is of interest and relevance only to the proxy server. The content may, in fact, be readable by anyone that examines the `Set-Pcookie` header.

`CommentURL="`*http_URL*`"`

> Optional. Because Pcookies could be used to derive or store private information about a user, the `CommentURL` attribute allows a proxy server to document how it intends to use the Pcookie. The user can inspect the information identified by the URL to decide whether to initiate or continue a session with this Pcookie.

`Max-Age=value`

> Optional. The `value` of the `Max-Age` attribute defines the lifetime of the Pcookie, in seconds. The delta-seconds `value` is a decimal non-negative integer. After delta-seconds seconds elapse, the client should discard the Pcookie. A value of zero means the Pcookie should be discarded immediately.

`Persist=value`

> Optional. The `value` of the `Persist` attribute determines whether the client should remember the value of the Pcookie across client invocations. The `value` must be either `yes` or `no`.

`Version=value`

> **Required**. The `value` of the `Version` attribute, a decimal integer, identifies the version of the state management specification to which the Pcookie conforms. For this specification, `Version=0` applies.

5.3 Client Role

5.3.1 Interpreting `Set-Pcookie` The client keeps separate track of state information that arrives via `Set-Pcookie` response headers from each proxy server (as distinguished by name or IP address and port). The client must ignore attribute-value pairs whose attribute it does not recognize, or whose value it does not understand. The client applies these defaults for optional attributes that are missing from a `Set-Pcookie` response header:

`Max-Age` The default behavior is to discard the Pcookie when the client exits.

`Persist` The default behavior is dictated by the presence or absence of a `Max-Age` attribute. If a `Max-Age` attribute is present, the default is `Persist=yes`. Otherwise the default is `Persist=no`.

5.3.2 Pcookie Management If a client receives a `Set-Pcookie` response header whose *NAME* is the same as a pre-existing Pcookie from the same proxy-host, the new Pcookie supersedes the old. However, if the `Set-Pcookie` has a value for `Max-Age` of zero, the (old and new) Pcookie is discarded. Otherwise a Pcookie persists (resources permitting) until whichever happens first, then gets discarded: its `Max-Age` lifetime is exceeded; or, if the `Persist=no` attribute is set, the client terminates the session.

Because clients have finite space in which to store Pcookies, they may also discard older Pcookies to make space for newer ones, using, for example, a least-recently-used algorithm, along with constraints on the maximum number of Pcookies that each proxy server may set.

If a `Set-Pcookie` response header includes a `CommentURL` attribute, clients that are also user agents should store that information in a human-readable form with the Pcookie, or, preferably, should allow the user to follow the `http_URL` link as part of a Pcookie inspection user interface.

User agents should allow the user to control Pcookie destruction, but they must not extend the Pcookie's lifetime beyond that controlled by the `Max-Age` and `Persist` attributes. An infrequently-used Pcookie may function as a ‘‘preferences file’’ for network applications, and a user may wish to keep it even if it is the least-recently-used Pcookie. One possible implementation would be an interface that allows the permanent storage of a Pcookie through a checkbox (or, conversely, its immediate destruction).

Privacy considerations dictate that the user have considerable control over Pcookie management. The **PRIVACY** section contains more information.

5.3.3 Sending Pcookies to the Proxy Server When it sends a request to a proxy server, the client sends a `Pcookie` request header if it has Pcookies that are applicable to the request, based on

- the proxy-host
- the Pcookie's age.

The syntax for the header is:

```
pcookie-hdr     =    "Pcookie:" 1#pcookie
pcookie         =    pcookie-value *(";" pcookie-av)
pcookie-av      =    pcookie-version
pcookie-value   =    NAME "=" VALUE
pcookie-version =    "Version" "=" value
NAME            =    attr
VALUE           =    value
```

The value of the pcookie-version attribute must be the value from the `Version` attribute of the corresponding `Set-Pcookie` response header. Otherwise the value for pcookie-version is `0`.

Note that there is no `CommentURL` attribute in the `Pcookie` request header that would correspond to the one in the `Set-Pcookie` response header. The client does not return the comment information to the proxy server.

The proxy applies the following rules to choose applicable pcookie-values to send in `Pcookie` request headers from among all the Pcookies it has received.

Domain Selection
: The client returns Pcookies to the proxy-host from which they came, but only when that proxy-host is being used as a proxy server for HTTP requests.

Max-Age Selection
: Pcookies that have expired should have been discarded and thus are not sent to a proxy server.

Note that multiple Pcookies can satisfy the criteria above. They are sent in the `Pcookie` header in arbitrary order.

6. PRIVACY

Informed consent should guide the design of systems that use Pcookies. A client should be able to find out how a proxy plans to use information in a Pcookie and should be able to choose whether or not those policies are acceptable. Both the client and the proxy server must assist informed consent.

6.1 Client (User Agent) Role

A client that is a user agent should provide users with a way to control and examine Pcookies. The control mechanisms provided should at least allow the user

- to completely disable the sending and saving of Pcookies.
- to determine whether a stateful proxy session is in progress.
- to control the saving of a Pcookie on the basis of the Pcookie's proxy-host.

Such control could be provided, for example, by mechanisms

- to notify the user when the user agent is about to send a Pcookie to the proxy server, to offer the option not to begin a session.
- to display a visual indication that a stateful proxy session is in progress.
- to let the user decide which Pcookies, if any, should be saved when the user concludes a window or user agent session.
- to let the user examine the contents of a Pcookie at any time.

6.2 Proxy Server Role

A proxy server should promote informed consent by adding `CommentURL` information to the Pcookies it sends. `CommentURL` can provide rich information in a multiplicity of languages.

7. SECURITY CONSIDERATIONS

7.1 Clear Text

The information in the `Set-Pcookie` and `Pcookie` headers is unprotected. Two consequences are:

1. Any sensitive information that is conveyed in them is exposed to intruders.
2. A malicious intermediary could alter the headers as they travel in either direction, with unpredictable results.

These facts imply that information of a personal and/or financial nature should only be sent over a secure channel. For less sensitive information, or when the content of the header is a database key, an origin server should be vigilant to prevent a bad `Pcookie` value from causing failures.

8. AUTHOR'S ADDRESS

David M. Kristol
Bell Laboratories, Lucent Technologies
600 Mountain Ave. Room 2A-333
Murray Hill, NJ 07974

Phone: (908) 582-2250
FAX: (908) 582-1239
Email: `dmk@bell-labs.com`