HTTP

1. **http请求种类（h0001）**
2. 简单请求（simple request）
3. 非简单请求（not-so-simple request）

**判断简单请求的种类的两个条件：**1）.请求方法必须是以下的一种

get 查询

head

post

2）.HTTP头只能包括以下信息

Accept

Accept-Language

Content-Language

Last-Event-ID

Content-Type只限于：[application/x-www-form-urlencoded,

multipart/form-data,text/plain]

DPR

Downlink

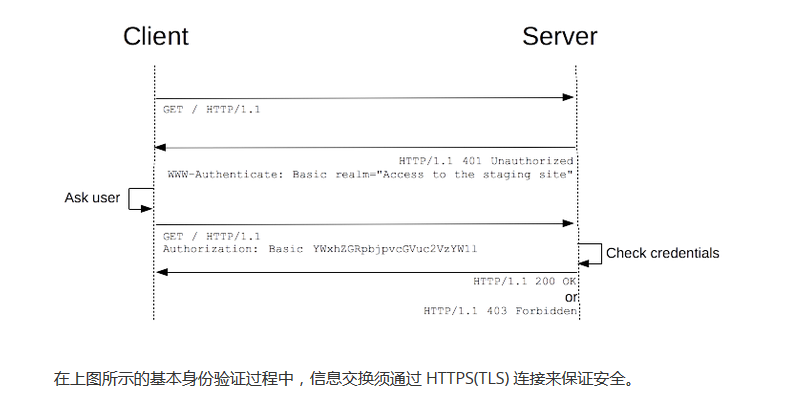
Save-Data

View-Width

Width

**不满足以上两个条件的视为非简单请求**

1. **authorization**



**区别于独立的头信息和响应状态码，资源认证和代理认证可以并存。**

# url与资源

## url

是uri的一个子集（http规范将uri作为其资源标识符，实际上http处理的只是url）

url也可以用http之外的其他协议来访问

如 e-mail ftp

mailto:president@whitehouse.gov

## 构成部分

url语法建立在9部分构成的通用格式

<scheme>://<user> :<password>@<host>:<port>/<path>;<params>?<query>#<frag>

方案 用户 密码 主机 端口 路径 参数 查询 片段

方案

如何访问资源（也就是协议）

大小写无关

用户名与密码

某些方案需要输入用户名和密码，如ftp。如果一些代理没有输入用户名和密码，如ie（会插入anonymous作为用户名，密码为IEUser）

主机与端口号

路径

说明资源位于服务器什么地方

参数

用 ；将其余路径分割，每一个路径段都可以有参数

[www.e.com/laalalal;sale=false/index.html;good=false](http://www.e.com/laalalal;sale=false/index.html;good=false)

查询

？a=1&b=2

片段

片段支持指向文档中一个特定的小节（文档中位置）

## 相对url

相对url是基于 基础url的。

基础url

在资源中显示提供

<base>

封装资源的基础url

当前资源文件的url

## url在浏览器地址栏中输入的自动扩展

主机名扩展

历史扩展

## url字符

由于url是可移植的，其需要对互联网上的所有资源命名，因而其在所有互联网协议上都可以安全传输（不能损失任何信息）很重要。

而一些协议（如简单邮件协议的传输方法会剥去一些特定字符），为避免这一问题，url只能使用一些较小的，通用的安全字符表中的字符。

同时也为了可阅读性，不可见，不能打印的字符

同时也需要通用的安全字符表之外的二进制数据或字符。（需要一种转义机制）

# HTTP报文

## 报文流

上游，下游：描述报文流向

请求 ，响应 上下游相反

在流动过程中，会经过代理

## 组成部分

简单的格式化数据块

起始行（对报文描述 ： start line）

首部块（包含属性的 ： header）

主体（数据 ：body）

起始行和首部就是由行分隔的ASCII文本。分隔符号为：一个回车符 + 一个换行符（CRLF） 或者 一个换行符

entity-body：实体

reason-phrase：原因短语--只对人有意义

请求格式

<method> <request-url><version>

<headers>

<entity-body>

响应格式

<version> < status> <reason-phrase>

<headers>

<entity-body>

## 方法

安全方法： GET ，HEAD

GET :

请求资源

HEAD:

作用：

1. 在不获取资源的情况下了解资源的情况
2. 通过查看响应中的状态码，看看某个对象是否存在
3. 查看首部，测试资源是否被修改了

服务端实现

遵循HTTP/1.1规范，必须确保服务端返回首部于GET返回的首部完全相同。

PUT:

向服务器写入文档，它的语义实际上让服务端用请求的主体部分来创建一个由所请求的url命名的新文档，如果url已经存在，就用这个主体替换它。

POST:

向服务端输入数据。

TRACE:

请求经过防火墙，代理，网关或其他一些应用，每个中间节点都可能修改原始的HTTP请求。

TRACE请求会在目的服务端发起一个“环会”诊断，当请求到最后一站的服务器，会弹回一条TRACE响应，并在响应主体中携带它收到的原始请求报文。这样就可以判断请求原始报文是否被修改，毁坏过。

OPTIONS：

请求服务器告知其支持的各种功能

可以询问支持的特定的方法

DELETE:

常用扩展方法：

LOCK:锁定资源 MKCOL：创建资源 COPY：赋值资源 MOVE：移动资源

## 状态码

100~199 信息状态码

100 continue

客户端发送一个 100 continue expect ，期待服务端返回一个是否会接收请求实体的 100 continue 响应。

返回 100 continue后再发送实体（但也要考虑服务端超过一段时间后不发送 100 continue，这时仍然要发送实体）

发送 100 continue前，服务端已经接收到实体了，应该不再发送100 continue状态。

代理如果知道下一跳服务器是否与 HTTP/1.1兼容，如果知道不兼容，则返回 417 expectation failed。除此之外，将expect 转发即可。

## 首部

### 通用首部

服务端，客户端通用首部

Connection : 连接有关选项

keep-alive

Date: 创建时间

MIME-Version: MIME类型

Transfer-Encoding: 对报文采取的编码方式

Update：对发送端发送想要‘升级’的新版本或则协议

Trailer：分块传输，列出报文拖挂部分的首部集合

Via: 报文经过的中间节点（代理，网关）

通用缓存首部

Cache-Control：报文缓存指示

Pragma：报文缓存指示（优先级低于Cache-Control）

### 请求首部

Client-IP : 客户端的机器的IP地址

UA-Color UA-CPU UA-Disp UA-OS UA-Pixels User-Agent

Client-IP 与 UA- 不在规范中，但是许多客户端都已经实现了（尽量不要用）

Form： 客户端用户的E-mail

Host: 服务器主机名

Referer： 全部的URI（包括路径和query）

Accept首部

Accept : 接收媒体类型

Accept-Charset ： 接受的字符集

Accept-Encoding ： 接受的编码方式

Accept-Language ： 接受的语言

TE ： 可以使用的扩展传输编码

条件请求

Expect 要求的服务端行为

If-Match 实体标记匹配，获取文件

If-None-Match 实体标记不一致，获取文件

If-Modified-Since 资源在指定日期后被修改，获取文件

If-Unmodified-Since 资源没有在指定日期后被修改，获取文件

If-Range 对文档某个范围进行请求

Range 如果服务器支持范围请求，请求资源的指定范围

安全请求首部

Authorization

Cookie

Coolie2 说明请求端支持的coolie版本

代理请求首部

Max-Forward 最大通过代理或者网关的次数（与trace方法一起使用）

Proxy-Authorization 与 Authorization首部相同，代理时认证采用

Proxy-Connection 与 Connection 首部相同，代理时连接使用

### 响应首部

Age 响应持续时间(从最初创建开始，暗示响应是通过中间节点，很可能是从代理缓存中传送过来)

Public

Retry-After 如果资源不可用，再次日期重试。

Server 服务端应用程序 和版本

Title

Warning 比原因短语中更详细一些的警告报文、

协商首部

Accept-Ranges 服务器可接受的范围类型（对此资源）

Vary 服务器查看其它首部的列表，根据这些首部内容挑选出最适合的资源版本发给客户端。

安全响应首部

Proxy-Authenticate 代理对客户端打的质询

Set-Cookie 设置cookie

Set-Coolie2 设置coolie版本

WWW-Authenticate 服务端对客户端的质询

### 实体首部

对应实体主体部分的首部，用于描述HTTP报文的负荷

Allow 列出了可对此实体执行的方法

Location 告知客户端实体实际位于何处，将接收端定向到资源(可能是新的)

内容首部

Content-Base 主体中相对url使用的基础url（规范中未定义）

Content-Encoding 对主体执行的编码方式

Content-Language

Content-Length 主体的长度或尺寸

Content-Location 资源实际所处的位置

Content-MD5 主体的MD5校验和

Content-Range 在整个资源中实体表示的字节范围

Content-Type 主体的mime类型

实体缓存首部

ETag 与此实体相关的实体标记(对应If-None-Match If-Match)

Expires 在这个时间后实体失效

Last-Modified 这个实体最后一次被修改后的日期和时间

### 扩展首部（自定义首部）

# 连接管理

几乎所有的HTTP通信都是由TCP/IP承载，TCP/IP是一种分组交换网络分层协议集。

## TCP连接

HTTP连接实际上就是TCP连接及其使用规则。

TCP为HTTP提供了一条可靠的比特传输通道。

TCP的数据流是分段的，是通过 IP分组（IP数据报）的小数据块来发送的。

HTTP over TCP over IP ,而HTTPS是在HTTP与TCP之间插入了一个 （TLS 或 SSL）密码加密层。

### 传输过程：

HTTP要传送一条报文，会以流的形式将报文数据的内容通过一条打开的TCP连接按序传输。

TCP收到数据流后，会将数据流砍成被称为段的小数据块，并将其放在IP分组中，通过互联网进行传输

而这些都是通过TCP/IP软件处理的。

**TCP连接的底层细节**

**85页**

### IP分组构成

一个IP分组首部

一个TCP 段首部

一个TCP数据块

### TCP性能

TCP性能很大程度决定了HTTP事务的性能

86页

HTTP的时延的影响因素

TCP连接建立握手

在建立一条新的连接之前（甚至是发送任意数据之前），tcp软件之间会交换一系列的ip分组，对连接的相关系数进行沟通。这对于小的http事务，消耗相对很大。

建立新的tcp连接时，会

客户端发送一个小的TCP分组（40~60字节），内部设置了一个特殊的SYN标记，说明这是一个连接请求

服务器接收连接，会对连接参数进行计算，并向客户端发送一个tcp分组，这个分组内的 SYN和 ACK标记都被置位，说明连接已被接受。

最后客户端发送一个确认信息（现代的TCP栈运行客户端在这里发送数据）

TCP慢启动拥塞控制

数据聚集的 Nagle算法

用于捎带确认的TCP延迟确认算法

TIME\_WAIT时延和端口耗尽

### 并行连接

相对于串行连接，同步等待上一个请求完成，再发起下一个请求。并行请求通常要快一些。

但是实际上由于宽带限制，并行加载的多个对象会竞争有限的宽带，而且会产生一些额外的开销。有可能使得加载速度变慢。（浏览器会限制连接总数，一般是4个）

### 持久连接

# 客户端识别与cookie

## 客户端识别的几种方式

HTTP首部（承载用户信息）

Form

用户email

User-Agent

浏览器信息

Referer

从哪个页面调到现在的页面

Authorization

auth登录

服务器向浏览器发送一个401的 Login Required

登陆后每次这个首部都发送用户信息。

用户名和密码

Client-IP

客户端IP地址

X-Forwarded-For

客户端IP地址

Cookie

客户端IP地址跟踪

用户登录

胖URL

路径中记录用户的身份的识别码

无法分享url，破坏缓存，无法直接敲击url进入

cookie

大多数缓存和浏览器都不允许对任何cookie进行缓存。

# cookie

cookie类型

会话cookie

设置了discard 或者没有设置expires 或 max-age 参数 ，即是会话cookie

持久cookie

cookie的域属性

服务端响应通过Set-cookie属性写入cookie，通过domain属性限定域，通过path限定请求路径。

版本为0的cookie返回首部属性

name=value

expires

domain

path

secure

必须通过SSL安全连接才能发送cookie

# 接口设计原则：

对所接收的内容宽松一点（预留多种可能），对所发送的内容严格一点。