

HTTP/1.1 规范中建议对于带有主体但没有 Content-Length 首部的请求，服务器如果无法确定报文的长度，就应当发送 400 Bad Request 响应或 411 Length Required 响应，后一种情况表明服务器要求收到正确的 Content-Length 首部。

15.3 实体摘要

尽管 HTTP 通常都是在像 TCP/IP 这样的可靠传输协议之上实现的，但仍有很多因素会导致报文的一部分在传输过程中被修改，比如有不兼容的转码代理，或者中间代理有误，等等。为检测实体主体的数据是否被不经意（或不希望有）地修改，发送方可以在生成初始的主体时，生成一个数据的校验和，这样接收方就可以通过检查这个校验和来捕获所有意外的实体修改了。⁵

服务器使用 Content-MD5 首部发送对实体主体运行 MD5 算法的结果。只有产生响应的原始服务器可以计算并发送 Content-MD5 首部。中间代理和缓存不应当修改或添加这个首部，否则就会与验证端到端完整性的这个最终目的相冲突。Content-MD5 首部是在对内容做了所有需要的内容编码之后，还没有做任何传输编码之前，计算出来的。为了验证报文的完整性，客户端必须先进行传输编码的解码，然后计算所得到的未进行传输编码的实体主体的 MD5。举个例子吧，如果一份文档使用 gzip 算法进行压缩，然后用分块编码发送，那么就对整个经 gzip 压缩的主体进行 MD5 计算。

347

除了检查报文的完整性之外，MD5 还可以当作散列表的关键字，用来快速定位文档并消除不必要的重复内容存储。除了这些可能的用法，一般不常用到 Content-MD5 首部。

作为对 HTTP 的扩展，在 IETF 的草案中提出了其他一些摘要算法。这些扩展建议增加新的 Want-Digest 首部，它允许客户端说明期望响应中使用的摘要类型，并使用质量值来建议多种摘要算法并说明优先顺序。

15.4 媒体类型和字符集

Content-Type 首部字段说明了实体主体的 MIME 类型。⁶MIME 类型是标准化的名字，用以说明作为货物运载实体的基本媒体类型（比如：HTML 文件、Microsoft Word 文档或是 MPEG 视频等）。客户端应用程序使用 MIME 类型来解释和处理其内容。

注 5：当然，这种方法对同时替换报文主体和摘要首部的恶意攻击无效。这只是为了检测不经意的修改。对付恶意篡改，需要使用别的机制，比如摘要认证。

注 6：在 HEAD 请求中，Content-Type 说明如果请求是 GET 时，将要发送的主体的类型。