

用 WWW-Authenticate 响应首部指定要访问的安全域。浏览器收到质询时，会打开一个对话框，请求用户输入这个域的用户名和密码。然后将用户名和密码稍加扰码，再用 Authorization 请求首部回送给服务器。

12.2.1 基本认证实例

图 12-2 是一个详细的基本认证实例。

- 在图 12-2a 中，用户请求了私人家庭相片 /family/jeff.jpg。
- 在图 12-2b 中，服务器回送一条 401 Authorization Required，对私人家庭相片进行密码质询，同时回送的还有 WWW-Authenticate 首部。这个首部请求对 Family 域进行基本认证。
- 在图 12-2c 中，浏览器收到了 401 质询，弹出对话框，询问 Family 域的用户名和密码。用户输入用户名和密码时，浏览器会用一个冒号将其连接起来，编码成“经过扰码的”Base-64 表示形式（下节介绍），然后将其放在 Authorization 首部中回送。
- 在图 12-2d 中，服务器对用户名和密码进行解码，验证它们的正确性，然后用一条 HTTP 200 OK 报文返回所请求的报文。

表 12-2 总结了 HTTP 基本认证的 WWW-Authenticate 和 Authorization 首部。

表12-2 基本认证首部

质询/响应	首部语法及描述
质询（服务器发往客户端）	网站的不同部分可能有不同的密码。域就是一个引用字符串，用来命名所请求的文档集，这样用户就知道该使用哪个密码了： WWW-Authenticate: Basic realm=quoted-realm
响应（客户端发往服务器）	用冒号（:）将用户名和密码连接起来，然后转换成 Base-64 编码，这样在用户名和密码中包含国际字符会稍微容易一些，也能尽量避免通过观察网络流量并只进行一些粗略的检查就可以获取用户名和密码情况的发生： Authorization: Basic base64-username-and-password

281

注意，基本认证协议并没有使用表 12-1 所示的 Authentication-Info 首部。

12.2.2 Base-64 用户名/密码编码

HTTP 基本认证将（由冒号分隔的）用户名和密码打包在一起，并用 Base-64 编码方式对其进行编码。如果不知道 Base-64 编码是什么意思，也不用担心。你并不需要对它有太多的了解，如果对此感兴趣，可以在附录 E 中读到所有与之有关的内容。简单来说，Base-64 编码会将一个 8 位字节序列划分为一些 6 位的块。用每个 6