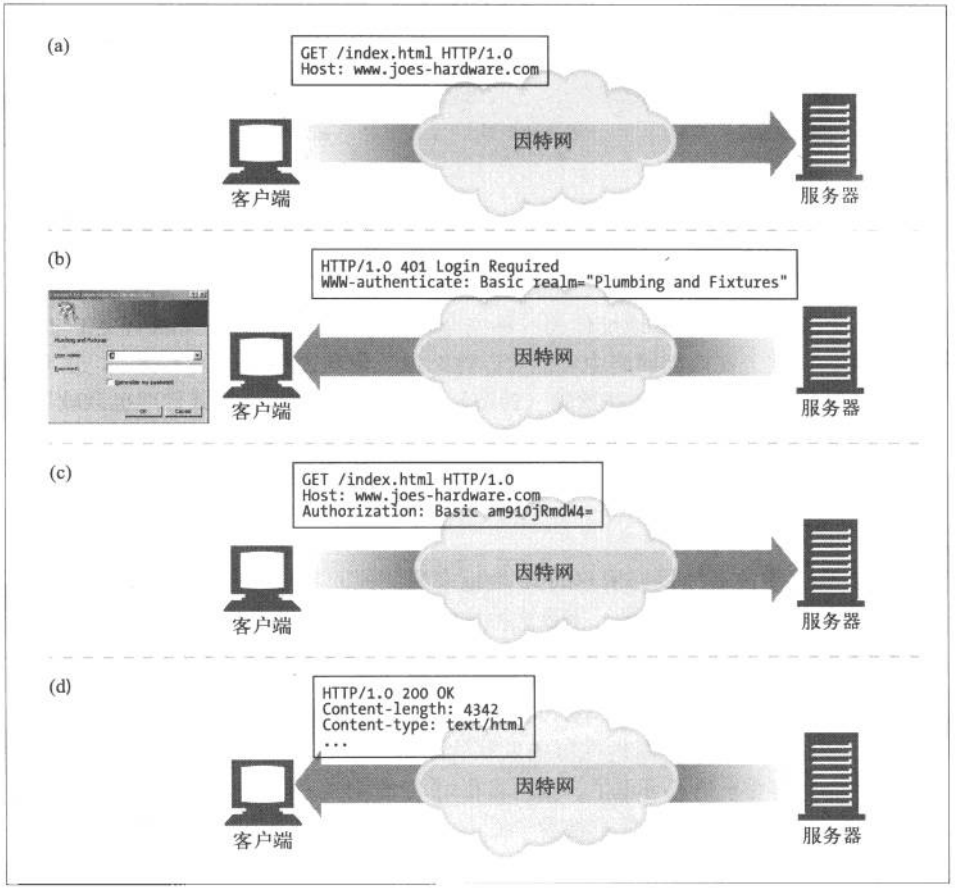

图 11-2　用 HTTP 认证首部注册用户名

- 只要用户输入了用户名和密码（对其身份进行完整性检查），浏览器就会重复原来的请求。这次它会添加一个 Authorization 首部，说明用户名和密码。对用户名和密码进行加密，防止那些有意无意的网络观察者看到。[3]
- 现在，服务器已经知道用户的身份了。
- 今后的请求要使用用户名和密码时，浏览器会自动将存储下来的值发送出去，甚至在站点没有要求发送的时候也经常会向其发送。浏览器在每次请求中都向服务器发送 Authorization 首部作为一种身份的标识，这样，只要登录一次，就可以在整个会话期间维持用户的身份了。

注 3：在第 14 章我们会看到，任何有这种想法的人，不用费多大事就可以轻易地将 HTTP 基本的认证用户名和密码破解出来。稍后将讨论一些更安全的技术。