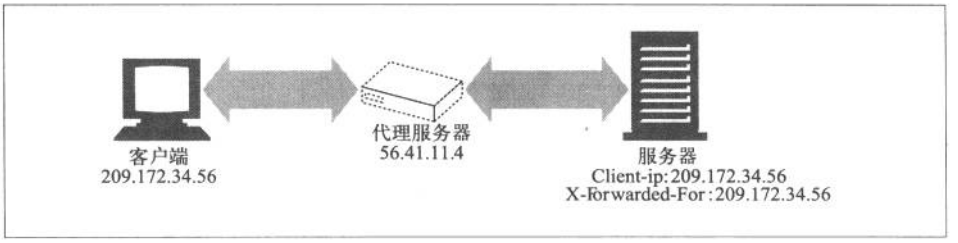


图 11-1 代理可以添加扩展首部，来传递原始客户端的 IP 地址

少数站点甚至将客户端 IP 地址作为一种安全特性使用，它们只向来自特定 IP 地址的用户提供文档。在内部网络中可能可以这么做，但在因特网上就不行了，主要是因为因特网上 IP 地址太容易被欺骗（伪造）了。路径上如果有拦截代理也会破坏此方案。第 14 章讨论了一些强大得多的特权文档访问控制策略。

## 11.4 用户登录

Web 服务器无需被动地根据用户的 IP 地址来猜测他的身份，它可以要求用户通过用户名和密码进行认证（登录）来显式地询问用户是谁。

为了使 Web 站点的登录更加简便，HTTP 中包含了一种内建机制，可以用 `WWW-Authenticate` 首部和 `Authorization` 首部向 Web 站点传送用户的相关信息。一旦登录，浏览器就可以不断地在每条发往这个站点的请求中发送这个登录信息了，这样，就总是有登录信息可用了。我们将在第 12 章对这种 HTTP 认证机制进行更加详细的讨论，现在我们先来简单地看一看。 260

如果服务器希望在为用户提供对站点的访问之前，先行登录，可以向浏览器回送一条 HTTP 响应代码 401 Login Required。然后，浏览器会显示一个登录对话框，并用 `Authorization` 首部在下一条对服务器的请求中提供这些信息。[2] 图 11-2 对此进行了说明。

此图中发生的情况如下所述。

- 在图 11-2a 中，浏览器对站点 www.joes-hardware.com 发起了一条请求。
- 站点并不知道这个用户的身份，因此在图 11-2b 中，服务器会返回 401 Login Required HTTP 响应码，并添加 `WWW-Authentication` 首部，要求用户登录。这样浏览器就会弹出一个登录对话框。 261

注 2：为了不让用户每发送一条请求都要登录一次，大多数浏览器都会记住某站点的登录信息，并将登录信息放在发送给该站点的每条请求中。