（续）

指　令	描　述
opaque	一个由服务器指定的数据串，应该由客户端不经修改地放在后继请求的 Authorization 首部中返回，这些后继请求应使用同一保护空间内的 URI。建议这个字符串采用 Base-64 或十六进制的数据
stale	一个标志，用来说明由于 nonce 值太过陈旧，前一条来自客户端的请求被拒绝了。如果 stale 为 TRUE（不区分大小写），客户端可能希望以新加密的响应重试请求，而不用再次提示用户输入新的用户名和密码。只有在服务器收到一条 nonce 无效，但摘要有效的请求（说明客户端知道正确的用户名 / 密码）时，才应该将 stale 设置为 TRUE。如果 stale 为 FALSE，或者除 TRUE 之外的其他值，或者没有提供 stale 指令，用户名和 / 或密码就是无效的，需要获取新的值

algorithm	一个字符串，说明了一对儿用来生成摘要和校验码的算法。如果没有提供这个字符串，就假定它为“MD5”。如果不识别此算法，就忽略这种质询（如果有多个算法的话，就使用另外一个）。
	在这份文档中，用“KD(secret,data)”来表示用密码“secret”对数据“data”使用摘要算法得到的字符串，而对数据“data”使用校验和算法得到的字符串则表示为“H(data)”。表示法“unq(X)”表示引用字符串“X”的值（不包含左右两边的引号）。
	对 MD5 和 MD5-sess 算法来说：
	`H(data) = MD5(data)`
	`HD(secret, data) = H(concat(secret, ":", data))`
	也就是说，摘要就是将密码的 MD5 与冒号和数据连接在一起。MD5-sess 算法目的是支持使用高效的第三方认证服务器

qop	这条指令是可选的，只是为了与 RFC 2069[6] 后向兼容才保留的。所有与此版本的摘要方案兼容的实现都应该使用它。 如果提供了这条指令，它就是由一个或多个标记构成的引用字符串，用来说明服务器所支持的“安全保障”值。值 auth 说明要进行认证，值 auth-int 说明要进行具有完整性保护的认证。一定要忽略那些不识别的选项
<extension>	未来可以通过这条指令进行扩展。要忽略所有不认识的指令

F.2　摘要Authorization指令

表 F-2 根据 RFC 2617 的描述，对每条摘要 Authorization 指令都进行了说明。最新的细节请参见官方规范。

575

表F-2　（来自RFC 2617的）摘要Authorization首部指令

指　令	描　述
username	指定域中的用户名
realm	在 WWW-Authenticate 首部中传送给客户端的域