这些派生封装层很容易把人弄晕。这也是有些读者觉得 RFC 2617 难懂的原因之一。为了简化，表 13-5 扩展了 H 和 KD 的定义，用 A1 和 A2 来表示摘要。

表13-5 展开的摘要算法备忘单

qop	算 法	展开的算法
未定义	<undefined>	MD5(MD5(A1):<nonce>:MD5(A2))
	MD5	
	MD5-sess	
auth	<undefined>	MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))
	MD5	
	MD5-sess	
auth-int	<undefined>	MD5(MD5(A1):<nonce>:<nc>:<cnonce>:<qop>:MD5(A2))
	MD5	
	MD5-sess	

13.2.6 摘要认证会话

客户端响应对保护空间的 WWW-Authenticate 质询时，会启动一个此保护空间的认证会话（与受访问服务器的标准根结合在一起的域就定义了一个“保护空间”）。

在客户端收到另一条来自保护空间的任意一台服务器的 WWW-Authenticate 质询之前，认证会话会一直持续。客户端应该记住用户名、密码、随机数、随机数计数以及一些与认证会话有关的隐晦值，以便将来在此保护空间中构建请求的 Authorization 首部时使用。

随机数过期时，即便老的 Authorization 首部所包含的随机数不再新鲜了，服务器也可以选择接受其中的信息。服务器也可以返回一个带有新随机数的 401 响应，让客户端重试这条请求；指定这个响应为 stale=true，表示服务器在告知客户端用新的随机数来重试，而不再重新提示输入新的用户名和密码了。

13.2.7 预授权

在普通的认证方式中，事务结束之前，每条请求都要有一次请求 / 质询的循环，参见图 13-4a。

如果客户端事先知道下一个随机数是什么，就可以取消这个请求 / 质询循环，这样客户端就可以在服务器发出请求之前，生成正确的 Authorization 首部了。如果客户端能在服务器要求它计算 Authorization 首部之前将其计算出来，就可以预先将 Authorization 首部发送给服务器，而不用进行请求 / 质询了。图 13-4b 显示了这种方式对性能的影响。