表13-6 算法中A2的定义（请求摘要）

qop	A2
未定义	<request-method>:<uri-directive-value>
auth	<request-method>:<uri-directive-value>
auth-int	<request-method>:<uri-directive-value>:H(<request-entity-body>)

表13-7 算法中A2的定义（响应摘要）

qop	A2
未定义	:<uri-directive-value>
auth	:<uri-directive-value>
auth-int	:<uri-directive-value>:H(<response-entity-body>)

cnonce 值和 nc 值必须是本报文所响应的客户端请求中的相应值。如果指定了 qop="auth" 或 qop="auth-int"，就必须提供响应 auth、cnonce 和 nonce 计数指令。

13.3 增强保护质量

可以在三种摘要首部中提供 qop 字段：WWW-Authenticate、Authorization 和 Authentication-Info。

通过 qop 字段，客户端和服务器可以对不同类型及质量的保护进行协商。比如，即便会严重降低传输速度，有些事务可能也要检查报文主体的完整性。

服务器首先在 WWW-Authenticate 首部输出由逗号分隔的 qop 选项列表。然后客户端从中选择一个它支持且满足其需求的选项，并将其放在 Authorization 的 qop 字段中回送给服务器。

qop 字段是可选的，但只是在后向兼容原有 RFC 2069 规范的情况下才是可选的。现代所有的摘要实现都应该支持 qop 选项。

RFC 2617 定义了两种保护质量的初始值：表示认证的 auth，带有报文完整性保护的认证 auth-int。将来可能还会出现其他 qop 选项。

13.3.1 报文完整性保护

如果使用了完整性保护（qop="auth-int"），H（实体的主体部分）就是对实体主体部分，而不是报文主体部分的散列。对于发送者，要在应用任意传输编码方式之前计算；而对于接收者，则应在去除所有传输编码之后计算。注意，对于任何含有多部份的内容类型来说，多部分的边界和每部分中嵌入的首部都要包含在内。

299