

指 令	描 述
nonce	在 WWW-Authenticate 首部中传送给客户端的那个与服务器相同的 nonce
uri	来自请求行请求 URI 中的 URI。由于代理可以在传输中修改请求行，所以会出现重复。进行正确的摘要验证计算可能需要原始 URI
response	这个就是实际的摘要——摘要认证的重点！响应是一个由 32 个十六进制数字组成的字符串，由沟通好的摘要算法生成，用来证明用户知道这个密码
algorithm	一个字符串，说明了用来生成摘要和校验和的一对儿算法。如果未提供，就将其假定为 MD5
opaque	服务器在 WWW-Authenticate 首部指定的数据串，应该由客户端不经修改地在后继请求的 WWW-Authenticate 首部中返回，这个请求应使用同一保护空间内的 URI
cnonce	如果发送了 qop 指令，就一定要使用这条指令，如果服务器没有在 WWW-Authenticate 首部字段中发送 qop 指令，就一定不能使用这条指令。 cnonce 值是客户端提供的不透明引用字符串值，客户端和服务端都用它来避免选择明文攻击，以提供双向认证以及一些报文一致性检查。 参见本附录稍后介绍的响应摘要和请求摘要计算
qop	说明客户端对报文应用的“安全保障”是什么。如果提供了这条指令，它的值就必须是服务器在 WWW-Authenticate 首部中说明的、它支持的可选值之一。这些值会影响请求摘要的计算方式。 它只是个单独的标记，而不是 WWW-Authenticate 中那样的可选值引用列表。这条指令是可选的，以保持对 RFC 2069 最小实现的后向兼容，但如果服务器说明它是通过在 WWW-Authenticate 首部字段中提供 qop 指令来支持 qop 的，就应该使用这条指令
nc	如果发送了 qop 指令，就一定要指定这条指令，如果服务器没有在 WWW-Authenticate 首部字段中发送 qop 指令，就一定不能使用这条指令。 其值是个十六进制值，表示客户端已经发送的包含 nonce 值的请求次数（包括当前请求在内）。比如，作为对指定 nonce 值的响应发送的第一条请求中，客户端会发送 nc="00000001"。 这条指令的目的是允许服务器通过维护自己保存的此计数值副本来发现请求重复——如果看到了两次相同的 nc 值，就说明请求是重放的
<extension>	未来可以通过这条指令进行扩展。所有不认识的指令都要忽略掉

## F.3 摘要Authentication-Info指令

表 F-3 根据 RFC 2617 的描述，对每条 Authentication-Info 指令都进行了说明。  
最新的细节请参见官方规范。

576