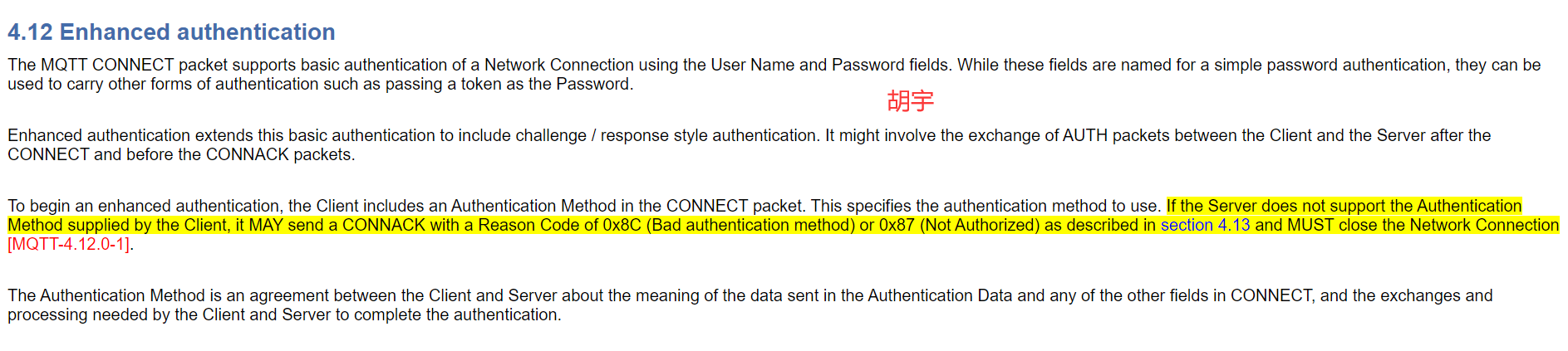
**1.MQTT5对于会话管理错误预防**

**（1）增强认证机制**

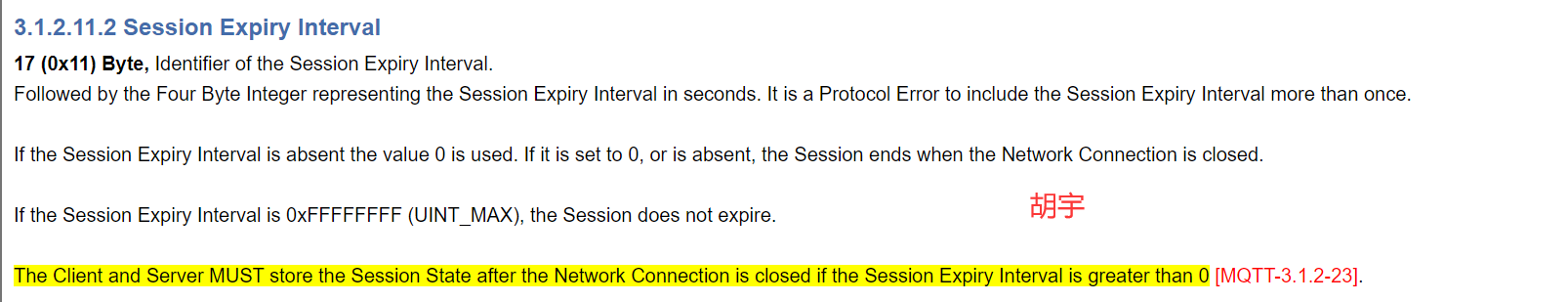
使用此机制需要客户端和服务端双方的支持, 基于更强的安全性考虑，MQTT v5 增加了新特性增强认证，增强认证包含质询/响应风格的认证，可以实现对客户端和服务器的双向认证，服务器可以验证连接的客户端是否是真正的客户端，客户端也可以验证连接的服务器是否是真正的服务器，从而提供了更高的安全性。增强认证依赖于认证方法和认证数据来完成整个认证过程，在增强认证中，认证方法通常为 SASL（ Simple Authentication and Security Layer ) 机制，使用一个注册过的名称便于信息交换。但是，认证方法不限于使用已注册的 SASL 机制，服务器和客户端可以约定使用任何质询/响应风格的认证。在原文档4.12处有相关内容。



**图1 增强认证机制**

**（2）会话过期间隔**

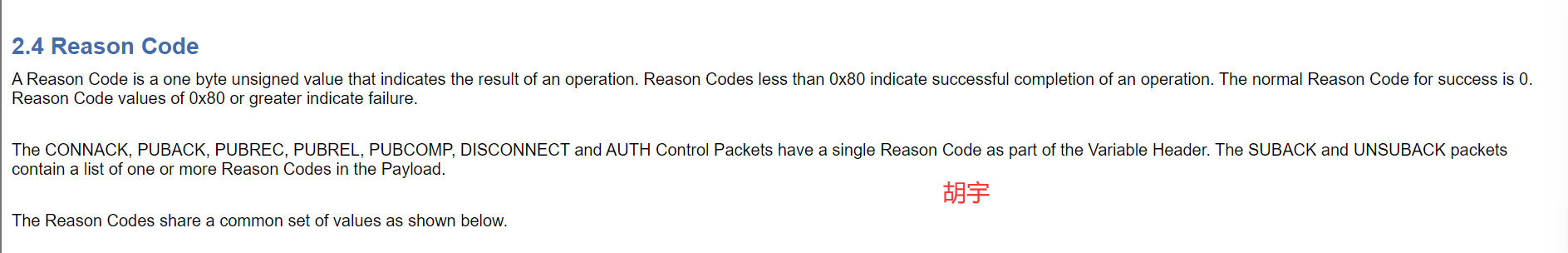
这个功能允许客户端指定服务器在客户端断开连接后应将会话保持多长时间。在之前的 MQTT 版本中，会话要么在断开连接后立即结束，要么无限期地保持下去。使用 MQTT 5.0，您可以指定一个具体的时间段，在断开连接后，会话仍然有效。这样可以更灵活地管理会话的生命周期，并节省服务器的资源，同时预防攻击者利用会话管理错误。在原文档3.1.2.11.2处有相关内容。



**图2 会话过期间隔**

**（3）原因码**

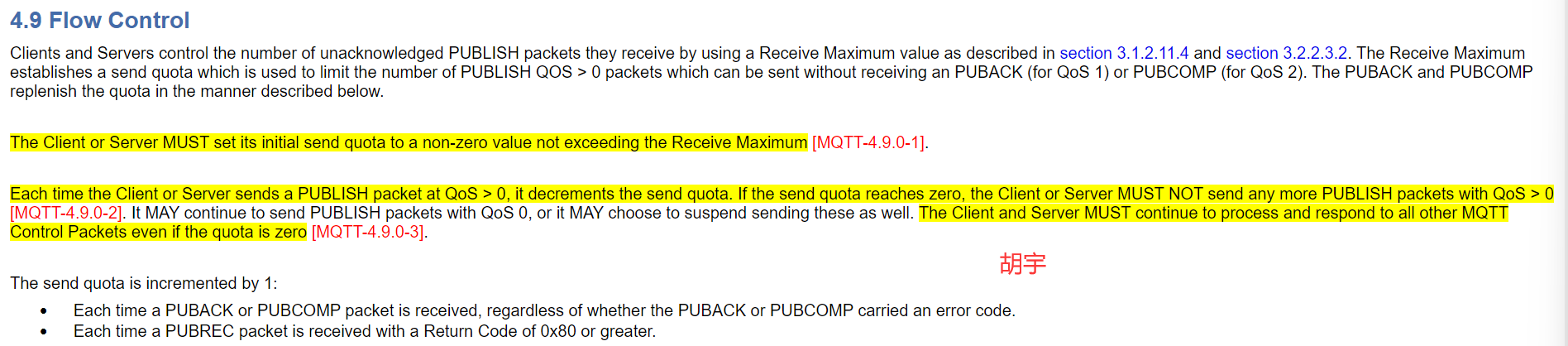
MQTT 5.0引入了原因码的概念，用于指示操作结果或错误类型。通过使用适当的原因码，服务器可以向客户端返回准确的错误信息，包括认证失败等。这有助于防止攻击者通过错误的会话管理进行非授权操作。在原文档2.4处有相关内容。



**图3 原因码**

**（4）流控制**

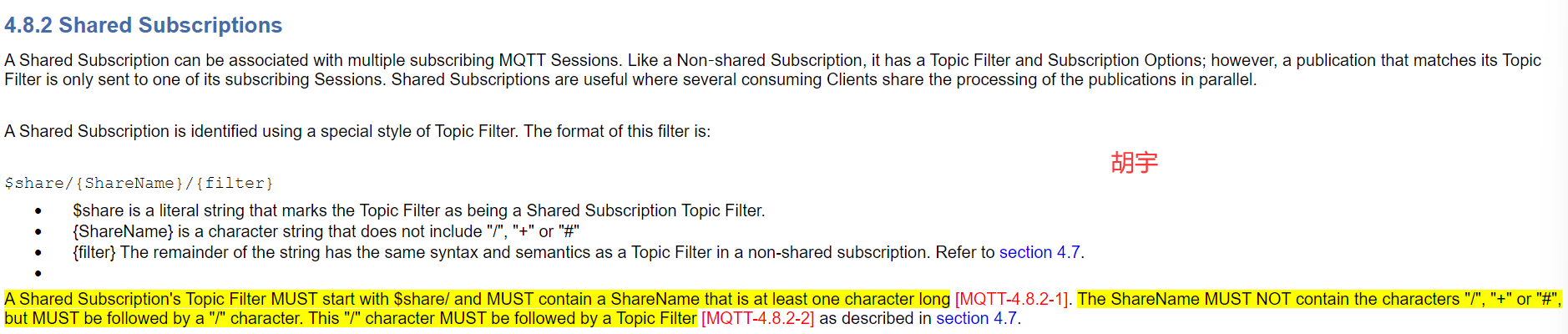
在MQTT里，流控制允许客户端和服务器独立地指定可靠消息（QoS>0）的数量，发送方在发送消息时保持低于此配额，以限制可靠消息的速率和数量，防止客户端被大量的消息淹没，导致会话管理错误。在原文档4.9处有相关内容。



**图4 流控制**

**（5）共享订阅**

MQTT 5.0引入了共享订阅的概念，允许多个客户端共享同一订阅，以便更好地管理和分发消息。通过使用共享订阅，可以限制非授权客户端对消息的订阅，减少潜在的非授权操作风险。在原文档4.8.2处有相关内容。

**图5 共享订阅**

**2.课上描述的未授权的遗嘱与保留消息问题的出现的预防方法**

在一个多租户的MQTT系统中，确保只有授权的客户端能够发布和订阅特定租户的主题是非常重要的。为了实现这一目标，系统可以采取以下措施来进行身份验证和授权检查：（1）客户端身份验证：在客户端连接到MQTT代理时，代理可以要求客户端提供租户ID作为用户自定义属性的一部分，例如使用属性键"tenantId"和相应的租户标识符作为属性值。通过验证客户端提供的租户ID，代理可以确认客户端的身份。（2）访问控制策略：MQTT代理需要实施严格的访问控制策略，以确保客户端只能与其拥有权限的租户资源进行交互。代理会根据客户端提供的租户ID来验证其发布和订阅操作的目标主题是否属于该租户。（3）遗嘱消息的验证：当代理接收到带有遗嘱消息的连接请求时，它会检查遗嘱消息中的"tenantId"属性。代理将验证该客户端是否有权将遗嘱消息发布到指定租户的主题上。只有经过授权的客户端才能设置和发布遗嘱消息，从而避免未经授权的遗嘱消息被发布到系统中。

通过这些身份验证和授权检查措施，系统可以有效地防止未经授权的客户端访问其他租户的资源，包括发布和订阅操作，以及设置遗嘱消息。这种方式可以确保每个租户只能访问其自己的资源，增强了系统的安全性和租户数据的隔离性。