Modbus/TCP 安全协议

协议规范

版本：V36 (2021-07-30)

日期：2021年7月30日

中文翻译版 | www.modbus.cn

本文件为 Modbus.org
官方规范文档的中文翻译版，仅供学习参考之用。官方英文原版请访问 www.modbus.org 获取。如翻译内容与英文原版存在歧义，以英文原版为准。

目 录

1 一致性级别

在标准文档中，应使用特定的标记来定义每项特定要求的重要性。这些标记（词汇）通过大写来突出显示。由于一致性规则可能以提交给标准机构成为国际标准为目标，因此「SHALL」和「MUST」词汇的选择应根据覆盖规范相关领域标准化的组织的规则进行。

术语	说明
最新约定	在标准文档中，应使用特定的标记来定义每项特定要求的重要性。这些标记（词汇）通过大写来突出显示。
合规性	满足所有 MUST/SHALL 要求的实现称为「无条件合规」。满足所有 MUST 要求但不满足所有 SHOULD 建议的实现称为「条件合规」。如果实现未能满足其实现的一个或多个 MUST/SHALL 要求，则该实现不合规。
MUST / SHALL / REQUIRED（必须）	包含「MUST/SHALL」一词的所有要求均为强制性要求。「MUST/SHALL」一词或形容词「REQUIRED」表示该项是实现的一项绝对要求。
MUST NOT / SHALL NOT（禁止）	包含「MUST NOT/SHALL NOT」一词的所有要求均为强制性要求。「MUST NOT」或「SHALL NOT」短语表示该项是规范的绝对禁止事项。
SHOULD / RECOMMENDED（建议）	包含「SHOULD」一词或形容词「RECOMMENDED」的所有建议被视为期望行为。在 uncommon 情况下，可能存在忽略此项的合理理由，但在选择不同方案之前，应充分理解其全部影响并仔细权衡。
MAY / OPTIONAL（可选）	「MAY」一词或形容词「OPTIONAL」表示该项是完全可选的。一个实现者可能因为特定市场需求或产品增强而选择包含该项；另一个实现者可能省略相同项。

2 规范性声明

本技术规范中的规范性声明按如下方式显式标注：

```
R-n.m: □□□□□□□□
```

其中「n.m」替换为要求声明标签编号，可以是层级编号（例如 R-1.2.3）或简单整数（例如 R-1）。每条声明包含且仅包含一个要求级别关键词（例如「MUST」）和一个一致性目标关键词（例如「Message」）。例如：「该 Message 必须使用 BER 编码」。

3 参考文献

参考文献	描述
[62443-3-3]	IEC 62443-3-3：系统安全要求和安全等级
[62443-4-2]	IEC 62443-4-2：IACS 组件技术安全要求
[MB]	Modbus 应用协议规范，V1.1b3，2012-04-26
[MBTCP]	Modbus TCP/IP 消息实现指南，V1.0b，2006-10-24
[RFC4492]	IETF RFC 4492，用于传输层安全（TLS）的椭圆曲线密码（ECC）密码套件
[RFC5246]	IETF RFC 5246，传输层安全（TLS）协议 v1.2，2008年8月
[RFC5280]	IETF RFC 5280，Internet x.509 公钥基础设施证书和证书吊销列表（CRL）配置文件，2008年5月
[RFC5746]	IETF RFC 5746，TLS 重协商指示扩展，2010年2月
[RFC6066]	IETF RFC 6066，TLS 扩展：扩展定义，2011年1月
[RFC6176]	IETF RFC 6176，禁止安全套接字层（SSL）版本 2.0，2011年3月
[TLS-PARAMS]	IANA 传输层参数类型注册表

4 缩略语与术语表

缩略语	说明
ADU	应用数据单元（Application Data Unit）
AuthZ	授权（Authorization）
CA	证书颁发机构（Certificate Authority）
CDP	CRL 分发点（CRL Distribution Point）
CRL	证书吊销列表（Certificate Revocation List）
HMAC	密钥散列消息认证码（Keyed-hash Message Authentication Code）
IANA	互联网数字分配机构（Internet Assigned Numbers Authority）
ICS	工业控制系统（Industrial Control System）
IEC	国际电工委员会（International Electrotechnical Commission）
MAC	消息认证码（Message Authentication Code）
mbap	Modbus 应用协议（Modbus Application Protocol）
mbaps	Modbus 安全应用协议（Modbus Security Application Protocol）
OID	对象标识符（Object Identifier），由国际电信联盟标准化
PEN	私有企业编号（Private Enterprise Number）
PDU	协议数据单元（Protocol Data Unit）
PKI	公钥基础设施（Public Key Infrastructure）
PRF	伪随机函数族（Pseudorandom Function Family）
RA	注册机构（Registration Authority）
SSL	安全套接字层（Secure Socket Layer）
TCP	传输控制协议（Transport Control Protocol）
TLS	传输层安全（Transport Layer Security）

5 引言

Modbus/TCP 协议广泛应用于工业控制系统（ICS）。Modbus/TCP 的规范可在 modbus.org 网站上找到。Modbus/TCP 规范定义了应用数据单元（ADU）。该 ADU 如下图所示：

图 1 Modbus/TCP ADU

传统 Modbus 协议数据单元（PDU）与 Modbus/TCP ADU 的区别在于，ADU 在帧的前端增加了 Modbus 应用协议（mbap）头部。

1996年，Modbus/TCP 协议在 IANA（互联网数字分配机构）注册，并被分配了系统端口号 502。在 IANA 注册过程中，由于 Modbus/TCP ADU 中的 mbap 头部，Modbus/TCP 协议被称为 mbap 协议。该名称一直沿用至今，在 IANA 中仍以 mbap/TCP 的名称注册在端口 502。

Modbus/TCP 安全协议是 Modbus/TCP 协议的安全变体，利用传输层安全（TLS）技术。IANA 已为 Modbus/TCP 安全协议分配了系统端口号 802。Modbus.org 已将在端口 802 注册的协议命名为 Modbus 安全应用协议，在 IANA 中注册为 mbap/TLS/TCP。

选择 TLS 作为安全传输协议，是在 [62443-3-3] 和 [62443-4-2] 语境下分析代表性工业数据流的结果。

下表列出了 mbap 通信配置文件在不同语境中使用的名称，例如通信配置文件、Modbus.org、IANA 注册表和本规范。为简洁起见，本规范的其余部分将使用 mbap 和 mbaps 分别指代 Modbus/TCP 和 Modbus/TCP 安全。

通信配置文件	Modbus.org	IANA 注册表	本规范（简称）
mbap/TCP	Modbus/TCP	系统端口 502 的 Modbus 应用协议	mbap
mbap/TLS/TCP	Modbus/TCP 安全	系统端口 802 的 Modbus 安全应用协议	mbaps

Modbus/TCP 安全原则

- Modbus/TCP 安全 @ 端口 802
- 基于 x.509v3 证书的身份认证和 TLS 认证
- 双向客户端/服务器 TLS 认证

- 使用通过证书传输的角色进行授权
- 授权规则为产品特定
- 不改变 mbap 协议

6 协议概述

6.1 概述

秉承 Modbus 的传统，mbaps 的要求保持简单，允许供应商围绕协议开发额外的基础设施，并允许与传统设备和现场总线向后兼容。mbaps 扩展了 [MBTCP] 和 [MB] 中定义的原始 mbap 协议。mbaps
定义了一个客户端-服务器协议，它是完整安全系统架构的一部分。如下图所示，mbap ADU 被 TLS 封装。

TLS 通过添加数据机密传输、数据完整性、防重放保护、通过证书的端点认证、以及通过嵌入证书中的信息（如用户和设备角色）进行授权，为 mbap 提供了安全聚焦的协议替代方案。

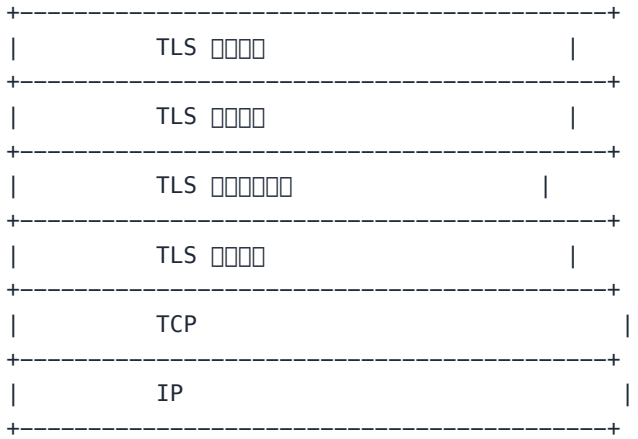
mbap 和 mbaps 协议分别类似于 http 及其安全变体 https。在 mbaps 中，mbap 协议通过 TLS 传输。TLS 通过 x.509v3 证书提供认证能力。mbaps 客户端和服务器必须配备这些证书才能参与 TLS 认证功能。

mbap 和 mbaps 之间的一个重要区别是，mbaps 提供了服务器调用授权功能的能力，其规则由供应商或客户驱动，利用通过 x.509v3 证书扩展字段提供的角色数据。该扩展使用 Modbus.org 的 IANA OID 注册。TLS 支持使用预共享密钥建立安全连接，但本规范不考虑其使用，因为不允许传输角色信息以提供授权功能。

6.2 传输层安全（TLS）简介

mbaps/TLS/TCP 配置文件使用 IETF RFC 5246 定义的安全 TLS 传输协议。[RFC5246] 定义了 TLS v1.2，并提供了对早期版本中已知漏洞的对策和缓解措施。虽然本规范基于 TLS v1.2，但随着新版本实现的广泛采用，将会考虑使用新版本。

TLS 由一组协议组成，如下图所示。其中的主要协议是 TLS 记录协议（TLS Record Protocol）。其余协议是由 TLS 记录协议承载的子协议，由 TLS 中间件管理。



mbap ADU 在 mbaps 配置文件中保持不变，被封装在 TLS 应用协议消息中。

TLS 握手协议：

- 在端点之间协商安全通道的密码学参数，包括算法、密钥等
- 提供基于 x.509v3 证书的双向客户端/服务器认证
- 从证书中提取客户端角色 OID
- 建立 TLS 会话

TLS 会话建立后，正常的 Modbus 请求和响应序列在安全的 TLS 应用协议通道中传输。在请求处理过程中，mbaps
协议处理器调用供应商特定的授权功能。该授权功能使用来自 mbap ADU 和连接的 x.509 客户端证书中提取的角色作为输入，评估角色到权限的算法。该算法根据对端角色确定是否可以处理该 ADU。如果授权功能确定 mbap ADU 代码无法处理，mbap 处理器将返回 01 – 非法功能 Modbus 异常代码。此授权过程在每次请求时执行，确保对请求流的完整验证。

7 服务定义

Modbus 应用层协议使用的标准功能码在 [MB] 规范中有详细描述。本规范不对标准功能码进行修改。

8 协议规范

8.1 概述

mbap ADU 的通信使用 [RFC5246] 定义的传输层安全协议（TLS）进行保护。mbap ADU 通过 TLS 应用协议传输。

TLS 在两个端点之间提供传输层安全。为此，TLS 端点执行 TLS 握手协议来协商安全参数并创建 TLS 会话。

8.2 TLS 握手

两个 mbaps 端设备要使用 TLS 进行安全通信，必须在 TLS 连接的端点之间建立安全上下文。TLS 握手协议建立安全上下文，即 TLS 会话。TLS 会话具有会话标识符，安全上下文由 [RFC5246] A.6 节定义的一组安全参数描述。

双向认证要求每个端点将其域证书链发送给远端端点。收到远端对等方的证书链后，TLS 端点将使用链中的下一个 CA 证书验证每个证书签名，直到验证到链的根。

TLS 完整握手协议定义在 [RFC5246] 第 7.3 节，如下表所示：

表 5 TLS 完整握手协议

消息	描述
1: ClientHello	TlsClient 向 TlsServer 发送 ClientHello 消息以开始协商过程。TlsClient 在消息中提供一个密码套件列表，该列表按客户端的偏好排序。
2: ServerHello	TlsServer 发送 ServerHello 消息作为 ClientHello 的响应。该消息标识一组可接受的密码算法，并返回新的 sessionID。
3: ServerCertificate	TlsServer 发送其证书链作为 Certificate 消息的载荷。该链包含服务器设备的域证书，以及每个签发 CA 的证书直到根 CA。服务器域证书也可以包含服务器的角色；此时该角色不被客户端使用。
4: VerifyServerCertSig	当对等方收到远端对等方的证书时，将通过以下方式进行验证：使用签发 CA 的公钥验证链中每个证书的签名、验证证书路径到受信任的根证书、检查链中每个证书的吊销状态。

消息	描述
5: ServerKeyExchange	TlsServer 向 TlsClient 发送 ServerKeyExchange 消息，提供用于设置预主密钥的数据。
6: CertificateRequest	TlsServer 向 TlsClient 发送 CertificateRequest 消息以获取客户端证书。
7: ServerHelloDone	TlsServer 向 TlsClient 发送 ServerHelloDone 消息，指示 ServerHello 及相关消息的结束。
8: ClientCertificate	TlsClient 发送其证书链作为 Certificate 消息的载荷。该链包含客户端设备的域证书，以及每个签发 CA 的证书直到根 CA。客户端终端证书还包含客户端的角色。服务器使用此角色来授权后续的应用层请求。
9: VerifyClientCertSig	当对等方收到远端对等方的证书时，将通过以下方式进行验证：使用签发 CA 的公钥验证链中每个证书的签名、验证证书路径到受信任的根证书、检查链中每个证书的吊销状态。
10: ClientKeyExchange	TlsClient 向 TlsServer 发送 ClientKeyExchange 消息。通过此消息设置预主密钥。
11: ChangeCipherSpec	TlsClient 向 TlsServer 发送 ChangeCipherSpec 消息，指示客户端后续发送的消息将使用新协商的密码规范和密钥。
12: Finished	TlsClient 向 TlsServer 发送 Finished 消息。此消息是第一个使用刚协商的算法、密钥和密钥保护的消息。
13: ChangeCipherSpec	TlsServer 向 TlsClient 发送 ChangeCipherSpec 消息，指示服务器后续发送的消息将使用新协商的密码规范和密钥。
14: Finished	TlsServer 向 TlsClient 发送 Finished 消息。此消息使用刚协商的算法、密钥和密钥保护。
15+n: ApplData()	n ::= {0..m}，应用数据传输
15+n+1: ApplData()	n ::= {0..m}，应用数据传输

TLS [RFC5246] 还提供会话恢复功能。服务器端缓存已知的最后安全状态，并将其与客户端和服务器 hello 中使用的会话 ID 配对。如果客户端缓存了安全上下文和 sessionID，它可以在下一次 ClientHello 中向服务器出示该 sessionID。如果该 sessionID 与服务器上缓存的 sessionID 匹配，服务器将立即更改密码规范，连接将恢复。这将 TLS 协商时间减少到 1 个应用往返时间，并消除了授权新对等方所需的公钥/私钥加密功能。此恢复将要求服务器缓存与连接客户端证书关联的角色，并将其与 sessionID 关联。

如果 ClientHello 出示的 sessionID 与已知服务器会话不匹配，则 serverHello 消息中返回新的 sessionID，并执行完整的 TLS 握手。

表 6 TLS 恢复握手

消息	描述
1: ClientHello	TlsClient 向 TlsServer 发送 ClientHello 消息以开始协商过程。TlsClient 在消息中提供密码套件列表，同时提供缓存的非零 sessionID。
2: ServerHello	TlsServer 发送 ServerHello 消息作为 ClientHello 的响应。该消息标识可接受的密码套件，返回相同的 sessionID，并包含 ChangeCipherSpec 记录。
2: ChangeCipherSpec	TlsServer 向 TlsClient 发送 ChangeCipherSpec 消息，指示服务器后续发送的消息将使用新协商的密码规范和密钥。
2: Finished	TlsServer 向 TlsClient 发送 Finished 消息。此消息是第一个使用刚协商的算法、密钥和密钥保护的消息。
3: ChangeCipherSpec	TlsClient 向 TlsServer 发送 ChangeCipherSpec 消息，指示客户端后续发送的消息将使用新协商的密码规范和密钥。
3: Finished	TlsClient 向 TlsServer 发送 Finished 消息。此消息使用刚协商的算法、密钥和密钥保护。
4+n: ApplData()	n ::= {0..m}，应用数据传输
4+n+1: ApplData()	n ::= {0..m}，应用数据传输

R-06: mbaps 端设备在执行 TLS 握手协议创建 TLS 会话时必须提供双向认证。

R-07: TlsServer 必须在 TLS 握手期间发送 CertificateRequest 消息。

R-08: TlsClient 在收到包含客户端证书请求的请求后，必须发送 ClientCertificate 消息。

R-10: 如果 TlsClient 未发送 ClientCertificate 消息，则 TlsServer 必须向 TlsClient 发送「致命警报」消息并终止连接。

R-11: 根据 RFC5246-7.2.2，TLS 连接在「致命警报」后不得恢复。

8.3 密码套件选择

生成的 TLS 会话的安全强度取决于 TLS 端点之间协商的密码套件。密码套件指定 TLS 会话将使用什么密码学技术来提供一定级别的安全性。

mbaps 中只应使用在 IANA 注册且目前不知道有弱点的密码套件。

R-12: 与 TLS 一起用于 mbaps 的密码套件必须在 IANA 注册表中列出。

R-13: 用于 mbaps 的 TLS 允许的密码必须支持使用 x.509v3 证书。

R-14: 使用 RSA 私钥时，mbaps 设备必须至少提供以下 TLS v1.2 密码套件：TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

R-66: 具有批量传输加密和 NULL 批量加密的客户端设备应始终将 NULL 批量传输密码套件放在密码套件优先级的最后。

R-67: 服务器设备应能够启用仅认证密码套件 TLS_RSA_WITH_NULL_SHA256 的使用。

8.4 mbaps 基于角色的客户端授权

mbaps 协议提供执行基于角色的客户端授权（AuthZ）的能力。客户端角色数据在其 x.509v3 域证书的扩展中传输。

当两个 TLS 端点之间建立 TLS 会话后，基于角色的客户端 AuthZ 的执行是一个两步过程。

在第一步中，mbaps 服务器获取 x.509v3 客户端域证书。此步骤发生在 mbaps 服务器收到完整握手协议中的消息 8 时。角色从 x.509v3 证书中提取并缓存。如果会话被恢复，此角色必须与恢复的会话关联。

角色扩展是 ASN1 编码的 UTF8 字符串。在示例角色扩展中，角色值为「Operator」（操作员）。

mbaps 基于角色的客户端 AuthZ 能力的第二步涉及使用提取的客户端角色和 Modbus 请求。这两个字段都是 mbaps AuthZ 算法的输入。AuthZ 算法使用已配置的角色到权限规则数据库，确定客户端是否被授权（AUTHORIZED）或未授权（NOT_AUTHORIZED）执行 mbaps 服务器接收到的 Modbus 功能码中指定的功能。如果请求未被授权，将返回 Modbus 异常代码 01 – 非法功能码。如果请求被授权，mbap 服务器将正常处理。

授权功能和角色到权限规则数据库可以存在于服务器设备上，也可以是远程的，需要使用单独的协议来确定请求的授权状态。这不属于本文档的范围。

R-16: mbaps 服务器设备应提供本节所述的基于角色的客户端 AuthZ。

R-17: 如果 mbaps 服务器设备提供基于角色的客户端 AuthZ，则必须符合本节中确定的要求。

R-18: 要提供 mbaps 基于角色的客户端授权能力，需要以下元素：x.509v3 客户端域证书「角色」扩展、mbaps 服务器 AuthZ 算法、mbaps 服务器角色到权限规则数据库。

R-19: mbaps 客户端设备必须配备其 x.509v3 域证书。

R-20: x.509v3 客户端域证书应包含角色扩展。

R-21: X.509v3 证书中的角色必须使用 Modbus.org PEM OID 1.3.6.1.4.1.50316.802.1

R-22: x.509v3 证书中的角色必须使用 ASN1:UTF8String 编码

R-65: 每个证书只能定义一个角色。整个字符串将被视为一个角色。

R-23: 如果 X.509v3 证书中未指定角色，mbaps 服务器必须向 AuthZ 算法提供 NULL 角色。

R-24: mbaps AuthZ 算法必须由设备供应商定义和提供。

R-25: 角色到权限规则数据库的设计（语法和语义）必须由设备供应商定义。

R-26:
特定应用的角色到权限规则数据库必须根据设备供应商的设计进行配置，并由最终用户在 mbaps 服务器中部署。

R-27: 特定应用的角色到权限规则数据库必须可由最终用户配置。

R-28: 特定应用的角色到权限规则数据库不得具有不可更改的硬编码默认角色。

R-29: x.509v3
客户端域证书中使用的角色值必须与设备供应商的角色到权限规则数据库设计一致。

R-30: mbaps 服务器必须从接收到的 x.509v3 客户端域证书中提取客户端角色。

R-31: 如果 mbap 协议处理器因授权拒绝请求，必须使用异常代码 01 – 非法功能码。

9 系统依赖

要参与解决方案架构，mbaps 设备依赖于公钥基础设施（PKI）的证书管理服务。其细节对 mbaps 服务器或客户端行为的实现没有实质性影响。

10 TLS 要求

10.1 TLS 版本

R-32: mbaps 设备必须提供 TLS v1.2 或更高版本。

R-33: mbaps 设备必须符合 [RFC5246] 的要求。

R-34: mbaps 设备不得降级协商到 TLS v1.1、TLS v1.0 或 SSL V3.0。

R-35: mbaps 设备不得协商使用 SSL v2.0 和 SSL v1.0，符合 [RFC6176]。

10.2 TLS v1.2 密码学

10.2.1 概述

R-36: mbaps 设备应提供计数器模式密码套件。计数器模式密码套件包括：TLS_RSA_WITH_AES_128_GCM_SHA256 {0x00,
0x9C}、TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 {0xC0, 0x2B}

R-37: mbaps 设备不得协商密码套件 TLS_NULL_WITH_NULL_NULL

R-38: mbaps 设备使用的任何密码套件以及在 TLS 握手协议交换中协商的密码套件必须在 [TLS-PARAMS] 中的 IANA TLS 密码套件注册表中列出。

10.2.2 TLS 密钥交换

R-39: mbaps 设备必须提供基于 RSA 技术的 TLS
客户端-服务器密钥交换，如强制密码套件所指定并在 [RFC5246] 中描述。

R-40: mbaps 设备应提供基于 ECC 技术的 TLS 客户端-服务器密钥交换。

R-61: 使用 ECC 技术的 mbaps 设备必须至少支持 P-256 NIST 曲线。

R-62: 使用 ECC 技术的 mbaps 设备必须至少支持最低密码套件
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

R-63: 使用 ECC 技术的 mbaps 设备必须使用 [RFC4492] 中的支持的椭圆曲线扩展在其 ClientHello 中指定所使用的曲线。

R-64: 使用 ECC 技术的 mbaps 设备必须使用 [RFC4492] 中的支持点格式扩展在其 ClientHello 中指定所使用的点格式。

10.2.3 TLS 认证

可以使用自签名设备证书针对信任锚进行认证。建议使用由证书颁发机构签名的证书进行认证。

应支持使用会话票据或恢复会话 ID 的会话恢复，以减少连接的握手时间。首选使用会话 ID 的会话恢复。在会话恢复中，服务器负责缓存和维护会话信息以供后续使用。这种方式得到了更广泛的支持，并且对客户端管理与其对等方的会话信息的要求更少。

会话票据将会话信息的负担放在客户端上。此信息由服务器加密并传输给客户端。在新会话中，此信息被传回服务器并用于重新建立连接。实现此操作所需的服务器资源较少，但会浪费网络资源，并且由于信息传输，重新建立连接需要更长时间。

R-41: mbaps 设备必须支持 TLS 客户端-服务器双向认证握手。

R-42: mbaps 设备应在客户端和服务器上支持 TLS 恢复会话握手。

R-43: mbaps 设备可在客户端和服务器上支持 TLS 会话票据恢复。

R-44: mbaps 服务器必须拒绝客户端未以证书响应客户端证书请求的 TLS 握手。

R-45: mbaps 设备应提供由证书颁发机构签名的 x.509v3 证书。

R-46: mbaps 设备在发送证书时必须发送整个证书链直到根 CA。

R-47: mbaps 设备提供的 x.509v3 证书必须符合 [RFC5280] 的要求。

10.2.4 TLS 加密

R-48: 如果 mbaps 设备将用于需要加密的场景，则必须从 [TLS-PARAMS] 中的 IANA TLS 密码套件注册表列表中选择具有所需加密指示符的密码套件。

R-49: 如果 mbaps 设备将用于不需要加密的场景，则必须从 IANA TLS 密码套件注册表列表中选择具有 NULL 批量加密指示符的密码套件。

10.2.5 TLS MAC

R-50: mbaps 设备不得使用 HMAC-MD5 散列算法。

R-51: mbaps 设备不得使用 HMAC-SHA-1 散列算法。

R-52: mbaps 设备必须提供 HMAC-SHA-256 散列算法。

R-53: mbaps 设备不得使用 NULL HMAC 散列算法。

10.2.6 TLS PRF

R-54: mbaps 设备不得提供 HMAC-SHA-1 散列算法用于 PRF 函数计算密钥块，如 [RFC5246] 第 5、6.3 和 8.1 节所定义。

R-55: mbaps 设备必须提供 HMAC-SHA-256 散列算法用于 PRF 函数计算密钥块，如 [RFC5246] 第 5、6.3 和 8.1 节所定义。

10.2.7 TLS 密码学进出口策略

R-56: mbaps
设备必须在其开发周期的早期确定其提供的密码学符合各自国家的进出口合规策略。

10.3 TLS 分片

R-57: mbaps 设备必须提供 [RFC6066] 中定义的最大分片长度协商扩展。

R-58: mbaps 设备必须提供协商 2^9（512）字节最大分片长度的能力，如 [RFC6066] 所定义。

10.4 TLS 压缩

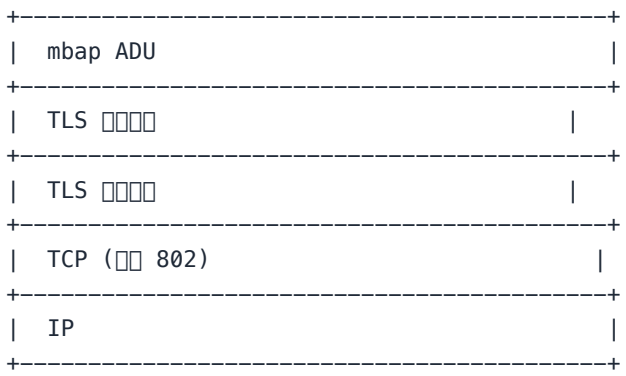
R-59: mbaps 设备必须将 ClientHello 消息的 TLS CompressionMethod 字段设置为 NULL 值。

10.5 TLS 会话重协商

R-60: mbaps 设备必须提供 [RFC5746] 中定义的 TLS 重协商指示扩展，以提供 TLS 会话的安全重协商。

11 附录 A：mbaps 数据包结构

下图显示了 TLS 协议在 TCP 上的分层。mbap ADU 被封装在 TLS 应用协议数据包中。mbaps 协议即通过 TLS 传输的 mbap 协议，位于 TCP 端口 802。



mbaps 使用的 TLS 记录层结构定义在 [RFC5246] 附录 A-1 中，其中：

- ContentType type = 23，应用协议
- ProtocolVersion version = {3,3}，对应 TLS v1.2
- uint16 length = 后续 TLSCiphertext.fragment 的字节数，不得超过 16384 + 2048（18432）
- fragment = TLSCompressed.Fragment 的加密形式，附带 MAC

对于 AES 等分组密码，分片类型为 GenericBlockCipher。如第 10.4 节所定义，CompressionMethod 设置为 NULL。因此，TLSCompressed.length 与未压缩的分片长度相同。

Generic Block 结构的内容元素是 mbap ADU。其结构定义如下：

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 length;
    select (SecurityParameters.cipher_type) {
        case stream: GenericStreamCipher;
        case block:  GenericBlockCipher;
        case aead:   GenericAEADCipher;
    } fragment;
} TLSCiphertext;

struct {
    opaque IV[SecurityParameters.record_iv_length];
    block-ciphered struct {
        opaque content[TLSCompressed.length];
        opaque MAC[SecurityParameters.mac_length];
        uint8 padding[GenericBlockCipher.padding_length];
        uint8 padding_length;
    };
```

```
} GenericBlockCipher;
```

— 本文档完 —