WAPIA

WAPI产业联盟团体标准

T/WAPIA 007.1-2010

无线局域网产品工程化实现指南
第1部分 WAPI与IEEE 802.11n

A Guide to Wireless Local Area Network Product Engineering Implementation -- Part 1: WAPI & IEEE 802.11n

2010-01-20 发布　　2010-01-20 实施

WAPI产业联盟 发布

目　　次

版权声明

前　言

本标准由WAPI产业联盟提出，由WAPI产业联盟归口。

本指导性技术文件主要起草单位：WAPI产业联盟“无线局域网产品工程化实现指南产品方案组”（广州杰赛科技股份有限公司、中国电子技术标准化研究所、国家无线电监测中心检测中心、国家密码管理局商用密码检测中心、方正集团、西安邮电学院、北京傲天动联技术有限公司、西安西电捷通无线网络通信股份有限公司、创锐讯通信技术（上海）有限公司、迈威科技（北京）有限公司、雷凌科技股份有限公司、弘浩明传科技(北京)有限公司、重庆邮电大学、西安电子科技大学等）。

本指导性技术文件主要起草人：周绍午、杨宏、苑克龙、李大为、韩康、朱志祥、刘靖非、铁满霞、胡亚楠、魏源谷、陈愈荣、杨学贤、李春南、聂小勇、龙昭华、肖龙、郭晓东、全红、董涌潮等。

WAPI产业联盟在无线局域网、无线有线一体化网络和网络安全标准化领域的所有标准，是与工业和信息化部宽带无线IP标准工作组紧密协作编制和发布的。

引　言

无线局域网鉴别与保密基础结构 WAPI（wireless local area network authentication and privacy infrastructure）为无线局域网中的数据链路层提供了安全解决方案，包括身份鉴别、密钥管理、数据加密、数据鉴别和重放保护等功能；IEEE802.11n 为无线局域网中媒体访问控制和物理层的高传输速率提供了解决方案，包括多入多出（MIMO）、空间多路复用与映射、天线选择、帧封装等技术。由于两种方案分别涉及不同的领域，它们之间并不存在直接的矛盾或冲突，是可以相互结合、互为补充的，WAPI 与 IEEE802.11n 的基本介绍参见附录 A。

WAPI 与 IEEE802.11n 的结合遵循以下基本原则：

a) 无线局域网中的非安全方案完全使用 IEEE802.11n；

b) 无线局域网中身份鉴别和密钥管理的安全方案完全使用 WAI 鉴别基础结构；

c) 无线局域网中数据传输保护的安全方案由 WPI 保密基础结构与 IEEE802.11n 的帧封装技术结合而成（WPI 保密基础结构参见附录 B）。

无线局域网产品工程化实现指南

第1部分 WAPI与IEEE802.11n

1 范围

本指导性技术文件规定了WAPI与IEEE802.11n融合的工程化实现的关键问题说明，包括服务质量控制字段如何处理、WPI完整性校验的数据组成、WPI的A-MSDU封装、WPI的A-MPDU封装、数据分组序号PN和重放计数器等内容。

本指导性技术文件适用于WAPI与IEEE802.11n标准融合的工程化实现的应用。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本指导性技术文件，然而，鼓励根据本指导性技术文件达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本指导性技术文件。

GB 15629.11-2003/XG1-2006 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第11部分：无线局域网媒体访问控制和物理层规范 第1号修改单

IEEE802.11n 草案 11.0 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求-第 11 部分：无线局域网媒体访问控制和物理层规范 第 11 部分：无线局域网媒体访问控制和物理层规范 补篇 5：增强的吞吐量

IEEE Std 802.11-2007 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求-第 11 部分：无线局域网媒体访问控制和物理层规范 第 11 部分：无线局域网媒体访问控制和物理层规范

3 服务质量控制字段

如果MPDU数据帧的MAC帧头中存在服务质量控制字段，则此字段的数据应包含在WPI完整性校验数据的组成当中。

4 WPI 完整性校验的数据组成

参与WPI完整性校验计算的数据来自于MAC头，由于部分字段值在传输等操作中会产生变化，并不是所有MAC头中的数据都被用于完整性校验计算（例如，持续时间字段），或者一些字段值在用于完整性校验计算的时候被屏蔽置为0。参与WPI完整性校验计算的数据组成如图1所示。

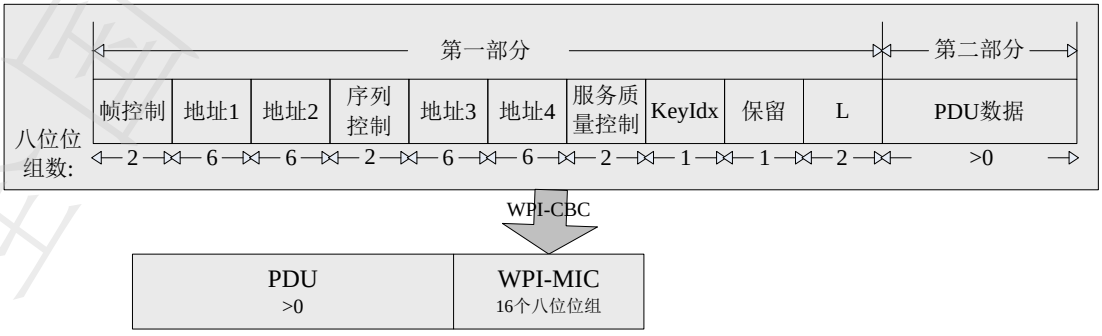

图 1 完整性校验数据组成

其中，完整性校验数据包含两部分内容：

第一部分：

——帧控制（比特 4、5、6、11、12、13 置为 0，比特 14 置为 1）：2 个八位位组；

——地址 1：6 个八位位组；

——地址 2：6 个八位位组；

——地址 3：6 个八位位组；

——序列控制（比特 4~15 置为 0）：2 个八位位组；

——地址 4：6 个八位位组；若 MAC 帧头中不存在地址 4，则该字段的 6 个八位位组的值均置为 0；

——服务质量控制：2 个八位位组；若 MAC 帧头包含服务质量控制字段，则该字段存在，与 MAC 帧头中包含的服务质量控制字段取值相同；

——KeyIdx：1 个八位位组；

——保留：1 个八位位组；

——L：2 个八位位组，该字段表示 PDU 数据的长度，按照大数结尾编码计算。

第二部分：

——PDU 数据：大于 0 个八位位组。

在计算完整性校验码 MIC 时需要使用的字段中，没有特意强调取值的比特位，应使用当前值进行 MIC 计算。

在WPI-SMS4中使用CBC-MAC模式计算完整性校验码MIC时，应保证完整性检验数据的长度为16个八位位组的整数倍。若完整性校验数据第一部分的长度不足16个八位位组的整数倍，应将第一部分扩展为16个八位位组的最小整数倍，扩展采用第一部分后面补零的方法；若完整性校验数据第二部分的长度不足16个八位位组的整数倍，应将第二部分扩展为16个八位位组的最小整数倍，扩展采用第二部分后面补零的方法。接收方验证校验时采用相同的处理。

5 WPI 的 A-MSDU 的封装

A-MSDU子字段结构如图2所示。

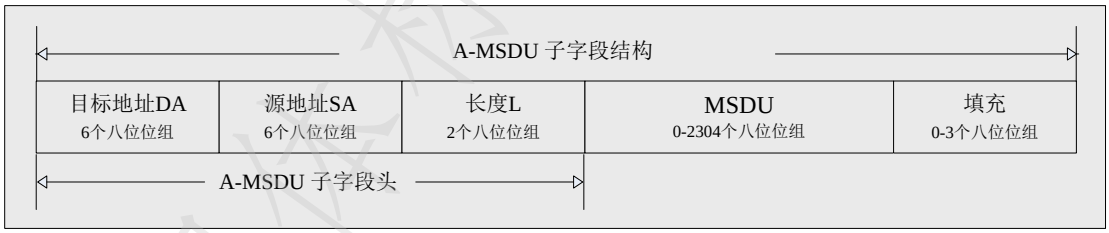

图 2 A-MSDU 子字段结构

A-MSDU 封装格式如图 3 所示。

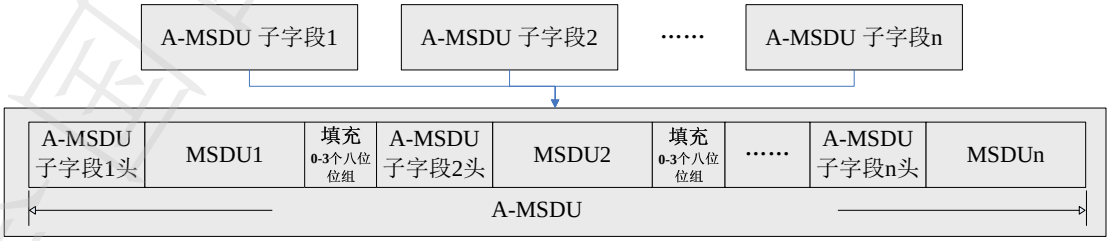

图 3 A-MSDU 封装格式

WPI 的 A-MSDU 封装格式如图 4 所示。

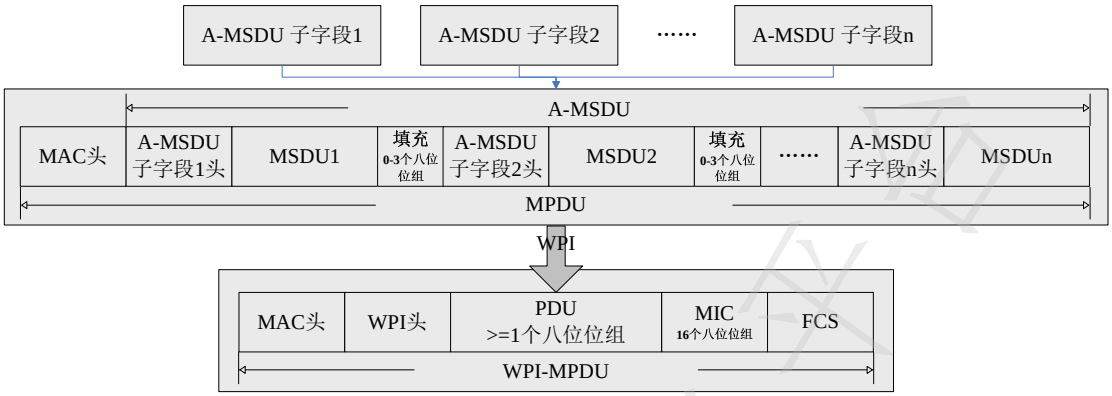

图 4　WPI 的 A-MSDU 封装格式

6　WPI 的 A-MPDU 的封装

A-MPDU子字段结构如图5所示。

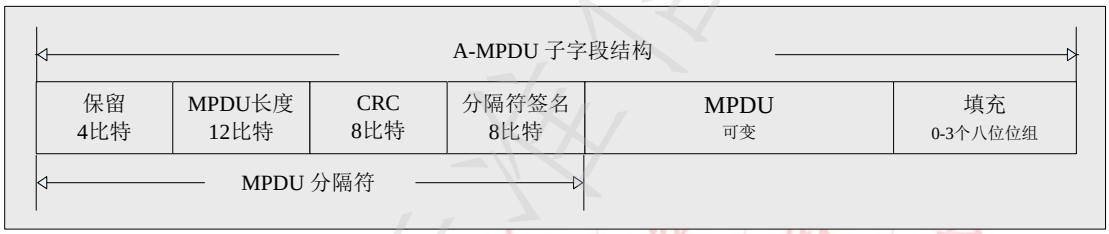

图 5　A-MPDU 子字段格式

A-MPDU封装格式如图6所示。

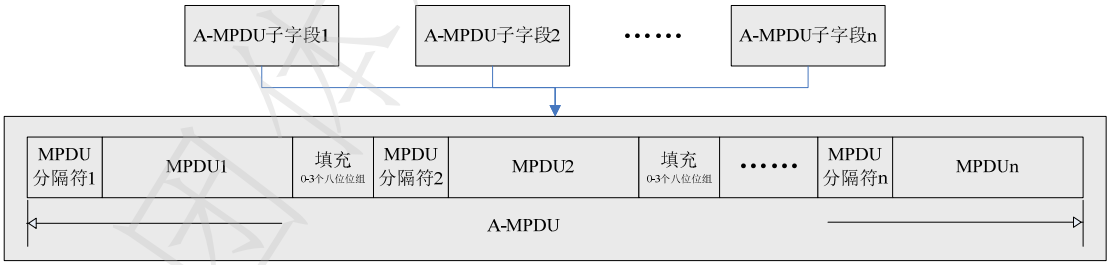

图 6　A-MPDU 封装格式

WPI 的 A-MPDU 封装格式如图 7 所示。

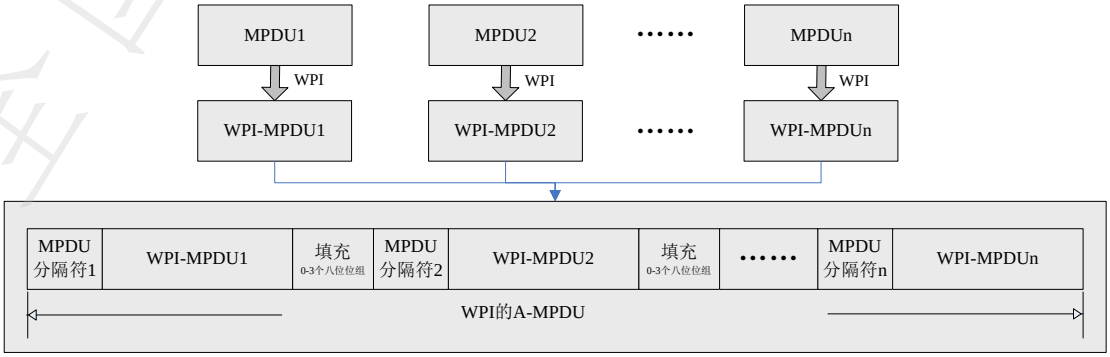

图 7　WPI 的 A-MPDU 封装格式

7 数据分组序号 PN 和重放计数器

对于所有的单播、组播和站间会话业务，发送端对于所有优先级不同的业务只使用同一个WPI中定义的单调递增的PN来加密数据，根据优先级设置的需要，可加密后完成发送；接收端对于接收到的所有优先级不同的业务,应针对不同优先级的业务使用不同的重放计数器分队列进行检查，利用接收到的帧中的PN检查是否存在重放情况。

附 录 A
（资料性附录）
WAPI 与 IEEE802.11n

A.1 WAPI

无线局域网鉴别与保密基础结构WAPI（wireless local area network authentication and privacy infrastructure）是用于提供无线局域网中的身份鉴别和数据机密性的安全机制，由无线局域网鉴别基础结构（WAI）和无线局域网保密基础结构（WPI）组成。其中：

——WAI（WLAN authentication infrastructure）是用于无线局域网中身份鉴别和密钥管理的安全方案；

——WPI（WLAN privacy infrastructure）是用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

注：关于 WAPI 安全机制的详细内容参见 GB 15629.11-2003/XG1-2006。

A.2 IEEE802.11n

IEEE802.11n 标准增强定义了 802.11 的媒体访问控制和物理层，实现了无线局域网内不低于 100Mbps 的高传输速率，从而能够支持高带宽、高质量的无线局域网服务。其中：

——物理层关键技术：包括多入多出（MIMO）、空间多路复用与映射、时空分组编码 STBC、低密度奇偶校验码 LDPC、天线选择等；

——媒体访问控制层关键技术：包括帧封装、多重轮询省电模式 PSMP、高低传输速率共存机制等。

注：关于 IEEE802.11n 标准的详细内容参见 IEEE802.11n 草案 11.0 和 IEEE Std 802.11-2007。

附 录 B
（资料性附录）
GB 15629.11-2003/XG1-2006 第 8.2 节--WPI 保密基础结构

B.1 WPI保密基础结构（GB 15629.11-2003/XG1-2006 中 8.2）

WPI 保密基础结构对 MAC 子层的 MPDU 进行加、解密处理，但对于 WAI 协议分组不进行加解密处理。WPI-SMS4 密码套件中采用的分组密码算法为 SMS4，下面详细说明 WPI-SMS4 密码套件的工作模式与封装结构。

B.2 WPI-SMS4 工作模式（GB 15629.11-2003/XG1-2006 中 8.2.1）

在 WPI-SMS4 中，完整性校验算法工作在 CBC-MAC 模式，数据保密采用的对称加密算法工作在 OFB 模式。两种模式如下图 B.1（GB 15629.11-XG1 中图 61u）：

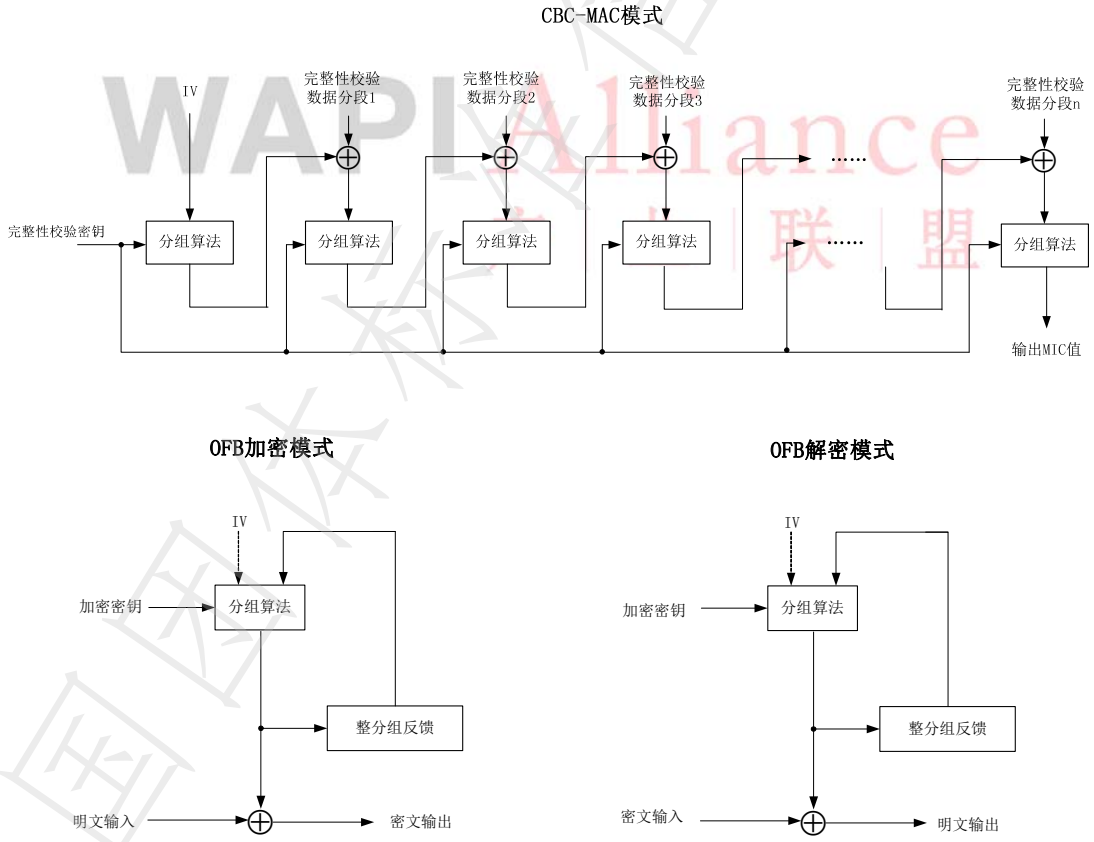

图 B.1 工作模式

B.3 密钥（GB 15629.11-2003/XG1-2006 中 8.2.2）

在证书鉴别过程中，ASUE 和 AE 首先通过 ECDH 交换并利用 KD-HMAC-SHA256 算法协商一个 16 个八位位组的基密钥 BK；在预共享密钥模式中，ASUE 和 AE 将所共享的密钥作为种子导出基密钥 BK。然后，在单播密钥协商过程中，ASUE 和 AE 分别交换一个随机数，利用 KD-HMAC-SHA256 算法和基密钥 BK 导出 96 个八位位组，前 64 个八位位组为单播会话密钥（第一个 16 个八位位组为单播加密密钥 UEK，第二个 16 个八位位组为单播完整性校验密钥 UCK，第三个 16 个八位位组为消息鉴别密钥 MAK，第四个 16 个八位位组为密钥加密密钥 KEK），后 32 个八位位组为下一次单播会话密钥协商过程的询问的种子，然后对

种子使用杂凑函数 SHA-256 计算得到长度为 32 个八位位组的下一次单播密钥协商过程的询问并保存。最后，在组播密钥/站间密钥通告过程中，ASUE 和 AE 或者发起端和对端分别对 16 个八位位组的通告主密钥 NMK 通过 KD-HMAC-SHA256 算法进行扩展，生成长度为 32 个八位位组的组播/站间会话密钥（前 16 个八位位组为组播/站间加密密钥，后 16 个八位位组为组播/站间完整性校验密钥）。

注：在 BSS 和 IBSS 模式中，可以使用基于证书的密钥管理或基于预共享密钥的密钥管理。在 IBSS 中，发起端 STA 和对端 STA 分别作为 AE 和 ASUE，每一个 STA 都需要作为发起端完成单播密钥协商过程和组播密钥通告过程，选择 MAC 地址大的 STA 发起的协商过程的单播数据密钥作为数据传输使用的密钥。

MAC 地址编码为 6 个八位位组，当进行 MAC 地址比较时，把 MAC 地址作为一个无符号的二进制数并且是按照大数结尾排列的。

在用户输入共享主密钥时，需支持十六进制和 ASCII 码字符两种输入方式。

B.4 封装与解封装（GB 15629.11-2003/XG1-2006 中 8.2.3）

WPI-SMS4 的 MPDU 封装结构如图 B.2（GB 15629.11-XG1 中图 61v）：

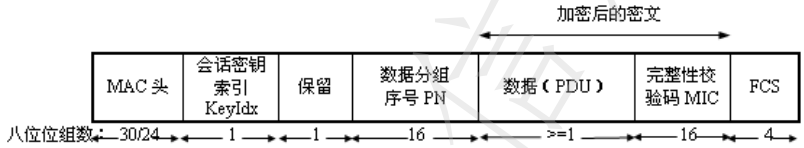

图 B.2 WPI-SMS4 的 MPDU 封装结构

其中：

——MAC 头字段，当地址 4 存在时，长度为 30 个八位位组；当地址 4 不存在时，长度为 24 个八位位组；

——KeyIdx 字段长度为 1 个八位位组，表示 USKID 或 MSKID 或 STAKeyID 值；

——保留字段长度为 1 个八位位组，默认值为 0；

——PN 字段长度为 16 个八位位组，表示一个整数，标识数据分组序号，该数据分组序号作为 OFB、CBC-MAC 模式下数据加密和校验时所需的 IV。数据分组序号 PN 字段按照小数结尾编码发送；

——PDU（数据）字段为 MPDU 数据，最大长度为 2278＝2312－18（WPI 头）－16（MIC）；

——MIC 字段长度为 16 个八位位组；

——FCS 字段长度为 4 个八位位组，为 MAC 帧格式的帧校验序列。

MIC 字段是利用完整性校验密钥采用 CBC-MAC 工作方式对完整性校验数据计算得到，MIC 计算时完整性校验数据的组成结构如图 B.3（GB 15629.11-XG1 中图 61w）：

图 B.3 完整性校验数据

其中，完整性校验数据包含两部分内容，叙述如下：

第一部分：

——帧控制字段（比特 4，5，6，11，12，13 置为 0，比特 14 置为 1），2 个八位位组；

——地址 1，6 个八位位组；

——地址 2，6 个八位位组；

——地址 3，6 个八位位组；

——序列控制字段（比特 4～15 置为 0），2 个八位位组；

——地址 4，6 个八位位组，若 MAC 帧头中不存在地址 4 时，则该字段的 6 个八位位组的值均置为 0；

——服务质量控制字段，2 个八位位组。若 MAC 帧头包含服务质量控制字段时，则该字段存在；

——KeyIdx 字段，1 个八位位组；

——保留字段，1 个八位位组；

——PDU 数据的长度 L，2 个八位位组。该字段按照大数结尾编码计算。

第二部分：

——PDU 数据，大于 0 个八位位组。

在 WPI-SMS4 中使用 CBC-MAC 模式计算完整性校验码 MIC 时，应保证完整性检验数据的长度为 16 个八位位组的整数倍。若完整性校验数据第一部分的长度不足 16 个八位位组的整数倍，应将第一部分扩展为 16 个八位位组的最小整数倍，扩展采用第一部分后面补零的方法；若完整性校验数据第二部分的长度不足 16 个八位位组的整数倍，应将第二部分扩展为 16 个八位位组的最小整数倍，扩展采用第二部分后面补零的方法。接收方验证校验时采用相同的处理。

数据发送时，WPI-SMS4 的 MPDU 封装过程如下：

a） 利用完整性校验密钥与数据分组序号 PN，通过工作在 CBC-MAC 模式的校验算法对完整性校验数据进行计算，得到完整性校验码 MIC；

b） 利用加密密钥与数据分组序号 PN，通过工作在 OFB 模式的加密算法对 MPDU 数据 || MIC 进行加密，得到 MPDU 数据 || MIC 的密文；

c） 封装后再组帧发送。

数据接收时，WPI-SMS4 的 MPDU 解封装过程如下：

a） 判断数据分组序号 PN 是否有效，若无效，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIReplayCounters 加 1；

b） 利用解密密钥与数据分组序号 PN，通过工作在 OFB 模式的解密算法对分组中的 MPDU 数据 || MIC 密文进行解密，恢复出 MPDU 数据 ||MIC 明文。若此时没有有效的解密密钥，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIDecryptableErrors 加 1；

c） 利用完整性校验密钥与数据分组序号 PN，通过工作在 CBC-MAC 模式的校验算法对完整性校验数据进行本地计算，若计算得到的值与分组中的完整性校验码 MIC 不同，则丢弃该数据，且将 MIB 值 gb15629dot11wapiStatsWPIMICErrors 加 1；

d） 解封装后将 MPDU 明文进行重组处理。

B.5 数据分组序号PN的使用规则（GB 15629.11-XG1 中 8.2.4）

a）在单播会话中

每次单播密钥更新后，ASUE 初始化 PN 值 0x5C365C365C365C365C365C365C365C36，AE 初始化 PN 值为 0x5C365C365C365C365C365C365C365C37，ASUE 和 AE 每次发送单播数据帧时，先对 PN 值加 2 后再使用。

当 ASUE 接收单播数据帧时，判断帧中对应于单播密钥标识 USKID 的 PN 值是否单调递增且为奇数，若不是，则丢弃该分组。

当 AE 接收单播数据帧时，判断帧中对应于单播密钥标识 USKID 的 PN 值是否单调递增且为偶数，若不是，则丢弃该分组。

AE 可根据时间或发送的数据包个数等策略更新单播密钥。此外，PN 值的溢出问题需通过 AE 更新单播密钥来解决。

b）在组播会话中

每次组播密钥更新后，AE 初始化 PN 值为 0x5C365C365C365C365C365C365C365C36，AE 每次发送组播数据帧时，先对 PN 值加 1 后再使用。

当 ASUE 接收到组播数据时，判断对应于组播密钥标识 MSKID 的 PN 值是否单调递增，若不是，则丢弃该分组。

AE 可根据时间或发送的数据包个数等策略更新单播密钥。此外，PN 值的溢出问题需通过 AE 更新组播密钥来解决。

c） 在站间会话中

每次站间密钥建立后，发起方初始化 PN 值为 0x5C365C365C365C365C365C365C365C36，发起者每次发送至对端的单播数据帧时，先对 PN 值加 1 后再使用。

当对端接收到利用站间密钥加密的单播数据时，判断对应于该站间密钥标识 STAKeyID 的 PN 值是否单调递增，若不是，则丢弃该分组。

站间密钥的发起方可根据时间或发送的数据包个数等策略更新站间密钥。此外，PN 值的溢出问题需通过站间密钥的发起方更新站间密钥来解决。