LoWPAN 与 6LoWPAN 的协议详解

1. 低功率无线个域网（LoWPAN）

WPAN 网络为在个人操作空间（Personal Operating Space, POS）内的无线通信设备通过无线方式连接起来的基础设施。POS 一般是指用户附近 10 米左右的空间范围。IEEE 802.15 工作组致力于 WPAN 网络的物理层和媒体访问层的标准化工作。

1) IEEE 802.15.1：蓝牙无线个人区域网络（Blue-Tooth），中速，近距
2) IEEE 802.15.2：IEEE 802.15.1 与 IEEE 802.11（WLAN）的共存问题
3) IEEE 803.15.3：高速无线个人区域网络（HR-WPAN）
4) IEEE 802.15.4：低速无线个人区域网络（LR-WPAN），低复杂度（Low complexity）、低成本（Low cost）、 低功耗（Low power consumption）、低速率 （Low data rate）

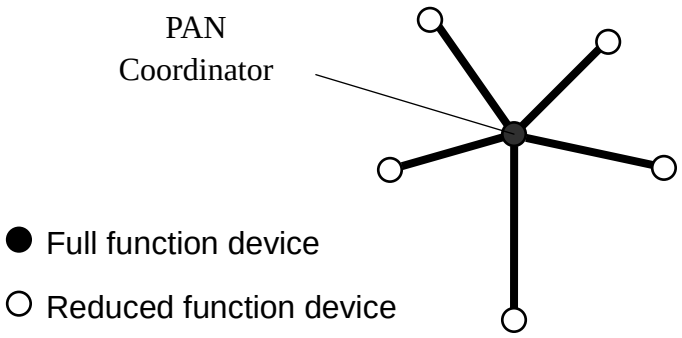
LoWPAN 一般指基于 IEEE 802.15.4 协议族建立的网络。

1.1 意义

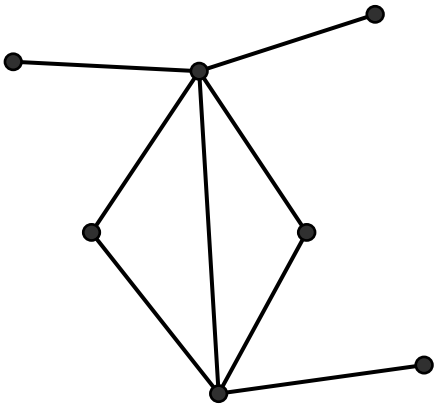
传感器和控制器之间的通信不需要很大的带宽，但是需要低延迟与低能耗，以保证系统长时间的工作。针对这类低成本、低功耗及低速率的应用，802.15.4 制定了设备间互操作的协议标准。

1.2 基本特征

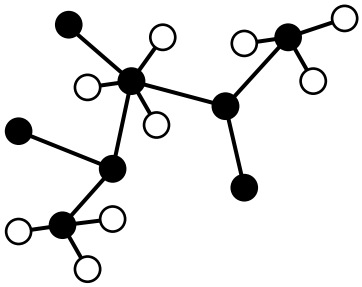
- 低功耗（支持低占空比小于 0.1%的应用）、低成本和低速率
- 支持频带：2.4 GHz，915 MHz，868 MHz
- 支持数据传输速率：250 Kbps(@2.4 GHz)，40 Kbps(@ 915 MHz)和 20 Kbps(@868 MHz)
- 通信距离：50 米左右
- 支持星型网络（如图所示）和点对点网络（如图所示）两种基本网络拓扑结构。网络中设备根据所具有的通信能力分为全功能设备（Full Function Device, FFD）和精简功能设备（Reduced Function Device, RFD）。FFD 可作为网络协调设备，与网络中的任何设备进行通信，支持任何类型的网络；RFD 不能作为网路协调设备，只能与网络协调设备进行通信，只支持星型网络
- 支持大规模网络动态地址编址：地址长度为 2 字节或 8 字节，星型网络中的设备地址为（网络号+设备号），点对点网络中的设备地址为源端设备或目标设备的地址
- 支持三种业务流类型：周期性数据、暂时性数据和低延迟数据
- 在星型网络中，通过最优化保障时隙个数（Guaranteed Time Slot），支 持低延迟应用
- 通过全握手协议（Fully Handshaked Protocol），实现可靠传输
- 采用 CSMA/CA 信道访问控制机制



星型网络

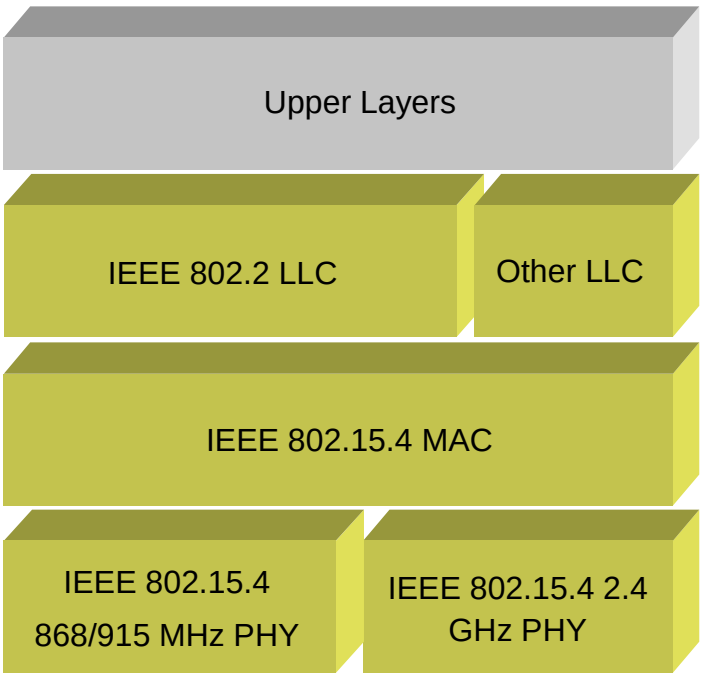


点对点网络



混合网络

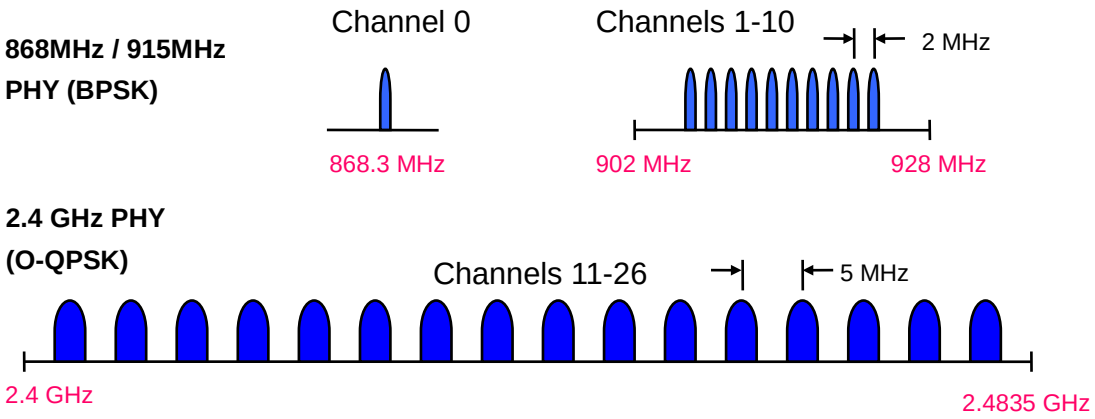
1.3 802.15.4 协议栈体系结构



1.3.1 PHY 子层

物理层定义了物理无线信道和 MAC 子层之间的接口，提供物理层数据服务和物理层管理服务。物理层定义的三个可用的载波频段和帧格式如下所述。

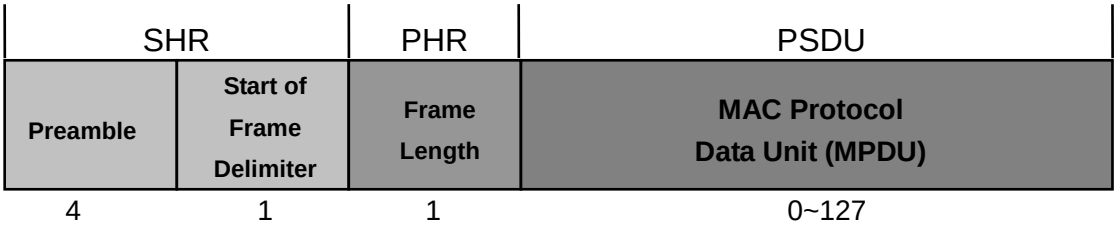
（1）可用频带



IEEE 802.15.4 可采用 868 MHz、915 MHz 和 2.4 GHz 三个载波频段用于收发数据。三个频段总共提供 27 个信道。868 / 925 MHz 采用 BPSK 调制模式，信道的最高数据速率为 20 Kbps，2.4 GHz 采用 O-QPSK 调制模式，最高数据速率可达 250 Kbps。

（2）物理帧格式

物理帧是指物理层发送的数据单元（Physical Protocol Data Unit, PPDU），是在 MAC 层协议数据单元（MAC Protocol Data Unit）之前，添加头部字节组成。物理帧头部字节的长度为 6 个字节，包括同步头部（Synchronization Header, SHR）和物理帧头部（Physical Header, PHR）。SHR 由前导（Preamble）和帧起始分割符（Start of Frame Delimiter, SFD）组成，SFD 的值固定为 0xA7。PHR 的长度为 1 个字节，其中 7 位表示帧长度，1 位保留，因此物理帧负载的长度不会超过 127 个字节。物理层的负载被称之为物理层服务数据单元（PHY Service Data Unit, PSDU），一般用来承载 MAC 协议数据单元（MAC Protocol Data Unit, MPDU）。至于 MPDU 的帧格式定义将在后面的章节中给出。



1.3.2 MAC 子层

MAC 子层使用物理层提供的服务实现设备之间的数据帧传输。MAC 子层提供数据服务和管理服务，包括 PAN 网络的关联建立与关联取消、同步、安全通信、信道接入、保障时隙和可靠传输机制等。这里主要介绍基于 CSMA/CA 的信道访问机制和数据传输模型，为下一章的报文分组与重组打下铺垫。

（1）MAC 帧格式

MAC 帧是指 MAC 层发送的数据单元（MAC Protocol Data Unit, MPDU），由 MAC 帧头（MAC Header, MHR）、MAC 层服务数据单元（MAC Protocol Service Data Unit, MSDU）和 MAC 帧尾（MAC Footer）。MHR 由帧控制信息（Frame Control）、序列 号（Data Sequence Number）和地址信息（Address Information）组成。MSDU 是指 MAC 帧的数据载荷，具有可变长度。MFR 为帧校验序列（Frame Check Sequence, FCS），是通过 ITU-T CRC 校验对 MHR 和 MSDU 部分进行运算得到的 16 位 CRC 校验序列。

MHR			MSDU	MFR
Frame Control	**Data Sequence Number**	**Address Information**	**Data Payload**	**FCS**
2	1	4~20	*n*	2

帧控制信息的长度为 2 个字节，包含帧类型、地址模式和其它控制信息。具体定义如所示。

帧类型	**安全使能**	**待发送**	**ACK请求**	**内部PAN**	**保留**	**目的地址模式**	**保留**	**源地址模式**
0~2	3	4	5	6	7~9	10~11	12~13	14~15

帧类型子域共 3 位，000 表示该帧为信标帧，001 表示数据帧，010 表示应答帧，011 表示命令帧；安全使能子域共 1 位，0 表示该帧不需要加密设置，1 表示该帧会受到密钥的保护；待发送子域共 1 位，1 表示设备在发送帧时又有另外的数据要发送到接收方；ACK 请求子域共 1 位，1 表示接收方在收到数据帧或命令帧之后需要返回 ACK；内部 PAN 子域共 1 位，1 表示 MAC 帧发送到同一 PAN 网络；目的地址模式和源地址模式的长度都为 2 位，这两个子域用于指定该 MAC 帧所采用的地址信息的类型，具体设置如所示。

目的地址模式与源地址模式子域的值

模式值	说明
00	不存在 PAN 标识符和地址域
01	保留
10	包含 16 位短地址的地址域
11	包含 64 位扩展地址的地址域

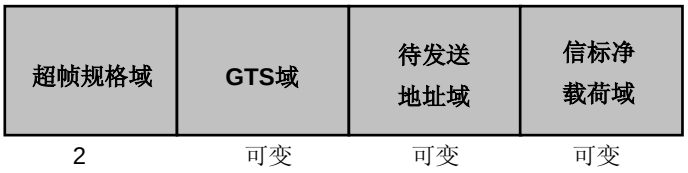
序列号的长度为 8 位，指定了每一个 MAC 帧的标识符。信标帧序列号（BSN）是由协调器根据当前存储在 MAC PIB 中的一个属性值（macBSN）设置的；数据帧和命令帧的序列号（DSN）是每个设备根据当前存储在 MAC PIB 中的一个属性值（macDSN）设置的；应答帧的序列号是通过拷贝数据帧或命令帧中的 DSN 而设置的。

地址信息的长度可变，最高可达 20 个字节，具体的定义格式如所示。

目的设备和源设备的地址都由两部分组成，即 PAN 标识符与设备地址。PAN 标识符用于指定设备所在的 PAN；根据帧控制域中地址模式的设置，设备地址可以采用长度为 2 个字节的短地址，也可以采用长度为 8 个字节的扩展地址。

MAC 帧的数据载荷具有可变长度，即不同类型的 MAC 帧具有不同长度的数据载荷。下面就介绍四种不同的 MAC 帧所包含的数据载荷的定义。

信标帧（Beacon Frame）



超帧规格域的长度为 2 个字节，指定了信标传输的时间间隔与超帧活动的时间长度等信息。信标传输的时间间隔（Beacon Interval, BI）由 BO（Beacon Order, BO）子域的值决定，两则之间的关系为：$BI=aBaseSuperframeDuration * 2^{BO}$，其中 0≤BO≤14；如果 BO=15，则协调器不传输信标帧。超帧活动的时间长度（Superframe Duration, SD）由 SO（Superframe Order）子域的值决定，两则之间的关系为：$SD=aBaseSuperframeDuration * 2^{SO}$，其中 0≤SO≤BO≤14；如果 SO=15，则在传输信标时，超帧不再处于活动状态。

GTS 域指定了 GTS 的个数和每个 GTS 的具体描述（包括设备短地址、GTS 开始时隙和 GTS 长度）。每个超帧最多含有 7 个 GTS，每个 GTS 的长度最多为 15 个时隙。

待发送地址域包含当前发送到协调器的消息的设备地址列表，最多为 7 个（包括短地址与扩展地址）。

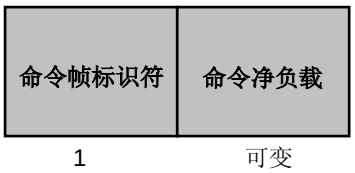
数据帧（Data Frame）

数据帧的负载包含上层请求 MAC 子层所传输的字节，其长度为可变。

应答帧（Acknowledge Frame）

应答帧 MHR 只包含帧控制信息、序列号和帧校验序列，不含有地址信息和数据载荷，因此应答帧的长度为 5 个字节。

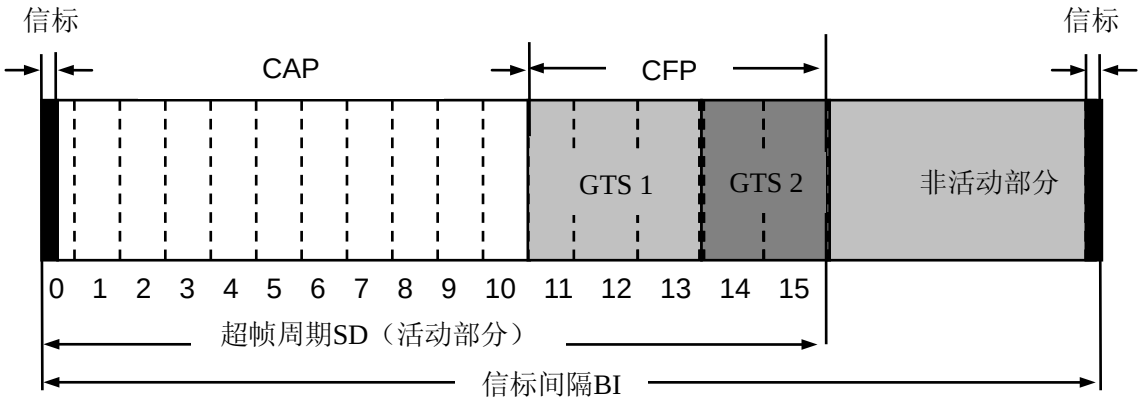
命令帧（Command Frame）



命令标识符用于标识命令帧的类型，如 0x01 表示连接请求，0x02 表示连接相应，0x04 表示数据请求，0x09 表示 GTS 请求。FFD 设备可传输和接收所有类型命令帧，而 RFD 设

备是有条件接收命令帧。在使用信标的 PAN 网络中，命令帧仅仅在竞争访问时段（Contention Access Period, CAP）传输，在不用信标的 PAN 网络中，命令帧可在任何时候传输。

（2）超帧结构



IEEE 802.15.4 采用基于竞争的介质访问机制，即 CSMA/CA，同时可以选用超帧（Superframe）结构组织网络内设备间的通信。

如果选用超帧结构，每个超帧以信标帧为开始，在这个信标帧中包含了由 PAN 协调器（Coordinator）设置的信标帧的间隔（BI）、超帧的活动周期（SD）和为节点分配的时隙等信息。超帧的活动周期被分成三个阶段：信标帧发送时段、竞争访问时段（Contention Access Period, CAP）和非竞争访问时段（Contention Free Period, CFP）。在超帧的 CAP 期间，网络设备使用带时隙的 CSMA/CA 访问机制，并且任何通信都必须在 CAP 期间完成，如果不能完成，则设备将推迟传输直到下一个超帧的 CAP 时期。在非竞争访问时段（Contention Free Period, CFP），PAN 协调器根据上一个超帧周期中网络设备申请的 GTS 情况，将非竞争访问时段分成若干个保障时隙（Guaranteed Time Slots, GTS），每个 GTS 由若干个时隙组成，时隙数目在设备申请 GTS 时指定。

需要注意的是，在信标帧的“信标控制”含有两个控制信标间隔（BI）和超帧周期（SD）长度的域，即 BO（Beacon Order）和 SO（Superframe Order），具体的计算方法为：

BI=aBaseSuperframeDuration * 2^{BO}，其中 0≤BO≤14；

SD=aBaseSuperframeDuration * 2^{SO}，其中 0≤SO≤BO≤14；

aBaseSuperframeDuration=aBaseSlotDuration * aNumSuperframeSlots

默认地，aBaseSlotDuration= 60 symbols，aNumSuperframeSlots=16。当设置 BO 和 SO 时，超帧周期部分的时隙数固定为 16，每个时隙的设置长度为：

960×2^{SO}/（Symbol Rate×16）= 60×2^{SO}/ Symbol Rate

因此，当数据包比较短或流量负载较轻的情况下，可以降低 BO 的值，并扩大 SO 与 BO 的比值。

如果不选用超帧结构，或在使用信标的 PAN 中不能确定信标，网络设备采用非时隙 CSMA/CA 访问机制。

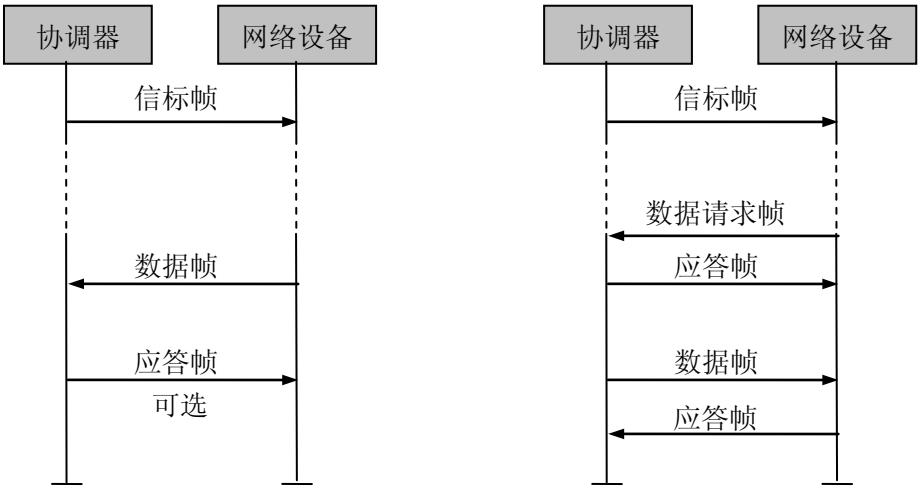
IEEE 802.15.4 采用的 CSMA/CA 机制的算法如所示。NB 记录退避的次数，CW 是竞争窗口的长度，它定义了在开始数据传输之前所需的执行的 CCA 的次数，默认值为 2。CW 这个变量仅在时隙 CSMA/CA 中使用。BE 为退避指数，决定了设备在接入信道之前需要等待的退避周期。对于非时隙 CSMA/CA 系统，或 maxBattLifeExt 设置为 FALSE 的时隙系统，

BE 被初始化为 macMinBE 的值(默认为 3);对于 maxBattLifeExt 设置为 TRUE 的时隙系统，它的值设置为 min(2, macMinBE)，以让采用延长电池寿命延长模式的网络设备具有较高的接入信道的优先级，从而降低网络设备的能耗。

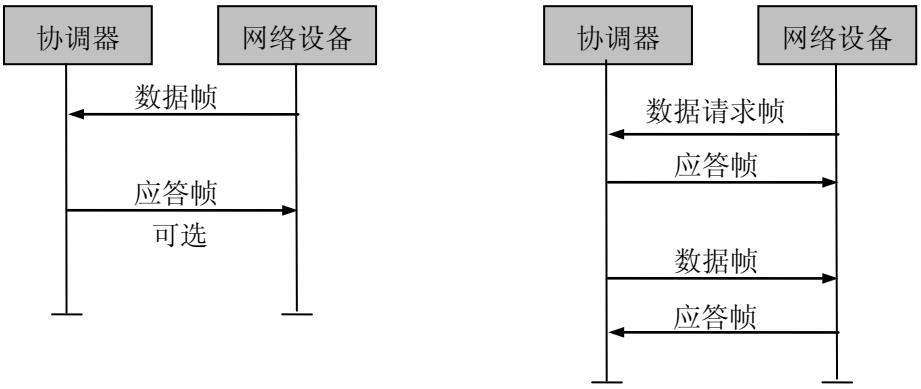
（3）数据传输模型

基于 IEEE 802.15.4 的低速无线个域网中存在三种数据传输方式：设备发送数据给协调器、协调器发送数据给设备、对等设备之间的数据传输。

在选用超帧结构的 PAN 中，网络设备发送数据给协调器的流程如所示，协调器发送数据给网络设备的流程如所示。

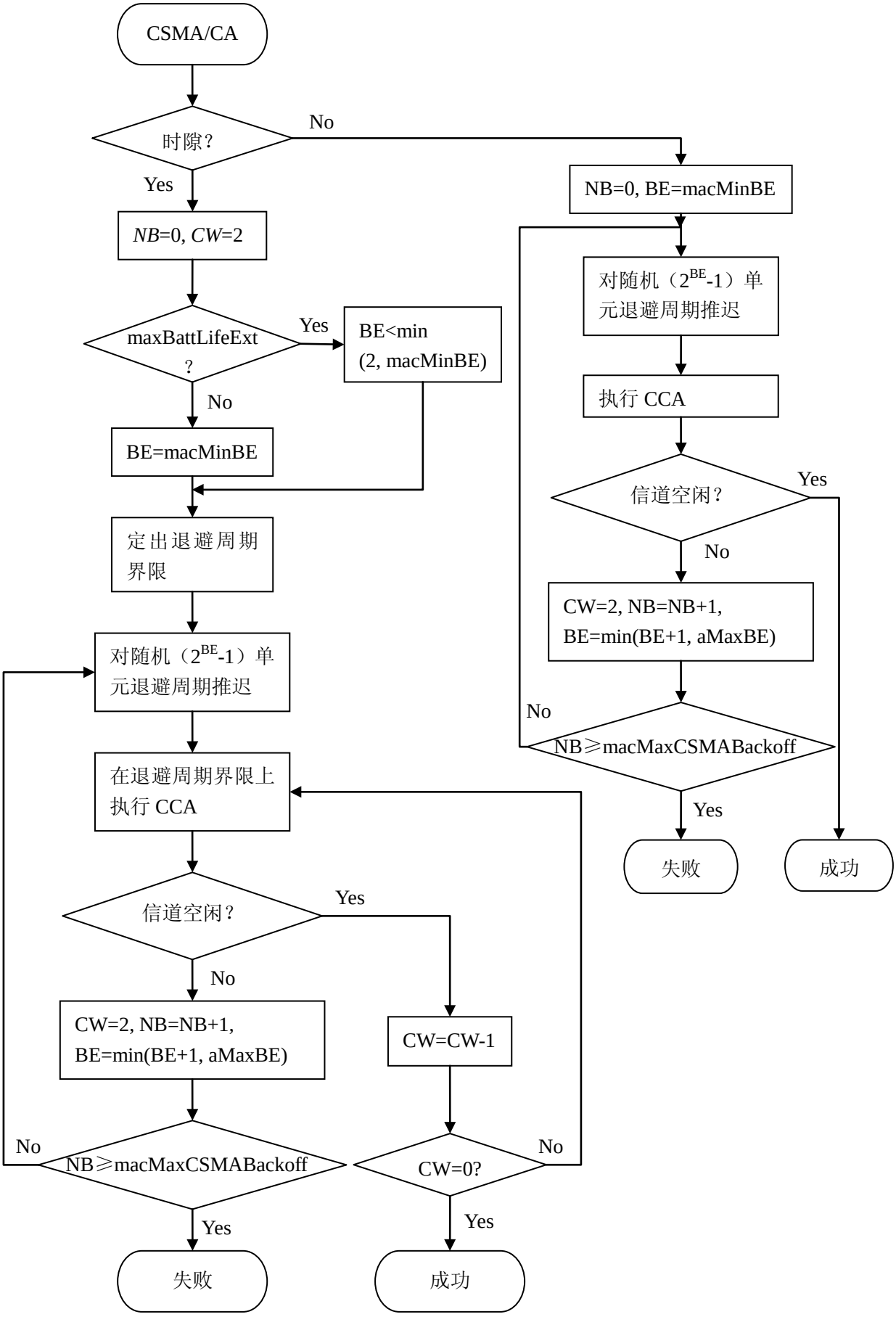


在不选用超帧结构的 PAN 中，网络设备发送数据给协调器的流程如所示，协调器发送数据给网络设备的流程如所示。

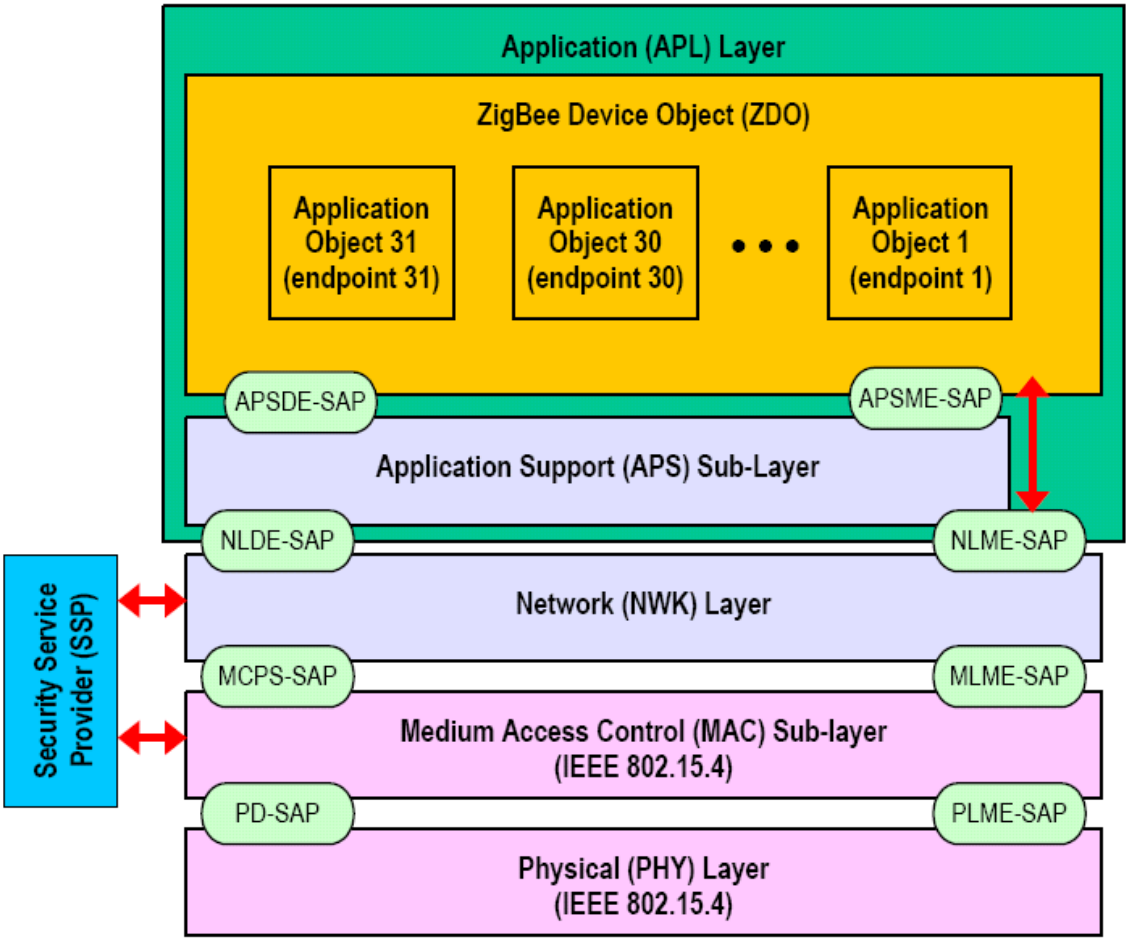


可见，在 802.15.4 中没有采用轮询模式（Polling）将网络设备的数据发送给协调器，即当网络设备需要发送数据时，采用竞争方式主动发送数据请求帧，而不是被动地等待协调器发送轮询帧，这种机制具有以下优点：

- 网络设备不需要等待轮询帧就可以进入信道检测与退避过程，然后发送数据，以此降低数据包的传输延迟；
- 在数据流量不是很密集的应用场景中，轮询帧会造成一定的电量浪费。802.15.4 所采用的 CSMA/CA 机制可以有效的降低能量的消耗。


CSMA/CA
时隙?
No
Yes
NB=0, BE=macMinBE
NB=0, CW=2
对随机（2^BE-1）单元退避周期推迟
maxBattLifeExt ?
Yes
BE<min (2, macMinBE)
执行 CCA
No
BE=macMinBE
信道空闲?
Yes
No
定出退避周期界限
CW=2, NB=NB+1, BE=min(BE+1, aMaxBE)
对随机（2^BE-1）单元退避周期推迟
No
NB≥macMaxCSMABackoff
在退避周期界限上执行 CCA
Yes
失败
成功
信道空闲?
Yes
No
CW=2, NB=NB+1, BE=min(BE+1, aMaxBE)
CW=CW-1
No
NB≥macMaxCSMABackoff
CW=0?
No
Yes
Yes
失败
成功

1.4 ZigBee 协议栈架构



整个协议栈的长度<32 KB，精简功能的节点可以将代码长度缩短到约 6 KB，协调器需要额外的 RAM，以保存与节点设备相关的数据、业务表和节点关联表。

1.4.1 网络层

网络层的功能包括：

- 启动网络
- 加入或退出网络
- 配置新的设备：根据需求配置节点的协议栈
- 地址分配：为加入网络的节点分配地址
- 同步网络中的设备：通过跟踪信标帧或轮询，使网络中的节点保持同步
- 安全：对发送和接受的数据包进行加密和解密操作
- 路由：将数据包转发到目的节点

1.4.2 应用层

ZigBee 应用层由应用支撑子层（APplication Support sub-layer, APS）、ZigBee 设备对象（ZigBee Device Object, ZDO）和制造商定义的应用对象（Manufacturer-defined Application Object）组成。

APS 的功能包括：

- 发现服务：在设备自身的操作空间中判定其它可操作的设备；
- 绑定服务：根据设备提供的服务和需求，绑定相关设备，并在绑定的设备之间转发消息。

ZDO 的功能包括：

- 定义设备在网络中的角色；
- 发起或响应绑定服务的请求；
- 在绑定的节点之间通过加密机制建安全的关系；

应用对象的功能包括：

- 根据 ZigBee 定义的应用描述，实现真实的应用；

1.5 802.15.4 与 802.11 的区别

- 在 802.11 中，CFP 位于 CAP 之前，而在 802.15.4 中，CFP 位于 CAP 之后；
- 在 802.11 中，数据传输的时间长度可以超过下一个信标帧，而在 802.15.4 中，所有的 GTS 必须在下一个信标帧开始之前结束，以保证信标帧的周期性不被破坏，从而保证 RFD 以规则的周期睡眠和唤醒，从而降低 RFD 的能耗。
- 在 802.11 中，没有限定退避的次数，而在 802.15.4 中，当退避次数超过一定阈值时，就宣告失败。
- 在 802.11 中，当节点检测到信道为忙时，就冻结时钟并停止退避，直到再次检测到信道为空时，重新启动始终并继续上一次退避过程。而在 802.15.4 中，退避的始终会在每次信标帧开始时进行重置，即在下一个超帧开始时重新开始退避过程。
- 在 802.11 中，需要在每个时隙中进行 CCA 操作，而在 802.15.4 中，将随机退避一段时间后再进行 CCA 操作。

1.6 802.15.4 与 802.15.1 的区别

	802.15.4 (ZigBee)	802.15.1 (Bluetooth)
典型应用	感知与控制设备 要求低功耗工作模式、长时间运行 数据报文的长度较短	手机与 PDA 之间的信息同步 蓝牙耳机 PDA 与打印机之间的连接
调频模式 符号速率 符号位信息 比特速率	DSSS (11 chips/ symbol) 62.5 K symbols/s 4 bits/ symbol ~128 kbit/second	FHSS (1600 hops / second) 1 M symbol / second 1 bit/symbol ~108-723 kbit/second

时隙长度	$60*2^{SO}$/SR (second) SO: Superframe Order SR: Symbol Rate	Adapt among 625 μS, 1875 μS, and 3125 μS, according to the packet length
主节点发现附属节点的时间间隔	30 ms	>3s, typically 20s
附属节点进入活动状态的时间	15 ms	3 s
活动节点访问信道的时间	15 ms	2 ms
期望的节点寿命	2+ years	typically 1 day

2. IPv6 over LoWPAN (6LoWPAN)

2.1 意义

IP 技术已经被普遍使用，并得到了广泛认可，而且 IP 技术作为一项开放的技术，不受知识产权的约束。IP 技术在低速无线个域网中的应用，可以利用一些现成的网络诊断、管理和授权工具和设备。

2.2. 问题

2.2.1 数据报文长度有限

虽然 IPv6 具有以下优点：（1）便于无状态地址分配与自动网络配置的实现；（2）可以满足大规模节点部署的需求；（3）将 802.15.4 嵌入到 IPv6 地址中；（4）可以实现与其它 IP 网络的互联，如 Internet。但是由于 802.15.4 的最大物理层数据报文长度为 127 字节，**IPv6 及上层协议的包头必须进行压缩**，以保证各层添加报头以后，数据报文仍然可以封装成一个帧，而不需要进行分组与重组。但是，IPv6 最少 1280 个字节的数据报文长度，使得必须采用分组与重装，如此长的数据包也给内存容量有限的 LoWPAN 网络设备带来了很大的挑战。

2.2.2 网络配置与管理的开销不能太大

由于 LoWPAN 网络设备的输入与输出能力都比较有限，而且网络可能部署在人不能及的地方，因此，为 LoWPAN 设计的网络协议应该不需要进行很多的配置，而是采用“即购即用”（Out of the box）的方式，即设备节点部署以后自动启动，当网络出现不可靠因素时进行自修复。网络的链路层协议及管理操作都不应该带来很大的开销。

LoWPAN 支持两种网络拓扑结构：星型网络与点对点网络。

在星型网络中，一些设备具有转发数据报文的能力，如果给这些设备添加一个网络接口，如 IEEE 802.11 无线网口或以太网口，则可以将该网络与无线网络或以太网络进行无缝地连

接。这也是我们提出将 IP 技术运用到 WPAN 的初衷。

在点对点网络中，网络设备需要转发数据报文，即通过多跳路由将数据报文传输到目的地。在 802.15.4 中，转发数据报文的网络设备为“全功能设备”，这些设备具有较高的能量和计算能力等。考虑到 802.15.4 可支持的报文长度较短，**路由协议的开销不能太大**，如不能给发送的数据报文添加太多额外的头部信息；网络设备之间不能交换过多控制报文适应拓扑的变化；而且受网络设备的存储空间与计算能力的限制，不能维护过大的路由表。此外，路由协议还需要考虑节点休眠的情况。

2.2.3 服务发现尽量简单

LoWPAN 中的设备应该采用简单的协议来发现、控制与维护其所提供的服务。在密集部署的场景中，将多个节点进行抽象以提供一个服务具有一定的意义。为此，需要设计新的协议。

2.2.4 安全

6LoWPAN 应用程序一般需要保证信息的保密性与完整性。安全保证机制可以在应用层、传输层、路由层或链路层实现。然而，不管是在哪一层，都需要考虑 LoWPAN 网络设备的程序代码长度、复杂度和带宽要求等方面的限制。在设计安全保证机制时，需要权衡代价与危险之间的关系。通常需要考虑的危险包括拦截攻击（Man-in-the-middle）和拒绝服务（Denial of service）。

IEEE 802.15.4 提出了基于 AES 的链路层安全保证机制，但是没有提出具体的实现细节，如密钥初始分发机制、密钥管理和高层的安全措施。

2.3 解决方法

在实现 6LoWPAN 时，一个基本的准则是“降低数据报文的长度、网络带宽、能量开销和处理开销”。具体包括以下几个方面：

（1）分组与重装：由于 IEEE 802.15.4 的物理层最大数据包长度为 127 字节，除去 MAC 帧添加的 25 个字节的头部，MAC 帧的净负载长度约为 102 个字节。如果采用链路层安全机制，如 AES-CCM-128 需要再添加 21 字节的头部，实际可用的负载空间为 81 字节，远远低于 IPv6 的最短数据报文长度（1280 字节），因此必须在 IP 以下添加一个分组与重装子层。

（2）报头压缩：如上所述，IEEE 802.15.4 大概只留给上层协议约 81 个字节的空间。IPv6 的头部需要占用 40 个字节，如果传输层使用 UDP 协议，则需要添加 8 个字节的头部，还剩 33 个字节可以供上层协议使用；如果使用 TCP 协议，则需要添加 20 个字节的头部，还剩 20 个字节可以供上层协议使用。可见，即使应用层的数据报文长度只有几十个字节也需要进行分组与重装。为尽量降低分组与重装的开销，比较有效的方式是对报文的头部进行压缩，IETF 4944 给出了一个报头压缩的方案。

（3）地址分配：通过 EUI-64 为 IEEE 802.15.4 接口产生一个唯一的接口标识，并基于此标识，采用无状态自动配置协议为网络设备分配 IP 地址。IETF4944 给出了一个无状态地址自动配置方案。

（4）路由协议：由于目前已经提出的几种路由协议，需要比较大的路由开销，如 AODV 协议中路由请求报文的长度为 48 个字节，受报文长度的限制，需要进行分组与重组操作，

因此不适用于 6LoWPAN 网络。理想的协议是，路由控制报文的长度尽量控制在单个 MAC 帧内。

（5）网络管理：将 IPv6 技术运用到 LoWPAN 的一个原因是重用现有的 IP 网络中的一些工具。但是，在重用的时候也同时需要考虑 LoWPAN 资源受限的特性。由于受内存空间、处理能力和报文长度的限制，传统的 SNMP 协议并不适用于 6LoWPAN 网络。6LoWPAN 的网络管理协议需要尽量采用自修复机制，以降低网络配置的开销。

（6）应用 程序与高层协议：传统的基于 XML 的协议，如 SOAP，并不适用于 6LoWPAN，因此需要提出更加简洁和压缩的应用层协议，并且还需要制定有关应用层之间的互操作性的规则。

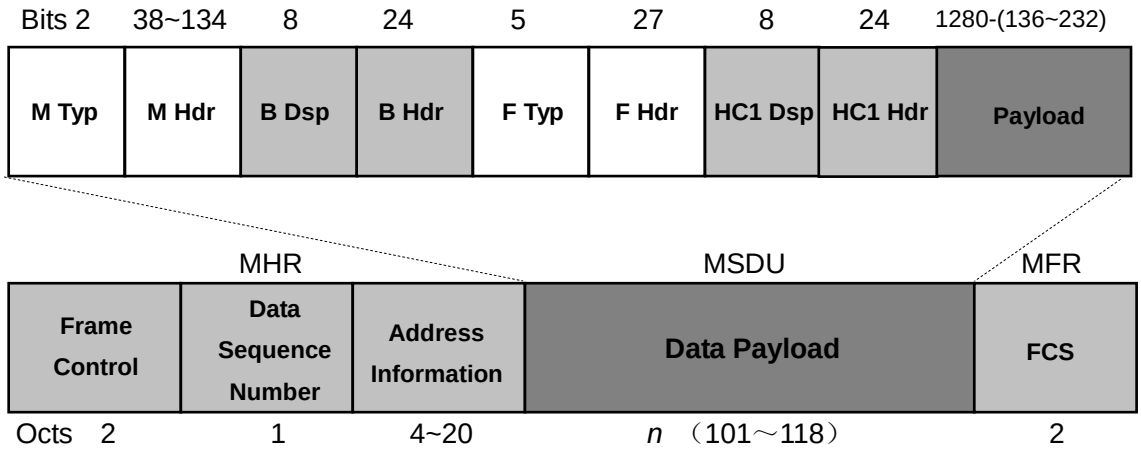
（7）安全：未来还需要为 6LoWPAN 网络的各层操作制定安全机制。比较关键的一点是在自组网络模式下，为位于各个位置的网络设备分配初始密钥，以加入到具有安全保证的网络中。

（8）实现方法：未来还需要制定有关实现以上机制与协议的具体准则，为 6LoWPAN 的长远发展打好基础。

2.3.1 6LoWPAN 适配层与帧格式

6LoWPAN 规定了其所采用的 IEEE 802.15.4 协议的一些属性：

- 在 IEEE 802.15.4 中，定义了四种帧类型，即信标帧、命令帧、答复帧和数据帧。6LoWPAN 将报文封装在数据帧中，并将数据帧头部“控制信息”中的“ACK 请求”设置为 1，以保证链路层的可靠性。
- 在 IEEE 802.15.4 中，定义了两类组织网络设备之间的通信方式，一种是“信标使能”，（Beacon-enabled）即采用超帧结构和时隙 CSMA/CA 机制；另一种是“非信标使能”(Non-beacon-enabled)，即 PAN 协调器不需要定时发送信标帧同步网络设备，通过非时隙 CSMA/CA 机制协调网络设备信道访问的时间。6LoWPAN 采用“非信标使能”模式，但是可以采用信标帧，辅助链路层的设备发现以及网络层的邻居发现。
- 在 IEEE 802.15.4 中，帧头部的源设备地址与目的设备地址可以只指定其中一个，也可以两个都不指定，但是 6LoWPAN 需要这两个地址都需要指定，同时也可以指定源设备与目的设备的 PAN 标识。
- 在 IEEE 802.15.4 中，定义了两种地址模式：16 位的短地址与 64 位的扩展地址。由于 16 位短地址是在网络设备与 PAN 协调器建立连接的时候分配的，因此地址会随着连接或 PAN 协调器的失效而失效。虽然 64 位地址没有该问题，但是在路由、邻居发现和网络配置方面的可扩展问题仍然存在。为支持链路级的广播，6LoWPAN 将每个 PAN 映射为一条 IPv6 链路。当需要向 PAN 中的某个网络设备广播数据时，指定目的设备所在的 PAN 的标识符，并将目的设备的地址设置为 0xFFFF。
- 在 IEEE 802.15.4 中，如果使用最长地址和加密机制，在 UDP 协议下，MAC 帧可用的静负载长度为 41 个字节，TCP 协议，可用的静负载长度为 33 个字节。6LoWPAN 指定数据报文的最大长度为 1280 字节，因此必须进行分组与重组。分组与重组的工作就是由适配层完成。



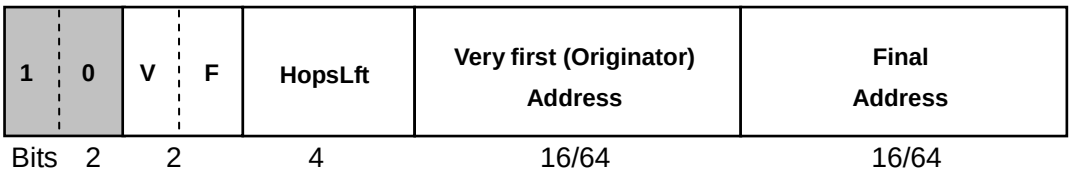
适配层对数据报文进行封装后，封装后的数据报文称为 LoWPAN 数据报文，并将它作为 MPDU 的数据载荷。封装的格式如图所示。数据报文主要添加了以下四类头部字节：

1. Mesh 地址头部（Mesh Addressing Header）
2. 广播头部（Broadcast Header）
3. 分组头部（Fragment Header）
4. 压缩头部（Header Compression Header）

需要注意的是，在适配层对数据报文进行封装时必须按以上顺序添加头部：Mesh 地址、每跳选项（如广播/多播地址）、分组头部和压缩头部。每一个头部都由两部分组成：头部类型（Header Type）和头部域（Header Fields）组成。类型部分的值与对应的类型如表所示。

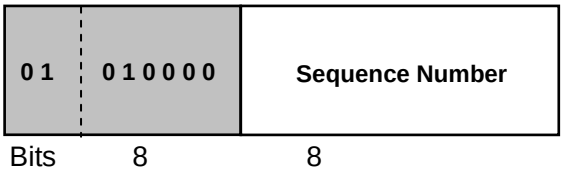
类型字节	类型	描述
00 xxxxxx	NALP	非 LoWPAN 数据报文
01 000001	IPv6	没有经过压缩的 IPv6 头部
01 000010	LOWPAN_HC1	经过压缩的 IPv6 头部
01 010000	LOWPAN_BC0	广播地址
01 1111111	ESC	转义字符，将头部类型的长度扩展为大于 1 个字节
10 xxxxxx	MESH	Mesh 地址
11 000xxx	FRAG1	报文的第一个分组
11 100xxx	FRAGN	报文接下去的分组

可见，报文的第一个头部类型 M Typ 为 MESH 地址（10），头部域部分包含有关跳数、源和目的地址的信息。Mesh 地址头部的具体格式如下所示。

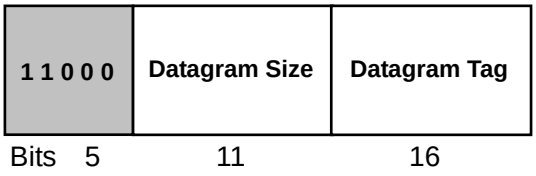


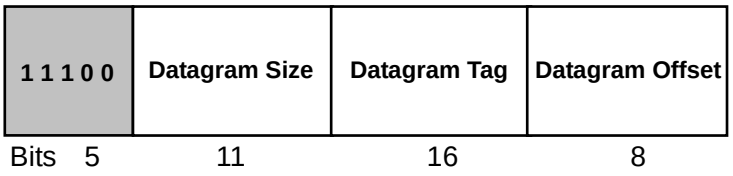
其中，V 位和 F 位分别标识报文源地址和目的地址的类型，0 表示 64 位扩展地址，1 表示 16 位短地址。HopsLft 表示到达目的网络设备的剩余跳数，最大为 14，当 HopsLft 等于 0xF 时，表示后一个字节为剩余跳数，这样就可以使最大跳数大于 14。

报文的第二个头部类型 B Dsp 为广播分发（01010000），头部域是一个长度为 1 个字节的序列号。广播分发头部的具体格式如下所示。



报文的第三个头部类型 F Typ 为报文分组（11000 或 11100），头部域包含报文长度、报文标签和报文偏移量等信息。首个报文分组和其余报文分组的格式如下所示。





在首个报文分组的头部域中包含报文长度与报文标签两个字段，其中报文长度最大为 1280（字节），报文标签最大为 65535。对于同一报文的所有分组来讲，这两个字段的值都是一样的。在其余报文分组的头部域中还包含报文偏移量，该字段的值用于标识该分组在整个报文中的位置。需要注意的是，这里以 8 字节为单位对报文进行分组，因此报文偏移量最大为 160。

当网络设备收到报文分组时，开辟一个与报文长度等长的缓冲区，将具有相同源设备地址、目的设备地址与报文标签的分组重组为一个报文，每个分组在整个报文中的位置由报文偏移量来确定。

在进行报文重组时，需要注意的一个问题是“分组重叠”。这里通过 IEEE 802.15.4 物理帧头部中的长度信息与报文头部中的报文偏移量来检测是否存在分组重叠。

报文的第四个头部类型 HC1 Dsp 为头部压缩（01000010），该部分的具体格式将在下一节中进行具体说明。

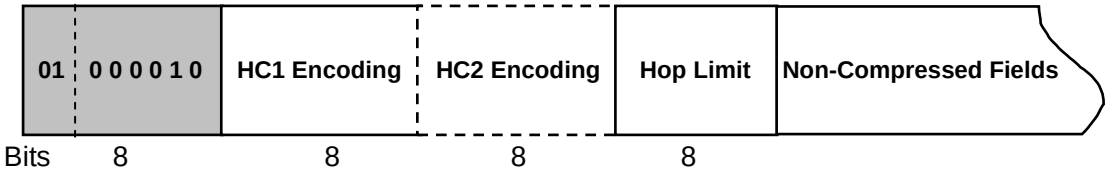
2.3.2 报头压缩

与现有的报头压缩机制相比，6LoWPAN 的报头压缩机制具有以下几个方面的不同：

1. 它不需要获得任何业务流的信息，只与当前链路相关；
2. 可以将第二层与第三层的报头集成起来进行压缩；
3. 在点对点网络中，进行压缩的报文可以转发给任一网络设备，而不需要提前建立任何上下文。

需要主要的是，经过压缩的报头长度可能不是字节的整数倍，因此需要进行填充操作。这里通过填充 0 保证报头的长度为字节的整数倍。

头部压缩的格式如下所示。



其中，HC1 Encoding 的每一个位用于指示 IPv6 报头的对应部分是否进行了压缩，具体的对应关系如下所示。

符号位	报头部分	值	意义
0, 1	源地址	0 0	PI, II
		0 1	PI, IC
		1 0	PC, II
		1 1	PC, IC
2, 3	目的地址	0 0	PI, II
		0 1	PI, IC
		1 0	PC, II
		1 1	PC, IC
4	业务流类型与标签	0	不压缩，业务流类型的长度为 8 位，标签的长度为 20 位
		1	业务流类型与标签为 0
5, 6	下一个头部	0 0	不压缩
		0 1	UDP
		1 0	ICMP
		1 1	TCP
7	HC2	0	HC1 后面为非压缩头部
		1	HC2 为第 5, 6 位指示的协议的压缩头部

以上表格中的 PI、PC、II 和 IC 的含义分别如下：

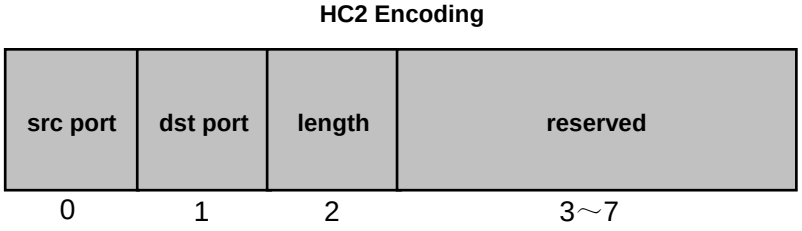
PI：IPv6 地址的前导部分在 Non-Compressed Fields 中；

PC：IPv6 地址的前导部分省略，默认为 0xFE80 0000 0000 0000；

II：IPv6 地址的接口标识部分在 Non-Compressed Fields 中；

IC：IPv6 地址的接口标识部分省略，默认为 Mesh 地址头部域中的源地址或目的地址。

HC2 为 1 时，紧接着 HC1 就是 HC1 的第 5, 6 位指示的协议的压缩头部，以 UDP 协议为例，可压缩的头部字段（除了校验码）有：源端口、目的端口和长度。UDP 压缩头部的具体格式为：



第 0 位用于指示源端口是否压缩。如果为 0 的话，表示不压缩，即端口号的长度为 16 位；如果为 1 的话，源端口号的长度为 4 位（#），实际的端口号为 **0xF0B0**+#；

第 1 位用于指示目的端口是否压缩。如果为 0 的话，表示不压缩，即端口号的长度为 16 位；如果为 1 的话，目的端口号的长度为 4 位（#），实际的端口号为 **0xF0B0**+#；

第 2 为用于指示 UDP 数据包的长度是否压缩。如果为 0 的话，表示不压缩；如果为 1 的话，UDP 头部的长度字段省略，通过 IPv6 的头部的长度字段减去 IPv6 与 UDP 之间的字段长度计算获得。

第 3～7 位为保留位。

未压缩部分的字段（Non-Compressed Fields）从 Hop Limit 开始，依次为 IPv6 头部（源地址前导/接口标识，目的地址前导/接口标识，业务流类型，业务流标签和下一个头部）和 UDP 头部（源端口、目的端口、长度和校验码）。

2.3.3 编址模式与无状态地址自动配置

IPv6 地址由前导（Prefix）和接口标识（Interface Identifier）两部分组成。前导的长度为 64 位，接口的长度也为 64 位。IEEE 802.15.4 网络设备可以使用 64 位的扩展地址，也可以使用 16 位的短地址。如果是 64 位的扩展地址，可以按照“IPv6 over Ethernet”标准将其转化为 128 位的 IPv6 地址。但是，对于 16 位的短地址，需要先按照以下格式将其转化为“伪 48 位地址”：

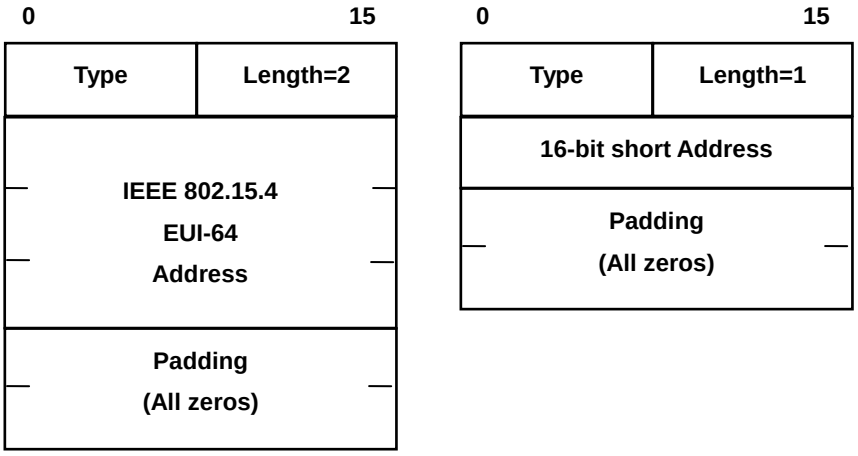
16_bit_PAN : 16_zero_bits : 16_bit_short_address

需要注意的是，通过以上方法形成的“伪 48 位地址”必须将“全局/局部”（U/L）位置为 0 以表明该地址不是一个全局的地址。

在此 64 位 IEEE 802.15.4 接口标识的基础上，添加 0xFE80::/64（::表示用 0 填满 64 位）前导形成 IPv6 链路局部地址（Link Local Address）。

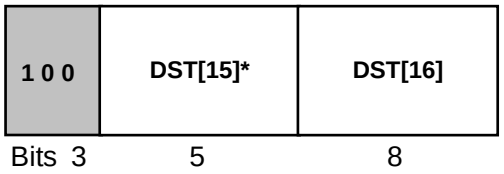
2.3.4 地址映射

（1）单播地址映射：将 IPv6 非多播地址映射为 IEEE 802.15.4 链路层单播地址



其中，Type=1 表示源地址，Type=2 标识目的地址；Length=2 表示 64 位地址，Length=1 表示 16 位地址。

（2）多播地址映射：将 IPv6 多播地址映射为 IEEE 802.15.4 多播地址



IEEE 802.15.4 多播地址以 100 开头，取 IPv6 多播地址 DST 的 3～7 位（即 DST[15]）和 8～15 位（即 DST[16]）组成。

2.3.5 安全考虑

- 以上采用的将 EUI-64 MAC 地址转化为 IPv6 地址的方法并不能保证地址的全球唯一性，因此需要采取避免地址重复的措施。
- IEEE 802.15.4 链路层邻居发现机制易受攻击，加上多跳路由，网络的安全性更加脆弱。因此需要尽量采用链路层安全机制来保证网络的安全。
- IEEE 802.15.4 指出了通过 AES 加密机制保证链路层的安全性，但是并没有指出具体的密钥管理方法。因此可以结合 FFD 的协调功能，来实现密钥管理。

参考文献

1. ***IEEE 802.15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)***. IEEE, New York, NY, 2003.
2. ZigBee Alliance. ***ZigBee Specification Version 1.0***. Online, available at http://www.zigbee.org, Dec. 2007.
3. N. Kushalnagar, G. Montenegro, and C. Schumacher. ***RFC 4919: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals***. IETF, 2007.
4. G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler. ***RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks.*** IETF, 2007.