ZigBee 新设备入网过程

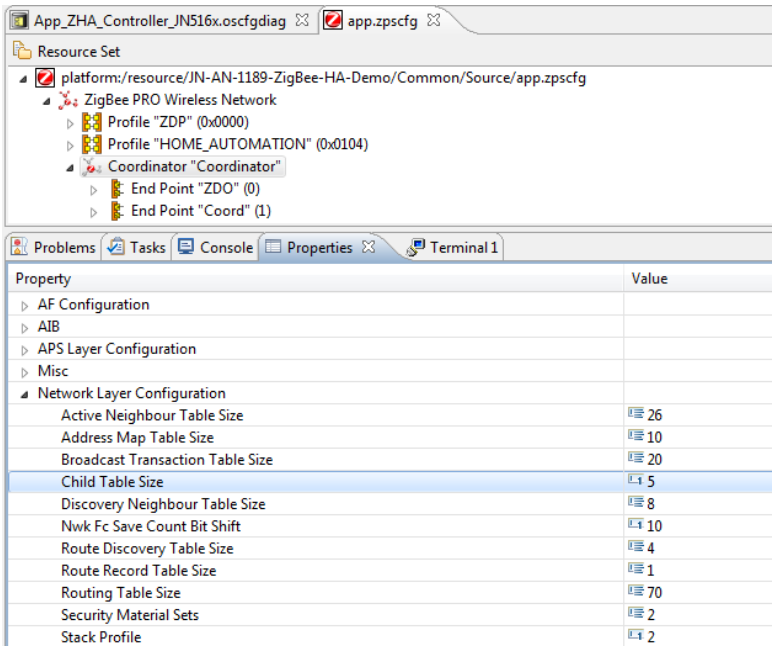
(shaozhong.liang@nxp.com)

1. Coodinator 创建网络

ZigBee 网络的建立由网络协调器 Coordinator 发起。在建立网络前，Coordinator 将进行信道扫描过程。包括能量扫描和主动扫描两个过程：首先对指定的信道或者默认的信道进行能量检测，以避免可能的干扰。以递增的方式对所测量的能量值进行信道排序，抛弃那么些能量值超出了可允许能量水平的信道，选择可允许能量水平的信道并标注这些信道是可用信道。接着进行主动扫描，搜索节点通信半径内的网络信息。这些信息以信标帧的形式在网络中广播，节点通过主动信道扫描方式获得这些信标帧，然后根据这些信息，找到一个最好的、相对安静的信道，通过记录的结果，选择一个信道，该信道应存在最少的 ZigBee 网络，最好是没有其他 ZigBee 设备。

配置网络参数（设置网络 ID）。找到合适的信道后，协调器将为网络选定一个网络标识符（PAN ID，取值<=0x3FFF），这个 ID 在所使用的信道中必须是唯一的，也不能和其他 zigbee 网络冲突，而且不能为广播地址 oxFFFF（此地址为保留地址，不能使用）。PAN ID 可以通过侦听其他网络的 ID 然后选择一个不会冲突的 ID 的方式来获取，也可以人为的指定扫描的信道后来确定不和其他网络冲突的 PAN ID。在 ZigBee 网络中有两种地址模式：扩展地址（64 位）和短地址（16 位），其中扩展地址由 IEEE 组织分配，用于唯一的设备标识；短地址用于本地网络中设备标识，在一个网络中，每个设备的短地址必须唯一，当节点加入网络时由其父节点分配并通过使用短地址来通信。对于协调器来说，短地址通常设定为 0x0000，上面步骤完成后，就成功初始化了 ZigBee 网状网络，之后就等待其他节点的加入。

Coordinator 允许直接相连的设备(Router 和 End Device)最大数目由 “Child Table Size”决定，默认参数为 5。如果需要容纳更多的终端设备入网，应该先让一些 Router 路由设备加入网络。这些 Router 设备充当 EndDevice 终端设备的父节点。

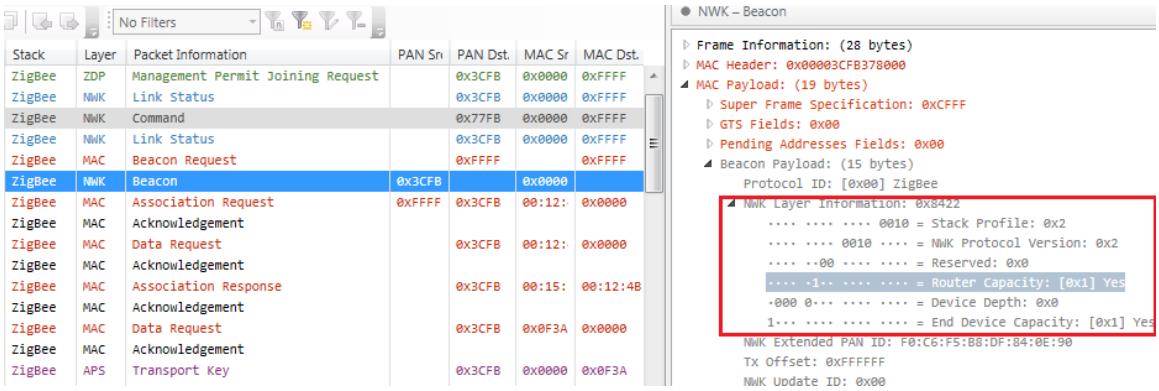


在 Coordinator 可以通过”ZPS_eAplZdoPermitJoining()”函数允许或者拒绝节点加入到网络中。

2. 终端设备 End Device 加入网络

对于 Factory New 新设备来说，首先会在预先设定的一个或多个信道上通过主动或被动扫描周围它可以找到的网络，寻找有能批准自己加入网络的父节点。如果没有合适的父节点的信息，那么表示入网失败，终止过程。如果发出的请求被批准，那么父节点同时会分配一个 16 位的网络地址，此时入网成功，子节点可以开始通信。如果请求失败，那么重新查找，继续发送请求信息，直到加入网络或者相邻表中没有合适的父节点。

Factory New 新设备将会发送一个 Beacon Request 帧，当在这个信道中的 Coordinator 收到该帧，将会回应 Beacon 帧。该 Beacon 帧包含了发送该帧的地址信息，以及是否允许其他设备以其子节点的方式加入。

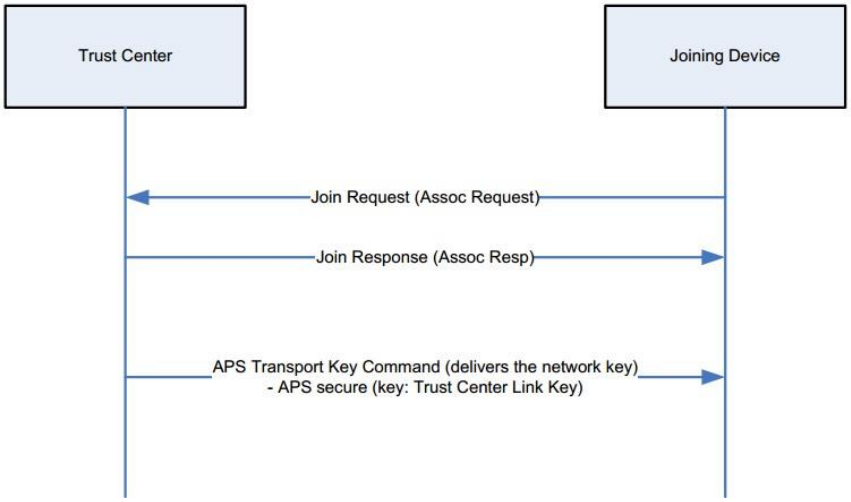


当新设备收到允许加入的 Beacon 帧后，发送关联请求(Associate Request)给 Coordinator 协调器。协调器收到后立即回复一个确认帧（ACK），同时向它的上层发送连接指示原语，表示已经收到节点的连接请求。但是这并不意味着已经建立连接，只表示协调器已经收到节点的连接请求。当协调器的 NWK 层接收到连接指示原语后，将根据自己的资源情况（存储空间和 LQI 能量）决定是否同意此节点的加入请求，然后给节点的 MAC 层发送响应。

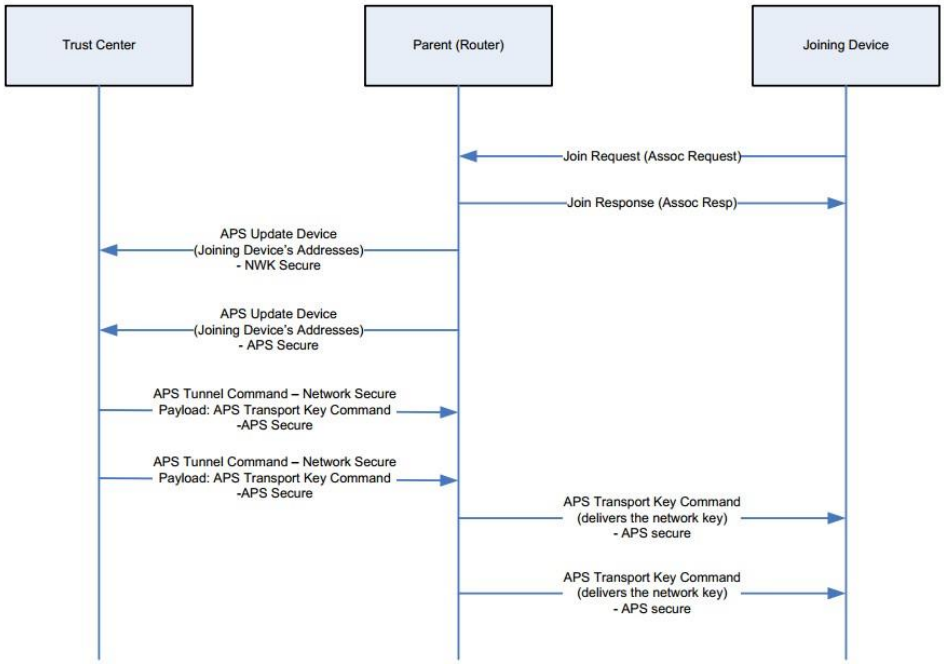
当新设备收到协调器加入请求命令的 ACK 后，新设备 MAC 将等待一段时间，接收协调器的连接响应。若协调器的资源足够，协调器会给新设备分配一个 16 位的短地址，并产生包含新地址和连接成功状态的连接响应命令。协调器在响应时间内同意节点加入，那么将产生关联响应命令(Associate Response)并缓存这个命令。当响应时间过后，新设备发送数据请求命令(Data Request)给协调器，协调器收到后立即回复 ACK，然后将缓存的关联响应命令发给新设备。如果在响应时间到后，协调器还没有决定是否 同意节点加入，那么新设备将试图从协调器的信标帧中提取关联响应命令，成功的话就可以入网成功，否则重新发送请求信息直到入网成功。

新设备收到关联响应命令后，立即向协调器回复一个确认帧（ACK），以确认接收到连接响应 命令，此时新设备将保存协调器的短地址和扩展地址，并且向上层协议栈发送连接确认原语，通告关联加入成功的信息。

传统入网，称为 Classic Commission Join 的方式加入 ZigBee 网络。传统入网过程如下：



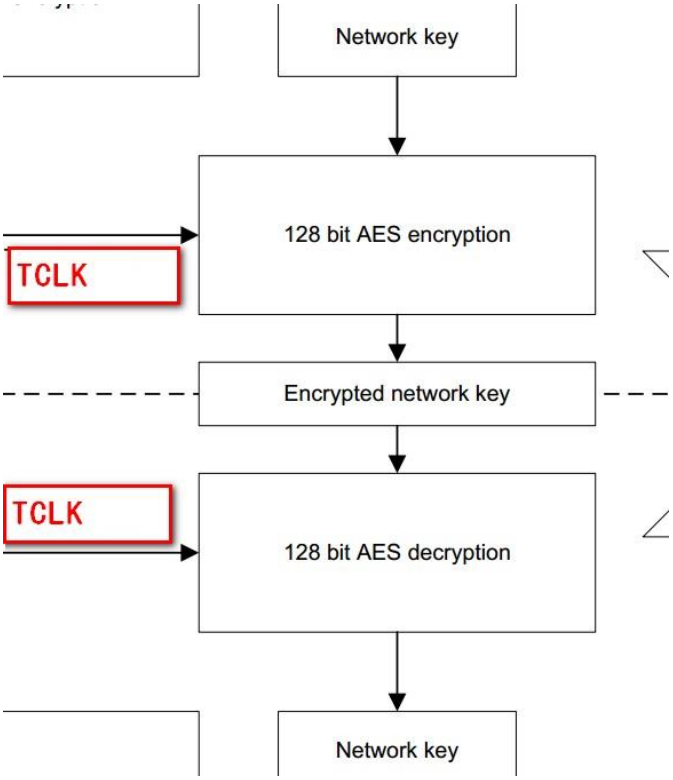
以 Trust Center（一般是协调器）作为父节点加入到网络中



以路由器作为父节点加入到网络中

3. 网络密钥 Network Key 交换过程

ZigBee 入网过程默认都是使能 SECURE 加密，子设备通过 Classic Commission Join 的方式入网时，父设备通过发送 Transport Key 消息将网络秘钥发送给子设备，这个秘钥称为 Network Key，该秘钥用于对网络内的通信数据进行加密。Network Key 在从父设备发送给子设备的过程中，如果以明文发送，则有可能会被其他设备监听到，导致 Network Key 被窃取，使得通信不安全。所以 ZigBee 协议中使用 Trust Center Link Key（TCLK）对通过 AES 128bit 加密算法对该 Network Key 进行加密，过程如下：



在 ZHA 的协议栈中，TCLK 是公开的一个 Key，在 ZHA Specification[3]里面 5.3.3 中提到

5.3.3 Security Parameters

SecurityTimeoutPeriod
Determined by the stack profile.

TrustCenterNetworkKey
The Trust Center will pick the network key. ZigBee HA devices shall not depend on pre-configured network keys to be commissioned or to interoperate.

Trust Center Link Key
0x5A 0x69 0x67 0x42 0x65 0x65 0x41 0x6C 0x6C 0x69 0x61 0x6E 0x63 0x65 0x30 0x39

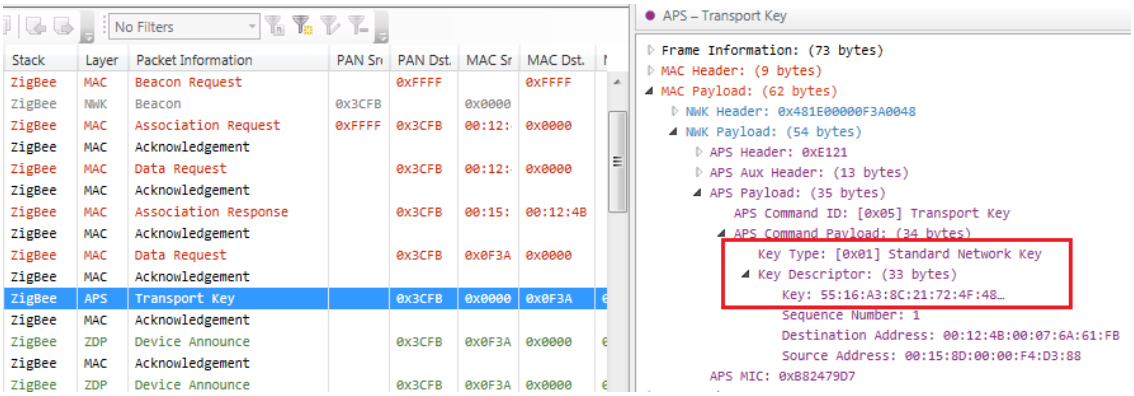
Note: *The Link Key is listed in little-endian format.*

The current network key shall be transported using the default TC link key in the case where the joining device is unknown or has no specific authorization associated with it. This allows for the case where alternative pre-configured link keys specifically associated with a device can be used as well.

在 ZLL 协议中规定默认的 Trust Center Link Key 和 ZHA 的默认 TCLk 是一样，在[1]的 8.1.6.2 节中，

Trust centre link key	0x5a 0x69 0x67 0x42 0x65 0x65 0x41 0x6c 0x6c 0x69 0x61 0x6e 0x63 0x65 0x30 0x39	Default key for communicating with a trust centre.

这也是为什么 ZLL 的灯能够成功加入到 ZHA 的网络中去，原因是他们使用的 TCLK 都是一样的，可以成功的加入到 ZHA 网络中。



了解过 ZigBee 安全机制的研究人员应该都知道，ZigBee End Device 在加入网络时采用了默认的 Trust center link key={0x5A 0x69 0x67 0x42 0x65 0x65 0x 41 0x6c 0x6c 0x69 0x61 0xe 0x63 0x65 0x 30 0x39}来向 Coordinator 获取网络的 Network Key，从而进入到该网络中。 这套安全机制由于采用了默认的 Link Key（全世界都知道的密钥），所以黑客很容易抓包并用默认的 Key 解码获取 Network Key 从而黑进这个网络，国外已经有人把飞利浦的智能灯泡当场黑掉了就是用的这个漏洞。

因此，在 ZigBee 3.0 协议中加入了 Install Code 机制，就是每个 End Device 加入到网络是采用独立的 Link Key，所以即使黑客抓到包，没有 Link Key 也 无法得到 Network Key 密钥。