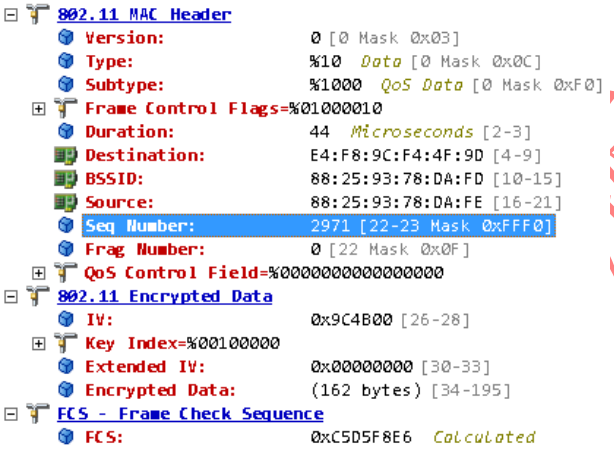
1.1. 设备入网

1.1.1. 一键配置方式

一键配置通过 802.11 数据包的特定区域传输数据完成数据传输。而 802.11 是 IEEE 制定的无线局域网协议，以 802.2 的逻辑链路控制封装来携带 IP 封包，因此能够以 802.2 SNAP 格式接收无线网络数据。如果开启 wifi 芯片的混杂模式监听空间中的无线信号，就会得到如下图所示的数据包：



802.11 空中数据包

从无线信号监听方的角度来说，不管无线信道有没有加密，Length、Destination、BSSID、Source、Seq、FCS 字段总是暴露的，因此实用信号监听方法存在从这些字段获取信息的可能。但从发送方的角度来说，由于操作系统的限制(比如 ISO 或者 Android)，BSSID 、Source、Seq、FCS 等字段的控制需要很高的控制权限，发送方一般是很难拿到的。综合这些客观条件，目前有组播方式和广播方式两种一键配置发包手段来完成信息的传输。

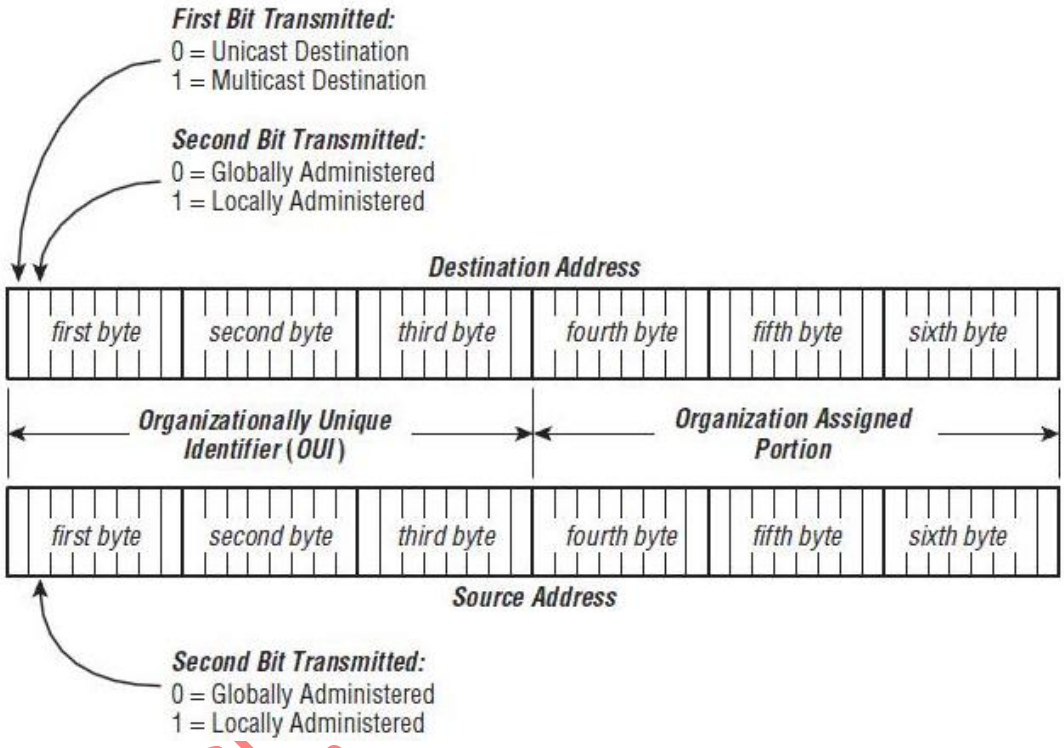
1.1.1.1. 一键配置应用层数据编码

应用层主要将一键配置相关的 SSID 和密码信息经过一定规则编码后进行传输。

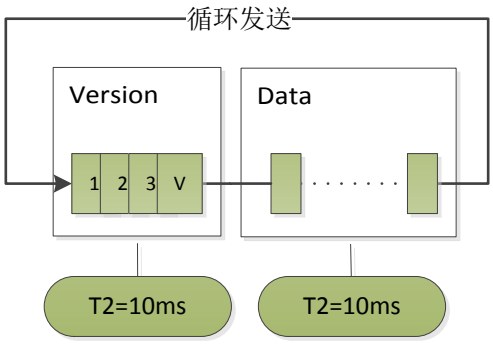
元素		备注
CRC8	[1Byte]	所有其他字段的 CRC8 校验和
Total Length	[1Byte]	总长度
PASS Length	[1Byte]	密码的长度
PASS	[<32Byte]	密码的实际内容
IP	[4Byte]	发送者的 IP 地址
Port	[2Byte]	发送者的工作端口
SSID	[<32Byte]	WIFI 网络 SSID

1.1.1.2. 组播一键配置分量

由于 802.11 处理组播时具有 Destination 的后三字节与目的组播地址后三字节相同的特性，在实际使用中可以使用组播地址的变化来传递信息。而 MAC 地址是以太网二层使用的一个 48bit（6 字节十六进制数）的地址，用来标识设备位置。MAC 地址分成两部分，前 24 位是组织唯一标识符（OUI, Organizationally unique identifier），后 24 位由厂商自行分配。MAC 地址有单播、组播、广播之分。单播地址(unicast address)表示单一设备、节点，多播地址或者组播地址(multicast address、group address)表示一组设备、节点，广播地址(broadcast address)是组播的特例，表示所有地址，用全 F 表示：FF-FF-FF-FF-FF-FF。当然，三层的 IP 地址也有单播、组播、广播之分。MAC 的结构如下图：



使用组播完成一键配置时，802.11 数据包的 Destination 字段中的 Organization Assigned Portion 的内容即为发送方填写的组播地址的后 23Bit。每一次发包过程可以传输 23Bit，整个发包过程先发 Version 数据，然后再发 Data 数据。循环连续发送，每包数据的间隔为 10ms，直到设备拿到所有信息并校验通过，然后通过 Socket 通知发送端。



为了提高可靠性，组播发包的过程的两个阶段必须按照一定规则进行编码和校验。以下是 Joylink3.0 对组播发包各阶段目的 IP 地址的规定：

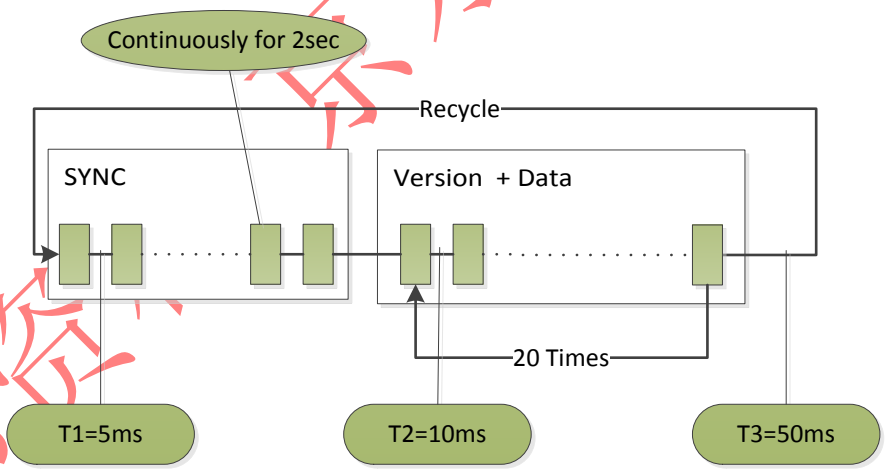
Version 阶段：
239.0.1.1
239.0.1.2
239.0.1.3
239.0.{Version}.4

Data 阶段：
239.{IndexByte}.{byte[i]}.{byte[i+1]}
其中：
{IndexByte}=(0*1bit)((byte[i]^ byte[i+1])*1bit)(Index*6bit)
Index 从 1 开始

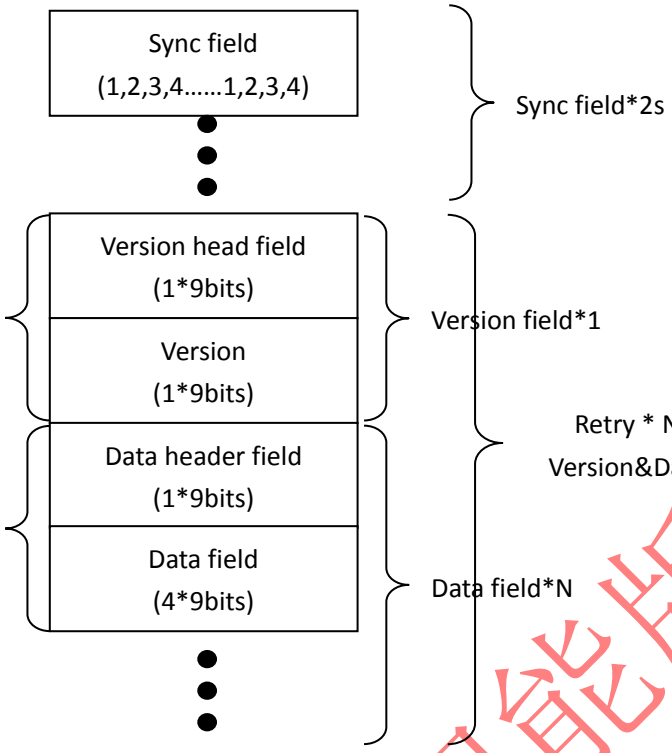
1.1.1.3. 广播一键配置分量

一键配置还可以基于 Length 这一字段传输信息，发送方可以通过改变其所需要发送数据包的长度进行很方便的控制。所以，只要制定出一套利用长度编码的通信协议，就可利用 802.2 SNAP 数据包中的 Length 字段进行信息传递。

在实际应用中，我们采用 UDP 广播包作为信息的载体。信息发送方向空间中发送一系列的 UDP 广播包，其中每一包的长度(即 Length 字段)都按照一定的规范进行编码，信息接收方利用混杂模式监听空间中的无线信号，并从数据链路层截取 802.2 SNAP 格式数据包，便可得到已编码的 Length 字段，随后接收方便可根据协议解析出需要的信息。整个广播发包过程分成同步阶段、Version 阶段，Data 阶段，其中同步阶段的数据包发包间隔为 5ms，Verson 和数据的发包间隔为 10ms，每轮结束后暂停 50ms。同步阶段需要持续发送 2 秒钟，Version 和数据阶段需要连续发送 20 次为一轮，然后不断重复发送同步阶段和数据阶段，如图所示：



从单轮广播一键配置发包的具体数据角度来看，Joylink3.0 对广播三个阶段的长度序列规定如下：



同步阶段：（连续反复发送如下周期为 4 的长度序列，并持续 2 秒）

Length1 = {(0*1bit)(0x1*8bit)}

Length2 = {(0*1bit)(0x2*8bit)}

Length3 = {(0*1bit)(0x3*8bit)}

Length4 = {(0*1bit)(0x4*8bit)}

Version 阶段：（长度为如下的连续 2 包数据构成 Version 单元）

Length1 = {(1*1bit)(0*5bit) (CRC8*3bit)}

Length2 = {(0*1bit)(Version*8bit)}

数据阶段：（长度为如下的连续 5 包数据构成一个包含 4 字节有效数据的单元）

Length1 = {(1*1bit)(Index*5bit)(CRC8*3bit)}

Length2 = {(0*1bit)(Byte(i+0)*8bit)}

Length3 = {(0*1bit)(Byte(i+1)*8bit)}

Length4 = {(0*1bit)(Byte(i+2)*8bit)}

Length5 = {(0*1bit)(Byte(i+3)*8bit)}