

智能中控与网络终端通讯协议

2020.07.21

Lane

Rev	Date	Author	Comments
V0.1	2020.6.23	Lane	Draft
V0.2	2020.7.20	Lane	使用外部通讯终端与服务器通讯协议
V0.3	2020.7.28	Allen	重新整理协议架构

1. 概述

本协议为智能中控与通讯模组之间的通讯协议，协议内容分为四部分：1、智能中控查询通讯模组版本和状态信息；2、智能中控与通讯模组网络信息交互；3、智能中控与通讯模组位置信息交互和透传；4、智能中控与通讯模组蓝牙信息交互和透传。智能中控与通讯模组之间的数据链路层使用 CAN2.0B 通讯，29 位 ID，通信速率采用 250 kbit/s。当发送方发送数据，没有收到回复时，需再次发送该帧数据。连续 3 次没有数据回复，可停止发送该帧数据。

2. 物理层

采用本协议的物理层应符合 ISO 11898-1:2003、SAE J1939-11:2006 中关于物理层的规定。本协议设备间的通信应使用 CAN 接口，通信速率采用 250 kbit/s。

3. 地址分配

地址(Hex)	设备	备注
0x10	智能中控	
0x20	通讯模组	

4. 帧格式

4.1.CAN 通信帧格式

采用本协议的设备应使用 CAN 扩展帧的 29 位标识符，具体每个位分配的相应定义应符合 SAE J1939-21:2006 中的相关规定。每个 CAN 数据帧包含一个单一的协议数据单元(PDU)。协议数据单元由七部分组成，分别是优先权、保留位、数据页、PDU 格式、特定 PDU、地址和数据域。

			R	DP																											...		
P					PF						PS						SA						DATA										
3					8						8						8						0~64										

协议数据单元 (PDU)

数据格式要求:

1. P 为优先级：从最高 0 设置到最低 7。所有控制消息的缺省优先级是 3，其他所有信息、专用、请求和 ACK 消息的缺省优先级是 6。本协议设为 0。
2. R 为保留位：备今后开发使用，本协议设为 0。
3. DP 为数据页：用来选择参数组描述的辅助页，本协议设为 0。
4. PF 为命令号。
5. PS 值为目标地址，发送此报文的地址。
6. SA 为源地址：发送此报文的源地址。
7. DATA 为数据域，Data 的数据格式参考第 4.2 章。
8. 本表第三行表示位数。

9. 当 9 字节或以上的数据传输时，可分多包传输。如数据内容长度为 20 字节，需要前 2 次数据长度为 8 字节，第 3 次数据长度为 4 字节。

4.2. 串口通信帧格式

在 CAN 上的 DATA 域，走的通信协议为从机和主机串口通信协议，串口通信协议帧格式见表格 1。

表格 1 帧格式

标识位	校验码	版本号	厂商编号	外设类型编号	命令类型	用户数据	标识位
1 byte	byte	byte	2byte	1byte	1 byte	n byte	1 byte
0x7E	VAR	0x00	0x00	0x00	VAR	VAR	0x7E

表 A.1 的内容说明如下：

- a) 标识位：采用 0x7e 表示，若校验码、消息头以及消息体中出现 0x7e，则要进行转义处理，转义规则定义如下：

0x7e <————> 0x7d 后紧跟一个 0x02；

0x7d <————> 0x7d 后紧跟一个 0x01；

转义处理过程如下：

发送消息时：消息封装——>计算并填充校验码——>转义；

接收消息时：转义还原——>验证校验码——>解析消息；

示例 1：发送一包内容为 0x30 0x7e 0x08 0x7d 0x55 的数据包，则经过封装如下：0x7e 0x30 0x7d 0x02 0x08 0x7d 0x01 0x55 0x7e；

- b) 校验码：从厂商编号到用户数据依次累加的累加和，然后取累加的低 8 位作为校验码；

示例 2：累加和为 0x1388，则校验码为 0x88；

- c) 版本号：标识通讯协议版本；
d) 厂商编号：外设从机的制造厂商代码；
e) 外设类型编号：每种外设唯一对应的一个类型编号，用于主机的外设接口驱动区别是何种外设发来的数据；外设类型编号见表 A.2；48
f) 命令类型：外设与主机进行各种数据交互的信息类型，命令类型分为通用协议和专有协议两大类：通用协议主要包括从机与主机基本的、必需的、共有的一些信息交互类型；专有协议则定义各型外设与主机特有的信息交互类型；命令类型见表 A.3；
g) 用户数据：指外设与主机交互的数据中除以上几个部分以外的由具体业务功能定制内容；
h) 通讯帧的数据采用大端（big-endian）的表示方式。

5. 错误码 Error Code

表格 2 错误码定义

值	描述
0x00	成功。
0x01	操作失败。
0x02	操作超时。
0x03	设备未准备好。

0x04	不支持的命令。
0x05	硬件错误。
0x06	参数错误。
0xFF	未知错误

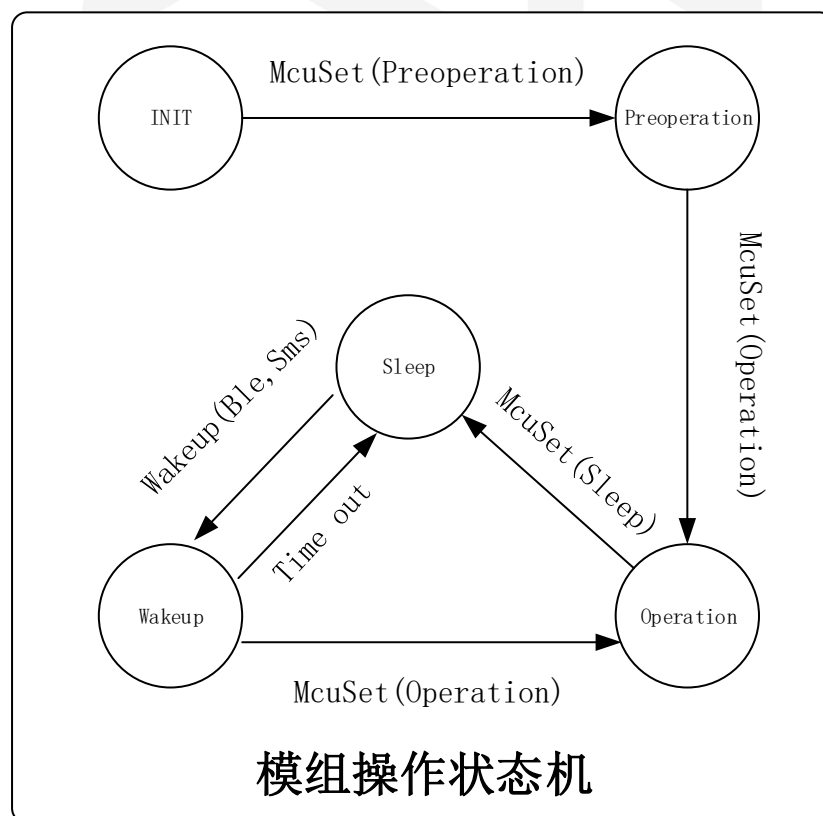
6. PF 命令号说明

表格 3 命令类型定义

命令号	命令类型	说明
0x10	网络管理消息	NMT message
0x20	命令消息	Command Message
0x30	事件消息	Event Message

6.1. NMT Message (网络管理消息)

心跳帧的周期为 2 秒，如果超过 3 秒没有收到对方的心跳帧，认为对方不在线。
节点工作状态机如图表 1



图表 1

6.1.1. SIM Heartbeat (0x01)

SIM 模组心跳消息。

SIM 模组发送给 MCU，MCU 不需要应答。模组运行起来，必须周期 (2 秒) 向主控 MCU

发送心跳包，心跳包不需要应答。

表格 4 心跳数据包格式定义。

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x01	命令码
1	Data Length	UINT8	0x01	数据长度
2	OperationState	UINT8		模组的操作状态。 0: 初始化状态。 1: Sleep State. 休眠状态。 2: Wakeup, 唤醒状态。 4: PreOperation State. 域操作状态。 5: Operation State. 操作状态。

表格 5 模组的操作状态定义

Value	Name	Meaning	NMT	CMD	EVENT
0	Init	初始状态，模组复位后，必须运行在该状态下。 1) 模组保持最低功耗，GPRS/GPS/BLE 不上电。	√	x	x
1	Sleep	休眠状态，模组进入 Sleep 后，至少要发送一次心跳通知 MCU，才能真正进入 Sleep 状态。 如果被唤醒，超时(5S)会再次进入 Sleep 状态。 SIM 模组：低功耗或者断电。 BLE 模组：低功耗或者断电。	x	x	x
2	Wakeup	唤醒状态，等待 MCU 的状态切换命令，如果 10 秒内没有 MCU 的指令，再次进入 Sleep 状态。 SIM 模组：低功耗或者断电。 BLE 模组：低功耗或者断电。	√	x	x
4	Pre-Operational	预操作状态，模组能够处理 NMT 消息和 CMD 消息，不处理 EVENT 消息。 SIM 模组：不工作。 BLE 模组：不工作。	√	√	x
5	Operational	操作状态，处理所有消息。当模组第一次从其他状态切换到 Operation 状态，所有的 Changed Event 都必须发送一遍。 SIM 模组：正常工作。 BLE 模组：正常工作。	√	√	√

6.1.2. MCU Heartbeat (0x02)

MCU 心跳消息，发送给模组，模组不需要应答。

主控 MCU 运行后，必须周期（默认 2 秒，可配置）向模组发送同步帧，同步帧不需要应答。

表格 6 MCU 心跳数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x02	命令码

1	Data Length	UINT8	0x04	数据长度
2	Interval Ms	UINT32	2000	同步帧的间隔, 单位 MS, 默认值为 2000Ms

6.1.3. SetOperationState (0x03)

设置 SIM 模组操作状态, MCU 发送给 SIM 模组, 模组需要应答。

表格 7 SetOperationState 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x03	命令码
1	Data Length	UINT8	0x04	数据长度
2	Operation State	UINT8	-	操作状态
	State Parameter	UINT8		操作状态参数: BIT[0-1]: GPRS 状态, 短信可唤醒。 0: 关闭 GPRS 电源。 1: GPRS 低功耗, TCP 连接中断, 短信可唤醒。 2: 保留 3: 全功能正常工作。 BIT[2-3]: GPS 工作状态。 0: 关闭 GPS 电源。 1: GPS 低功耗, 不用实时获取定位信息, 唤醒后可快速定位。 2: 保留 3: 全功能正常工作。 BIT[4-5]: BLE 模组工作状态。 0: 关闭 BLE 电源。 1: BLE 低功耗, 可发送广播, 可以接收连接。 2: 保留 3: 全功能正常工作。

表格 8 SetOperationState 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x11	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.2. SIM Command Message (命令消息)

所有的 Command Message, 等待应答的超时事件为 1 秒。

6.2.1. GetSimID (0x11)

读 SIM 模组身份信息。

表格 9 GetSimID 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x11	命令码
1	Data Length	UINT8	0x01	数据长度
2	Protocol Version	UINT8	1-255	MCU 和 SIM 的传输协议版本号，从 1 开始，每次更改传输协议，必须兼容上一个版本，并且版本号累加 1。

表格 10 GetSimID 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x11	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义
3	Protocol Version	UINT16		协议版本号
6-13	Ver Desc	Version descriptor		SIM 模组版本号描述符。
	SN			SIM 模组序列号

6.2.2. GetSimCfg (0x12)

获取 SIM 模组的终端参数信息

表格 11 GetSimCfg 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8	0x01	数据长度
2	CfgInfo	CfgInfo Struct		获取的终端参数信息结构，参考表格 12

表格 12 CfgInfo 数据格式

起始字节	字段	数据类型	描述及要求
0	参数总数	BYTE	
1	参数项列表		参数项格式见表格 13

表格 13 终端参数项

字段	数据类型	描述及要求
参数 ID	DWORD	参数 ID 定义及说明表目
参数长度	BYTE	
参数值		DWORD 或 STRING，若为多值参数，则消息中使用多个相同 ID 的参数项，如调度中心电话号码

参数列表参考协议“易马达电动车【中控-服务器】通信协议”第 6.8 章“终端参数设置各参数项定义及说明”。

表格 14 GetSimCfg 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.2.3. SetSimCfg (0x13)

获取 SIM 模组的配置信息。

表格 15 SetSimCfg 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x13	命令码
1	Data Length	UINT8		数据长度
2	CfgInfo	CfgInfo Struct		参数项格式见表格 13

表格 16 SetSimCfg 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x13	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.2.4. GetSms (0x14)

获取 SIM 模组的短消息信息，如果有多条，仅返回最后一条，成功读取后自动删除。

表格 17 GetSms 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x14	命令码
1	Data Length	UINT8		数据长度。

表格 18 GetSms 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x14	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

3	Sms	UINT8[n]		短消息内容, n <= 128。
---	-----	----------	--	------------------

6.2.5. SendDataToSvr (0x15)

MCU 发送数据到网络服务器，SIM 模组接收到该命令后，必须把数据透明转发到服务器，只有数据成功发送到服务器，才能给 MCU 返回响应码“SUCCESS”。

如果当前没连接到服务器，必须返回一个失败响应码。

如果当前模组无法发送数据，返回错误码“BUSY”。

如果当前模组发送数据，期望的事件内没有接收到 Svr 的响应，返回错误码“RCV_RSP_TIMEOUT”

表格 19 SendDataToSvr 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x15	命令码
1	Data Length	UINT8	0x00	数据长度
2	Data	UINT8[n]		传输的数据, n <= 128

表格 20 SendDataToSvr 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x15	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.2.6. GetFileInfo(0x16)

读取文件信息。

智能固件更新启动请求，通讯模组接收后必须主动发送固件更新数据（0x16 命令）。固件升级目标不仅要包括智能中控固件，还要包括其他设备。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x16	命令码
1	Data Length	UINT8	0x00	数据长度
2	File Type	UINT8		文件类型： 1：智能中控固件。 2：按键板固件。 其他值：保留。

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x16	命令码
1	Data Length	UINT8		数据包长度

2	Result	UINT8		参见错误码的定义
3-6	File Length	UINT32		文件长度
7	Version Desc	UINT8		文件的版本描述符

6.2.7. GetFileContent (0x17)

读取文件内容。

Request 定义:

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x17	命令码
1	Data Length	UINT8	0x00	数据长度
2	File Type	UINT8		文件类型: 1: 智能中控固件。 2: 按键板固件。 其他值: 保留。
4	offset	UINT32		偏移

Response 定义:

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x17	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义
4	offset	UINT32		偏移
	File Data	UINT8[128]		文件数据

6.3. BLE Command Message (命令消息)

6.3.1. GetBleID (0x30)

读 BLE 模组身份信息。

表格 21 GetBleID 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x30	命令码
1	Data Length	UINT8	0x01	数据长度

表格 22 GetBleID 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x30	命令码

1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义
	Capacity	UINT16		BLE 模组的能力描述，定义如下。 BIT[0]:是否支持信标，0-不支持，1-支持。 BIT[1-15]:保留
6-13	Ver Desc	Version descriptor		BLE 模组版本号描述符。
	MAC			蓝牙模组 MAC 地址。

6.3.2. GetBleCfg (0x31)

获取 SIM 模组的配置信息

表格 23 GetBleCfg 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x31	命令码
1	Data Length	UINT8	0x01	数据长度

表格 24 GetBleCfg 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x31	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义
3	BleCfg	BleCfg Struct		Ble 模组配置信息

表格 25 BleCfg 数据包格式定义

Index	Name	Type	Value	Descriptor
0	BleName	CHAR[32]		蓝牙广播名称

6.3.3. SetBleCfg (0x32)

设置通讯模组配置信息。

表格 26 SetBleCfg 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x32	命令码
1	Data Length	UINT8	0x00	数据长度
	BleCfg Info	BleCfg Struct		蓝牙广播名称

表格 27 SetBleCfg 响应数据包格式定义

Index	Name	Type	Value	Descriptor
-------	------	------	-------	------------

0	Cmd	UINT8	0x32	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.3.4. GetBleCtrlEn (0x33)

设置蓝马模组的控制使能。

表格 28 GetBleCtrlEn 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x33	命令码
1	Data Length	UINT8	0x00	数据长度

表格 29 GetBleCtrlEn 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x33	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义
2	Ctrl Enable	UINT16		控制状态码。 BIT[0]:信标扫描使能, 0-Disable;1-Enable. BIT[1-15]:保留

6.3.5. SetBleCtrlEn (0x43)

设置蓝马模组的控制使能。

表格 30 SetBleCtrlEn 请求数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x43	命令码
1	Data Length	UINT8	0x00	数据长度
2	Ctrl Enable	UINT16		控制状态码。 BIT[0]:信标扫描使能, 0-Disable;1-Enable. BIT[1-15]:保留

表格 31 SetBleCtrlEn 响应数据包格式定义

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x43	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.4. Sim Event Message (事件消息)

2 个事件消息的发送最小间隔为 100 毫秒,

所有的 Event Message，等待应答的超时事件为 1 秒。

6.4.1. DevStateChanged Event(0x80)

连接状态改变事件

智能中控定时查询通讯模组状态。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8	0x01	数据长度
3	Connection State	UINT16		设备状态定义： BIT[0]: GPRS 连接状态，0-未连接；1-连接。 BIT[1]: GPS 定位状态，0-未定位；1-已定位。 BIT[2]: 短信息状态，0-没有，1-有。 BIT[3-15]:保留。
4	CSQ	UINT8		GPRS 信号强度，0 到 31 之间(99 表示无信号)，数值越大表明信号质量越好
5	SNR	UINT8		GPS 信号强度，信噪比 (00 – 99) dbHz，典型值在 0 ~ 50 之间，SNR 虽可达到 99，但极罕见，50 已是非常好的情况
6	Satellites In View	UINT8		GPS 可见卫星数(0 – 16)

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.4.2. LocationChanged Event(0x81)

定位坐标值改变事件。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8	0x01	数据长度
2	longitude	Int32		经度，发送方乘(1E7)发送，接收方必须除(1E7) 0: 表示没有获取到定位。
6	latitude	Int32		纬度，发送方乘(1E7)发送，接收方必须除(1E7) 0: 表示没有获取到定位。

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x12	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.4.3. RcvSvrData Event(0xA0)

通讯模组收到服务器数据时，主动向智能中控发送该命令，智能中控收到该命令后，会回复操作结果和需要回复给服务器的数据，通讯模组需回复操作结果，并将回复给服务器的数据透传给服务器。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0xA0	命令码
1	Data Length	UINT8		数据长度
3	Data	UINT8[n]		透传数据内容，长度可变，最大为 128 字节

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0xA0	命令码
1	Data Length	UINT8		数据包长度
3	Result	UINT8		参见错误码的定义
4	Data	UINT8[n]		透传数据内容，长度可变，最大为 128 字节

6.4.4. RcvFile Event(0xA1)

接收文件事件，当模组接收到一个完整的文件之后，发送改事件通知 MCU。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0xA1	命令码
1	Data Length	UINT8	0x01	数据长度
2	File Type	UINT8		文件类型： 1：智能中控固件。 2：按键板固件。 其他值：保留。
3	Version Desc	VerDesc Struct		文件的版本描述符

Response 定义：

Index	Name	Type	Value	Descriptor
-------	------	------	-------	------------

0	Cmd	UINT8	0xA1	命令码
1	Data Length	UINT8		数据包长度
2	Result	UINT8		参见错误码的定义

6.5. Ble Event Message (事件消息)

6.5.1. Authentication Event(0x90)

连接身份验证，如果验证通过则允许连接，否则不允许连接。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x90	命令码
1	Data Length	UINT8		数据长度
3	Data	UINT8[n]		身份验证数据

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x90	命令码
1	Data Length	UINT8		数据包长度
3	Result	UINT8		参见错误码的定义

6.5.2. BleStateChanged Event(0x91)

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x91	命令码
1	Data Length	UINT8	0x01	数据长度
3	Connect State	UINT8		设备状态定义： BIT[0]: BLE 连接状态，0-未连接；1-连接。 BIT[1-7]:保留。
	MAC	UINT8[6]		连接 BLE 的终端的设备(手机)MAC。

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x91	命令码
1	Data Length	UINT8		数据包长度

2	Result	UINT8		参见错误码的定义

6.5.3. BeaconChanged Event(0x92)

待定

6.5.4. RcvBleData Event(0x93)

通讯终端收到蓝牙透传数据时，通讯模组需要发送该命令，将透传数据发送给智能中控，智能中控收到该命令时，需要回复操作结果和需要透传的数据。通讯模组需要回复操作结果，并将透传数据发送给蓝牙连接设备。

Request 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x93	命令码
1	Data Length	UINT8		数据长度
3	Data	UINT8[n]		透传数据内容，长度可变，最大为 128 字节

Response 定义：

Index	Name	Type	Value	Descriptor
0	Cmd	UINT8	0x93	命令码
1	Data Length	UINT8		数据包长度
3	Result	UINT8		参见错误码的定义
4	Data	UINT8[n]		透传数据内容，长度可变，最大为 128 字节