无线数据通信产品

EIC-ZC10　ZigBee无线数传

通信协议

北京东方讯科技发展有限公司

重要提示：

英文缩写对照表

APN	接入点名称 *Access Point Name*
APP	应用业务 *Application*
BG	边际网关 *Border Gateway*
BGP	边际网关协议 *Border Gateway Protocol*
BSC	基站控制器 *Base Station Controller*
BSS	基站系统 *Base Station System*
BSSGP	基站系统GPRS协议 *BSS GPRS Protocol*
BTS	基站收发系统*Base Transceiver System*
CDR	呼叫详细记录 *Call Detail Record*
CGF	计费网关功能 *Charging Gateway Function*
CSD	电路交换数据 *Circuit Switch Data*
DDN	数字数据网 *Digital Data Network*
DHCP	动态主机配置协议 *Dynamic Host Configuration Protocol*
DNS	域名系统 *Domain Name System*
DSC	数据业务中心 *Data Service Center*
DTU	数据终端单元 *Data Terminal Unit*
EGP	外部网关协议 *External/Exterior Gateway Protocol*
EIGRP	外部Internet组路由协议 *External/Exterior Internet Group Routing Protocol*
EMC	电磁兼容 *Electro Magnetic Compatibility*
ESP	静电防护 *Electro Static Precautions*
ETSI	欧洲电信标准协会 *European Telecommunications Standards Institute*
GGSN	GPRS支持节点网关 *Gateway GPRS Support Node*
GMSC	移动交换中心网关 *Gateway MSC*
GPRS	通用分组无线业务 *General Packet Radio Service*
GSM	全球移动通信系统 *Global System for Mobile Communications*
GSN	GPRS支持节点 *GPRS Support Node*
GTP	GPRS隧道协议 *GPRS Tunneling Protocol*
GTP-id	GTP标识 *GTP Identity*
HLR	注册地信息注册器 *Home Location Register*
HSCSD	高速电路交换数据 *High Speed Circuit Switch Data*

IGMP	互联网组管理协议 *Internet Group Management Protocol*
IGRP	互联网网关路由协议 *Internet Gateway Routing Protocol*
IN	智能网 *Intelligent Network*
IP	互联网协议 *Internet Protocol*
ISDN	综合数字业务网络 *Integrated Services Digital Network*
ISP	互联网业务提供商 *Internet Service Provider*
L2TP	第二层隧道协议 *Layer 2 Tunneling Protocol*
LA	位置区域 *Location Area*
LLC	逻辑链路控制 *Logical Link Control*
MAP	移动应用部分 *Mobile Application Part*
MDNS	移动域名系统 *Mobile Domain Name System*
MDTU	移动数据终端单元 *Mobile Data Terminal Unit*
MIB	管理信息库 *Management Information Base*
MS	移动台 *Mobile Station*
MSC	移动交换中心 *Mobile Switching Center*
MT	移动终端 *Mobile Terminal*
MTBF	平均故障时间 *Mean Time Between Failure*
MTTR	平均维护时间 *Mean Time To Recovery*
N/A	不可用 *Not Applicable*
NAS	网络接入服务器 *Network Access Server*
NAT	网络地址转换 *Network Address Translation*
NTP	网络时间协议 *Network Time Protocol*
O&M	运行和维护 *Operations & Maintenance*
PAP	密码授权协议 *Password Authentication Protocol*
PDP	分组数据协议 *Packet Data Protocol*
PDN	分组数据网络 *Packet Data Network*
PLMN	公众陆地移动网络 *Public Land Mobile Network*
POS	销售终端 *Point of Sales*
PTM-G	点对多点群呼 *Point-to-Multipoint Group Call*
PTM-M	点对多点多播 *Point-to-Multipoint Multicast*
QoS	服务质量 *Quality of Service*
RA	路由范围 *Routing Area*

RADIUS	远程授权拨入用户服务 *Remote Authentication Dial In User Service*
RIP	路由信息协议 *Routing Information Protocol*
RSC	注册业务中心 *Register Service Center*
RTOS	实时操作系统 *Real Time Operating System*
RTP	实时传输协议 *Real-time Transport Protocol*
RTU	远方终端单元 *Remote Terminal Unit*
RSVP	资源预留协议 *Resource reSerVation Protocol*
SCADA	监控与数据采集系统 *Supervisory Control and Data Acquisition*
SGSN	GPRS服务支持节点 *Serving GPRS Support Node*
SIM	用户标识模块 *Subscriber Identify Module*
SMS	短消息业务 *Short Message Service*
SMSC	短消息服务中心 *Short Message Service Center*
SNMP	简单网络管理协议 *Simple Network Management Protocol*
STK	SIM卡工具包 *SIM Tool Kits*
TCP	传输控制协议 *Transmission Control Protocol*
TDMA	时分多址 *Time Division Multiple Access*
TMN	电信管理网络 *Telecommunication Managed Network*
UDP	用户自带寻址信息协议 *User Datagram Protocol*
UIM	用户标识模块 *User Identify Module*
UMTS	通用移动电信系统 *Universal Mobile Telecommunication System*
USSD	非结构化补充业务数据 *Unstructured Supplementary Service Data*
UTK	UIM卡工具包 *UIM Tool Kits*
VLR	访问地注册器 *Visitor Location Register*
WAN	广域网 *Wide Area Network*
WAP	无线应用协议 *Wireless Application Protocol*
WDDN	无线DDN *Wireless Digital Data Network*

目 录

第一章　数据流向定义

这里要弄清楚几个定义：

ZigBee设备：也就是ZigBee无线数传EIC-ZC10

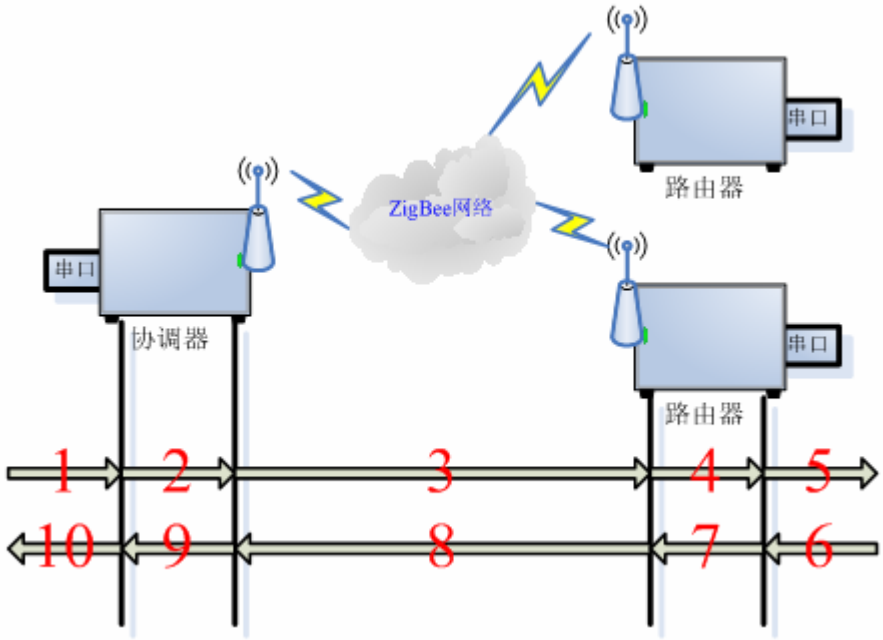
串口设备：　指的是与ZigBee设备相连的设备，例如终端采集器或者电脑等。

协调器：　　ZigBee网络的建立者，一个网络中有且只能有一个协调器。

路由器：　　ZigBee网络中的单元，具有路由功能。

节点：　　ZigBee网络中的单元，不具有路由功能。

下图是一个ZigBee网络的数据流向定义。



1：协调器通过串口收到上位机数据

2：协调器处理串口收到的上位机数据

3：协调器通过ZigBee网络将数据发送给路由器，或，路由器从ZigBee网络收到协调器发来的数据

4：路由器处理从ZigBee网络收到的数据

5：路由器通过串口将数据发送给下位机

6：路由器通过串口收到下位机数据

7：路由器处理串口收到的下位机数据

8：路由器通过ZigBee网络将数据发送给协调器，或，协调器从ZigBee网络收到路由器发来的数据

9：协调器处理从ZigBee网络收到的数据

10：协调器通过串口将数据发送给上位机

1.1 工作模式

从数据是否透明来看，可以分为透明传输和非透明传输。

从工作模式来看，可以分为协调器(Coordinator)、路由器(Router)、端节点(End Device)三种。

1.2 透明协议

透明协议，表示数据不经过任何处理，直接转发到另一节点。

对于协调器而言，透明协议仅用于下发节点是广播的情况。

对于路由器和端节点而言，透明协议下，数据只会在本节点和协调器之间透明传输。

注意：在透明协议下，进入参数设置状态的方法是在启动后的10秒内，发送连续的3个加号(+)，也即发送“+++”进入非透明协议状态，这时可以进行参数设置。

1.3 非透明协议

非透明协议指的是在非透明传输模式下的数据协议。包括串口通信协议和无线通信协议。串口通信协议指的是ZigBee设备和串口设备之间的数据通信协议。

1.3.1 数据包格式

串口通信的一个数据帧结构如下：

HEAD	TYPE	ADDR	LQI	LEN	DATA	TAIL
1字节	1字节	2字节	1字节	2字节	LEN	1字节

字段意义：

字段	字段释义	长度	意义
HEAD	Package Header	1	数据包头
TYPE	Package Type	1	数据类型
ADDR	Address	2	节点地址
LQI	Link Quality Indicator	1	链路质量
LEN	Data Length	2	数据长度
DATA	Valid Data	LEN	有效数据
TAIL	Package Tail	1	数据包尾

1.3.1.1 数据包头(HEAD)

长度：1字节。

定义：数据包的第一个字节。

描述：数据包头字节必须是0xAA。

1.3.1.2 数据类型(TYPE)

长度：1字节。
定义：数据包的类型。
描述：此字节的7,6位表示数据类型，5,4,3,2,1,0位保留

第7位	第6位	表示的数据类型
0	**0**	ZigBee向串口设备发送数据
0	**1**	串口设备向ZigBee发送数据
1	**0**	ZigBee向串口设备发送命令
1	**1**	串口设备向ZigBee发送命令

1.3.1.3 节点地址(ADDR)

长度：2字节。
定义：节点地址。注意：这个地址是用户自定义的地址，而不是短地址。
描述：ZigBee向串口设备发送数据或命令时，表示的是节点的源地址，也就是串口设备说从哪个节点收到；串口设备向ZigBee发送数据或命令时，表示的是节点的目的地址，也就是串口设备向哪个ZigBee节点发送。正常通信的地址范围是0x0000~0x0FFF。可容纳4096个节点。
注意：0x0000、0xFFFF是保留地址。0x0000为协调器专用地址，0xFFFF表示广播地址。

1.3.1.4 链路质量(LQI)

长度：1字节。
定义：收到的数据包的链路质量。
描述：链路质量仅在ZigBee向串口设备发送时为有效值，表示数据包所在节点的链路质量。如果是串口设备向ZigBee发送数据或命令，则此字节被忽略，可赋值为0。

1.3.1.5 数据长度(LEN)

长度：2字节。
定义：数据包中有效数据的长度。
描述：数据包中DATA部分的长度，以字节为单位。

1.3.1.6 有效数据(DATA)

长度：用户定义长度，由LEN字段来定义数据长度。
定义：有效的实际数据。
描述：通信中的实际数据，是真正有效的数据。

1.3.1.7 数据包尾(TAIL)

长度：1字节。
定义：数据包的最后一个字节。
描述：数据包尾字节必须是0xBB。

1.3.2 命令数据

当数据类型(TYPE)字段的第7位为1时，数据包为命令帧。有效数据(DATA)部分表示具体的命令。命令数据帧的数据结构如下：

HEAD	TYPE	ADDR	LQI	LEN	DATA	TAIL
1字节	1字节	2字节	1字节	2字节	LEN	1字节

ITYPE	IDATA
1字节	LEN-1

字段意义：

字段	字段释义	长度	意义
ITYPE	Item Type	1	命令项类型
IDATA	Item Data	LEN-1	命令项内容

其中命令项类型字节定义如下：

ITYPE	表示的数据类型
0x00	参数读取
0x01	参数设置
0x02	命令反馈
0x03~0xF0	待定
0xF1~0xFF	保留

1.3.2.1参数读取(0x00)

参数读取数据帧是一种特殊的命令数据帧，命令项类型为0x00。

从ZigBee设备获取参数的方法是向ZigBee设备发送参数读取数据帧，此时IDATA为0x00。此命令要求设备返回所有的设备参数。

ZigBee设备收到参数读取命令后，将返回设备的所有参数。设备各项参数定义如下：

参数项	位	描述

基本信息	8	Bit0：通讯模式，0-透明，1-非透明 Bit2~1：节点类型，00-协调器，01-路由器，10-节点，11-保留 Bit3：休眠功能，0-禁用，1-启用 Bit7~4：串口波特率，0000-300，0001-600，0010-1200，0011-2400，0100-4800，0101-9600，0110-19200，0111-38400，1000-57600，1001-76800，1010-115200
串口参数	8	Bit1~0：数据位，00-5位，01-6位，10-7位，11-8位 Bit3~2：校验位，00-无，01-奇，10-偶数，11-保留 Bit4：停止位，1-1位，0-2位 Bit5：流控功能，0-禁用，1-启用 Bit7~6：保留
本地EP号	8	本地End Point序号
目标EP号	8	目的End Point序号
通讯通道	32	通讯通道(Channel)
PAN ID	16	PAN ID
Cluster ID	8	Cluster ID
Reserve	8	保留字节
Profile ID	16	Profile ID
Device ID	16	Device ID
本地地址	16	本地地址
目标地址	16	目标地址
缓冲区大小	16	透明模式下串口接收打包最大长度
超时时间	16	透明模式下串口接收打包最长超时时间

1.3.2.2参数设置(0x01)

参数设置数据帧是一种特殊的命令数据帧，命令项类型为0x01。

向ZigBee设备发送参数设置数据帧，各项参数定义与4.1.2.1中表格中定义相同。

收到参数设置命令后，ZigBee设备会返回一个命令反馈，参考4.1.2.3中的描述。

1.3.2.3命令反馈(0x02)

命令反馈帧用于反馈命令信息，例如参数设置完毕，参数设置错误，帧格式错误，等等。

参数项	位	描述
反馈信息	8	0x00：参数设置成功。 0x01：命令格式不正确。 0xFF：无此命令。

1.3.3 举例

```
->向串口发送"123"的数据
->AA 40 00 00 00 00 03 31 32 33 BB
 |--|--|-----|--|-----|--------|--|
 |头|类|地址 |LQ|长度 |  数据  |尾|

->向串口发送参数获取命令
->AA C0 00 00 00 00 01 00 BB
 |--|--|-----|--|-----|--|--|
 |头|类|地址 |LQ|长度 |数|尾|

<-设备返回参数命令
<-AA 80 00 00 00 00 19 00 51 03 01 02 00 00 00 11 00 00 00 00 01 28 00 00 00 00 00 01 01 00 00 64 BB
  AA 80 00 00 00 00 19 00 51 03 01 02 00 00 00 15 1A AD 30 00 01 28 00 00 00 00 00 08 01 00 00 64 BB
 |--|--|-----|--|-----|-------------------------------------------------------------------------|--|
 |头|类|地址 |LQ|长度 |                                  数据                                   |尾|

->向设备发送参数设置命令
->AA C0 00 00 00 00 19 01 51 03 01 02 00 00 00 11 00 00 00 00 01 28 00 00 00 00 00 01 01 00 00 64 BB
  AA C0 00 00 00 00 19 01 51 03 01 02 00 00 00 13 1B BB 00 00 01 29 00 00 00 00 00 01 01 09 00 66 BB
 |--|--|-----|--|-----|-------------------------------------------------------------------------|--|
 |头|类|地址 |LQ|长度 |                                  数据                                   |尾|

->向串口发送设备重启命令
->AA C0 00 00 00 00 02 03 00 BB
 |--|--|-----|--|-----|-----|--|
 |头|类|地址 |LQ|长度 |数据 |尾|

->向串口发送恢复出厂设置命令
->AA C0 00 00 00 00 02 04 00 BB
 |--|--|-----|--|-----|-----|--|
 |头|类|地址 |LQ|长度 |数据 |尾|

<-设备返回参数设置状态
<-AA 80 00 00 00 00 02 02 00 BB   //参数设置成功
<-AA 80 00 00 00 00 02 02 01 BB   //命令已执行
<-AA 80 00 00 00 00 02 02 FE BB   //格式错误
<-AA 80 00 00 00 00 02 02 FF BB   //无此命令
 |--|--|-----|--|-----|-----|--|
 |头|类|地址 |LQ|长度 |数据 |尾|
```