中国科学院沈阳自动化研究所
SHENYANG INSTITUTE OF AUTOMATION, CAS

引领无线技术　实现无限工厂

WIAPA-GW1498 无线网关串口接口命令

用户指南

中国科学院沈阳自动化研究所

商标

中国科学院沈阳自动化研究所、SIA、WIA 和 WIA-PA 标志为中国科学院沈阳自动化研究所的注册商标，产权为中国科学院沈阳自动化研究所所有，不得非法使用。

版权所有

声明

本文档是“原样”提供，不附带任何形式的保证、明示及暗示，但包括不限于适销性或针对特定用途适用性的保证。

此文件可能包含技术错误或其他错误。更正和改进可能会被纳入新版本的文件。

对于没有按照本文档正常操作使用产品而造成的一切伤害与损失，中国科学院沈阳自动化研究所不承担任何责任和义务。

中国科学院沈阳自动化研究所保留在任何时间对产品及服务作出更正、修改、改进和改善，或者停止任何产品及服务的权利，恕不另行通知。客户应获取最新的有关信息，然后下订单，并应确认这些资料是最新的且是完整的。

文件编号： WIAPA-GW1498 无线网关串口接口命令用户指南

最近一次修订： 2009 年 7 月 1 日

目 录

第一章 概述

本章简要介绍WIA-PA（Wireless Networks for Industrial Automation – Process Automation）网络及WIA-PA网络串口接口命令。

1.1 WIA-PA 网络

WIA-PA 网络是一种高可靠，超低功耗的无线分层网络，第一层是 Mesh 结构，由网关设备及路由设备构成；第二层是星型结构，由路由设备及终端设备或手持设备构成。WIA-PA 网络不仅适用于家庭自动化、环境检测、医疗护理等低速率、低成本、近距离、数据量较少的无线传感器网络采集和监控系统，而且特别适用于工业过程自动化领域。比如石油、石化、污水处理、安全监控、资产管理、能量管理及冶金等等。

WIA-PA网络主要包括四类设备：

- 终端设备：终端设备装有传感器或执行器，安装在工业现场，直接与生产流程连接。
- 路由设备：路由设备完成WIA-PA网络中的无线报文中转。
- 网关设备：网关设备连接上位机和WIA-PA网络，它同时提供WIA-PA网络与工厂内其它网络的接口。
- 上位机：上位机是用户、网络管理及维护人员与WIA-PA网络交互的平台，用户可以通过上位机网络管理软件对WIA-PA网络进行配置及与终端设备进行数据信息交互。

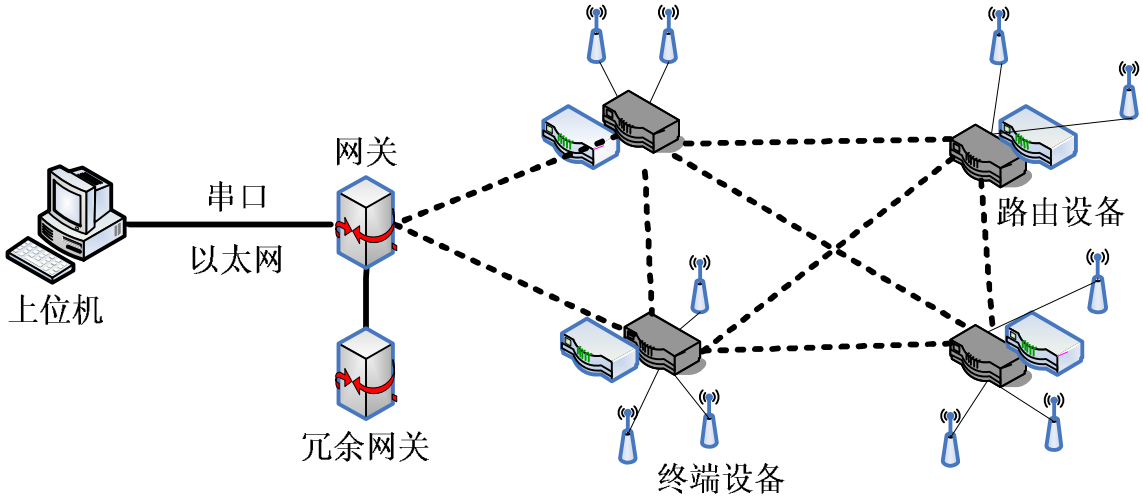

图1 WIA-PA网络结构

1.2 串口接口命令

WIA-PA网络串口接口命令提供了一个应用于管理与配置WIA-PA网络及通过串口发送与接收终端设备的数据信息的软件接口，通过使用串口接口命令，用户可以获取WIA-PA网络的信息。

串口接口命令提供两种串口通信方式：

- **命令**—包括请求与响应两种命令方式，命令一般用于用户通过上位机向网络发送数据信息以及配置与管理整个网络。
- **上报**—主要是网络向用户上位机发送的网络事件与诊断数据信息。

第二章 串口接口命令

2.1 串口接口命令

WIAPA-GW1498无线网关串口接口命令为用户应用提供了一个明确的串口接口。这个串口接口提供一个由数据收发管脚（TX，RX）组成的端口。通过这个端口，用户能够通过WIA-PA网络进行收发数据，以及配置网络等操作。

2.1.1 串口参数

表1 串口参数

波特率	57600
起始位	1
数据位	8
奇偶校验位	1
停止位	1

2.1.2 数据类型

表2 数据类型

数据类型	长度
unsigned long	4 bytes
unsigned short	2 bytes
unsigned char	1 byte

2.1.3 HDLC 包格式

WIAPA-GW1498无线网关串口协议按照HDLC包格式成帧，具体描述见RFC 1662。对应一个命令只成一帧，HDLC包格式如下图2所示：

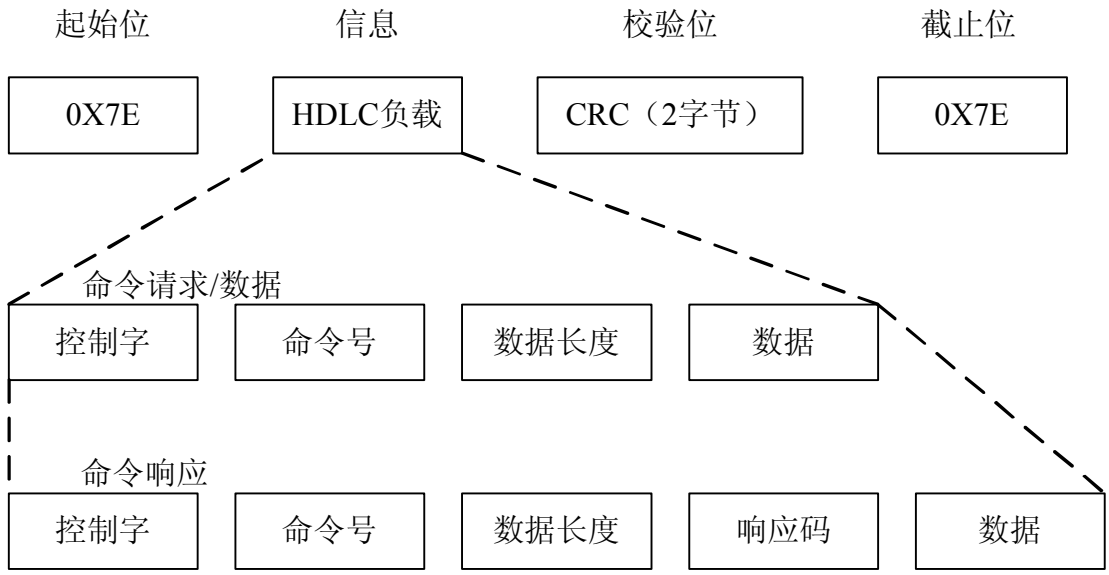

图2 HDLC包格式示意图

2.1.4 命令

命令包括可靠的请求消息及响应消息，具体可以分为发送和接收数据、事件及报警命令，网络与系统状态命令及管理命令。

2.1.4.1 命令 0x10 向设备写数据

此命令用来用户通过上位机将一段数据写到无线网关，无线网关把数据透明传输到指定的设备，其中设备使用 MAC 地址唯一标志。

表3 向设备写数据请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x10
3	数据长度	unsigned char	
4-11	MAC 地址	unsigned char[8]	
12-n	数据负载	unsigned char[]	

表4 向设备写数据响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x10
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数 0x03=无效设备

2.1.4.2 **命令** 0x11 **修改** Join Key

此命令用来用户通过上位机使网络产生新的 Join Key，并广播给所有网络设备。

表5 修改Join Key请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x11
3	数据长度	unsigned char	
4-19	Join Key	unsigned char[16]	

表6 修改Join Key响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x11
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数

2.1.4.3 命令 0x12 修改 Network ID

此命令用来用户通过上位机使网络产生新的 Network ID，并广播给所有网络设备。

表7 修改Network ID请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x12
3	数据长度	unsigned char	
4-5	Network ID	unsigned short	

表8 修改Network ID响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x12
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数

2.1.4.4 命令 0x13 读网络信息

此命令用来用户通过上位机读取整个网络的基本信息，包括 Network ID，网络设备最大容量，网络设备个数及网络超帧长度。

表9 读网络信息请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x13
3	数据长度	unsigned char	

表10 读网络信息响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x13
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数
5-6	Network ID	unsigned short	
7-8	超帧长度	unsigned short	
9-12	网络最大容量	unsigned long	
13-16	在网设备个数	unsigned long	

2.1.4.5 命令 0x14 读设备信息

此命令用来用户通过上位机读取网络设备的基本信息，其中设备使用 MAC 地址唯一标志，设备基本信息包括设备短地址、设备状态、设备采样周期、传感器类型及设备电池电压。

表11 读设备信息请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x14
3	数据长度	unsigned char	
4-11	MAC 地址	unsigned char[8]	

表12 读设备信息响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x14
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数 0x03=无效设备
5-6	网络地址	unsigned short	
7-14	MAC 地址	unsigned char[8]	
15	状态	unsigned char	0x00=激活状态 0x01=加入状态 0x02=在网状态 0x03=离开状态
16-17	采样周期（秒）	unsigned short	
18	传感器类型	unsigned char	
19-22	电池电压（伏）	unsigned long	

2.1.4.6 命令 0x15 读下一设备信息

此命令用来用户利用设备短地址通过上位机读取网络设备基本信息，网络设备基本信息包括设备短地址、设备状态、设备采样周期、传感器类型及设备电池电压。

表13 读下一设备信息请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x15
3	数据长度	unsigned char	
4-5	短地址	unsigned short	

表14 读下一设备信息响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x15
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数 0x03=无效设备
5-6	网络地址	unsigned short	
7-14	MAC 地址	unsigned char[8]	
15	状态	unsigned char	0x00=激活状态 0x01=加入状态 0x02=在网状态 0x03=离开状态
16-17	采样周期（秒）	unsigned short	
18	传感器类型	unsigned char	
19-22	电池电压（伏）	unsigned long	

2.1.4.7 命令 0x16 删除设备

此命令用来用户通过上位机删除网络中的某一设备，设备使用 MAC 地址唯一标志。

表15 删除设备请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x16
3	数据长度	unsigned char	
4-11	MAC 地址	unsigned char[8]	

表16 删除设备响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x16
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数 0x03=无效设备
5-12	MAC 地址	unsigned char[8]	

2.1.4.8 命令 0x17 复位设备

此命令用来用户通过上位机复位网络某设备，通过复位设备，可以改变设备状态，重新使设备加入网络，设备使用 MAC 地址唯一标志。

表17 复位设备请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x17
3	数据长度	unsigned char	
4-11	MAC 地址	unsigned char[8]	

表18 复位设备响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x17
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数 0x03=无效设备
5-12	MAC 地址	unsigned char[8]	

2.1.4.9 命令 0x18 过滤网络信息

此命令用来过滤网络信息，对网络信息（数据、报警及事件信息）进行筛选与屏蔽。

表19 过滤网络信息请求报文

报文字节	描述	类型	值
1	控制	unsigned char	0x01
2	命令号	unsigned char	0x18
3	数据长度	unsigned char	
4	信息类型	unsigned char	数据信息 = 0x01 报警信息 = 0x02 事件信息 = 0x03

表20 过滤网络信息响应报文

报文字节	描述	类型	值
1	控制	unsigned char	0x02
2	命令号	unsigned char	0x18
3	数据长度	unsigned char	
4	响应码	unsigned char	0x00=OK 0x01=无效命令 0x02=无效参数
5	信息类型	unsigned char	数据信息 = 0x01 报警信息 = 0x02 事件信息 = 0x03

2.1.5 上报

上报主要包括系统网络向用户上报事件及报警信息。

2.1.5.1 上报 0x19 设备离线报警

此上报是当网络设备不能与网络进行通信，网络上报给用户的报警信息。

表21 设备离线报警报文

报文字节	描述	类型	值
1	控制	unsigned char	0x03
2	命令号	unsigned char	0x19
3	数据长度	unsigned char	
4	报警号	unsigned short	
5	报警类型	unsigned char	0x00
6-13	MAC 地址	unsigned char[8]	

2.1.5.2 上报 0x1A 设备低电压报警

此上报是当网络设备的电池电压低于工作电压而不能正常工作时，网络上报给用户的报警信息。

表22 设备低电压报警报文

报文字节	描述	类型	值
1	控制	unsigned char	0x03
2	命令号	unsigned char	0x1A
3	数据长度	unsigned char	
4	报警号	unsigned short	
5	报警类型	unsigned char	0x01
6-13	MAC 地址	unsigned char[8]	

2.1.5.3 上报 0x1B 设备低可靠性报警

此上报是当设备的通信可靠性低于某一设定的可靠性标准（比如 99%）时，网络上报给用户的报警信息。

表23 设备低可靠性报警报文

报文字节	描述	类型	值
1	控制	unsigned char	0x03
2	命令号	unsigned char	0x1B
3	数据长度	unsigned char	
4	报警号	unsigned short	
5	报警类型	unsigned char	0x02
6-13	MAC 地址	unsigned char[8]	

2.1.5.4 上报 0x1C 系统网络复位事件

此上报是当系统网络重被复位，网络上报给用户的事件信息。

表24 系统网络复位事件报文

报文字节	描述	类型	值
1	控制	unsigned char	0x03
2	命令号	unsigned char	0x1C
3	数据长度	unsigned char	
4	事件号	unsigned short	
5	事件类型	unsigned char	0x00
6-13	MAC 地址	unsigned char[8]	

2.1.5.5 上报 0x1D 设备加入网络事件

此上报是当新设备加入网络时，网络上报给用户的事件信息。

表25 设备加入网络事件报文

报文字节	描述	类型	值
1	控制	unsigned char	0x03
2	命令号	unsigned char	0x1D
3	数据长度	unsigned char	
4	事件号	unsigned short	
5	事件类型	unsigned char	0x01
6-13	MAC 地址	unsigned char[8]	

2.1.6 HDLC 包处理示例

示例一：从上位机构建一个 HDLC 包通过串口发送给设备，本例是用户通过上位机如何构建一个 HDLC 包移除网络中的某一设备，设备的 MAC 地址为为 00 00 00 00 00 00 00 7D。（所有的数值为 16 进制表示）

步骤 1 定义 HDLC 包负载

命令号 => 14

控制字 => 01

MAC 地址 => 00 00 00 00 00 00 00 7D

HDLC 包负载		
控制字	**命令号**	**内容**
01	14	00 00 00 00 00 00 00 7D

步骤 2 计算 CRC

使用 CRC-16-IBM 算法多项式 $X^{16}+X^{15}+X^2+1$ 得到十六进制数据序列“01 14 00 00 00 00 00 00 00 7D”的 CRC 为 A4 27，然后附在 HDLC 包负载后面，但是根据 RFC1662，CRC 发送时低字节在前。

HDLC 包负载	**CRC**
01 14 00 00 00 00 00 00 00 7D	27 A4

步骤 3 字节变换

按照下面字节变换规则对 HDLC 包负载中的“7D”或“7E”进行变换。

7D => 7D 5D

7E => 7D 5E

变换后的 HDLC 包负载与 CRC 如下所示。

HDLC 包负载	**CRC**
01 14 00 00 00 00 00 00 00 7D 5D	27 A4

步骤 4 添加起始位与起始截止位

起始位	**HDLC 包负载**	**CRC**	**截止位**
7E	01 14 00 00 00 00 00 00 00 7D 5D	27 A4	7E

最终的发送报文序列位：7E 01 14 00 00 00 00 00 00 00 7D 5D 27 A4 7E

示例二：如何解析一个从设备发过来的 HDLC 包，本例是用户通过上位机如何解析一个

读设备信息命令的响应 HDLC 包。（所有的数值为 16 进制表示）

起始位	HDLC 包负载	CRC	截止位
7E	02 12 00 00 0D 00 00 00 00 00 00 00 7D 5D 03 00 28 01 00 00 03 21	4F 16	7E

步骤 1 去掉起始位与起始截止位

HDLC 包负载	CRC
02 12 00 00 0D 00 00 00 00 00 00 00 7D 5D 03 00 28 01 00 00 03 21	4F 16

步骤 2 字节变换

按照下面字节变换规则对 HDLC 包负载中的“7D”或“7E”进行变换。

7D 5D => 7D

7D 5E => 7E

变换后的 HDLC 包负载与 CRC 如下所示。

HDLC 包负载	CRC
02 12 00 00 0D 00 00 00 00 00 00 00 7D 03 00 28 01 00 00 03 21	4F 16

步骤 3 验证 CRC

使用 CRC-16-IBM 算法多项式 $X^{16}+X^{15}+X^2+1$ 对 HDLC 包中的 CRC 进行校验，在这个例子中，校验成功。

HDLC 包负载
02 12 00 00 0D 00 00 00 00 00 00 00 7D 03 00 28 01 00 00 03 21

步骤 4 分解 HDLC 包负载

最终的 HDLC 包负载如下所示：

HDLC 包负载
02 12 00 0D 00 00 00 00 00 00 00 00 7D 03 00 28 01 00 00 03 21

控制字	命令号	响应码	消息内容
02	12	00	00 0D 00 00 00 00 00 00 00 00 7D 03 00 28 01 00 00 03 21

对于命令号 0x12，结合响应报文结构与消息内容，解析如下：

数据长度	网络地址	MAC 地址	状态	采样周期	传感器类型	电池电压
0D	00 0D	00 00 00 00 00 00 00 00 7D	03	00 28	01	00 00 03 21

从上可以看出，这是一个成功的设备信息响应报文，设备信息具体内容如下：

网络地址 = 13

Network ID = 00 00 00 00 00 00 00 00 7D

状态 = 在网状态

采样周期 = 40 秒

传感器类型 = 压力传感器

电池电压 = 3.520 伏