



基于以太网的 TCP/IP 通讯 用户手册

无锡信捷电气股份有限公司

资料编号: PD07 20220324 1.0

	目录	
基于以太网的 TCP/IP 通讯 用户手册	以太网通讯概述	1
	以太网参数的配置	2
	接线方式及通讯协议	3
	以太网通讯指令	4
	手册更新日志	

基本说明

- ◆ 感谢您购买了信捷以太网型可编程序控制器。
- ◆ 本手册主要介绍以太网型可编程序控制器的以太网通讯功能。
- ◆ 在使用产品之前，请仔细阅读本手册，并在充分理解手册内容的前提下，进行接线。
- ◆ 软件及编程方面的介绍，请查阅相关手册。
- ◆ 请将本手册交付给最终用户。

用户须知

- ◆ 只有具备一定的电气知识的操作人员才可以对产品进行接线等其他操作，如有使用不明的地方，请咨询本公司的技术部门。
- ◆ 手册等其他技术资料中所列举的示例仅供用户理解、参考用，不保证一定动作。
- ◆ 将该产品与其他产品组合使用的时候，请确认是否符合有关规格、原则等。
- ◆ 使用该产品时，请自行确认是否符合要求以及安全，对于本产品故障而可能引发机器故障或损失时，请自行设置后备及安全功能。

责任申明

- ◆ 手册中的内容虽然已经过仔细的核对，但差错难免，我们不能保证完全一致。
- ◆ 我们会经常检查手册中的内容，并在后续版本中进行更正，欢迎提出宝贵意见。
- ◆ 手册中所介绍的内容，如有变动，请谅解不另行通知。

联系方式

如果您有关于本产品的使用问题，请与购买产品的代理商、办事处联系，也可以直接与信捷公司联系。

- ◆ 总部地址：江苏省无锡市滨湖区建筑西路 816 号
- ◆ 服务热线：400-885-0136
- ◆ 总机：0510-85134136
- ◆ 传真：0510-85111290
- ◆ 网址：www.xinje.com
- ◆ 邮箱：xinje@xinje.com

WUXI XINJE ELECTRIC CO., LTD. 版权所有

未经明确的书面许可，不得复制、传翻或使用本资料及其中的内容，违者要对造成的损失承担责任。保留包括实用模块或设计的专利许可及注册中提供的所有权力。

二〇一八年 八月

目 录

1. 以太网通讯概述	1
1-1. 以太网的基本概念	2
1-1-1. 分配 IP 地址	2
1-1-2. 设定 PC 网络地址信息	2
1-1-3. PING 命令	3
1-2. TCP/IP 协议	7
1-2-1. 端口号	7
1-2-2. UDP 协议	7
1-2-3. TCP 协议	7
2. 以太网参数的配置	9
2-1. 以太网参数介绍	10
2-1-1. IP 地址相关参数	10
2-1-2. 功能规格	10
2-2. 以太网参数在编程软件中的配置	11
2-3. 以太网参数在 XINJEConfig 中的配置	12
3. 接线方式及通讯协议	14
3-1. 接线方式	15
3-2. MODBUS TCP 通讯协议	15
3-2-1. MODBUS TCP 通讯概述	15
3-2-2. MODBUS 通讯地址	15
3-2-3. MODBUS 通讯功能码	15
3-3. 自由格式通讯协议	16
4. 以太网通讯指令	17
4-1. 以太网通讯指令概述	18
4-1-1. 创建 TCP 连接/UDP 端口监听[S_OPEN]	18
4-1-2. 通讯终止[S_CLOSE]	21
4-1-3. 自由格式通讯-发送[S_SEND]	22
4-1-4. 自由格式通讯-接收[S_RCV]	23
4-1-5. MODBUS 通讯[M_TCP]	24
4-1-6. 以太网通讯案例	25
4-2. 通讯口参数的读写指令	40
4-2-1. 串口参数的读取[CFGCR]	40
4-2-2. 串口参数的写入[CFGCW]	41
4-2-3. IP 地址设置指令[IPSET]	42
4-2-4. 串口参数的名称及设定	44
4-2-5. 通讯口参数通讯案例	45
4-3. 以太网通讯相关标志位和寄存器	46
4-4. 以太网通讯错误一览表	47
手册更新日志	48

1. 以太网通讯概述

本章主要介绍以太网的几个基本概念以及 TCP IP 协议。

1. 以太网通讯概述	1
1-1. 以太网的基本概念	2
1-1-1. 分配 IP 地址	2
1-1-2. 设定 PC 网络地址信息	2
1-1-3. PING 命令	3
1-2. TCP IP 协议	7
1-2-1. 端口号	7
1-2-2. UDP 协议	7
1-2-3. TCP 协议	7

1-1. 以太网的基本概念

在进行以太网通讯之前，需要先了解以太网通讯的几个基本概念，如 IP 地址分配、PC 网络地址及设定等。

1-1-1. 分配 IP 地址

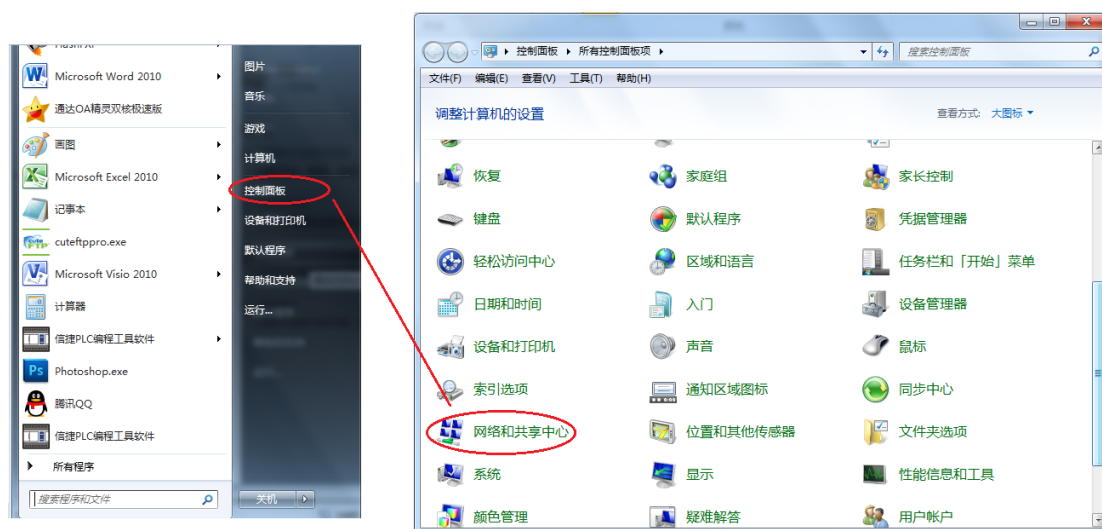
如果编程设备（如 PC）使用网卡连接到工厂局域网（或者是互联网），则编程设备和 PLC 必须处于同一子网中。IP 地址与子网掩码相结合即可指定设备的子网。

网络 ID 是 IP 地址的第一部分，即前三个八位位组（例如 IP 地址为 211.154.184.16，则 211.154.184 代表网络 ID），它决定用户所在的 IP 网络。子网掩码的值通常为 255.255.255.0；然而由于您的计算机处于工厂局域网中，子网掩码可能有不同的值（例如，255.255.254.0）以设置唯一的子网。子网掩码通过与设备 IP 地址进行逻辑 AND 运算来定义 IP 子网的边界。

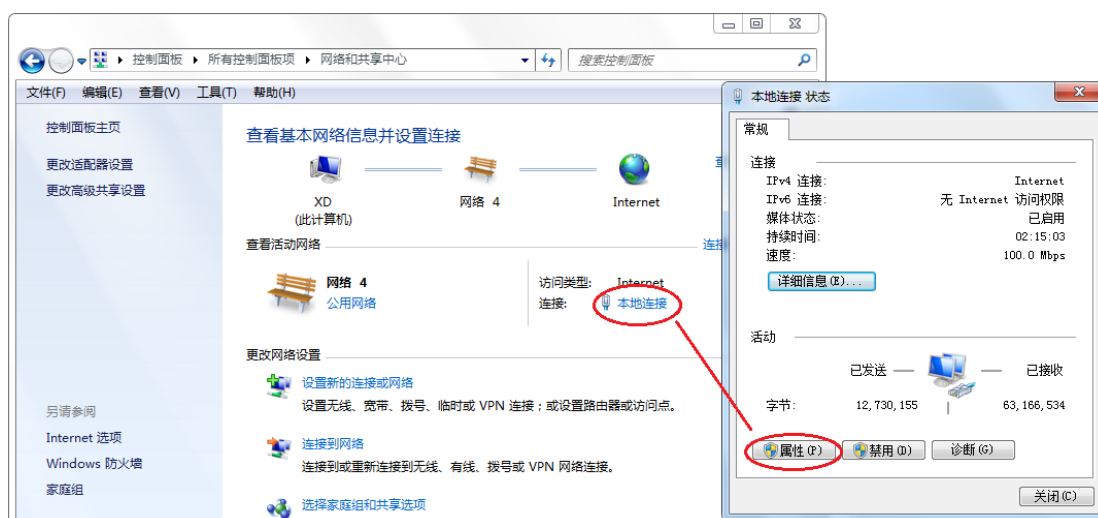
1-1-2. 设定 PC 网络地址信息

如果您使用的是 WIN7 操作系统，您可以通过以下步骤来分配或检查编程设备的 IP 地址：

1、打开“控制面板”-“网络和共享中心”：



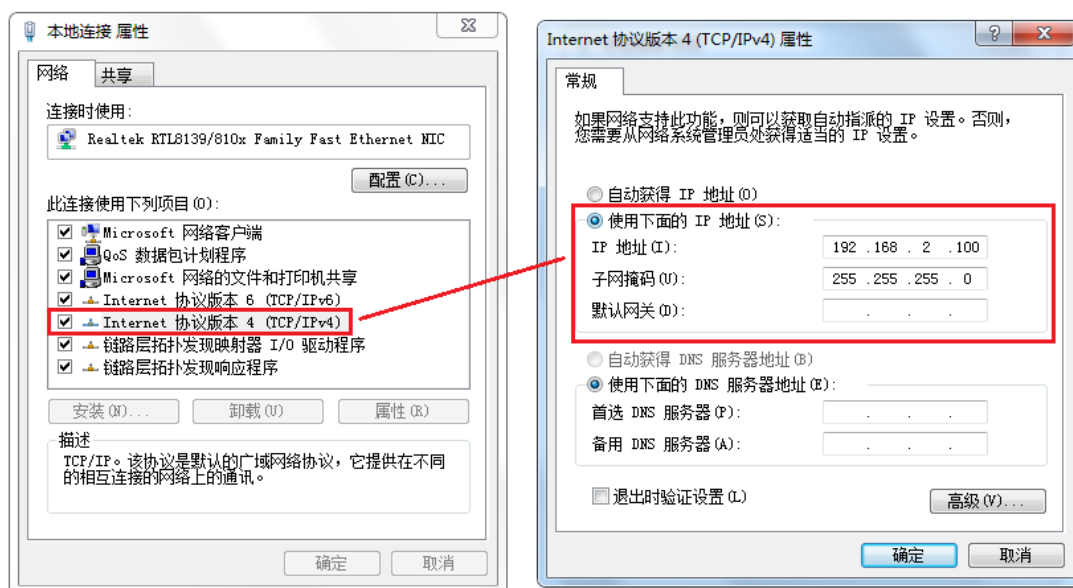
2、点击“本地连接”，查看属性：



3、设定 PC 的 IP 地址，使其与 PLC 处于同一子网下。

假设 PLC 的 IP 地址为 192.168.2.1，则需将 PC 的 IP 地址设为具有相同网络 ID 的地址（如：

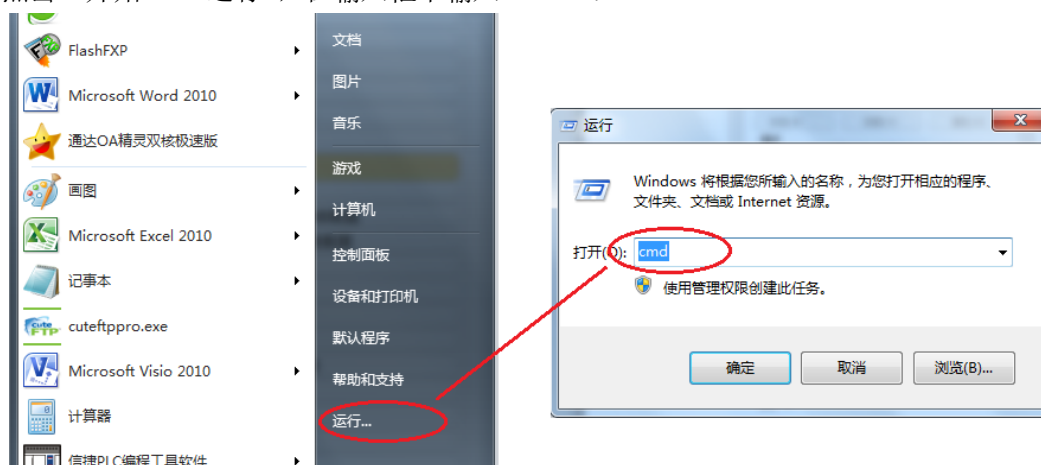
192.168.2.200), 设定子网掩码为 255.255.255.0。默认网关可留空。这样, 可使 PC 连接到 CPU。如下图所示:



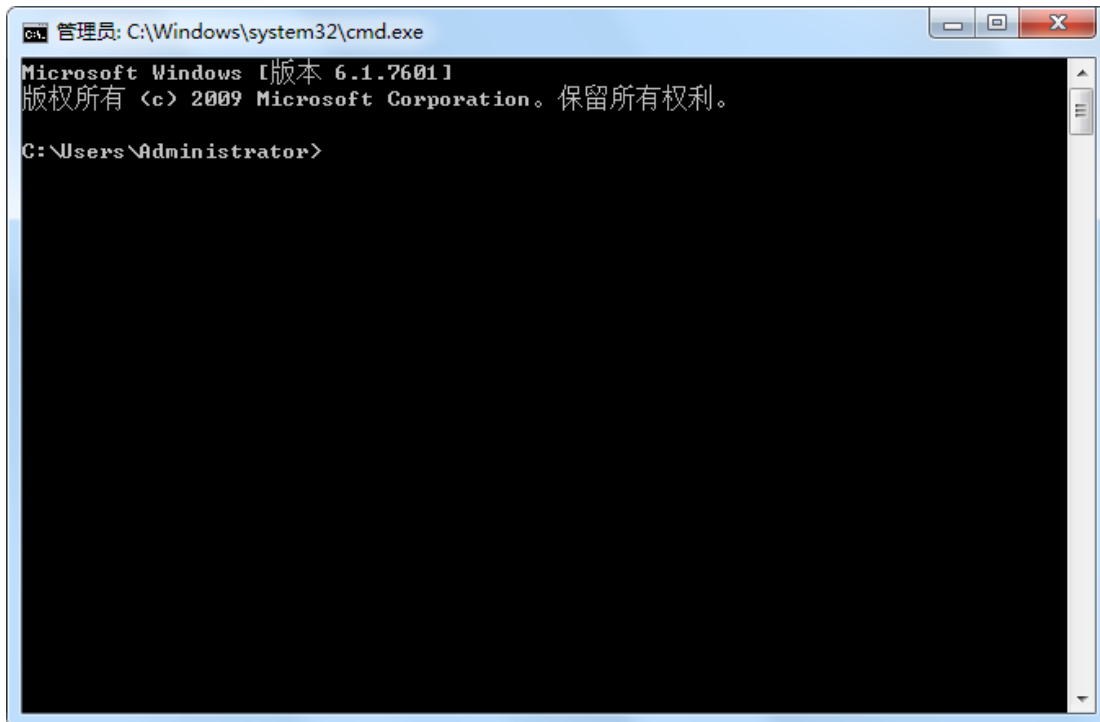
1-1-3. PING 命令

通过 PING 命令, 可以检查本地 TCP/IP 协议是否正常, 以及是否可正常连接局域网中的其他电脑。如果您的电脑是 Win7 操作系统, 可按如下步骤操作:

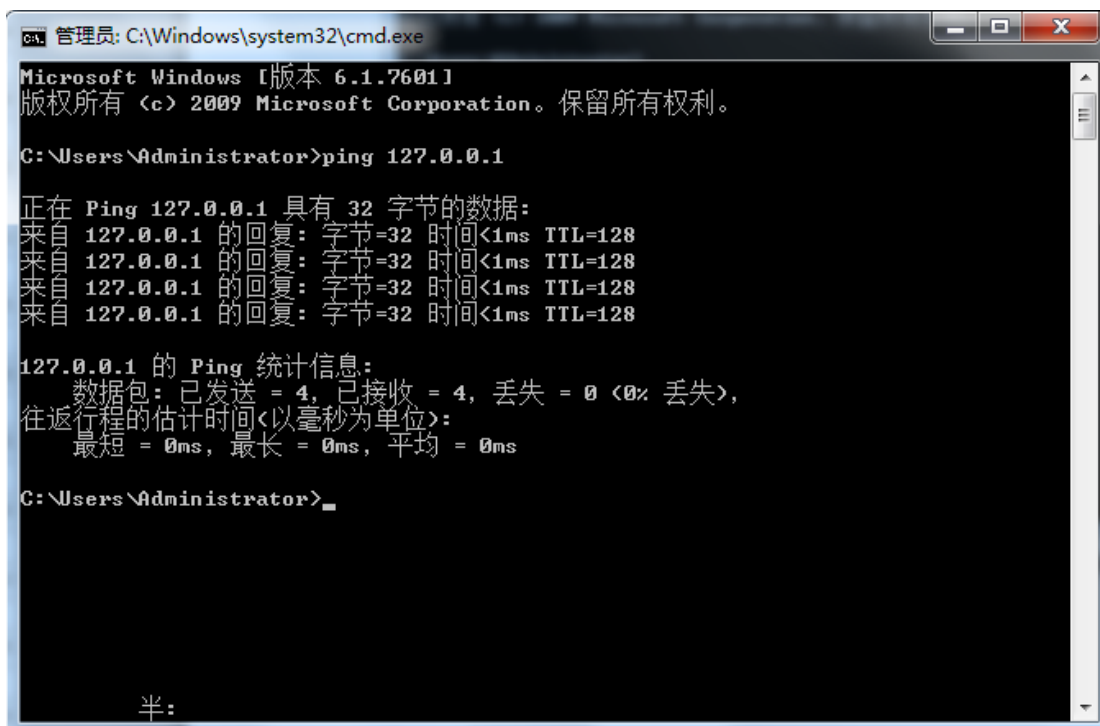
- 1、点击“开始”-“运行”, 在输入框中输入“cmd”:



2、点击确定，弹出命令窗口：

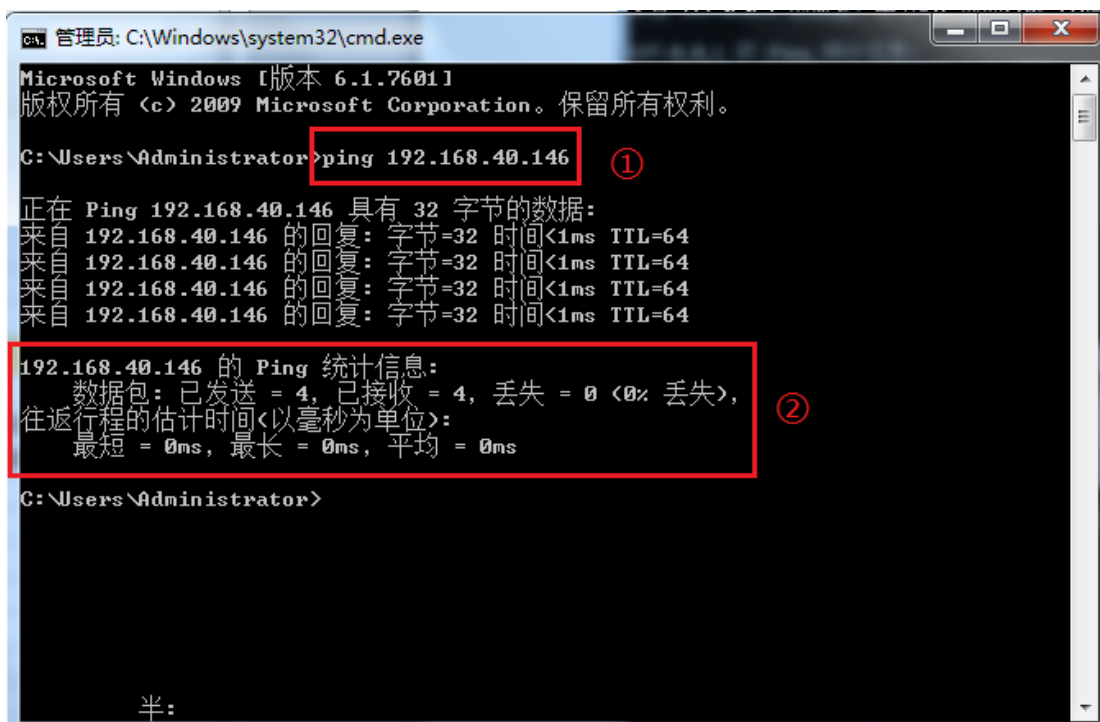


3、输入“ping 127.0.0.1”命令来检查本地的 TCP/IP 协议是否是正常的，发送与接收的数据相同就是正常的，如下图所示：



4、输入“ping 网络设备 ip”命令，检查本机是否能连接局域网其它电脑：

(1) ①处输入“ping 192.168.40.146”命令，按回车后②处为 ping 的结果，“0%丢失”表示可正常连接 IP 地址为 192.168.40.146 的电脑；



```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

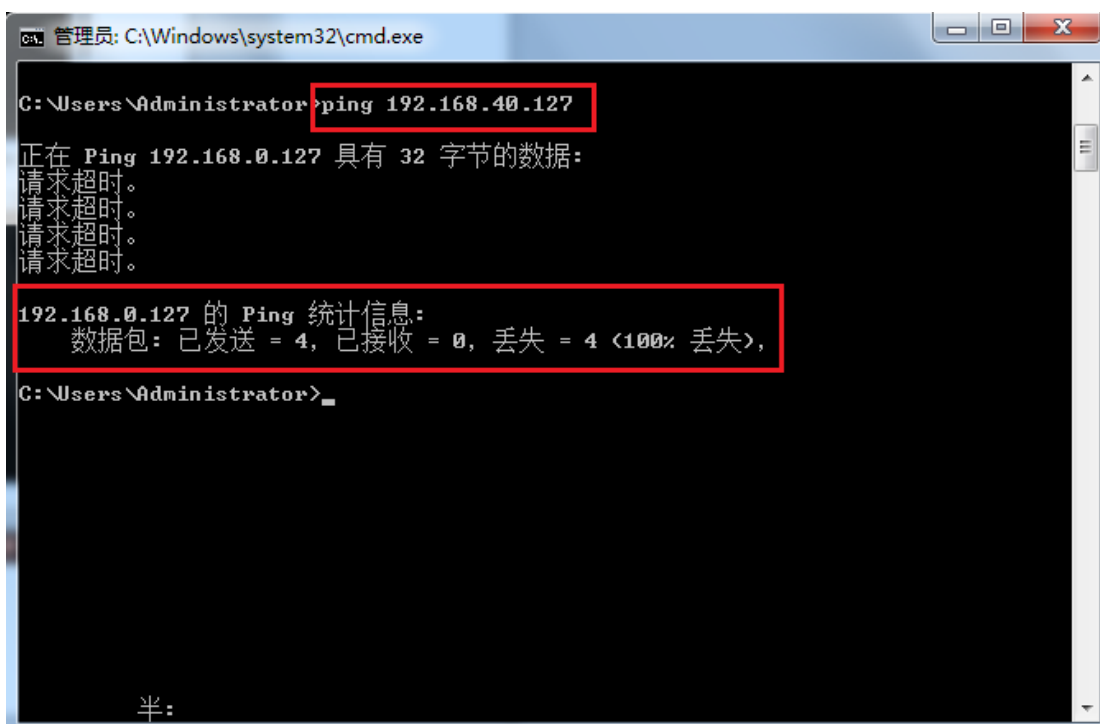
C:\Users\Administrator>ping 192.168.40.146 ①

正在 Ping 192.168.40.146 具有 32 字节的数据:
来自 192.168.40.146 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.40.146 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.40.146 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.40.146 的回复: 字节=32 时间<1ms TTL=64

192.168.40.146 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms ②

C:\Users\Administrator>
```

(2) ①处输入“ping 192.168.40.127”命令，按回车后②处为 ping 的结果，“100%丢失”表示不能正常连接 IP 地址为 192.168.40.127 的电脑；



```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 192.168.40.127

正在 Ping 192.168.0.127 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.0.127 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Administrator>
```

注意：

(1) 统计信息里，只有显示数据包“0%丢失”才表示通讯连接正常。

(2) “ping 网络设备 ip”命令仅可以 ping 四次，若想一直 ping，可以使用“ping 网络设备 ip -t”命令，如下图所示：

A screenshot of a Windows command prompt window. The title bar shows the path "C:\Windows\system32\cmd.exe - ping 127.0.0.1 -t". The main area displays the output of the command "ping 127.0.0.1 -t". It starts with "Microsoft Windows [版本 10.0.17763.2061]" and "(c) 2018 Microsoft Corporation。保留所有权利。". Below that is the command input "C:\Users\qusiya>ping 127.0.0.1 -t". The response begins with "正在 Ping 127.0.0.1 具有 32 字节的数据:" followed by multiple lines of successful replies: "来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128". Each line also has a small green square icon at the end. The list continues down to "来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=128". At the bottom right corner of the terminal window, there are three icons: a red X, a yellow triangle, and a blue circle.

1-2. TCP/IP 协议

TCP/IP 协议是现在比较通用的以太网通信协议,与开放互联模型 ISO 相比,采用了更加开放的方式,它已经被美国国防部认可,并被广泛应用于实际工程。TCP/IP 协议可以用在各种各样的信道和底层协议(如 T1、X.25 以及 RS232 串行接口)之上。确切地说,TCP/IP 协议是包括 TCP 协议、IP 协议、UDP 协议、ICMP 协议和其他一些协议的协议组。

1-2-1. 端口号

在以太网中,基于 TCP 协议或 UDP 协议的通信必须使用端口号才能与上层应用进行通信,端口号的范围从 0 到 65535,有一些端口号对应有默认功能,比如用于浏览网页服务的 80 端口,用于 FTP 服务的 21 端口,用于 MODBUS TCP 通信的 502 端口等等。

1-2-2. UDP 协议

UDP 为用户数据协议,是使用一种协议开销最小的简单无连接传输模型。UDP 协议中没有握手机制,因此协议的可靠性仅等同于底层网络。无法确保对发送、回复消息提供保护。对于数据的完整性,UDP 还提供了校验和,并且通常用不同的端口号来寻址不同函数。

UDP 组播是 Internet 组管理协议,简称 IGMP。组播传输是在发送者和每一接收者之间实现点对多点的网络连接,用于典型的一主多从模式,有效地解决了单点发送、多点接收的问题,能够大量节约网络带宽、降低网络负载。

1-2-3. TCP 协议

1、TCP 的基本原理

TCP 协议为传输控制协议(Transport Control Protocol),是一种面向连接的、可靠的传输层协议。面向连接是指一次正常的 TCP 传输需要通过在 TCP 客户端和 TCP 服务端建立特定的虚电路连接来完成。要通过 TCP 传输数据,必须在两端主机之间建立连接。

在通过以太网通信的主机上运行的应用程序之间,TCP 提供了可靠、有序并能够进行错误校验的消息发送功能。TCP 能保证接收和发送的所有字节内容和顺序完全相同。TCP 协议在主动设备(即发起连接的设备)和被动设备(即接收连接的设备)之间创建连接。**连接建立后,任一方均可发起数据传送。**

TCP 协议是一种“流”协议,这意味着消息中不存在结束标志,所有接收到的消息均被认为是数据流的一部分。例如,客户端设备向服务端发送三条消息,每条均为 20 个字节。服务器只看到接收到一条 60 字节的“流”(假设服务器在收到三条消息后执行一次接收操作)。

2、套接字(Socket)的基本概念

套接字(Socket)是通信的基石,是支持 TCP/IP 协议的网络通信的基本操作单元。它是网络通信过程中端点的抽象表示,包含进行网络通信必须的五种信息:连接使用的协议、本地主机的 IP 地址、本地进程的协议端口、远端主机的 IP 地址、远端进程的协议口。

应用层通过传输层进行数据通信时,TCP 会遇到同时为多个应用程序进程提供并发服务的问题。多个 TCP 连接或多个应用程序进程可能需要通过同一个 TCP 协议端口传输数据。为了区别不同的应用程序进程和连接,许多计算机操作系统为应用程序与 TCP/IP 协议交互提供了套接字接口。应用层可以和传输层通过套接字接口,区分来自不同应用程序进程或网络连接的通信,实现数据传输的并发服务。

3、建立套接字(Socket)连接

建立套接字连接至少需要一对套接字,其中一个运行于客户端(也称之为 TCP 客户端),称为 ClientSocket,另一个运行于服务端(也称之为 TCP 服务器),称为 ServerSocket。

套接字之间的连接过程分为三个步骤:服务端监听,客户端请求,连接确认。

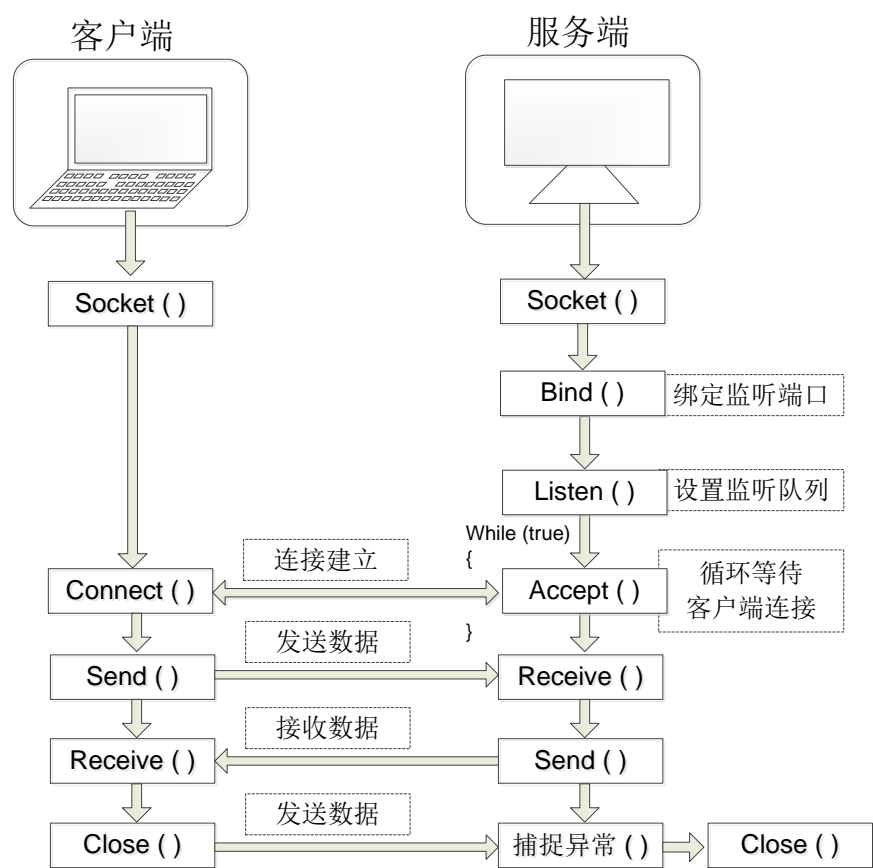
服务端监听：服务端套接字并不定位具体的客户端套接字，而是处于等待连接的状态，实时监控网络状态，等待客户端的连接请求。

客户端请求：指客户端的套接字提出连接请求，要连接的目标是服务端的套接字。为此，客户端的套接字必须首先描述它要连接的服务端的套接字，指出服务端套接字的地址和端口号，然后就向服务端套接字提出连接请求。

连接确认：当服务端套接字监听到或者说接收到客户端套接字的连接请求时，就响应客户端套接字的请求，建立一个新的线程，把服务端套接字的描述发给客户端，一旦客户端确认了此描述，双方就正式建立连接。而服务端套接字继续处于监听状态，继续接收其他客户端套接字的连接请求。

创建套接字连接时，可以指定使用的传输层协议，套接字可以支持不同的传输层协议(TCP 或 UDP)，当使用 TCP 协议进行连接时，该套接字连接就是一个 TCP 连接。

TCP 通讯示意图：



上图中，服务端的套接字处于监听状态，客户端向服务端提出连接请求，服务端接收到连接请求并发送回复确认信息给客户端，客户端收到后向服务端发送确认信息，完成资源分配后，一个 TCP 连接成立，此过程称为“三次握手”。

连接建立后，客户端和服务端进行数据的收发，数据收发完成后，客户端或服务端均可以发起连接关闭请求，经过“四次握手”后，TCP 连接关闭，一切数据收发中断。

2. 以太网参数的配置

本章主要介绍以太网的基本参数以及参数分别在 XDPPro 编程软件和 XINJEConfig 配置工具中的配置方法。

2. 以太网参数的配置	9
2-1. 以太网参数介绍	10
2-1-1. IP 地址相关参数	10
2-1-2. 功能规格	10
2-2. 以太网参数在编程软件中的配置	11
2-3. 以太网参数在 XINJEConfig 中的配置	12

2-1. 以太网参数介绍

2-1-1. IP 地址相关参数

以太网通讯中需设定 IP 地址作为每台设备的唯一标识。IP 地址的设定共有四项参数，下图分别是编程软件和 XINJEConfig 配置工具里的 IP 地址设置界面。



IP 地址获取方式

支持 IP 地址自动获取、静态设定功能，PLC 出厂时初始设置为自动获取。

自动获取方式：子网中存在 DHCP 服务器时，IP、子网掩码、默认网关由 DHCP 服务器分配。无 DHCP 服务器时，网络参数使用默认值：

IP 地址：192.168.6.6

子网掩码：255.255.255.0

默认网关：192.168.6.1

静态指定方式：用户分配 IP、子网掩码、默认网关信息。仅支持私有 IP 地址信息。

IP 地址类型	IP 地址范围	IP 设备数量
A 类私有地址	10.0.0.0-10.255.255.255	16777216
B 类私有地址	172.16.0.0-172.31.255.255	1048576
C 类私有地址	192.168.0.0-192.168.255.255	65535

UDP 组播地址

IP 地址类型	IP 地址范围	IP 地址
D 类地址	224.0.0.0~224.0.0.255	预留的组播地址（永久组地址）
	224.0.1.0~224.0.1.255	公用组播地址
	224.0.2.0~238.255.255.255	用户可用的组播地址（临时组地址）
	239.0.0.0~239.255.255.255	本地管理组播地址

注：建议用户使用 224.0.2.0~238.255.255.255 之间的 IP 地址。

2-1-2. 功能规格

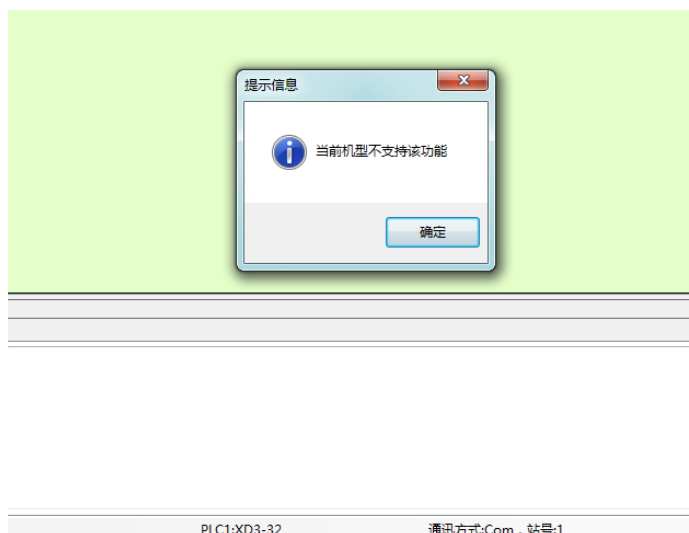
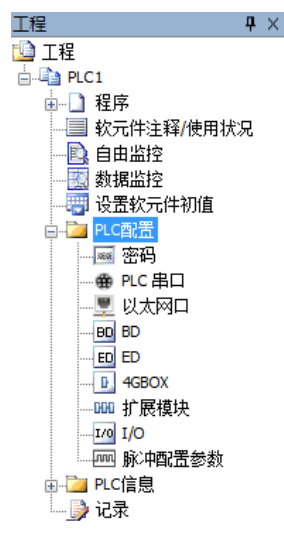
项目	参数
通讯通道数	以太网系列：2 通道（同一个 IP） XDH/XLH/XG2 系列：1 通道
通讯速度	100Mbps
站点最大间距	100 米
网络拓扑	线型、星型

通讯类型	最大网络节点数
自由格式 TCP	32
UDP 单播	32
UDP 组播	32
Modbus TCP 客户端	32
Modbus TCP 服务端	4

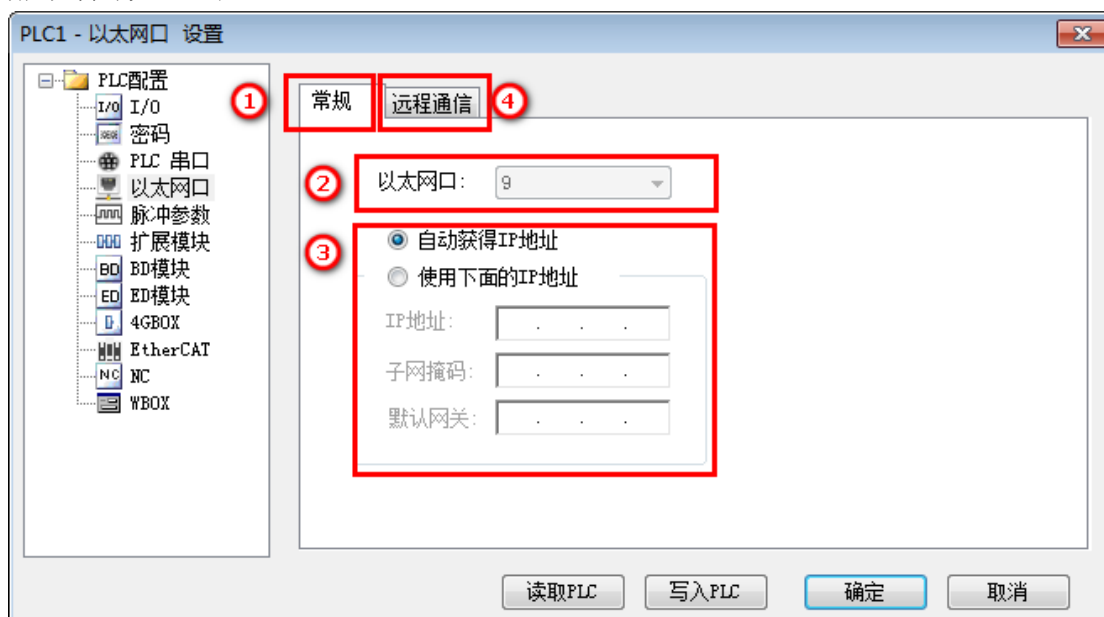
注： TCP 协议最多 32 个，包括自由格式 TCP 和 Modbus TCP；
 UDP 协议最多 32 个，包括 UDP 单播和 UDP 组播。
 XDH、XLH 系列暂不支持 UDP 组播。
 UDP 组播功能仅 3.7.2 及以上固件版本的以太网型 PLC 支持。

2-2. 以太网参数在编程软件中的配置

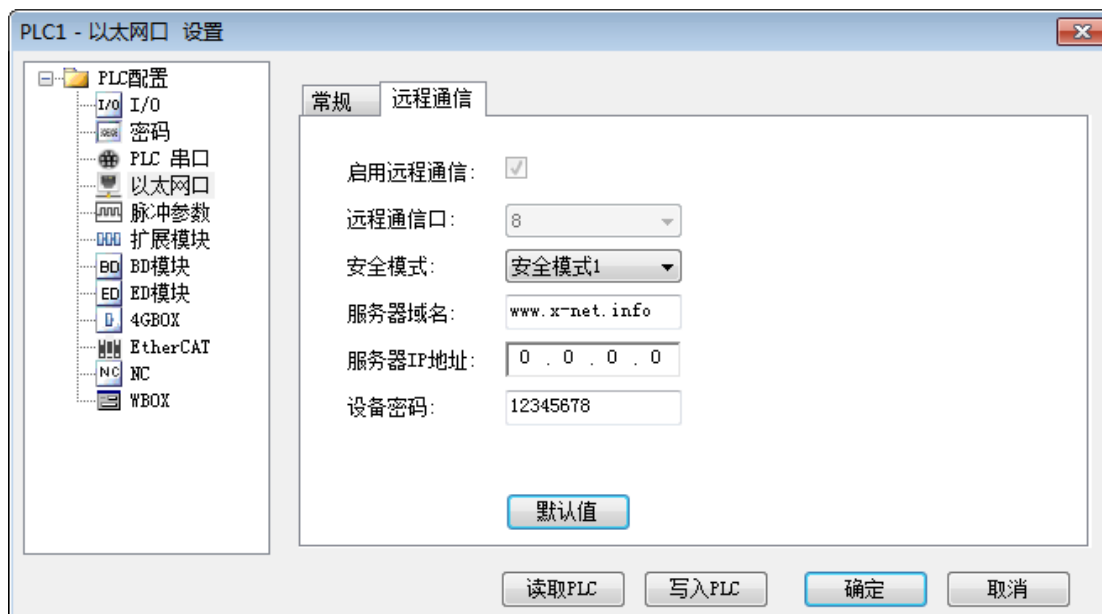
打开信捷 PLC 编程工具软件，软件左侧工程一栏中找到“PLC 配置”→“以太网口”，如下图。单击图标打开“以太网口”窗口，提示“当前机型不支持该功能”，并且无法对当前窗口做任何操作，如下图所示。



当前机型为以太网型 PLC 时，打开“以太网口”窗口，标签处于活跃可编辑状态，如下图所示。各部分功能说明详见 2-1 节。

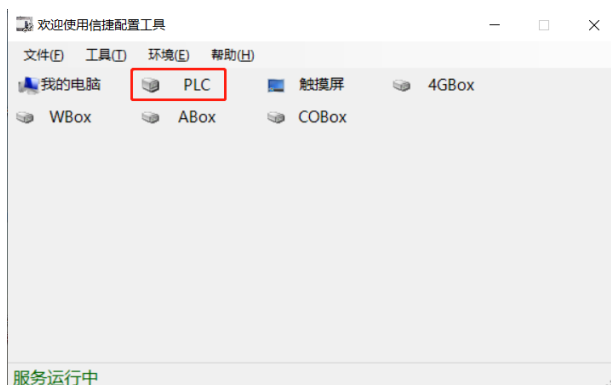


选择远程通信进入窗口如下图所示，可以配置远程参数，在局域网中通信不需要设置该项参数，所有参数配置完成后 PLC 重新上电，参数生效。

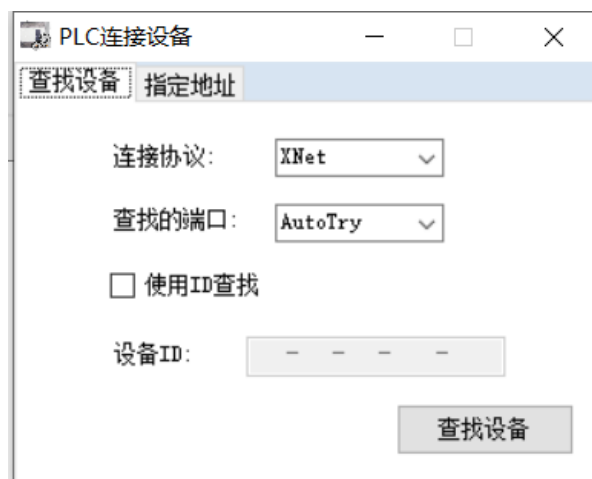


2-3. 以太网参数在 XINJEConfig 中的配置

以太网机型在进行 XINJEConfig 配置时，使用编程线缆连接 PLC 和电脑，双击或右键打开 XINJEConfig 配置工具，在打开配置工具中选择 PLC



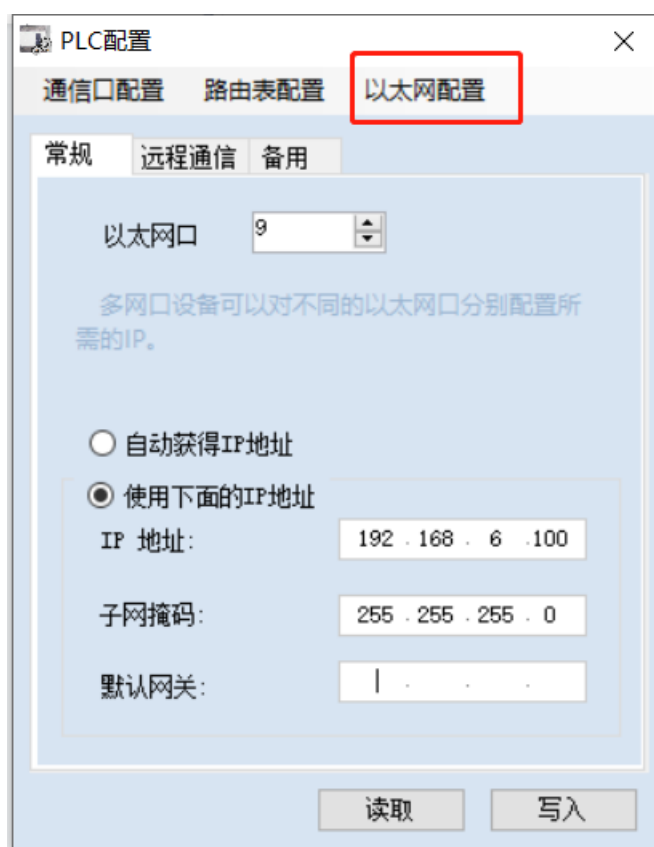
在弹出的对话框中可以选择查找设备或指定地址两种方式进行对 PLC 的通信口或以太网口进行参数配置。如下图所示：



当使用查找设备时，需要选择当前串口连接所使用的协议与查找的端口号，当选用指定地址时，需要填写当前所要连接 PLC 的 IP 地址，最后点击查找设备或连接设备，进行对所需要的 PLC 进行配置操作。



在进行对以太网参数进行配置时，选择以太网配置，配置项说明详见 2-1-1 节，功能与 XDPPro 的配置相同。



3. 接线方式及通讯协议

本章主要介绍以太网通讯的接线方式、MODBUS TCP 通讯协议、自由格式通讯协议内容。

3. 接线方式及通讯协议	14
3-1. 接线方式	15
3-2. MODBUS TCP 通讯协议	15
3-2-1. MODBUS TCP 通讯概述	15
3-2-2. MODBUS 通讯地址	15
3-2-3. MODBUS 通讯功能码	15
3-3. 自由格式通讯协议	16

3-1. 接线方式

以太网机型物理接口为 RJ45，接线时推荐选择超五类 UTP 和 STP 网线，单段长度建议不超过 100 米。交换机类型建议为百兆/千兆自适应交换机。

3-2. MODBUS TCP 通讯协议

3-2-1. MODBUS TCP 通讯概述

MODBUS TCP 结合了以太网物理网络和网络标准 TCP/IP 以及以 MODBUS 作为应用协议标准的数据表示方法。MODBUS TCP 通信报文被封装于以太网 TCP/IP 数据包中，MODBUS 协议规范一帧数据的最大长度为 256 个字节。

MODBUS TCP/IP 的通信系统中有两种类型的设备：MODBUS TCP/IP 客户端和服务端设备。

MODBUS 客户端：

客户端（TCP Client）主动向服务器（TCP Server）发起连接请求，连接建立成功，仅允许客户端主动发起通讯请求。

以太网机型作为 MODBUS TCP 客户端时，通过 S_OPEN 指令建立 TCP 连接，通过 M_TCP 指令发起 MODBUS 请求。

注意：PLC 支持的客户端数量如下：

固件版本	PLC 型号	支持客户端数量
3.7.2 以下版本	XD5E/XL5E/XDME/XLME/XDH/XLH	4 个
3.7.2 版本	XD5E/XL5E/XDME/XLME	8 个
	XDH/XLH	16 个

MODBUS 服务器：

服务器主动监听 502 端口，等待客户端连接请求，连接建立成功，响应符合 Modbus TCP 协议规范的数据通讯请求。

以太网机型上电默认开启此服务，最大响应不超过 4 个 TCP 连接。

3-2-2. MODBUS 通讯地址

可编程控制器作为 Modbus 服务器时，内部软元件编号与对应的 Modbus 地址编号可以参考信捷 PLC 编程手册《XD/XL 系列可编程控制器用户手册【基本指令篇】》以及《XG 系列可编程控制器用户手册【基本指令篇】》第 6-2 章节 Modbus 通讯功能篇。

3-2-3. MODBUS 通讯功能码

信捷以太网机型支持 Modbus 通讯功能码如下表所示：

功能码	功能	功能描述
01H	读线圈指令	读取0X类型地址，最大数量2000个
02H	读输入线圈指令	读取1X类型地址，最大数量2000个
03H	读保持寄存器内容	读取4X类型地址，最大数量125个
04H	读输入寄存器指令	读取3X类型地址，最大数量125个
05H	写单个线圈指令	写单个0X类型地址
06H	写单个寄存器指令	写单个4X类型地址
0FH	写多个线圈指令	写0X类型地址，最大数量1976个
10H	写多个寄存器指令	写4X类型地址，最大数量123个

3-3. 自由格式通讯协议

基于以太网的自由通信分为两大类：TCP 和 UDP，以太网机型采用 TCP 方式通信时可以作为 TCP 客户端（TCP 客户端），也可以作为 TCP 服务端（TCP 服务器）。

- 1、作为 TCP 客户端，主动与 TCP 服务器建立 TCP 连接，并绑定套接字 ID。
- 2、作为 TCP 服务器，等待 TCP 客户端与之建立 TCP 连接，并绑定套接字 ID。
- 3、使用 UDP，监听指定的本机端口，并绑定套接字 ID。

基于以上三种形式，可以实现以太网上的自由通信。自由格式通讯是以数据块的形式进行数据传送，受 PLC 缓存的限制，单次发送和接收的数据量最大为 1000 个字节。

自由格式通讯的关键参数：

数据缓冲方式：8 位、16 位

- 1、选择 8 位缓冲形式进行通讯时，通讯过程中寄存器的高字节是无效的，PLC 只利用寄存器的低字节进行发送和接收数据。
- 2、选择 16 位缓冲形式进行通讯时，PLC 将接收的数据，先低字节再高字节储存；PLC 发送数据时，先发送低字节再发送高字节。
- 3、接收数据包长度大于设定接收长度时，数据按 16 位存储方式存储。

4. 以太网通讯指令

本章主要介绍以太网通讯指令的介绍、通讯口参数读写指令的介绍、相关标志位和寄存器、错误一览表等内容。

4. 以太网通讯指令

17

4-1. 以太网通讯指令概述

18

4-1-1. 创建 TCP 连接/UDP 端口监听[S_OPEN]

18

4-1-2. 通讯终止[S_CLOSE]

21

4-1-3. 自由格式通讯-发送[S_SEND]

22

4-1-4. 自由格式通讯-接收[S_RCV]

23

4-1-5. MODBUS 通讯[M_TCP]

24

4-1-6. 以太网通讯案例

25

4-2. 通讯口参数的读写指令

40

4-2-1. 串口参数的读取[CFGCR]

40

4-2-2. 串口参数的写入[CFGCW]

41

4-2-3. IP 地址设置指令[IPSET]

42

4-2-4. 串口参数的名称及设定

44

4-2-5. 通讯口参数通讯案例

45

4-3. 以太网通讯相关标志位和寄存器

46

4-4. 以太网通讯错误一览表

47

4-1. 以太网通讯指令概述

以太网通讯指令包括：通讯任务的开启和关闭、发送/接收数据、MODBUS TCP。使用以太网指令时，请按照以下步骤进行：

（1）开启通讯任务：确认通信协议和通信类型，配置通信参数，创建 TCP 连接/UDP 端口监听，并绑定套接字 ID。

（2）实现数据通信：开启成功的通讯任务，实现以太网自由通信或 MODBUS TCP 数据通讯。

（3）关闭通讯任务：当与目标通讯设备通讯完成后，或 TCP 连接出现异常时，需要关闭通讯任务。

4-1-1. 创建 TCP 连接/UDP 端口监听[S_OPEN]

1) 指令概述

通讯任务创建指令，与终止通讯任务指令 S_CLOSE 配合使用。

创建 TCP 连接/UDP 端口监听[S_OPEN]			
16 位指令	S_OPEN	32 位指令	-
执行条件	边沿触发	适用机型	XD5E、XDME、XDH、XG、XL5E、XLME、XLH
固件要求	V3.5.3 及以上	软件要求	V3.5.3 及以上

2) 操作数

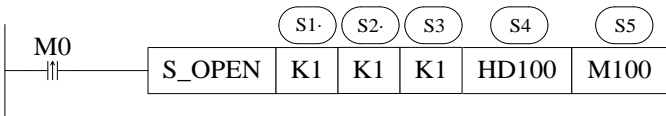
操作数	作用	类型
S1	指定建立通讯任务的套接字 ID	16 位，BIN
S2	指定通讯类型	16 位，BIN
S3	指定本机的通讯模式	16 位，BIN
S4	指定参数块起始地址	16 位，BIN
S5	指定标志起始位置	位

3) 适用软元件

操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m	
S1	●								●										
S2	●								●										
S3	●								●										
S4	●																		
S5														●					

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 通讯任务创建指令，M0 一次上升沿调用创建一次 TCP 连接或开启一次 UDP 端口监听。
- S1：套接字 ID，范围：K0~K63。注意：同时建立的套接字数量不超过 64 个，TCP 数量不超过 32 个，UDP 数量不超过 32 个。
- S2：通信类型，范围：K0、K1、K2；K0 为 UDP，K1 为 TCP，K2 为 UDP 组播（XDH、XLH 系列暂不支持）。

- S3: 模式选择, 范围: K0、K1; K0 为服务器, K1 为客户端。
 - S4: 参数块起始地址, 共占用 S4~S4+8 连续 9 个寄存器。
 - S5: 标志起始位置, 共占用 S5~S5+9 连续 10 个线圈。
- 注意: 1、服务器需要先打开套接字, 等待客户端的连接, 否则套接字可能会建立不成功。
- 2、UDP 组播功能仅 3.7.2 及以上固件版本以太网型的 PLC 支持。
- 3、XDH、XLH 系列暂不支持 UDP 组播。
- 该指令可以通过“指令配置”中的“以太网连接配置”面板配置, 如下图所示:



注意: 红框内配置参数需要“写入 PLC”生效。

- 通讯任务异常操作, 以太网错误标志 SM1921 被置位, 记录错误信息至 SD1920 和 SD1921, 详见章节 [4-3. 以太网通讯相关标志位和寄存器](#)。

以上图为例, HD0 为首的地址块和 M0 为首的标志位置的功能定义如下图所示:

SOpen配置指令帮助界面			
本机端口	HD0	连接中标志	M0
目标IP第一段 (例: 192)	HD1高字节	已连接标志	M1
目标IP第二段 (例: 168)	HD1低字节	发送中标志	M2
目标IP第三段 (例: 0)	HD2高字节	已发送标志	M3
目标IP第四段 (例: 1)	HD2低字节	接收中标志	M4
目标端口	HD3	已接收标志	M5
数据缓冲方式	HD4	关闭中标志	M6
接收超时时间 (10ms)	HD5	Modbus TCP通信标志	M7
预留	HD6	TCP异常标志	M8
实际接收字节数 (Byte)	HD7	错误标志	M9
错误码	HD8		

参数说明:

S_OPEN 指令创建的通讯任务分为三类：TCP 客户端、TCP 服务器、UDP。三种类型使用的参数有所区别，具体情况下：

通信类型	本机端口	目标 IP	目标端口	缓冲方式	超时时间	接收字节数	错误码
TCP 客户端	-	√	√	√	√	√	√
TCP 服务器	√	-	-	√	√	√	√
UDP	√	√	√	√	√	√	√

1、本机端口

取值范围为 1-60000，502 和 531 为特殊端口不可用。本机端口仅允许被一个通讯任务使用。

2、目标 IP

目标 IP 是指目标通信设备的 IP 地址，取值范围为 0-254，和本机在同一个子网内。

3、目标端口

目标通讯设备的网络端口号。取值范围 1-65535。进行 MODBUS TCP 通讯，目标端口必须为 502。

4、数据缓冲方式

Bit0 取值为 0 时，使用 8 位存储方式；为 1 时，采用 16 位存储方式。

实际接收数据包大于设定接收长度时，自动转换为 16 位存储方式。

Bit1 取值为 0 时，使用自动接收模式；为 1 时，使用用户接收模式。

自动接收：在接收时，如果对方发送太快，自动将来不及接收的数据丢弃；不接收或接收超时也会丢弃对方发送的数据。

用户接收：在接收时，如果对方发送太快来不及接收，会存在缓存区内，不丢弃任何数据，可以保证接收数据的完整性。

注意：此模式仅在发送太快造成接收丢失时使用，一般不建议使用该模式，且该模式必须使用常开/闭线圈触发接收，防止缓存区溢出。

5、接收超时时间

指 PLC 产生接收数据请求到该动作终止的总时间。取值范围 0-65536，单位是 10ms。设置为 0 表示不启用接收超时，连续接收数据；设为非 0 时，启用接收超时。接收超时时间对 S_RCV 和 M_TCP 指令有效。

如设置接收超时 300ms：请求产生开始等待对方回应 300ms，成功接收数据后立即终止，超过 300ms 未能接收到有效数据，结束当前指令并报接收超时错误。

6、TCP 保活

(1) 取值为 0 时，不启用 TCP 保活功能。

(2) 取值非 0 时，启用 TCP 保活功能。

一段时间内连接处于非活动状态，开启保活的一端将向对方发送保活探测，如果在设定的保活时间内发送端没有收到响应报文，则对方主机将被确认为不可到达，此时客户端会将不能到达主机对应的套接字进行一次关闭连接操作。触发时间为 1~5min，异常时置位“TCP 异常标志”。

注：TCP 保活功能仅 3.7.2 及以上固件版本以太网型的 PLC 支持。

7、接收数据长度

执行 S_RCV 指令，实际接收数据的长度，单位字节。

8、错误码

以太网自由格式通讯和 Modbus TCP 通讯发生异常时的错误信息，详见章节 [4-4. 以太网通讯错误一览表](#)。

9、标志位

通讯相关的标志位功能说明如下表所示：（以 Mn 为首地址说明）

位地址	标志位	功能说明
Mn	连接中标志	连接建立过程中，M（n）置 ON
M（n+1）	已连接标志	连接建立完成时，M（n+1）置 ON
M（n+2）	发送中标志	数据发送过程中，M（n+2）置 ON
M（n+3）	已发送标志	发送数据完成时，M（n+3）置 ON
M（n+4）	接收中标志	数据接收过程中，M（n+4）置 ON
M（n+5）	已接收标志	接收数据完成时，M（n+5）置 ON
M（n+6）	关闭中标志	正在关闭当前连接时，M（n+6）置 ON
M（n+7）	MODBUS TCP 通信中标志	正在执行 M_TCP 指令时，M（n+7）置 ON
M（n+8）	TCP 异常标志	TCP 连接异常时，M（n+8）置 ON
M（n+9）	错误标志	发生通讯错误时，M（n+9）置 ON

4-1-2. 通讯终止[S_CLOSE]

1) 指令概述

通讯终止指令，需和 S_OPEN 指令配合使用。

通讯终止[S_CLOSE]			
16 位指令	S_CLOSE	32 位指令	-
执行条件	边沿触发	适用机型	XD5E、XDME、XDH、XG、XL5E、XLME、XLH
固件要求	V3.5.3 及以上	软件要求	V3.5.3 及以上

2) 操作数

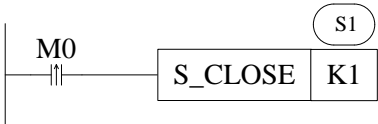
操作数	作用	类型
S1	指定关闭的套接字 ID	16 位，BIN

3) 适用软元件

操作数	字软元件											位软元件						
	系统								常数	模块		系统						
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m
S1	●								●									

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 通讯任务终止指令，M0 上升沿来临时，终止通信任务。
注意：该指令无法单独使用，需和 S_OPEN 指令配合使用。
- S1：指定要关闭的套接字 ID，可指定寄存器或常数，范围：K0~K63。
- 指令执行后，基于此套接字 ID 的 M_TCP、S_SEND、S_RCV 指令将无法执行。

4-1-3. 自由格式通讯-发送[S_SEND]

1) 指令概述

自由格式通讯发送指令，需和 S_OPEN、S_CLOSE 指令配合使用。

自由格式通讯-发送[S_SEND]			
16 位指令	S_SEND	32 位指令	-
执行条件	边沿触发	适用机型	XD5E、XDME、XDH、XG、XL5E、XLME、XLH
固件要求	V3.5.3 及以上	软件要求	V3.5.3 及以上

2) 操作数

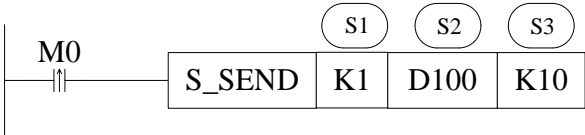
操作数	作用	类型
S1	指定所在套接字 ID	16 位，BIN
S2	指定发送数据的本地寄存器首地址	16 位，BIN
S3	指定发送数据个数	16 位，BIN

3) 适用软元件

操作数	字软元件											位软元件						
	系统								常数	模块		系统						
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m
S1	●								●									
S2	●																	
S3	●								●									

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 自由格式通讯发送指令，M0 的一次上升沿进行一次数据的发送。
注意：该指令无法单独使用，需和 S_OPEN、S_CLOSE 指令配合使用。
- S1：套接字 ID，可指定寄存器或常数，范围：K0~K63。
- S2：本地寄存器发送首地址。
- S3：发送数据的字节数量，可指定寄存器或常数。
- 该指令直接在梯形图窗口中输入。
- 使用时，需注意所在套接字 ID 中 S_OPEN 指令中的数据缓冲类型（16 位/8 位）。
- 当缓冲位数为 8 位时，只发送寄存器的低字节数据，例如：要发送 D100~D107 寄存器中的低字节数据时，S3 应设为 8。
- 当缓冲位数为 16 位时，寄存器的高低字节数据都将被发送，例如：要发送 D100~D107 中的高、低字节数据时，S3 应设为 16，且发送时，低字节在前高字节在后。

4-1-4. 自由格式通讯-接收[S_RCV]

1) 指令概述

自由格式通讯接收指令，需和 S_OPEN、S_CLOSE 指令配合使用。

自由格式通讯-接收[S_RCV]			
16 位指令	S_RCV	32 位指令	-
执行条件	常开/闭、边沿触发	适用机型	XD5E、XDME、XDH、XG、XL5E、XLME、XLH
固件要求	V3.5.3 及以上	软件要求	V3.5.3 及以上

2) 操作数

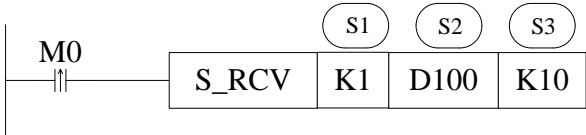
操作数	作用	类型
S1	指定所在套接字 ID	16 位，BIN
S2	指定接收数据的本地寄存器首地址	16 位，BIN
S3	指定接收数据个数	16 位，BIN

3) 适用软元件

操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m	
S1	●								●										
S2	●																		
S3	●								●										

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 自由格式通讯接收指令，M0 的一次上升沿进行一次数据的接收。
注意：该指令无法单独使用，需和 S_OPEN、S_CLOSE 指令配合使用。
- S1：套接字 ID，可指定寄存器或常数，范围：K0~K63。
- S2：本地寄存器接收首地址。
- S3：接收数据的字节数量，可指定寄存器或常数。
- 该指令直接在梯形图窗口中输入。
- 使用时，需注意所在套接字 ID 中 S_OPEN 指令中的数据缓冲类型（16 位/8 位）。
- 当缓冲位数为 8 位时，接收的数据只存放在低字节中，例如：要接收 8 个字节数据，依次存放在 D100~D107 这 8 个寄存器的低字节中，此时，S3 应设为 8。
- 当缓冲位数为 16 位时，寄存器的高低字节中都会存放接收的数据，例如：要接收 16 个字节数据，依次存放在 D100~D107 这 8 个寄存器中，此时，S3 应设为 16。且接收时，低字节在前高字节在后。

4-1-5. MODBUS 通讯[M_TCP]

1) 指令概述

PLC 作为客户端时，实现 MODBUS TCP 协议的数据收发指令。与创建通讯任务指令 S_OPEN、终止通讯指令 S_CLOSE 指令配合使用。

MODBUS TCP 通讯[M_TCP]			
16 位指令	M_TCP	32 位指令	-
执行条件	边沿触发	适用机型	XD5E、XDME、XDH、XG、XL5E、XLME、XLH
固件要求	V3.5.3 及以上	软件要求	V3.5.3 及以上

2) 操作数

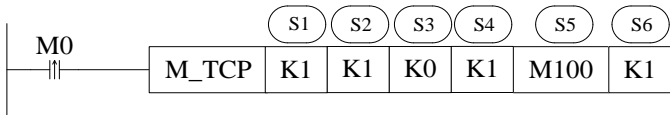
操作数	作用	类型
S1	指定远端站号	16 位, BIN
S2	指定 MODBUS 通讯功能码	16 位, BIN
S3	指定目标首地址	16 位, BIN
S4	指定通讯寄存器或线圈数量	16 位, BIN
S5	指定本地首地址	16 位, BIN
S6	指定套接字 ID	16 位, BIN

3) 适用软元件

操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m	
S1	●								●										
S2	●								●										
S3	●								●										
S4	●								●										
S5	●																		
S6	●								●										

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- MODBUS TCP 通讯指令，M0 的一次上升沿进行一次 MODBUS TCP 通讯。
- S1：远端通讯站号，范围：K0~K247。
- S2：MODBUS 通讯功能码。
- S3：目标首地址，此处为 MODBUS 通讯地址，具体可查看《XD、XL 系列可编程控制器用户手册(基本指令篇)》6-2-3。
- S4：通讯数据个数。
- S5：本地首地址。
- S6：套接字 ID，指定使用的 TCP 连接，目标端口必须为 502。
- 该指令无法单独使用，需和 S_OPEN、S_CLOSE 指令配合使用。
- M_TCP 指令仅当 PLC 作为客户端时生效，实现 MODBUS TCP 协议的数据收发。

- 注意：ModbusTCP 作为服务器，不需要写通讯指令，客户端建立套接字写好通讯指令即可。
- 该指令需要通过“指令配置”中的“MODBUS TCP 配置”面板配置，如下图所示：



功能码选择说明：

数值	功能码	数值	功能码
K1	读线圈	K3	读寄存器
K2	读输入离散量	K4	读输入寄存器
K5	写单个线圈	K6	写单个寄存器
K15	写多个线圈	K16	写多个寄存器

4-1-6. 以太网通讯案例

例 1：通过下面程序，实现 PLC 上电后自动创建 TCP 客户端、TCP 服务器、UDP 三种形式的通讯任务，并在每个通讯任务的基础上实现数据的收发。1 号 PLC 的 IP 地址是 192.168.1.12，2 号 PLC 的 IP 地址是 192.168.1.6。

注意：服务器需要先打开套接字，等待客户端的连接，否则套接字可能会建立不成功

程序操作：

(1) 1 号 PLC 上电后作为 TCP 客户端主动向 2 号 PLC 的 TCP 服务器服务端口 1111 建立 TCP 连接并绑定套接字 ID 为 1，连接建立成功后向 2 号 PLC D2600~D3149 内发送 D1000~D1549 的低八位数据，同时一直接收来自 2 号 PLC D2000~D2399 的数据存放到寄存器 D1600~D1999 的低八位。当 TCP 连接发生异常时或在设定的保活时间内发送端没有收到响应报文(此处保活时间设置为 2s)，主动关闭 TCP 连接并重建连接。

由于不同系列 PLC 的以太网口数量存在不同，因此在使用通讯相关线圈 SM1902 或 SM1903 时，请注意加以区分此时网线连接 PLC 第几个以太网口。(SM1902 为连接网络设备标志，使用在双网口机型第一个网口或单网口机型连接至交换机/路由/其他网络设。SM1903 为连接网络设备标志，使用在双网口机型第二个网口连接至交换机/路由/其他网络设备)

1 号 PLC 程序如下：



客户端套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

TCP (K1)

工作模式

客户端(K1)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.6

目标端口

1111

接收模式

自动接收

保活时间(s)

2

占用空间:

HD100-HD109, M100-M109

读取PLC

写入PLC

确定

取消

2 号 PLC 程序如下：



服务器套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

TCP (K1)

工作模式

服务器(K0)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

1111

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

0 . 0 . 0 . 0

目标端口

0

接收模式

自动接收

保活时间(s)

2

占用空间:

HD100~HD109, M100~M109

读取PLC

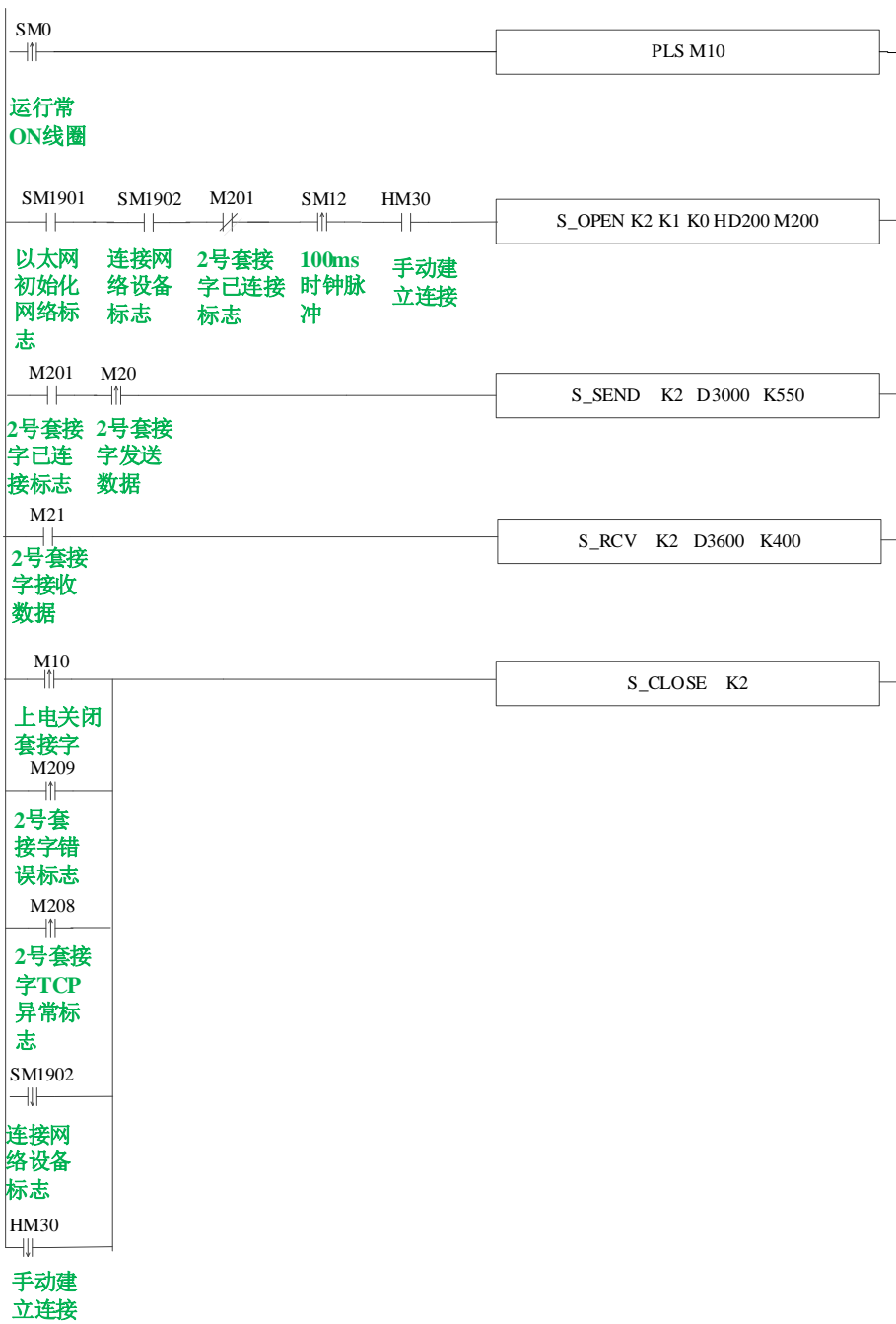
写入PLC

确定

取消

(2) 1 号 PLC 上电后作为 TCP 服务器主动监听 1001 端口，等待 2 号 PLC 的 TCP 客户端设备建立 TCP 连接并绑定套接字 ID 为 2, 连接建立成功后向连接设备 2 号 PLC 发送 D3000-D3549 的低八位数据，同时一直接收来自连接设备 2 号 PLC 的数据，将数据存放到寄存器 D3600-D3999 的低八位。当 TCP 连接发生异常时或在设定的保活时间内发送端没有收到响应报文(此处保活时间设置为 2s)，主动关闭 TCP 连接并重建连接。

1 号 PLC 程序如下：



服务器套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K2

通讯类型

TCP (K1)

工作模式

服务器 (K0)

参数起始地址

HD200

标志起始地址

M200

“基本设置” 程序下载后生效！

本机端口

1001

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.6

目标端口

1111

接收模式

自动接收

保活时间(s)

2

占用空间:

HD200~HD209, M200~M209

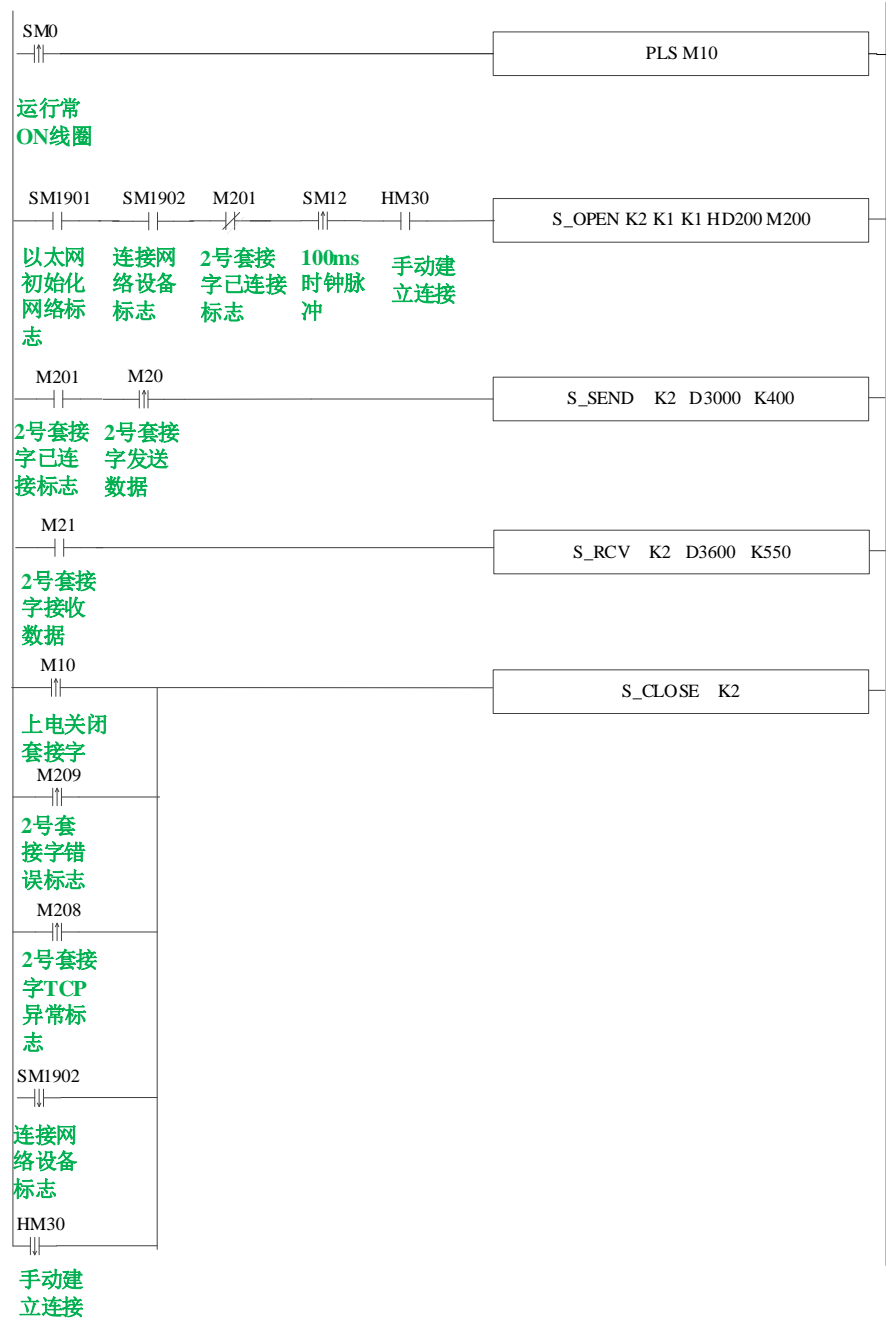
读取PLC

写入PLC

确定

取消

2 号 PLC 程序如下：



客户端套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K2

▼

通讯类型

TCP (K1)

▼

工作模式

客户端(K1)

▼

参数起始地址

HD200

标志起始地址

M200

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

▼

接收超时(10ms)

0

目标设备IP

192.168.1.12

目标端口

1001

接收模式

自动接收

▼

保活时间(s)

2

▼

占用空间:

HD200~HD209, M200~M209

读取PLC

写入PLC

确定

取消

（3）1 号 PLC 上电后采用 UDP 方式通讯，IP 地址为 192.168.1.12，设定本机端口为 1002，目标 IP 为 192.168.1.6，目标端口为 3000，并绑定套接字 ID 为 3，连接建立成功后向设备 2 号 PLC 发送 D4000-D4549 的低八位数据，同时一直接收来自 PLC2 的数据存放到寄存器 D4600~D4999 的低八位。当 UDP 单播在连接发生异常时，主动关闭 UDP 单播连接并重建连接。

1 号 PLC 程序如下：



UDP 套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K3

通讯类型

UDP (K0)

工作模式

客户端(K1)

参数起始地址

HD400

标志起始地址

M400

“基本设置”程序下载后生效！

本机端口

1002

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.6

目标端口

3000

接收模式

自动接收

保活时间(s)

0

占用空间:

HD400~HD409, M400~M409

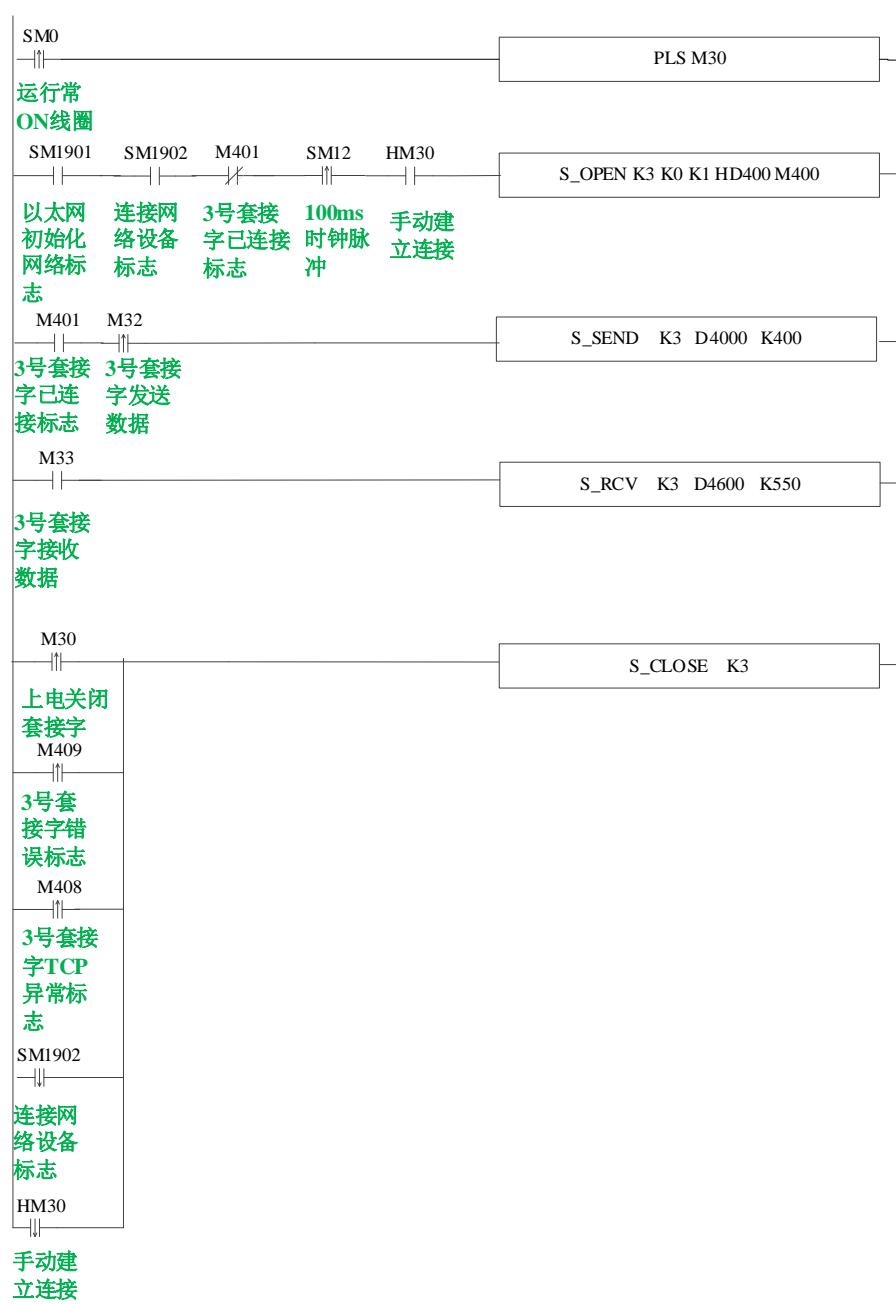
读取PLC

写入PLC

确定

取消

2 号 PLC 程序如下：



UDP 套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K3

通讯类型

UDP (K0)

工作模式

客户端(K1)

参数起始地址

HD400

标志起始地址

M400

“基本设置”程序下载后生效！

本机端口

3000

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.12

目标端口

1002

接收模式

自动接收

保活时间(s)

0

占用空间:

HD400~HD409, M400~M409

读取PLC

写入PLC

确定

取消

例 2：通过下面程序，实现 PLC 上电后自动向 MODBUS-TCP 服务器设备 A 和 B 通信，PLC 的 IP 地址是 192.168.1.12，设备 A 的 IP 地址是 192.168.1.6，Modbus 站号是 1，设备 B 的 IP 地址是 192.168.1.14，Modbus 站号是 1。

注意： ModbusTCP 作为服务器，不需要写通讯指令。

由于不同系列 PLC 的以太网口数量存在不同，因此在使用通讯相关线圈 SM1902 或 SM1903 时，请注意加以区分此时网线连接 PLC 第几个以太网口。（SM1902 为连接网络设备标志，使用在双网口机型第一个网口或单网口机型连接至交换机/路由/其他网络设。SM1903 为连接网络设备标志，使用在双网口机型第二个网口连接至交换机/路由/其他网络设备）

程序操作：

（1）PLC 上电后作为 TCP 客户端主动向设备 A 的 TCP 服务器服务端口 502 建立 TCP 连接并绑定套接字 ID 为 1，连接建立成功后以 1s 一次的频率将 D1000-D1019 的值写给设备 A 的 4x100-4x119。当 TCP 连接发生异常时或在设定的保活时间内发送端没有收到响应报文（此处保活时间设置为 2s），主动关闭 TCP 连接并重建连接。

（2）PLC 上电后作为 TCP 客户端主动向设备 B 的 TCP 服务器服务端口 502 建立 TCP 连接并绑定套接字 ID 为 2，连接建立成功后以 1s 一次的频率将 D1000-D1019 的值写给设备 A 的 4x200-4x219。当 TCP 连接发生异常时或在设定的保活时间内发送端没有收到响应报文(此处保活时间设置为 2s)，主动关闭 TCP 连接并重建连接。

程序如下：





1 号套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

TCP(K1)

工作模式

客户端(K1)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.6

目标端口

502

接收模式

自动接收

保活时间(s)

2

占用空间:

HD100-HD109, M100-M109

读取PLC

写入PLC

确定

取消

1 号套接字 M_TCP 配置信息如下：

Modbus Tcp指令配置界面

套接字ID

K1

本地首地址

D1000

Modbus TCP

站点号

K1

功能码

0x10 写多个寄存器

数据地址

K100

数量

K20

确定

取消

2 号套接字 S_OPEN 配置信息如下：

S_OPEN参数配置

基本设置

套接字ID

K2

通讯类型

TCP(K1)

工作模式

客户端(K1)

参数起始地址

HD200

标志起始地址

M200

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

192.168.1.14

目标端口

502

接收模式

自动接收

保活时间(s)

2

占用空间:

HD200-HD209, M200-M209

读取PLC

写入PLC

确定

取消

2 号套接字 M_TCP 配置信息如下：

Modbus Tcp指令配置界面

套接字ID

K2

本地首地址

D1000

Modbus TCP

站点号

K1

功能码

0x10 写多个寄存器

数据地址

K200

数量

K20

确定

取消

例 3：通过下面程序，实现 PLC 上电后自动创建 UDP 组播通讯任务，当连接发生异常时主动关闭 UDP 组播连接并重新建连接。实现一发多收。1 号 PLC 的 IP 地址是 192.168.1.6，2 号 PLC 的 IP 地址是 192.168.1.12，3 号 PLC 的 IP 地址 192.168.1.14。

由于不同系列 PLC 的以太网口数量存在不同，因此在使用通讯相关线圈 SM1902 或 SM1903 时，请注意加以区分此时网线连接 PLC 第几个以太网口。（SM1902 为连接网络设备标志，使用在双网口机型第一个网口或单网口机型连接至交换机/路由/其他网络设。SM1903 为连接网络设备标志，使用在双网口机型第二个网口连接至交换机/路由/其他网络设备）

程序操作：

- （1）PLC1 上电后采用 UDP 组播方式通讯，设定目标 IP 为 230.0.0.0，目标端口为 7000，并绑定套接字 ID 为 1，建立连接成功后，1 号 PLC 以 1s 一次的频率发送 D1000-D1499 的低八位数据，2 号和 3 号 PLC 一直接收来自 PLC1 的数据存放到寄存器 D1000~D1499 的低八位。
- （2）PLC2 上电后采用 UDP 组播方式通讯，设定目标 IP 为 230.0.0.0，目标端口为 7000，并绑定套接字 ID 为 1，建立连接成功后，2 号 PLC 一直接收来自 PLC1 的数据存放到寄存器 D1000~D1499 的低八位。
- （3）PLC3 上电后采用 UDP 组播方式通讯，设定目标 IP 为 230.0.0.0，目标端口为 7000，并绑定套接字 ID 为 1，建立连接成功后，3 号 PLC 一直接收来自 PLC1 的数据存放到寄存器 D1000~D1499 的低八位。

1 号 PLC 程序如下：



UDP 组播 S_OPEN 参数配置如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

UDP组播(K2)

工作模式

客户端(K1)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

230.0.0.0

目标端口

7000

接收模式

自动接收

保活时间(s)

0

占用空间:

HD100-HD109, M100-M109

读取PLC

写入PLC

确定

取消

2 号 PLC 程序如下：



UDP 组播 S_OPEN 参数配置如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

UDP组播(K2)

工作模式

客户端(K1)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

230.0.0.0

目标端口

7000

接收模式

自动接收

保活时间(s)

0

占用空间:

HD100~HD109, M100~M109

读取PLC

写入PLC

确定

取消

3 号 PLC 程序如下：



UDP 组播 S_OPEN 参数配置如下：

S_OPEN参数配置

基本设置

套接字ID

K1

通讯类型

UDP组播(K2)

工作模式

客户端(K1)

参数起始地址

HD100

标志起始地址

M100

“基本设置”程序下载后生效！

本机端口

0

缓冲方式

8位

接收超时(10ms)

0

目标设备IP

230.0.0.0

目标端口

7000

接收模式

自动接收

保活时间(s)

0

占用空间:

HD100-HD109, M100-M109

读取PLC

写入PLC

确定

取消

4-2. 通讯口参数的读写指令

在进行以太网通讯时，为保证通讯的正常实现，建议在编写通讯程序时，配合使用通讯口参数读/写指令。先通过调用通讯参数读指令，把对应通讯口上的参数读取到指定的寄存器组中，用户再根据需要修改寄存器组中对应的值，然后把修改过的寄存器组的值通过通讯参数写指令写到对应的通讯口配置中。

4-2-1. 串口参数的读取[CFGCR]

1) 指令概述

将串口参数读取到本机内指定的寄存器里。

串口参数的读取[CFGCR]			
16 位指令	CFGCR	32 位指令	-
执行条件	常开/闭线圈、边沿触发	适用机型	XD、XL、XG 全系列
固件要求	-	软件要求	V3.4 及以上

2) 操作数

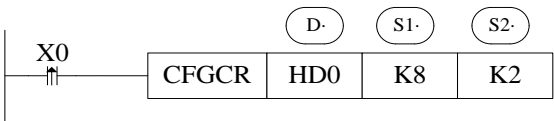
操作数	作用	类型
D	指定本地寄存器首地址编号	16 位，BIN
S1	指定读取串口参数的个数	16 位，BIN
S2	指定读取的串口编号	16 位，BIN

3) 适用软元件

操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn. m	
D	●																		
S1	●	●							●										
S2	●								K										

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 操作数 S1：读取串口参数占用的寄存器个数，一般为 8（以太网机型为 9）。
- 操作数 S2：串口号范围：K0~K5。K0：COM0、K1：COM1、K2：COM2 或 COM2-RS232 或 COM2-RS485、K3：COM3、K4：COM4、K5：COM5。
- 将串口 2 的 8 个参数读取到 HD0~HD7 中。具体参数的名称和定义见 4-2-4 节内容。

4-2-2. 串口参数的写入[CFGCW]

1) 指令概述

将本机内指定寄存器里的数值写入到指定串口中。

串口参数的写入[CFGCW]			
16 位指令	CFGCW	32 位指令	-
执行条件	常开/闭线圈、边沿触发	适用机型	XD、XL、XG 全系列
固件要求	-	软件要求	V3.4 及以上

2) 操作数

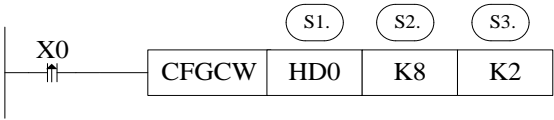
操作数	作用	类型
S1	指定本地寄存器首地址编号	16 位, BIN
S2	指定写入串口参数的个数	16 位, BIN
S3	指定写入的串口编号	16 位, BIN

3) 适用软元件

操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn. m	
S1	●																		
S2	●	●							●										
S3	●								K										

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。
M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作



- 操作数 S2：写入串口参数占用的寄存器个数，一般为 8（以太网机型为 9）。
- 操作数 S3：串口号范围：K0~K5。K0：COM0、K1：COM1、K2：COM2 或 COM2-RS232 或 COM2-RS485、K3：COM3、K4：COM4、K5：COM5。
- 将 HD0~HD7 中的数值写入到串口 2 的参数里。具体参数的名称和定义见 4-2-4 节内容。

4-2-3. IP 地址设置指令[IPSET]

1) 指令概述

设置本机的 IP 地址。

IP 地址设置[IPSET]			
16 位指令	IPSET	32 位指令	-
执行条件	边沿触发	适用机型	XDE、XD5E、XG、XL5E、XLME
固件要求	V3.5.3b 及以上	软件要求	V3.5.3 及以上

2) 操作数

操作数	作用	类型
S0	指定本地寄存器首地址	16 位整数
S1	指定寄存器个数 (K4、K12)	16 位整数
S2	指定本地串口号 (K9)	16 位整数

3) 适用软元件

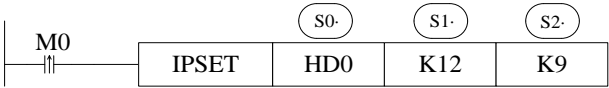
操作数	字软元件											位软元件							
	系统								常数	模块		系统							
	D	FD	TD	CD	DX	DY	DM	DS	K/H	ID	QD	X	Y	M	S	T	C	Dn.m	
D0	•								•										
D1	•								•										
D2	•								•										

注：D 表示 D、HD；TD 表示 TD、HTD；CD 表示 CD、HCD、HSCD、HSD；DM 表示 DM、DHM；DS 表示 DS、DHS。

M 表示 M、HM、SM；S 表示 S、HS；T 表示 T、HT；C 表示 C、HC。

4) 功能和动作

《指令形式》



- 指令含义：将 HD0-HD11 内的网络参数写入到 PLC 的以太网口中。

地址	功能	举例	查看方式
HD0	IP 地址	192	十进制
HD1		168	十进制
HD2		51	十进制
HD3		103	十进制
HD4	子网掩码	255	十进制
HD5		255	十进制
HD6		255	十进制
HD7		0	十进制
HD8	默认网关	192	十进制
HD9		168	十进制
HD10		51	十进制
HD11		1	十进制

- S0：指定本地寄存器的首地址。
- S1：固定为 K4 或 K12。
K4：只写入 IP 地址，例如：IP 地址：192.168.51.103；

K12: 将 IP 地址、子网掩码、默认网关都写入到 PLC 的以太网口;

例如: IP 地址: 192.168.51.103

子网掩码: 255.255.255.0

默认网关: 192.168.51.1

- S2: 固定为 K9, PLC 的以太网口参数固定为 K9。

注意:

- (1) 写入参数后, 需将 PLC 重新上电才可生效;
- (2) 当前为自动获取 IP 地址时, 执行 IPSET 指令会将 IP 地址改为固定 IP;
- (3) 将 IP 都设为 0, 可将固定 IP 改为自动获取 IP。

- 以太网口参数相关寄存器地址:

地址	功能	类型	查看方式
SD1930	IP 地址	只读	十进制
SD1931		只读	十进制
SD1932		只读	十进制
SD1933		只读	十进制
SD1934	子网掩码	只读	十进制
SD1935		只读	十进制
SD1936		只读	十进制
SD1937		只读	十进制
SD1938	默认网关	只读	十进制
SD1939		只读	十进制
SD1940		只读	十进制
SD1941		只读	十进制

注意: 以太网口参数寄存器均为只读, 如需修改 IP 地址, 必须使用 IPSET 指令。

4-2-4. 串口参数的名称及设定

假设 HD0~HD14 对应串口参数，则各寄存器代表的参数名称及设定如下表所示：

参数地址	参数名称及设定				
	MODBUS 通讯时 (HD0=1)	自由格式通讯时 (HD0=2)	X-NET 通讯时		Ethernet 通讯时 (HD0=3)
			OMMS (HD0=3)	TBN (HD0=3)	
HD0	网络种类 1: MODBUS; 2: 自由格式; 3: X-NET 通讯; 4: MODBU-TCP				
HD1	MODBUS 站号 1~254	波特率 见附表 1	网络号 0~32767	网络号 0~32767	网络号 IP 地址高两字节
HD2	传输模式 0: RTU 128: ASCII	帧格式 见附表 2	站点号 0~100	站点号 0~100	站点号 IP 地址低两字节
HD3	波特率 见附表 1	Free 属性 bit7: 1: 有起始符 0: 无起始符 bit6: 1: 有终止符 0: 无终止符	物理层类型 0: PHY_RS485 1: PHY_SOF (单向光纤环网) 2: PHY_OFPP (光纤点点网) 3: PHY_RS232 4: PHY_RS422 5: PHY_TTL (TTL 电平网)		
HD4	帧格式 见附表 2	起始符	链路层类型 0: TBN 1: HDN 2: CCN 3: PPFD 4: PPU 5: Ethernet		
HD5	重试次数 0~5	终止符	OMMS 属性 128: 支持周期通信, 否则不支持	波特率 见附表 1	子网掩码高两字节
HD6	回复超时 0~65535	帧超时时间 0~255	OMMS 波特率 见附表 1	令牌循环时间 1~60000 (ms)	子网掩码低两字节
HD7	发送前延时 0~255	回应超时时间 0~65535 (0 为无限等待)	OMMS 从站列表 数组中每个字节的 每一位表示该从站 是否可以访问 (主 站时有效, 即站点 号为 1)	最大站点数 1~100	网关地址高两字节
HD8	-	-	-	-	网关地址低两字节

【注】：表格中不包含自由格式通讯模式下的“缓冲位数”，故“缓冲位数”不能通过 CFGCR 和 CFGCW 指令读写，但可使用 MOV 指令读写，“缓冲位数”地址见附录 3。

附表 1：波特率

数值	波特率	数值	波特率	数值	波特率	数值	波特率
1	300 bps	7	19200 bps	13	256000 bps	19	1000000 bps
2	600 bps	8	28800 bps	14	288000 bps	20	1200000 bps
3	1200 bps	9	38400 bps	15	384000 bps	21	1500000 bps
4	2400 bps	10	57600 bps	16	512000 bps	22	2400000 bps
5	4800 bps	11	115200 bps	17	576000 bps	23	3000000 bps
6	9600 bps	12	192000 bps	18	768000 bps		

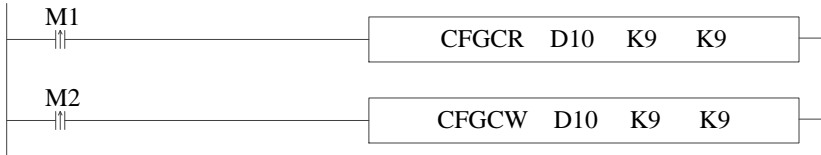
附表 2：帧格式

停止位		校验位			数据位长度		
Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
00: 1 位 01: 1.5 位 10: 2 位		000: 无 001: 奇 010: 偶 011: 空 100: Mask			000: 5 位 001: 6 位 010: 7 位 011: 8 位 100: 9 位		

4-2-5. 通讯口参数通讯案例

例 1：通过参数读指令 [CFGCR]和写指令[CFGCW]将 PLC 的网络参数读取到寄存器 D10~D18 连续 9 个寄存器中，在作修改后将 D10~D18 连续 9 个寄存器的网络参数写入到 PLC 的串口设置中。

PLC 编写的指令如下：



PLC1-自由监控				
监控 添加 修改 删除 删除全部 上移 下移 置顶 置底				
寄存器	监控值	字长	进制	注释
D10	0003	单字	16进制	
D11	C0A8	单字	16进制	IP地址前两位，C0对应K192，A8对应K168
D12	003C	单字	16进制	IP地址后两位，00对应K0，3C对应K60
D13	0000	单字	16进制	
D14	0005	单字	16进制	
D15	FFFF	单字	16进制	子网掩码前两位，分别对应255.255
D16	FF00	单字	16进制	子网掩码后两位，分别对应255.0
D17	C0A8	单字	16进制	默认网关前两位，分别对应192.168
D18	0001	单字	16进制	默认网关后两位，分别对应0.1

当 M1 置位后，触发 PLC 的网络参数读取，修改完网络参数后，置位 M2，即可将修改后的网络参数写入 PLC，写入后 PLC 断电再上电串口参数生效。

4-3. 以太网通讯相关标志位和寄存器

通讯相关寄存器

地址	查看方式	功能	说明
SD1905	16 进制	IP 网络号	IP 地址的前两个字节
SD1906	16 进制	IP 站点号	IP 地址的后两个字节
SD1907	16 进制	子网掩码	子网掩码的前两个字节
SD1908	16 进制		子网掩码的后两个字节
SD1909	16 进制	默认网关	默认网关的前两个字节
SD1910	16 进制		默认网关的后两个字节
SD1920	10 进制	发生异常的套接字 ID	发生异常的套接字 ID，仅在连接未建立时生效
SD1921	10 进制	错误码	1: 套接字 ID 不在限定范围内 2: 未注册的套接字 ID，发起了通讯请求 3: 通讯类型错误，不在允许范围 0---TCP 1---UDP 4: TCP 连接数超限，最大 32 个 5: UDP 连接数超限，最大 32 个 6: 通讯模式错误，不在允许范围，0---Server 1---Client
SD1930	10 进制	IP 地址	IP 地址的第 1 个字节
SD1931	10 进制		IP 地址的第 2 个字节
SD1932	10 进制		IP 地址的第 3 个字节
SD1933	10 进制		IP 地址的第 4 个字节
SD1934	10 进制	子网掩码	子网掩码的第 1 个字节
SD1935	10 进制		子网掩码的第 2 个字节
SD1936	10 进制		子网掩码的第 3 个字节
SD1937	10 进制		子网掩码的第 4 个字节
SD1938	10 进制	默认网关	默认网关的第 1 个字节
SD1939	10 进制		默认网关的第 2 个字节
SD1940	10 进制		默认网关的第 3 个字节
SD1941	10 进制		默认网关的第 4 个字节

通讯相关线圈

地址	功能	说明
SM1900	登陆远程服务器成功标志	远程连接成功置 ON
SM1901	以太网功能初始化完成标志	MODBUS TCP Server/TCP IP/ XNET
SM1902	连接网络设备标志	双网口机型第一个网口或单网口机型连接至交换机/路由/其他网络设备
SM1903	连接网络设备标志	双网口机型第二个网口连接至交换机/路由/其他网络设备
SM1921	以太网错误标志	产生 SD1921 中的任意错误时置 ON

4-4. 以太网通讯错误一览表

错误码	错误说明
0	通讯正常
1	需要 OPEN 的套接字已经建立了连接
2	创建套接字时返回错误
3	绑定到指定的端口失败
4	TCPServerAccept 失败
5	TCPClientConnect 失败
6	调用 Send、Recv、Close 时，指定的套接字未建立连接
7	调用 Send 返回失败
8	调用 Recv 返回失败
10	指定的发送数据长度大于允许范围
11	指定的接收数据长度大于允许范围
20	UDP 通讯时，收到的数据不是来自指定的 IP
21	UDP 通讯时，收到的数据不是来自指定的 Port
30	实际收到的数据长度大于指定长度
31	实际收到的数据长度小于指定长度
40	接收超时
50	指定目标端口号错误，MODBUS TCP 不是 502 端口； 使用端口越界（不在 1~60000 之间）
100	接收错误
101	接收超时
182	站号错误
183	发送缓存区溢出
400	功能码错误
401	地址错误
402	长度错误
403	数据错误
404	从站忙
405	内存错误（擦写 Flash）

手册更新日志

本手册的资料编号记载在手册封面的右下角，关于手册改版的信息汇总如下：

序号	资料编号	章节	更新内容
1	PD07 20220106 1.0	3-2-1	增加客户端数量
2	PD07 20220324 1.0	4-1-1	增加 TCP 保活说明
		4-1-6	更新通讯案例



微信扫一扫，关注我们



无锡信捷电气股份有限公司
WUXI XINJE ELECTRIC CO., LTD.

地址：江苏省无锡市滨湖区建筑西路 816 号

总机：0510-85134136

传真：0510-85111290

网址：www.xinje.com

邮箱：xinje@xinje.com

全国技术服务热线：400-885-0136