**TCP modbus 以VM7000为例**

http://simg.sinajs.cn/blog7style/images/common/sg_trans.gif

    TCP modbus預設的port 是502，，不是80。TCP調試助手在這裡下載  http://www.eastcent.com/Download/Software/tcp-assist.htm

   VM7000的Ethernet必須先設定好。和電腦在同一個局域網，假設IP為 192.168.0.199

範例一，讀取Ch1 ~ Ch6的數值

   發送hex ： 000100000006010400640006 ，得到以下結果。說明如下：

[](http://photo.blog.sina.com.cn/showpic.html#blogid=4dda073c0102wn7p&url=http://album.sina.com.cn/pic/001qopcMzy769BLrIf40e)

先了解 TCP modbus的格式：

1： MBAP header 有 7個 bytes（紅色粗體）

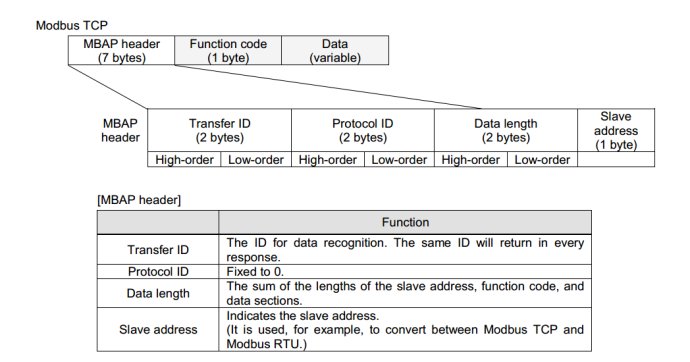
**00010000000601**0400640006

第一和第二個bytes 0001是Transfer ID，，兩個bytes，我們設為00 01

第三和第四個bytes 0000是Protocol ID ，，兩個bytes，預設為0000

第五和第六個bytes 0006是Data length，，兩個bytes，內容是以下這幾個bytes總數相加： Slave address（一個byte），function code（一個byte），Data長度（四個bytes,讀取暫存器的位置兩個bytes，讀取資料個數兩個bytes)

第七個byte是slave address , 我們設為 01

以上就是MBAP header的部分，共7個bytes。接下來就是function code和data  
[](http://photo.blog.sina.com.cn/showpic.html#blogid=4dda073c0102wn7p&url=http://album.sina.com.cn/pic/001qopcMzy769Erb9EWa6)

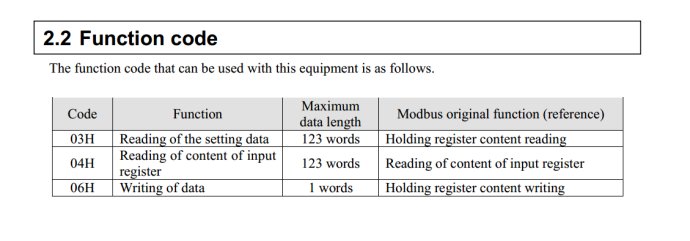
2：Function Code 和data

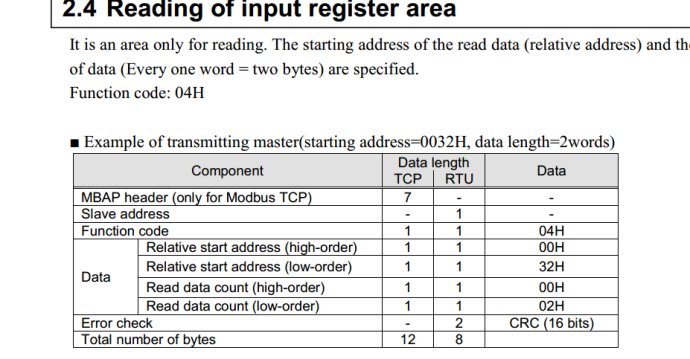
   第八個byte是funciton code，目的是讀取6個channel的溫度點，所以function code就用04

   第九，十兩個bytes是讀取的開始位置（相對位置），讀取1,6channel，相對位置的開始就是64，看參考資料二的，第2-6頁。所以是 00 64

   第十一，十二兩個bytes是讀取的數據個數（不是byte個數，每個數據是兩個bytes），共6筆數據，所以是 00 06

  总共发送12个bytes。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=4dda073c0102wn7p&url=http://album.sina.com.cn/pic/001qopcMzy76dUmFxpx0b)



3：回傳數據

00 01 00 00 00 0F 01 04 0C **F6 3C 00 00 FF FF 13 88 13 88 13 87**

共21個 bytes， 從第10個byte到第21個bytes才是數據內容，共12個bytes。兩個bytes代表一個數據。就是6個channel的值（紅色粗體字）。

两个bytes怎么转化为数据呢？

Channel 1就是 F6 3C , 超過 7FFF的就是負值 ，要減去 65536。所以這個溫度就是 -25.00 度。 F6 3C大於7FFF，所以要換算成十進位 ，F63C = 64036 , j減去 65536 = -2500 ，再除以100 ，就是數值  -25.00了

Channel 2 是 00 00 ，那就是0，不需轉換

Channel 3 ,是 FFFF , 算法和Channel 1 ，因為大於 7FFF，所以要減去 65536。計算結果是 -0.01

Channel 4 是 13 88 ，因為小于 7FFF，直接換算10進位，再除100，得出數值為 50.00

範例二·，開始記錄和停止記錄

發送 hex ： **00010000000601**060064AA01

  紅色粗體的7個bytes就是MBAP，看範例一的說明。

  第8個byte 06就是function code， 06是寫入register

  第9，10個byte，就是相對位置，查看通訊手冊的第2-20頁，得知run/stop 的相對位置是00 64

 第11,12個byte就是指令了，  AA01是run， AA00是stop

  如果回傳值是12個bytes，那就是成功執行。如果是9個bytes，就是有錯誤，要查錯誤代碼的意義，在2-2頁

參考資料：

1：TCP調試助手 ： http://www.eastcent.com/Download/Software/tcp-assist.htm

2：VM7000A PAPERLESS RECORDER COMMUNICATION FUNCTION OPERATION MANUAL  ，Mar.2014 Rev 5