

第 19 章：以太網通訊與安全防護

I-8437/8837, I-7188EG, 7186EG 與 Wincon-8xx7 有內建 網路高流量保護功能, 能防止諸如 惡意連續的 TCP SYN, TCP FIN, ... 等攻擊 (TCP flood attack) .

19.1: 網路安全防護

有幾種方式可以 經由 以太網路 來存取 Wincon-8xx7 內的資料.

1. 使用 Modbus TCP 通訊規約, Port 編號 502. (ISaGRAF 軟件 與 SCADA / HMI 就是這樣連的)
2. 使用 ftp (比如在 PC 上執行 Internet Explorer, 鍵盤輸入 “ftp://10.0.0.103”)
3. 使用 telnet (比如在 PC 上開啓一個 “Command” 視窗, 鍵盤輸入 “telnet 10.0.0.103”)
4. 使用 Web server (Wincon 的 Web HMI 功能使用的方式)

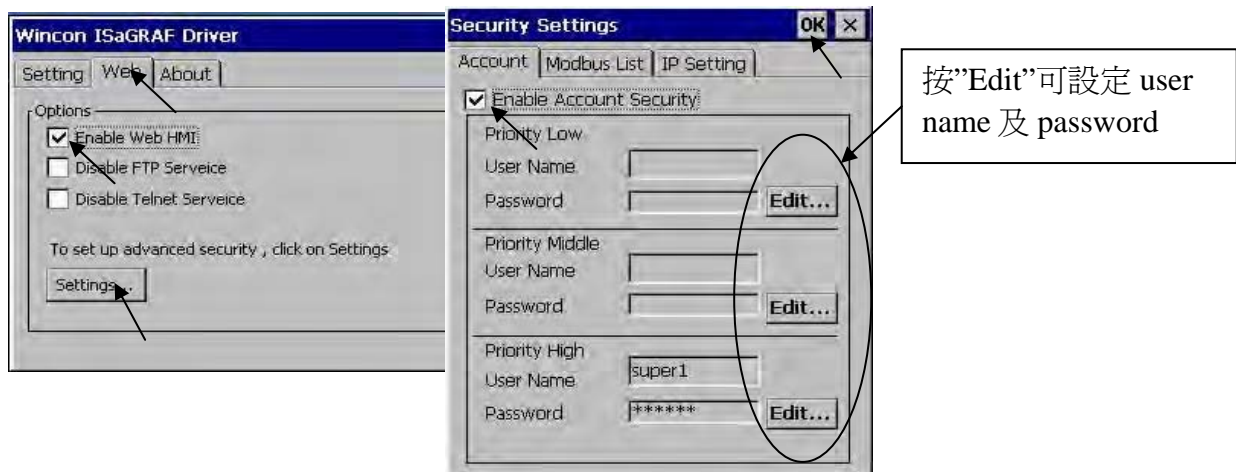
注意: 1. 若是使用 I-8xx7 與 I-7188EG, 只有方式 1 可使用.

2. 若是使用 W-8047 / 8347 / 8747 / 8046 / 8346 / 8746 , 要使用 “ftp”, “telnet”, “Web HMI” 與 “Modbus TCP/IP”, 請連您的 PC/HMI 到其上的 LAN1 網口, 並且請使用 ICP DAS 的 Industrial Ethernet Switch 產品 “NS-205” 或 “NS-208” .

爲了安全, 您可以 開啓 Wincon 驅動程式的對話框, 關閉第 2 及第 3 項功能, 如下.

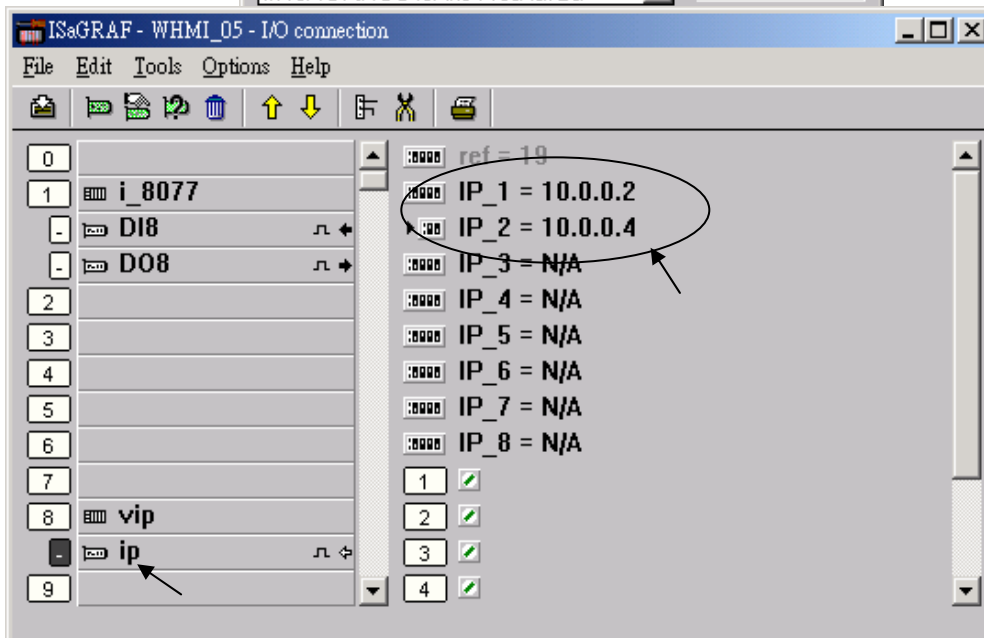
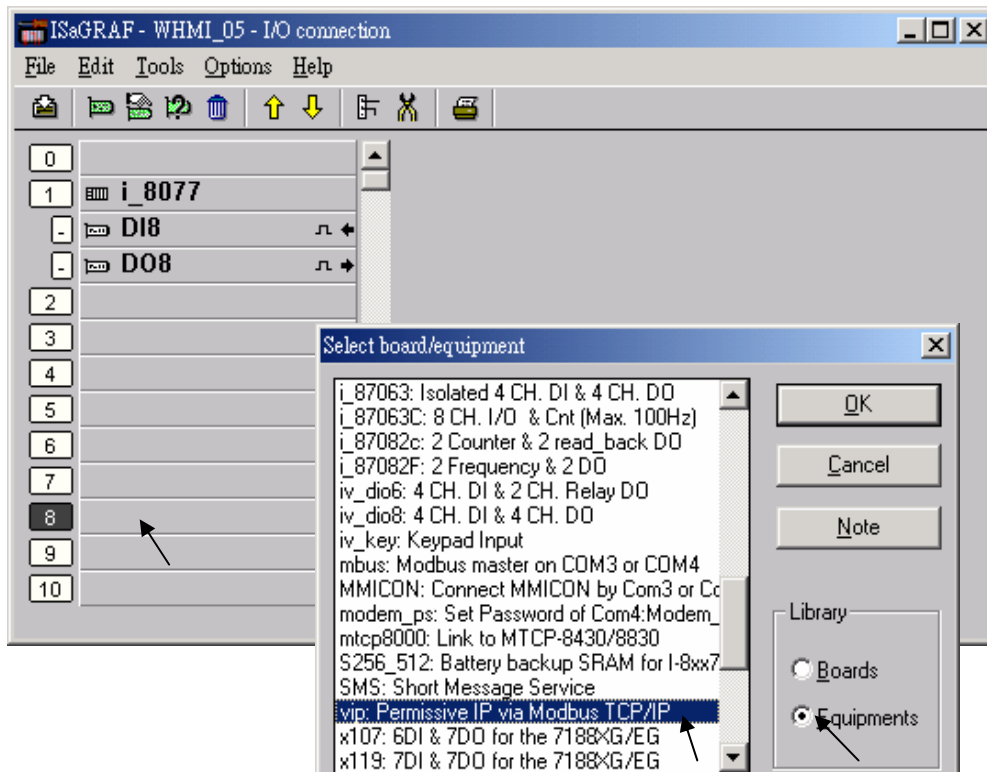


關於第 4 項, 請設好必要的 User name 及 Password 來保護.



關於第一項 Modbus TCP/IP 的保護, 使用者可以在控制器上設定最多只開放到 8 組 PC / SCADA / HMI 的 IP 可允許連進來, 方法如下.

請在 ISaGRAF I/O 連結視窗內使用“vip”虛擬板卡. 最多可設立 8 組 IP 允許用 Modbus TCP/IP 通訊規約連進來. 若控制器內沒有使用“vip”, 那表示, 任何 IP 都允許用 Modbus TCP/IP 連進來. 如果使用了“vip”但都設為“N/A”將沒有任何 IP 允許用 Modbus TCP/IP 連進來. (包含 ISaGRAF 也連不進來)



19.2: 使用 UDP 來傳遞或接收訊息 到 PC / HMI 或設備

若用 W-8347 / 8747 , 可以選 LAN1 或 LAN2 的其中一個網口來使用 UDP 功能. 並請用 ICP DAS 的 Industrial Ethernet Switch 產品 NS-205/208. (啓用 W-8347/8747 的 LAN2, 請參閱 附錄 F)

請確認控制器驅動是否為 I-7188EG: 2.18 版, I-8437/8337: 3.20 版, W-8xx7: 3.37 版 或更高版本. 請在 I/O 連結視窗內連上 1 個 udp_ip, 之後於程式內使用 udp_recv 與 udp_send 來接收或傳遞訊息.

The screenshot shows the ISaGRAF configuration interface with the following parameters:

```

ref = 127A
this_port = 12001
this_ip = xxx.xxx.xxx.
reserved = 0
Send_Time_Gap = 250
reserved = 0
reserved = 0
reserved = 0
reserved = 0
port1 = 12001
to_ip1 = 5000
port2 = 12001
to_ip2 = N/A
    
```

Annotations in the image provide details for these parameters:

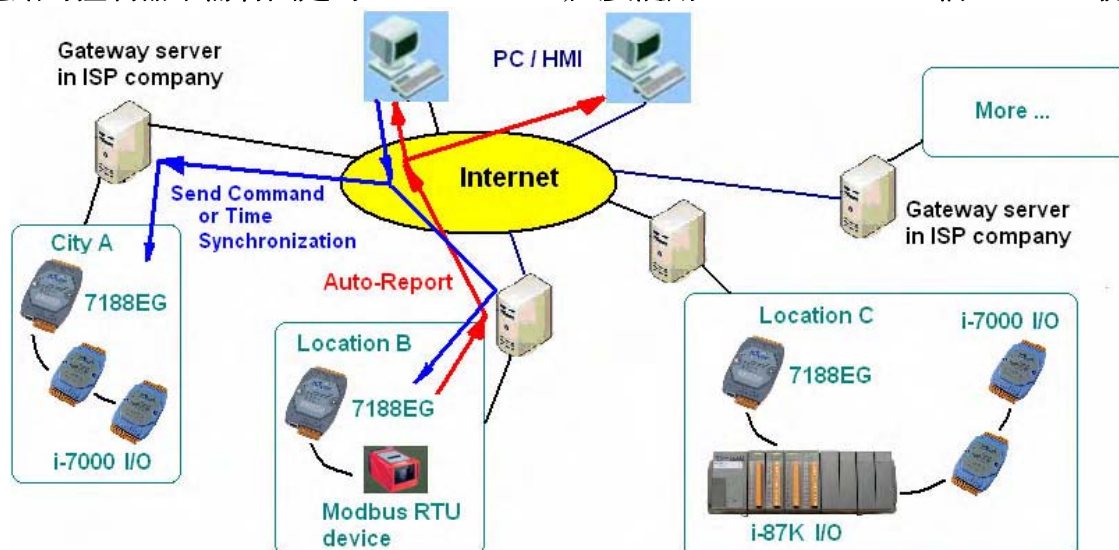
- “Send_Time_Gap” 參數:** 每筆要傳出去的 Message 需間隔多久, 才可傳第 2 筆. 單位為 ms. 可以設成 10 ~ 5000. 跟遠方接收的設備特性有關.
- “This_port” 參數:** 設定 UDP Server 是要使用那個 UDP Port 編號來接收訊息. 建議是設成 1000~65535 號. 內定值是 12001 號
- “This_ip” 參數:** 只有使用雙網口的 Wincon-8x47 / 8x46 才需設定. 設定要使用 UDP 功能在那個 IP 上 (雙網口的 Wincon-8x47 / 8x46 的 LAN1 與 LAN2 需設為不同的 IP, 若要啓用 LAN2, 請參考附錄 F).

下方這些參數只有要使用 UDP 傳送功能的 Wincon 與 I-8437/8837 與 I-7188EG 才需要設, 若不啓用它, 請將 IP 設為 N/A

IP1 到 IP4 參數: 啓用的 UDP 傳送功能是要傳送訊息到遠方那個 IP. Wincon 最多可設 4 個 IP 連線, 7188EG and i-8437/8837 最多可設前 2 個 IP 連線.

Port1 到 Port4 參數: 對應的遠方 IP1 到 IP4 是使用 UDP 規約的那個 Port 編號?

i-7188EG, i-8437/8837 與 W-8347/8747 可使用 UDP 功能主動回報“採集”與“控制”資料到 區網或遠方 Internet 的 PC/HMI. 遠方的 PC / HMI 在收到此資料後, 也可被動對 Wincon 作“時間校正”或下達必要的“控制命令”. 範例程式與說明, 請參考 ISaGRAF FAQ-065. 此應用有一個優點, 位於各個地點的控制器不需有固定的“Internet IP”, 只要能上 Ethernet Port 上網 Internet 就可用.



UDP_Recv:

此函式可用來測試與接收遠方 PC 或設備所傳過來的 UDP 訊息.

如以下 ST 程式碼:

```
(* 測試是否有 UDP 訊息傳進來, 若有也會收進來 *)  
(* Msg1 宣告為 internal Message 變數 *)  
(* 如果 udp_recv() 回傳 " (2 個單引號中間無資料 為 空字串), 表示沒有資料傳進來 *)  
Msg1 := udp_recv() ;
```

注意:

1. W-8xx7 的 UDP 功能的接收的 buffer 大小為 8192 byte , 包含每個字串的結尾符號 1 byte 而 I-7188EG 與 I-8437/8837 的接收的 buffer 大小則為 2048 byte.
2. 如果一次進來太多個字串 導致 接收的 buffer 無法及時消化掉, 新進來的字串會取代掉 最早進來的那筆 字串.

UDP_Send:

此函式可用來傳送訊息到遠方 PC 或設備. (7188EG , I-8x37 不支持 UDP 傳送功能)

如以下 ST 程式碼:

```
(* TMP 宣告為 Internal Boolean 變數 *)  
(* 第 1 個參數: 傳送到那個 UDP 連線, 可以是 1 到 4. 定義在 虛擬 I/O 板 "udp_ip" 內 *)  
(* 第 2 個參數: 要傳送出去的 Message *)  
(* 若 udp_send() 傳回 True 表示成功, False 表示 buffer 滿了 或 該連線未在 "udp_ip" 內定義好 *)  
TMP := udp_send( 1, 'Alarm1' ) ;
```

注意:

1. W-8xx7 的 UDP 功能的傳送的 buffer 大小為 2048 byte , 包含每個字串的結尾符號 1 byte 表示 每個 ISaGRAF PLC Scan 最多只能傳送出 2048 個 byte .
2. 請不要很頻繁的傳送大量資料出去, 跟 "udp_ip" 內的 "Send_Time_Gap" 參數有關, 若資料太多了, 消化不掉, 會積在傳送的 buffer 內, Buffer 若滿了, 使用 udp_send() 會傳回 False, 表示滿了, 無法再塞入更多的 Message. 每個 PLC Scan 對每個 UDP 連線, 只能消化 1 筆 Message (傳出 1 筆)

範例程式:

請參考 Wincon-8xx7 CD-ROM:\napdos\isagraf\wincon\demo\ **Wdemo_19** 與 **Wdemo_20** 或

ftp://ftp.icpdas.com/pub/cd/wincon_isagraf/napdos/isagraf/wincon/demo/

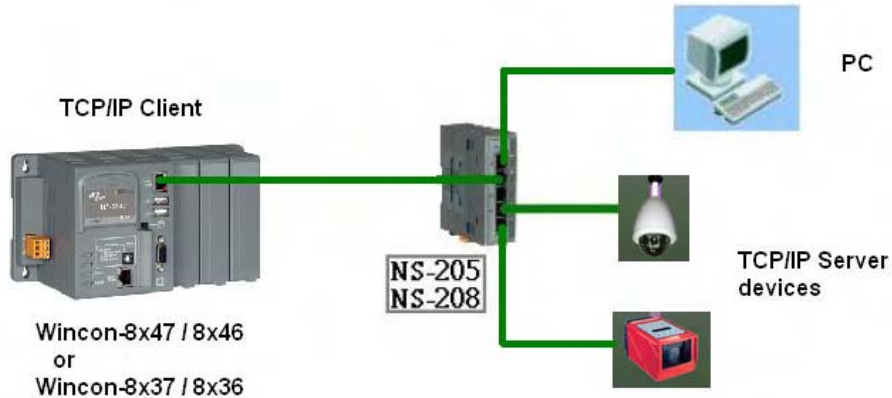
如果您的 ISaGRAF 內找不到 "udp_ip", "udp_recv" 與 "udp_send" 請到以下網址下載

<http://www.icpdas.com/products/PAC/i-8000/isagraf.htm> "ICP DAS Utilities For ISaGRAF.zip". 並執行其內的 "Setup.exe" 來安裝到您 PC 的 ISaGRAF 軟件內.

測試工具: 有個好用的工具程式可在 PC 的 "Command" 視窗上執行來接收 Wincon-8xx7 傳出的 UDP 訊息. 位於 W-8xx7 CD-ROM:\napdos\isagraf\some_utility\udp_test\udp.exe 或 ftp://ftp.icpdas.com/pub/cd/wincon_isagraf/napdos/isagraf/some_utility/udp_test/ 內

19.3: 使用 TCP / IP Client 功能來 傳送 / 接收 / 主動回報 訊息

Wincon-8xx7 / 8xx6 從它的 驅動程式 3.36 版起 支持TCP / IP Client功能. 請訪問以下網址取得 <http://www.icpdas.com/products/PAC/i-8000/isagraf-link.htm> . 若您的ISaGRAF軟件上找不到 虛擬 I/O 板 ”Tcp_clie” 與 , 請到 <http://www.icpdas.com/products/PAC/i-8000/isagraf.htm> 下載 “ICP DAS Utilities For IsaGRAF.zip” . 並執行其內的 “Setup.exe” 來安裝到您 PC 的 ISaGRAF軟件內



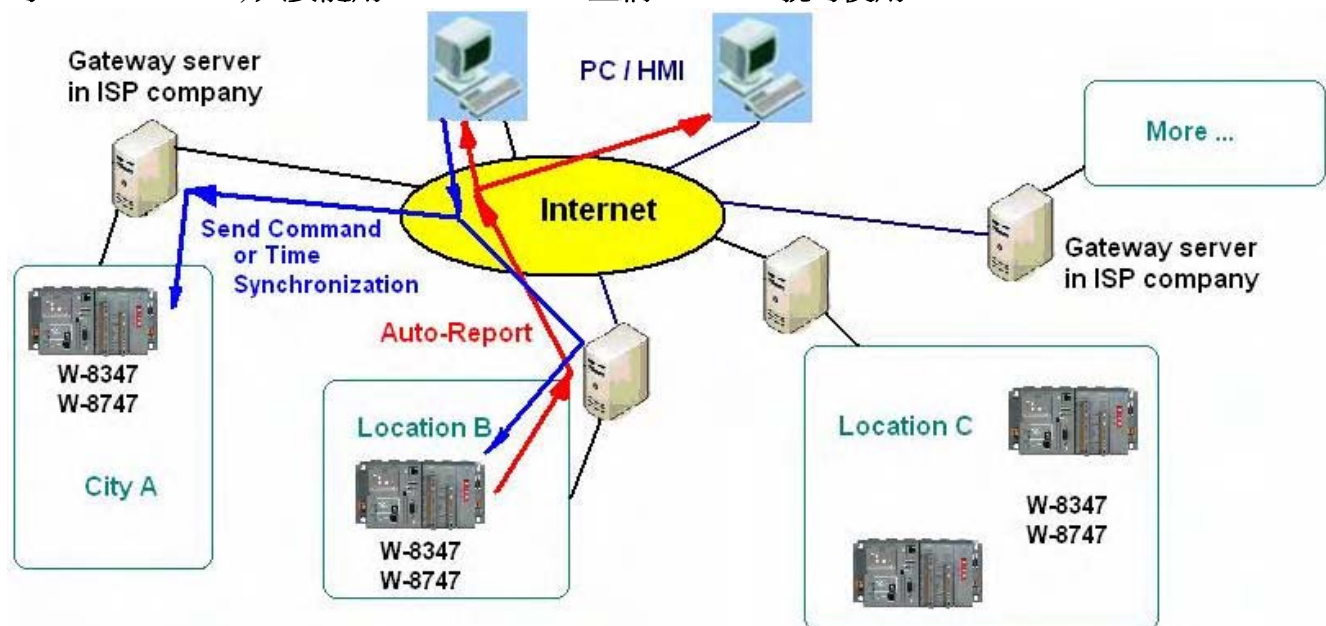
使用 TCP / IP Client功能的 範例程式為Wdemo_32.pia, Wdemo_33.pia 與Wdemo_60.pia (可到以下網址下載 ftp://ftp.icpdas.com/pub/cd/wincon_isagraf_napdos_isagraf_wincon_demo/)

注意: 要跟 W-8xx7 的 TCP/IP Client 連線的遠方的 PC 或設備需支持 TCP/IP Server 功能才連的上.

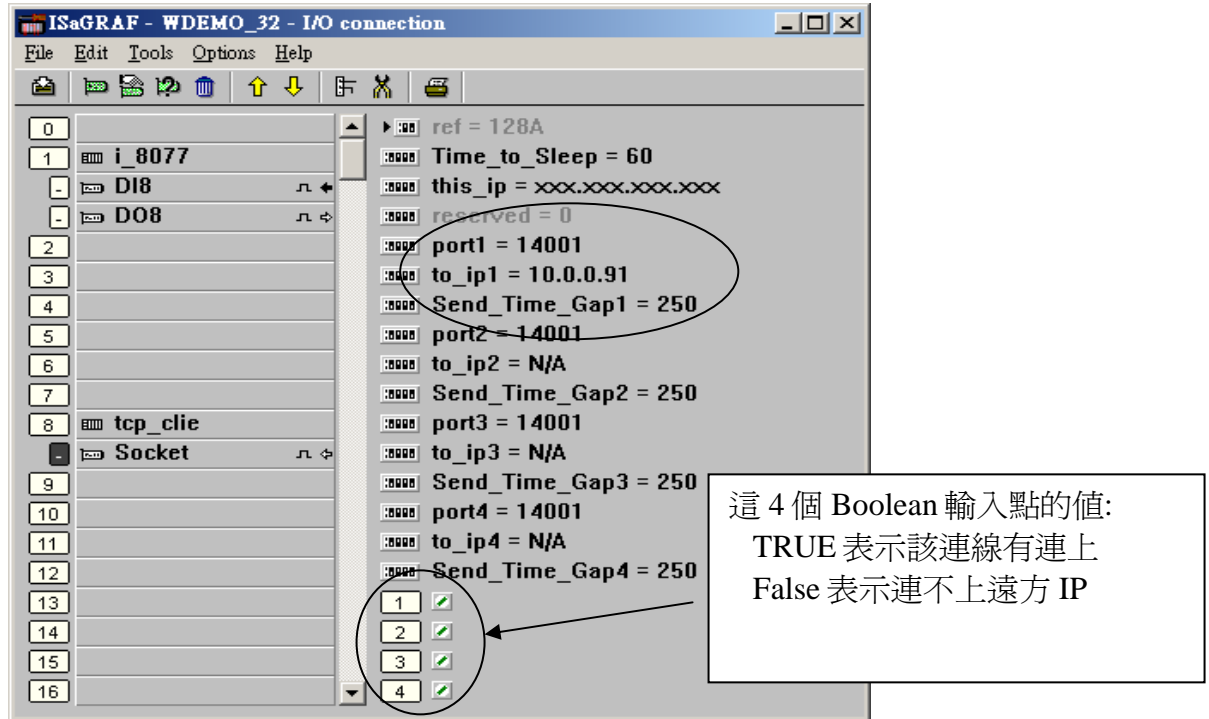
***** 好用的應用 *****

(更多的說明與範例程式, 請參考 www.icpdas.com – FAQ – Software – ISaGRAF - 064)

Wincon-8347 與 W-8747 可使用 TCP / IP Client 連線功能 主動回報 “現場採集資料” 或 “控制資料” 到遠方的 PC / HMI . 遠方的 PC / HMI 在收到此資料後, 也可被動對 Wincon 作 “時間校正” 或下達必要的 “控制命令” . 此應用有一個很大的優點, 位於各個地點的 Wincon 不需有固定的 ”Internet IP” , 只要能利用 Ethernet Port 上網 Internet 就可使用.



要使用 TCP / IP Client, 請先在 I/O 連結視窗內連上 “Tcp_clie”. 最多可連 4 個遠方 IP.



“Time_to_sleep” 參數: 值可以是 10 到 600, 或 0. 單位為秒. 設為 0 表示, 永遠與遠方 TCP / IP Server 設備 保持連線 (除非是通訊有問題). 設為 10 到 600 秒, 表示若經過了這段時間以上沒有任何資料傳出 或 接收, 自動先關閉 TCP / IP 連線. 但只要有 新訊息要送出, 就會自動再連上.

“this_ip” 參數: 只有使用雙網口的 Wincon-8x47 / 8x46 才需設定. 設定要使用 TCP / IP Client 功能 在那個 IP 上 (雙網口的 Wincon-8x47 / 8x46 的 LAN1 與 LAN2 需設為不同的 IP, 若要啓用 LAN2, 請參考附錄 F)

“port1” 到 “port_4” 參數: 設定成跟遠方的 TCP / IP Server 設備 所使用的 port 編號一樣.

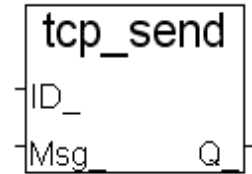
“to_ip1” 到 “to_ip4” 參數: 遠方的 TCP / IP Server 設備的 IP 地址. 若不使用, 請設為 “N/A”

“Send_Time_Gap1” 到 “Send_Time_Gap4” 參數: 每筆要傳出去的 Message 需間隔多久, 才可傳 第 2 筆. 單位為 ms. 可以設成 10 ~ 5000. 跟遠方接收的設備特性有關.

設好 “Tcp_Clie” 的所有參數後, 就可在程式內使用 “Tcp_send” 或 “Tcp_rcv” 函式 來 傳送 或 接收 TCP / IP 訊息.

Tcp_send

TCP Client 傳送 Message 到遠方的 TCP / IP Server (可以是 PC 或 設備)



注意:

每個 Wincon-8xx7 TCP / IP Client 連線的 傳送 buffer 大小為 4096 byte. 如果傳送太頻繁 使得 Wincon 來不及消化掉, 導致 傳送 buffer 滿的話, 會把最早的 1 個或數個未被送出的 Message 刪掉, 來容納新的 TCP / IP Message. 每個 PLC Scan 每個連線最多只能傳出 1 個 TCP / IP Message. 傳送的時間 間隔 需在 “Tcp_clie” 的 “Send_Time_Gap” 內定義好 (跟遠方設備特性有關)

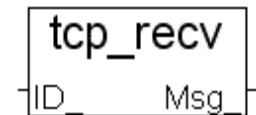
ID_	Integer	傳送到那個 TCP / IP 連線, 可以是 1 到 4 (各連線參數定義於 “Tcp_Clie” 虛擬板卡內)
Msg_	Message	要傳出的 Message

回傳值:

Q_	Boolean	True: 表示成功, False 表示 有錯誤發生 (比如, ID_設錯, 設成比 4 大, 或該連線沒在 “Tcp_clie” 內定義好 .
----	---------	---

Tcp_recv

TCP Client 接收遠方 TCP / IP Server (PC 或設備) 送過來的 Message



注意:

W-8xx7 的 TCP / IP Client 的接收 buffer 大小為 4096 byte. 如果太多資料傳進來, 來不及消化掉導致 buffer 滿了, 最早進來的 1 筆或數筆 Message 會被刪掉, 用來容納新進來的 Message.

ID_	Integer	傳送到那個 TCP / IP 連線, 可以是 1 到 4 (各連線參數定義於 “Tcp_Clie” 虛擬板卡內)
-----	---------	---

回傳值:

Msg_	Message	收到的 Message. 若回傳" (2 個單引號中間無資料 為 空字串), 表示 沒有資料傳進來
------	---------	--

有個好用的 “Tcp_Server” 工具程式 可將 PC 模擬(仿真) 成 TCP / IP Server. 它放在

Wincon-8xx7 CD-ROM: \napdos\isagraf\some_utility\ 或

ftp://ftp.icpdas.com/pub/cd/wincon_isagraf/napdos/isagraf/some_utility/ 內

請把整個 “Tcp_server” 目錄 Copy 到你的 PC 內, 之後開啓一個 “Command” 視窗, 鍵盤輸入 “tcp3 <port_No>” 來執行它, 比如 “tcp3 14001”

這個工具程式 會等 TCP / IP Client (W-8xx7) 連進來, 然後接收它的訊息並顯示, 同時會 回覆 相同的訊息給 Wincon-8xx7 的 TCP / IP Client.

使用 TCP / IP Client 功能的 範例程式為 Wdemo_32.pia, Wdemo_33.pia 與 Wdemo_60.pia (可到以下網址下載 ftp://ftp.icpdas.com/pub/cd/wincon_isagraf/napdos/isagraf/wincon/demo/)