



Integrated Systems and Control
Research and Development
1652 Stillwater St.
White Bear Lake, MN 55110

DATE: October 22, 2003
TO: ISAC Users
FROM: Ron Follmer
RE: PCMNET Peer To Peer (P2P) Application Notes

Revision history

7/10/2003 original

Background

Beginning with the release of V7.20 firmware for the ISAC PCMNET Control, a Peer to Peer communications protocol has been added to allow multiple PCMNET controls on an Ethernet LAN to exchange Point values with minimal user programming.

The PCMNET P2P protocol operates in a network "Client/Server" model. If a PCMNET needs to "read" a Point value from another Peer on the network, it is considered to be a "Client" of the network. Conversely, the Peer that will receive the request for Point data is considered to be a "Server" of the network. A particular PCMNET can be a Server for any number of Clients that make requests for data. The Server PCMNET can receive and process requests from any device on the network regardless if whether that device is defined as a "Peer" in the programming of the Server. On the other hand the Client PCMNET that is making the request for Point data MUST know the IP address of the Server, so the Server must be defined as a "Peer" in the programming of the Client PCMNET. The following paragraph describes the process of defining a Peer. In general, it is best and least confusing if all the Peers that will communicate with each other are defined in each Peer's programming.

Defining the Ethernet Configuration of each PCMNET on the Network

Before communications can be enabled between two or more PCMNETs on an Ethernet network, each individual PCMNET board must be configured to access the network. This involves setting the various parameters in the Ethernet Port Configuration screen such that the board can be accepted as a network device. Changes to values on this screen are not adopted by the hardware until the PCMNET board is Reset by cycling power or by software initialized reset action.

Referring to the Ethernet Port Configuration screen in the firmware or the Simulator software, the required settings are described below.

ETHERNET PORT CONFIGURATION

Hostname: This field holds a description that is used when the Ethernet network contains a DHCP Server computer which will provide IP addresses to devices attached

to the network automatically. In most cases the default value of "PCMNET" is recommended. When a DHCP Server computer lists this host name, a unique serial number will be appended to the end of the host name ie "PCMNET774". That way each and every PCMNET board on the network will have a unique host name. This full host name is also displayed on the Run Mode Menu screen.

Deflt Domain Name: When your network contains a Server computer that has defined a Domain Name, you may enter that domain name for this PCMNET board. An example of a Domain Name is "PCMNET774.ronscomputer.com". Private networks may or may not maintain a domain name so this field is optional. The default value for this field is blank.

DHCP Enabled?(Y/N): Enter "Y" if your network contains a DHCP Server computer that will provide IP address and the subnet mask for all the devices connected to the network. If your network does not contain a DHCP Server computer, then enter "N". When the value is "N", you must provide a valid IP addresses and the subnet mask value below.

BOOTP Enabled?(Y/N): Enter "Y" if your network does not contain a DHCP Server, but does contain a BOOTP Server. A BOOTP Server is a predecessor of the DHCP Server.

Default IP: The default IP address is the address that will be assigned to this PCMNET board when neither a DHCP or BOOTP Server is provided on your network. For a "unsupervised" local network, IP addresses in the range of 10.0.0.1 to 10.0.0.255 or 192.168.0.1 to 192.168.0.255 are typically used. If you have a "supervised" network, one that contains many devices not involved with your control system, there is probably someone who has determined what IP range to use and ALL the devices on the network MUST adhere to that policy. EACH AND EVERY DEVICE ON THE ETHERNET MUST HAVE A UNIQUE IP ADDRESS. Note that the Subnet Mask parameter MUST be coordinated with the default IP addresses (discussed below).

Default Subnet Mask: The Subnet Mask limits the ranges of IP addresses that can be addressed by a particular device. This parameter MUST be coordinated with the default IP address discussed above. In most cases a Subnet Mask of "255.255.255.0" is used. If your network is "supervised", this mask value will be established already and should be set the same as all the other devices. A Subnet Mask of "255.255.255.0" will enable up to 256 devices to access each other on the network, ie 10.0.0.0 to 10.0.0.255 are all IP addresses that will be accessable within the default mask of "255.255.255.0".

Default DNS IP: If your network provides a DNS Server that allows domain names to be used to access peer devices rather than IP address, then enter the IP address of the DNS Server. If no DNS Server is present on the network, enter the "Default IP" address described above in this field. THIS FIELD MUST HAVE A VALUE THAT IS NOT BLANK.

Alternate DNS IP: Your network may have more than one DNS Server. Enter the secondary DNS Server IP in this field. If there is none or only one DNS Server, leave this field BLANK or enter "0.0.0.0".

Default Gateway IP: If your network provides a Gateway Server to allow accessing of other networks or the Internet directly, enter the IP address of that Gateway Server. If there is no Gateway Server, enter the "Default IP" address described above. THIS FIELD MUST HAVE A VALUE THAT IS NOT BLANK.

Telnet Server Enabled?(Y/N): The PCMNET contains a Telnet Protocol Server which allows a User with a computer and Telnet Client software (such as ITERM) to access the PCMNET via the Ethernet network and see the same interface screens available to Users who connect with the PCMNET via Modem or direct serial cable. Generally this server is always Enabled. Depending on the network design, an administrator may wish to disable this access means. Enter “Y” to enable this server.

Telnet Port#: The standard port number for this protocol is 23. Some network designs may wish to change this port number.

HTTP Server Enabled?(Y/N): The PCMNET contains an Http Protocol Server which allows Users to access information in the PCMNET via Browser software. Generally this server is always Enabled. Depending on the network design, an administrator may wish to disable this access means. Enter “Y” to enable this server.

HTTP Port#: The standard port number for this protocol is 80. Some network designs may wish to change this port number.

ModbusTCP Server Enabled?(Y/N): The Peer to Peer communications between PCMNETs is done using the Modbus TCP Protocol. You must ensure that this parameter is set to “Y” to allow Peer to Peer communications. A setting of “Y” is the default setting. In rare instances when only one PCMNET is used in a control system, you may want to disable this protocol server for security reasons.

ModbusTCP Port#: The standard port number for this protocol is 502. Some network designs may wish to change this port number.

Use 10BaseT for Mailboxes?(Y/N): PCMNET Mailbox logic may be configured to send email alarm messages. It is necessary to direct whether those email interchanges should be attempted via the Ethernet port or be reserved for a Dialup connection to send via the Internet. Enter “Y” if all email activity should be directed to the Ethernet 10BaseT port. Note that there is a similar question asked on the Dialup Internet Configuration screen; entering “Y” will automatically change the other configuration to “N”. They are mutually exclusive.

Email Check Interval: When a POP Server has been defined in the Email Configuration Screen, the PCMNET will attempt to retrieve incoming emails that adhere to a specific format and structure. This parameter determines the number of seconds between retrieval attempts. By default, the value is 300 seconds, 5 minutes.

Log Email?(Y/N): Enter “Y” if you want all Mailbox emails sent or received to be logged in the Activity Log. By default this value is “N”.

Defining PCMNET Peers on the Network

To allow one PCMNET (Peer) on a LAN to communicate with another PCMNET (Peer), the must know each other’s IP address. The IP address and a few other pieces of information for each Peer that will be conversing is entered in the “Peer Definition” screen. This screen is accessed from the Program Mode Menu -> “8) Remote I/O Definitions Menu” -> “2) 10BaseT Ethernet Peer Definitions “. Select the particular Peer (up to 16 Peers can be defined), or select an undefined one to define a new Peer. When the Peer has been selected, the “ETHERNET I/O DEVICE DEFINITION “ is displayed.

ETHERNET I/O DEVICE (Peer) DEFINITION

Description: Any 15 character text description. This text will be displayed on the select menu and other places that the peer is referenced.

Hostname or IP Addr: Enter the IP address of the Peer being defined if static IP's are used. If there is a server with DNS on the LAN, you can use a domain name in place of an IP address (ie fred.mynetwork.net).

Type(1=Generic,2=ISAC-Smart): If this peer is to be used for pure I/O and it is not another ISAC PCMNET control, select Generic. Otherwise, for any PCMNET P2P, select ISAC-Smart. At the time of this writing, no pure Ethernet I/O devices (Generic) have been qualified for use with the PCMNET.

Enabled(Y/N): Enter "N" if you wish to ignore the use of this Peer. This is used to temporarily remove a Peer from any P2P communication attempts to save network time delays due to timeouts waiting for a Peer to be available.

Default Data Format(W=word,F=float): All ISAC-Smart PCMNET controls actually will force this setting to be "T" for text data format. It will automatically be set to "T" in this case. Only dumb Ethernet I/O devices will require a setting of W or F (none have been qualified for use with the PCMNET as of yet).

Float Byte Order(H=high first,L=low first): Define the word-order that the Peer will require. By default all PCMNET P2P controls use "H" (high word first). This default can be changed for a PCMNET in the "System Definitions" screen. The only reason that this setting would not be "H", is if a remote device such as a GUI, requires a particular order for all devices on a LAN being monitored.

Pt to Enable Reads(0=never,1-480,999=always): The user may elect to prevent Reads from this Peer based on PCMNET programming. A setting of "0" will prevent all reads, a setting of "999" will always enable reads of Point data from this Peer. A Point number will specify logic to control this feature.

Pt to Enable Writes(0=never,1-480,999=always): The user may elect to prevent Writes to this Peer based on PCMNET programming. A setting of "0" will prevent all writes, a setting of "999" will always enable writes of Point data to this Peer. A Point number will specify logic to control this feature.

Control Mode for Writes(N=norm,C=chg): The user may select "N", which will force writes to Peer Point values each scan cycle. The frequency of this Peer scan may be specified in the "System Definition" screen. Entering "C" means that a value to be written to a Peer will only be sent if the value changes.

Application Best Practice

We recommend that the Peers be defined exactly the same in each of the Peer's programming. For instance if there are 3 Peers (we'll call them Pcm1, Pcm2 and Pcm3) in the network, define Peer #1 as Pcm1 in the programming of all 3 PCMNETs. In fact, once the programming for Pcm1 has been completed, the "PR.dif" file of the program can be copied directly to the program file sets of Pcm2 and Pcm3. If a Peer's program refers to Peer #1, and it is referring to itself, the firmware detects this and it will actually exchange point data with itself. That way a nearly identical program can be written for all the Peers and Peer #1 will refer to the same physical controller regardless of which Peer's program is doing the reference.

Getting Point Data from a Peer

There is a Rule Operand function defined that will specify a Point value of a particular Peer defined in the Trinet program.

PRxx_yyy: Using a Rule operand such as PRxx_yyy (where xx=peer# and yyy=point#) will specify a Point value located in a Peer device. For instance PR1_100 will be evaluated and cause the value of Point 100 in Peer #1 to be retrieved and used wherever the PR1_100 operand is found. This operand may be used anywhere a Rule Operand is permitted.

If a Peer is unavailable/unreachable for more than a few minutes, the last known value will be substituted if one has been successfully obtained in the past. If the Peer has never been able (since the last reset/powerup) to obtain a PR value, it will read as a 0.0 or OFF value.

If a local Point has a default "Equal To" value definition of PRxx_yyy, and the remote Peer is unavailable/unreachable, Rules written for that local Point will take priority and allow the value of the local Point to be determined from the Rule rather than from the PR... value. In this way, local logic can take over if the remote Peer device is off-line.

In the majority of cases, the PRxx_yyy function will be used to fetch a remote value to place into a local Point value. Care must be taken to ensure that the local Point and the remote Point are of the same type. For instance, it would make no sense to place a Time of day value retrieved from Peer 1's Point 100 (a time type point) and place it's value into a digital local Point. The remote Point and the local Point should be of the same types.

Putting/Sending a Point value to a remote Peer

To actively send a Point value to a Peer, a Rule must be used. New for the P2P PCMNET, is that all Rules may modify local Points OR they may be used to modify a remote Point located in a Peer. To accomplish this, enter "PRxx_yyy" in place of the usual Point Number in the top/first field of a Rule Definition. In fact, three different types of values may be entered as the "object" of a Rule. Entering "230" will mean local Point 230. Entering "P230" will also refer to local Point 230. Lastly, entering "PRxx_yyy" will refer to a remote Peer Point value (no local Point change will result).

Other Rule Operands of interest

ETH: This Rule function returns a True/ON result when the Ethernet Port has a valid IP address (if DHCP or BOOTP is used) and is ready for use.

DTH: Rule function returns a True/ON result when a valid Dial-up Internet connection has been established. This means that an ISP has been called via Modem, a valid username and password has been validated, and an IP address and mask has been obtained.

MBD: Rule function returns True/ON when one or more Internet-dependent Mailbox has been triggered and is waiting for a valid Internet connection before accomplishing it's email or other Internet/Ethernet function. This function is useful to trigger logic to force a

Dial-up connection when an alarm condition exists and needs to be reported. Once a valid Internet connection is present, the Mailbox logic will complete it's work. Note that you must ensure that the Dialup connection is designated as the email port (as apposed to the Ethernet port which is always ready).

NST: Rule function returns the average network scan time for both Peer to Peer and Modbus network activity combined. The value returned is in seconds.

ALM: Rule List function which can examine the Alarm Log and return a True/ON value when an open (still pending) alarm condition exists in the log. Using the code for a Peer Communications failure will allow the user's logic to detect that any of the Peers is not communicating or even that a particular Peer is not communicating. Here is the current list of codes and an example of the function to detect ANY Peer that has stopped communicating.

<u>Alarm Description</u>	<u>PCMNET Alarm Type</u>
Bad CRC/Network Errors	2
Relay/DO Fault	3
Low Battery	4
AI Range Error	5
Act'ly Log Full	6
Prog Corrupted	7
User Log Alarm	8
Trinet Pwr Fail	9
Mailbox Failure	10
Alarm Point ON	11
Local Access	15
No Network	1
User Log Corrupted	13
Act'ly Log Corrupted	14
Mn't Log Corrupted	15
Alarm Log Corrupted	16
Modbus Ntwk Slave Error	17
Ethernet Chan Error	18
XML Parse/Create Error	19
Ethernet Ntwk Peer Error	20

Syntax: *ALM alarm type, alarm related item#, alarm related point.*

The *alarm related item* is: The item number such as the Mailbox # recorded along with Mailbox Failures. Enter 0 to ignore related item.

The *alarm related point* is: The point number that is recorded along with certain alarm types such as "Alarm Point ON". Enter 0 to ignore point.

Example: *ALM 20, 0, 0* returns TRUE if any Ethernet Peer records an open alarm in the Alarm Log.