Quick Talking to ControlLogix (PCCC-style)

1 Packet Formats

1.1 TCP Socket

The "explicit unconnected messaging" we are doing uses a normal TCP socket opened to remote TCP port 0xAF12 (or 44818 decimal).

For this to work you need to enable PCCC command processing in RSLogix ... which means little more than mapping AB file numbers to ControlLogix data objects. It is easiest to create arrays of 16-bit INT's in the ControlLogix, otherwise the tendency for ControlLogix to like 32-bit alignment will complicate your exchange.

2 Ethernet/IP "Register Session"

This packet must be issued on a new TCP socket to register a formal Ethernet/IP session. A 4-byte "session handle" is returned that MUST be reused on all future requests. Technically, we should issue an "Unregister Session" command before ending, but closing the socket works as well.

2.1 Request (You send to ControlLogix)

Offset	Value	2.2 Description
0 / 0x00 **1 / 0x01**	**0x65** **0**	Ethernet/IP Encapsulation Command: Register Session
2 / 0x02 **3 / 0x03**	**0x04** **0**	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 **5 / 0x05** **6 / 0x06** **7 / 0x07**	**0** **0** **0** **0**	Set session handle – remote server will fill in.
8 / 0x08 **9 / 0x09** **10 / 0x0A** **11 / 0x0B**	**0** **0** **0** **0**	Status – remote server will fill in.
12 / 0x0C **13 / 0x0D** **14 / 0x0E** **15 / 0x0F** **16 / 0x10** **17 / 0x11** **18 / 0x12** **19 / 0x13**	**XX** **XX** **XX** **XX** **XX** **XX** **XX** **XX**	Sender/Client Context – 8 bytes you can do anything with. Server will echo these back unchanged, so you can place sequence number or other hints here.
20 / 0x14 **21 / 0x15** **22 / 0x16** **23 / 0x17**	**0** **0** **0** **0**	Header Options Field – MUST be zero (0)
24 / 0x18 **25 / 0x19**	**0x01** **0**	Register Protocol Version – MUST be one (1)
26 / 0x1A **27 / 0x1B**	**0** **0**	Register Options – MUST be zero (0)

2.3 Response (You receive from ControlLogix)

Offset	Value	2.4 Description
0 / 0x00 **1 / 0x01**	**0x65** **0**	Ethernet/IP Encapsulation Command: Register Session
2 / 0x02 **3 / 0x03**	**0x04** **0**	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 **5 / 0x05** **6 / 0x06** **7 / 0x07**	**SH** **SH** **SH** **SH**	Session handle returned as 32-bit value. You do not place any meaning on this other than to return the same 4 bytes in every Ethernet/IP Encapsulation Header until you disconnect. An example Session Handle is 0x0F022200
8 / 0x08 **9 / 0x09** **10 / 0x0A** **11 / 0x0B**	**0** **0** **0** **0**	Status – if not ZERO (0), some error occurred. See ODVA/CIP specification Vol 2, Chapter 2 for error code meanings. You should NOT receive any if you follow these packet formats and there are no hardware faults.
12 / 0x0C **13 / 0x0D** **14 / 0x0E** **15 / 0x0F** **16 / 0x10** **17 / 0x11** **18 / 0x12** **19 / 0x13**	**XX** **XX** **XX** **XX** **XX** **XX** **XX** **XX**	Sender/Client Context – your 8 bytes will be returned here
20 / 0x14 **21 / 0x15** **22 / 0x16** **23 / 0x17**	**0** **0** **0** **0**	Header Options Field – MUST be zero (0)
24 / 0x18 **25 / 0x19**	**0x01** **0**	Register Protocol Version – MUST be one (1)
26 / 0x1A **27 / 0x1B**	**0** **0**	Register Options – MUST be zero (0)

3 Ethernet/IP Unconnected Send – SLC500 Read

Use this packet to query a "SLC5 File" defined in the ControlLogix.

3.1 SLC500 Read Request (You send to ControlLogix)

Offset	Value	Description
0 / 0x00 1 / 0x01	0x6F 0	Ethernet/IP Encapsulation Command: Read RR Data
2 / 0x02 3 / 0x03	(0x36) 0	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 5 / 0x05 6 / 0x06 7 / 0x07	SH SH SH SH	Session handle – return the value you obtained from Register Session
8 / 0x08 9 / 0x09 10 / 0x0A 11 / 0x0B	0 0 0 0	Status .
12 / 0x0C 13 / 0x0D 14 / 0x0E 15 / 0x0F 16 / 0x10 17 / 0x11 18 / 0x12 19 / 0x13	XX XX XX XX XX XX XX XX	Sender/Client Context – 8 bytes you can do anything with. Server will echo these back unchanged, so you can place sequence number or other hints here.
20 / 0x14 21 / 0x15 22 / 0x16 23 / 0x17	0 0 0 0	Header Options Field – MUST be zero (0)
24 / 0x18 25 / 0x19 26 / 0x1A 27 / 0x1B	0 0 0 0	Interface Handle – MUST be zero (0)
28 / 0x1C 29 / 0x1D	(0x0A) 0	Command Timeout in Seconds – 10 is a good number
30 / 0x1E 31 / 0x1F	0x02 0	CPF item count – should be 2
32 / 0x20 33 / 0x21 34 / 0x22 35 / 0x23	0 0 0 0	CPF Address Item – two 16-bit zero (0) for NULL address type (this is only used for connected messaging or I/O messaging)
36 / 0x24 37 / 0x25	0xB2 0	CPF Data Item Type – B2 is unconnected or UCMM
38 / 0x26 39 / 0x27	(0x26) 0	CPF Data Item Length (in BYTES) – adjust to correct length
40 / 0x28	0x52	CIP Connection Manager Service = Unconnected Send
41 / 0x29	0x02	Length (in WORDS) of CIP IOI Path
42 / 0x2A 43 / 0x2B	0x20 0x06	Logical Segment, Class=0x06 (Connection Manager)
44 / 0x2C 45 / 0x2D	0x24 0x01	Logical Segment, Instance=0x01
46 / 0x2E	0x0A	Priority / Ticks multiplier, 0x0A means normal priority, multiple by about 1 second
47 / 0x2F	(0x09)	Given above multiplier, this means Time out in 9 seconds
48 / 0x30 49 / 0x31	(0x18) 0	Length of CIP message we are 'unconnected sending' (in BYTES)
50 / 0x32	0x4C	PCCC Object Service Code
51 / 0x33	0x02	Length (in WORDS) of CIP IOI Path
52 / 0x34 53 / 0x35	0x20 0x06	Logical Segment, Class=0x67 (Rockwell Specific, PCCC Object)
54 / 0x36 55 / 0x37	0x24 0x01	Logical Segment, Instance=0x01

56 / 0x38 **57 / 0x39** **58 / 0x3A** **59 / 0x3B** **60 / 0x3C** **61 / 0x3D** **62 / 0x3E** **63 / 0x3F**	**0** **0x01** **0** **0** **0** **0** **0** **0**	PCCC addressing info – just use these defaults.
64 / 0x40	**0x0F**	PCCC CMD / Command (see DF1 manual #17706516 at www.ab.com)
65 / 0x41	**0**	PCCC STS / Status – send as zero
66 / 0x42 **67 / 0x43**	**(0x01)** **(0)**	PCCC TNS / Transaction Number – should vary between each poll
68 / 0x44	**0xA2**	PCCC FNC = Protected Typed Logical Read with 3 address fields
69 / 0x45	**(0x06)**	Byte Count to Read
70 / 0x46	**(0x07)**	File Number defined in ControlLogix – limited 0 to 255
71 / 0x47	**0x89**	File Type = 16-bit INTEGER – see DF1 manual for other types
72 / 0x48	**(0)**	Read starting at this element
73 / 0x49	**0**	Sub-Element – only used for bit or structured data file types
??	***0***	***WARNING – must PAD if byte 48 is ODD – but NO PAD in this example!!***
74 / 0x4A	**0x01**	Length of "Connection Path" – route through ControlLogix Backplane
75 / 0x4B	**0**	Reserved – must be zero
76 / 0x4C	**(0x01)**	Route to ControlLogix Backplane – MUST be one (1)
77 / 0x4D	**0**	Which SLOT – normally ControlLogix CPU is in slot 0

3.2 SLC500 Read Response (You receive from ControlLogix)

Offset	Value	3.3 Description
0 / 0x00 **1 / 0x01**	**0x6F** **0**	Ethernet/IP Encapsulation Command: Read RR Data
2 / 0x02 **3 / 0x03**	**(??)** **0**	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 **5 / 0x05** **6 / 0x06** **7 / 0x07**	**SH** **SH** **SH** **SH**	Session handle
8 / 0x08 **9 / 0x09** **10 / 0x0A** **11 / 0x0B**	**(??)** **(??)** **(??)** **(??)**	Status - should be zeros, bad "encap" error is not
12 / 0x0C **13 / 0x0D** **14 / 0x0E** **15 / 0x0F** **16 / 0x10** **17 / 0x11** **18 / 0x12** **19 / 0x13**	**XX** **XX** **XX** **XX** **XX** **XX** **XX** **XX**	Sender/Client Context – 8 bytes you can do anything with. Server will echo these back unchanged, so you can place sequence number or other hints here.
20 / 0x14 **21 / 0x15** **22 / 0x16** **23 / 0x17**	**0** **0** **0** **0**	Header Options Field – MUST be zero (0)
24 / 0x18 **25 / 0x19** **26 / 0x1A** **27 / 0x1B**	**0** **0** **0** **0**	Interface Handle – MUST be zero (0)
28 / 0x1C **29 / 0x1D**	**(0x0A)** **0**	Command Timeout in Seconds – 10 is a good number
30 / 0x1E **31 / 0x1F**	**0x02** **0**	CPF item count – should be 2
32 / 0x20 **33 / 0x21** **34 / 0x22** **35 / 0x23**	**0** **0** **0** **0**	CPF Address Item – two 16-bit zero (0) for NULL address type (this is only used for connected messaging or I/O messaging)

36 / 0x24 **37 / 0x25**	**0xB2** **0**	CPF Data Item Type – B2 is unconnected or UCMM
38 / 0x26 **39 / 0x27**	**(??)** **0**	CPF Data Item Length (in BYTES)
40 / 0x28	**0xCC**	PCCC Object Service Code or'd with 0x80 to indicate REPLY
41 / 0x29 **42 / 0x2A** **43 / 0x2B**	**0** **0** **0**	Response codes – should all be ZERO. If byte 42 is NOT zero, an error occurred. Byte 42 will be the GRC or General Response Code. See ODVA manual for how to decode bytes following GRC
44 / 0x2C **45 / 0x2D** **46 / 0x2E** **47 / 0x2F** **48 / 0x30** **49 / 0x31** **50 / 0x32** **51 / 0x33**	**0** **0** **0** **0** **0** **0x01** **0** **0**	PCCC addressing info – notice 4-byte pieces swapped.
52 / 0x34	**0x4F**	PCCC CMD or'd with 0x40 to indicate REPLY
53 / 0x35	**0**	PCCC STS – if not zero, PCCC error, see DF1 manual
56 / 0x42 **57 / 0x43**	**??** **??**	PCCC TNS / Transaction Number – should MATCH what you sent
58 / 0x44 **59 / 0x45**	**??** **??**	Little-endian data word, 1 of 3 in this example
60 / 0x46 **61 / 0x47**	**??** **??**	Little-endian data word, 2 of 3 in this example
62 / 0x48 **63 / 0x49**	**??** **??**	Little-endian data word, 3 of 3 in this example

4 Ethernet/IP Unconnected Send – SLC500 Write

Use this packet to write a "SLC5 File" defined in the ControlLogix.

4.1 SLC500 Write Request (You send to ControlLogix)

Offset	Value	Description
0 / 0x00 1 / 0x01	0x6F 0	Ethernet/IP Encapsulation Command: Read RR Data
2 / 0x02 3 / 0x03	(0x3C) 0	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 5 / 0x05 6 / 0x06 7 / 0x07	SH SH SH SH	Session handle – return the value you obtained from Register Session.
8 / 0x08 9 / 0x09 10 / 0x0A 11 / 0x0B	0 0 0 0	Status
12 / 0x0C 13 / 0x0D 14 / 0x0E 15 / 0x0F 16 / 0x10 17 / 0x11 18 / 0x12 19 / 0x13	XX XX XX XX XX XX XX XX	Sender/Client Context – 8 bytes you can do anything with. Server will echo these back unchanged, so you can place sequence number or other hints here.
20 / 0x14 21 / 0x15 22 / 0x16 23 / 0x17	0 0 0 0	Header Options Field – MUST be zero (0)
24 / 0x18 25 / 0x19 26 / 0x1A 27 / 0x1B	0 0 0 0	Interface Handle – MUST be zero (0)
28 / 0x1C 29 / 0x1D	(0x0A) 0	Command Timeout in Seconds – 10 is a good number
30 / 0x1E 31 / 0x1F	0x02 0	CPF item count – should be 2
32 / 0x20 33 / 0x21 34 / 0x22 35 / 0x23	0 0 0 0	CPF Address Item – two 16-bit zero (0) for NULL address type (this is only used for connected messaging or I/O messaging)
36 / 0x24 37 / 0x25	0xB2 0	CPF Data Item Type – B2 is unconnected or UCMM
38 / 0x26 39 / 0x27	(0x2C) 0	CPF Data Item Length (in BYTES) – adjust to correct length
40 / 0x28	0x52	CIP Connection Manager Service = Unconnected Send
41 / 0x29	0x02	Length (in WORDS) of CIP IOI Path
42 / 0x2A 43 / 0x2B	0x20 0x06	Logical Segment, Class=0x06 (Connection Manager)
44 / 0x2C 45 / 0x2D	0x24 0x01	Logical Segment, Instance=0x01
46 / 0x2E	0x0A	Priority / Ticks multiplier, 0x0A means normal priority, multiple by about 1 second
47 / 0x2F	(0x09)	Given above multiplier, this means Time out in 9 seconds
48 / 0x30 49 / 0x31	(0x1E) 0	Length of CIP message we are 'unconnected sending' (in BYTES)
50 / 0x32	0x4C	PCCC Object Service Code
51 / 0x33	0x02	Length (in WORDS) of CIP IOI Path
52 / 0x34 53 / 0x35	0x20 0x06	Logical Segment, Class=0x67 (Rockwell Specific, PCCC Object)
54 / 0x36 55 / 0x37	0x24 0x01	Logical Segment, Instance=0x01

56 / 0x38 **57 / 0x39** **58 / 0x3A** **59 / 0x3B** **60 / 0x3C** **61 / 0x3D** **62 / 0x3E** **63 / 0x3F**	**0** **0x01** **0** **0** **0** **0** **0** **0**	PCCC addressing info – just use these defaults.
64 / 0x40	**0x0F**	PCCC CMD / Command (see DF1 manual #17706516 at www.ab.com)
65 / 0x41	**0**	PCCC STS / Status – send as zero
66 / 0x42 **67 / 0x43**	**(0x01)** **(0)**	PCCC TNS / Transaction Number – should vary between each poll
68 / 0x44	**0xAA**	PCCC FNC = Protected Typed Logical Read with 3 address fields
69 / 0x45	**(0x06)**	Byte Count to Write
70 / 0x46	**(0x07)**	File Number defined in ControlLogix – limited 0 to 255
71 / 0x47	**0x89**	File Type = 16-bit INTEGER – see DF1 manual for other types
72 / 0x48	**(0x05)**	Write starting at this element
73 / 0x49	**00**	Sub-Element – only used for bit or structured data file types
74 / 0x4A **75 / 0x4B**	**??** **??**	Little-endian data word, 1 of 3 in this example
76 / 0x4C **77 / 0x4D**	**??** **??**	Little-endian data word, 2 of 3 in this example
78 / 0x4E **79 / 0x4F**	**??** **??**	Little-endian data word, 3 of 3 in this example
??	***0***	***WARNING – must PAD if byte 48 is ODD – but NO PAD in this example!!***
80 / 0x50	**0x01**	Length of "Connection Path" – route through ControlLogix Backplane
81 / 0x51	**0**	Reserved – must be zero
82 / 0x52	**(0x01)**	Route to ControlLogix Backplane – MUST be one (1)
83 / 0x53	**0**	Which SLOT – normally ControlLogix CPU is in slot 0

4.2 SLC500 Write Response (You receive from ControlLogix)

Offset	Value	4.3 Description
0 / 0x00 **1 / 0x01**	**0x6F** **0**	Ethernet/IP Encapsulation Command: Read RR Data
2 / 0x02 **3 / 0x03**	**(??)** **0**	Length of data attached to Ethernet/IP Encapsulation Header
4 / 0x04 **5 / 0x05** **6 / 0x06** **7 / 0x07**	**SH** **SH** **SH** **SH**	Session handle
8 / 0x08 **9 / 0x09** **10 / 0x0A** **11 / 0x0B**	**(??)** **(??)** **(??)** **(??)**	Status – should be zeros
12 / 0x0C **13 / 0x0D** **14 / 0x0E** **15 / 0x0F** **16 / 0x10** **17 / 0x11** **18 / 0x12** **19 / 0x13**	**XX** **XX** **XX** **XX** **XX** **XX** **XX** **XX**	Sender/Client Context – 8 bytes you can do anything with. Server will echo these back unchanged, so you can place sequence number or other hints here.
20 / 0x14 **21 / 0x15** **22 / 0x16** **23 / 0x17**	**0** **0** **0** **0**	Header Options Field – MUST be zero (0)
24 / 0x18 **25 / 0x19** **26 / 0x1A** **27 / 0x1B**	**0** **0** **0** **0**	Interface Handle – MUST be zero (0)
28 / 0x1C	**(0x0A)**	Command Timeout in Seconds – 10 is a good number

29 / 0x1D	**0**	
30 / 0x1E **31 / 0x1F**	**0x02** **0**	CPF item count – should be 2
32 / 0x20 **33 / 0x21** **34 / 0x22** **35 / 0x23**	**0** **0** **0** **0**	CPF Address Item – two 16-bit zero (0) for NULL address type (this is only used for connected messaging or I/O messaging)
36 / 0x24 **37 / 0x25**	**0xB2** **0**	CPF Data Item Type – B2 is unconnected or UCMM
38 / 0x26 **39 / 0x27**	**(??)** **00**	CPF Data Item Length (in BYTES)
40 / 0x28	**0xCC**	PCCC Object Service Code or'd with 0x80 to indicate REPLY
41 / 0x29 **42 / 0x2A** **43 / 0x2B**	**0** **0** **0**	Response codes – should all be ZERO. If byte 42 is NOT zero, an error occurred. Byte 42 will be the GRC or General Response Code. See ODVA manual for how to decode bytes following GRC
44 / 0x2C **45 / 0x2D** **46 / 0x2E** **47 / 0x2F** **48 / 0x30** **49 / 0x31** **50 / 0x32** **51 / 0x33**	**0** **0** **0** **0** **0** **0x01** **0** **0**	PCCC addressing info – notice 4-byte pieces swapped.
52 / 0x34	**0x4F**	PCCC CMD or'd with 0x40 to indicate REPLY
53 / 0x35	**0**	PCCC STS – if not zero, PCCC error, see DF1 manual
56 / 0x42 **57 / 0x43**	**??** **??**	PCCC TNS / Transaction Number – should MATCH what you sent