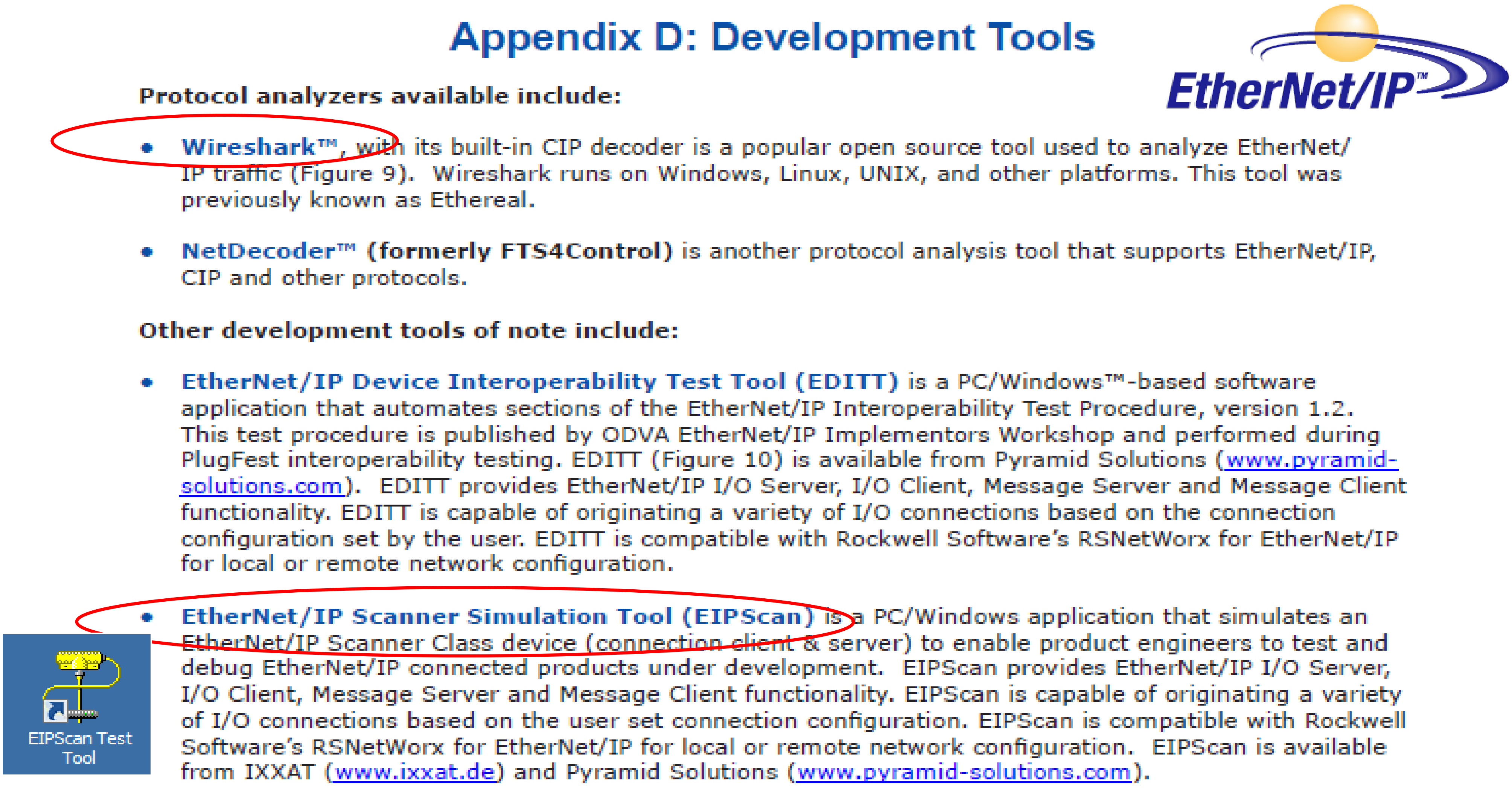
How To Use EIPScan To Read/Write Ethernet/IP Data via EKI-1242EIMS

Enabling an Intelligent Planet

Overview

- ✓ This is an example on how to configure the EKI-1242EIMS Ethernet/IP Slave module to connect with EtherNet/IP Scan Test Tool from Pyramid Solutions. It is possible to use this document as a guide on how to set up any "generic" EtherNet/IP module from Advantech under EtherNet/IP Scan Test Tool, ESTT.
- ✓ This application note assumes that ESTT are installed and working correct. The ESTT is set up to read and write 32 bytes of I/O data from and to the EKI-1242EIMS Ethernet/IP Slave module.

Recommend Test Tool via ODVA



Appendix D: Development Tools

Protocol analyzers available include:

- **Wireshark™**, with its built-in CIP decoder is a popular open source tool used to analyze EtherNet/IP traffic (Figure 9). Wireshark runs on Windows, Linux, UNIX, and other platforms. This tool was previously known as Ethereal.

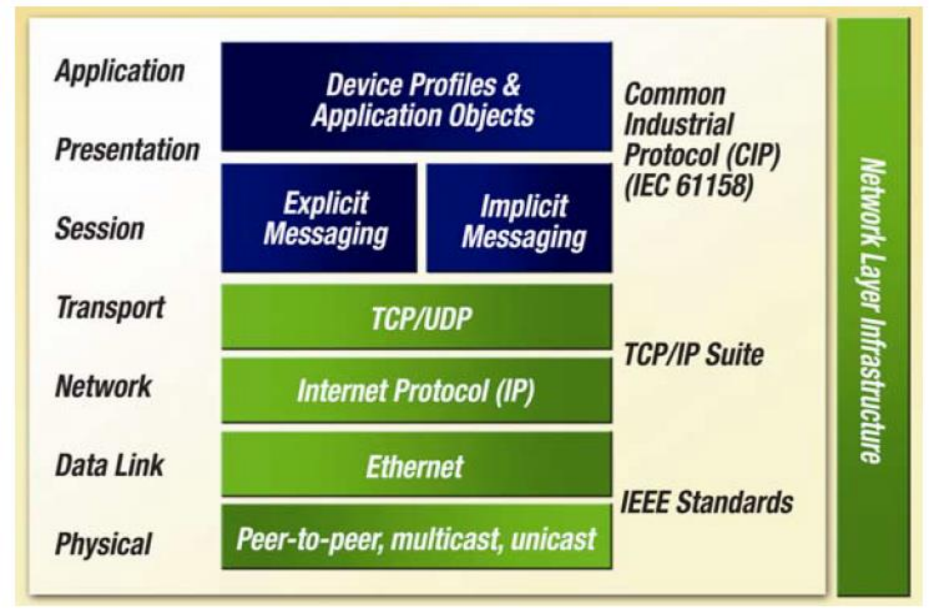
- **NetDecoder™ (formerly FTS4Control)** is another protocol analysis tool that supports EtherNet/IP, CIP and other protocols.

Other development tools of note include:

- **EtherNet/IP Device Interoperability Test Tool (EDITT)** is a PC/Windows™-based software application that automates sections of the EtherNet/IP Interoperability Test Procedure, version 1.2. This test procedure is published by ODVA EtherNet/IP Implementors Workshop and performed during PlugFest interoperability testing. EDITT (Figure 10) is available from Pyramid Solutions (www.pyramid-solutions.com). EDITT provides EtherNet/IP I/O Server, I/O Client, Message Server and Message Client functionality. EDITT is capable of originating a variety of I/O connections based on the connection configuration set by the user. EDITT is compatible with Rockwell Software's RSNetWorx for EtherNet/IP for local or remote network configuration.

- **EtherNet/IP Scanner Simulation Tool (EIPScan)** is a PC/Windows application that simulates an EtherNet/IP Scanner Class device (connection client & server) to enable product engineers to test and debug EtherNet/IP connected products under development. EIPScan provides EtherNet/IP I/O Server, I/O Client, Message Server and Message Client functionality. EIPScan is capable of originating a variety of I/O connections based on the user set connection configuration. EIPScan is compatible with Rockwell Software's RSNetWorx for EtherNet/IP for local or remote network configuration. EIPScan is available from IXXAT (www.ixxat.de) and Pyramid Solutions (www.pyramid-solutions.com).

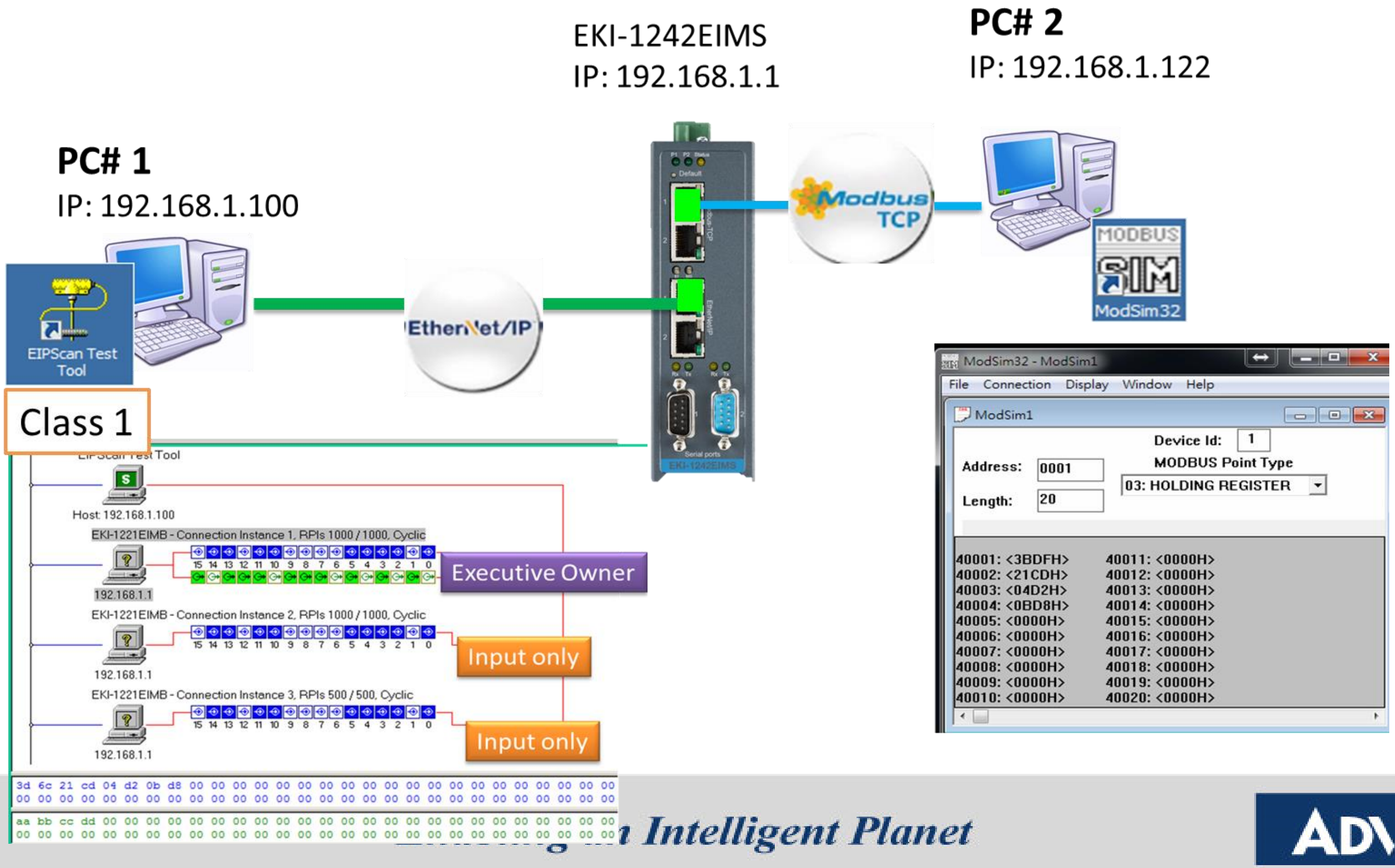
Using EIPSCAN Tool to Request Data



Application	Device Profiles & Application Objects		Common Industrial Protocol (CIP) (IEC 61158)	Network Layer Infrastructure
Presentation				
Session	Explicit Messaging	Implicit Messaging		
Transport	TCP/UDP		TCP/IP Suite	
Network	Internet Protocol (IP)			
Data Link	Ethernet		IEEE Standards	
Physical	Peer-to-peer, multicast, unicast			

EKI-1242EIMS Connection Scenario

- Set up EKI-1242 modbus session to active polling data from modbus simulator tool and then using EIPScan Scanner Tool to read/write Ethernet/IP Class 1 UDP I/O Mapping data & Class 3 TCP specific Session data



Host: 192.168.1.100

EKI-1221EIMB - Connection Instance 1, RPIs 1000 / 1000, Cyclic
192.168.1.1

EKI-1221EIMB - Connection Instance 2, RPIs 1000 / 1000, Cyclic
192.168.1.1

EKI-1221EIMB - Connection Instance 3, RPIs 500 / 500, Cyclic
192.168.1.1

```
3d 6c 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
aa bb cc dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Device Id: 1
Address: 0001
MODBUS Point Type: 03: HOLDING REGISTER
Length: 20

```
40001: <3BDFH>      40011: <0000H>
40002: <21CDH>      40012: <0000H>
40003: <04D2H>      40013: <0000H>
40004: <0BD8H>      40014: <0000H>
40005: <0000H>      40015: <0000H>
40006: <0000H>      40016: <0000H>
40007: <0000H>      40017: <0000H>
40008: <0000H>      40018: <0000H>
40009: <0000H>      40019: <0000H>
40010: <0000H>      40020: <0000H>
```

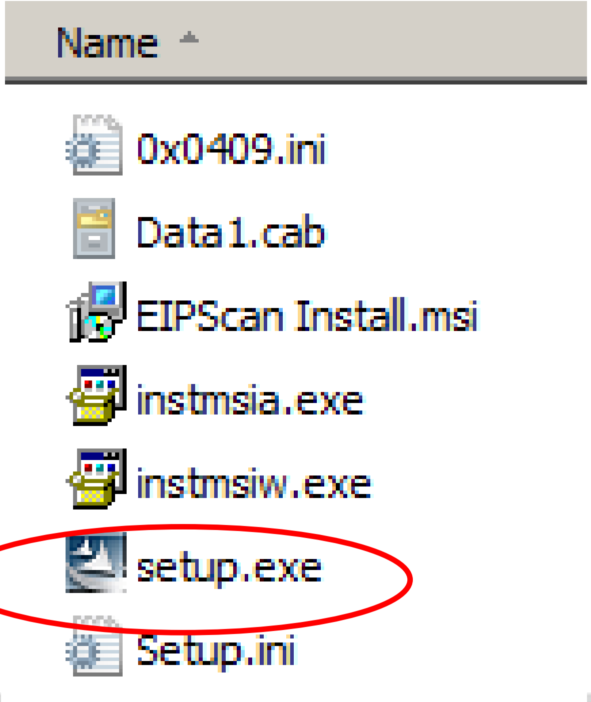
Step by Step

1. Install EIPScan Tool to your PC.
2. Make sure your PC Network are the same subnet with EKI-1242EIMS
3. PC#2 set up Modsim Tool
4. PC#2 setup EKI-1242EIMS WEBGUI
    A. Network are Bridge mode <PC#1&2 are in the same subnet>
    B. Ethernet/IP Not Exception code
    C. Modbus TCP data polling setting <Polling PC#2 modsim>
5. Using EIPScan Tool to read Class 1 data
6. Using EIPScan Tool to read Class 3 data

Notice: PC#1& PC#2 don’t modify the setting/submit in the same time.

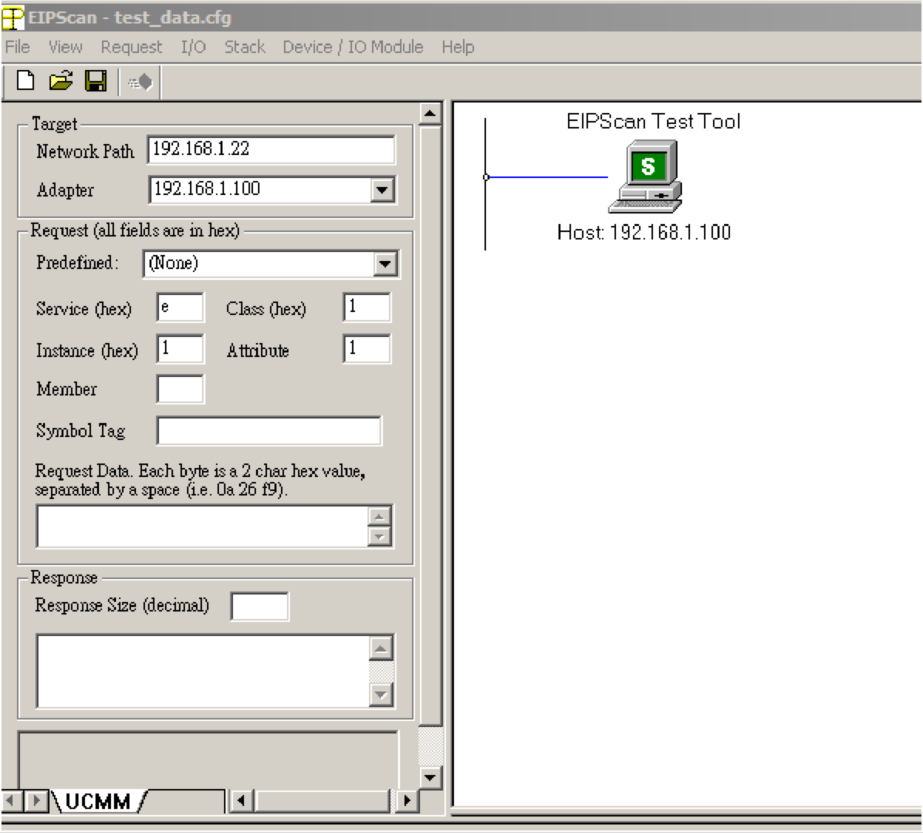
Install EIPSCAN Tool in PC (1/7)

- EIPSCAN Tools is freeware to provide customer how to use Ethernet/IP
- Unzip we provide “EIPScan Install v1_20” and Click Setup.exe to install



Name

- 0x0409.ini
- Data1.cab
- EIPScan Install.msi
- instmsia.exe
- instmsiw.exe
- setup.exe
- Setup.ini



EIPScan - test_data.cfg

Target

Network Path: 192.168.1.22

Adapter: 192.168.1.100

Request (all fields are in hex)

Predefined: (None)

Service (hex): e

Class (hex): 1

Instance (hex): 1

Attribute: 1

Member:

Symbol Tag:

Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

Response

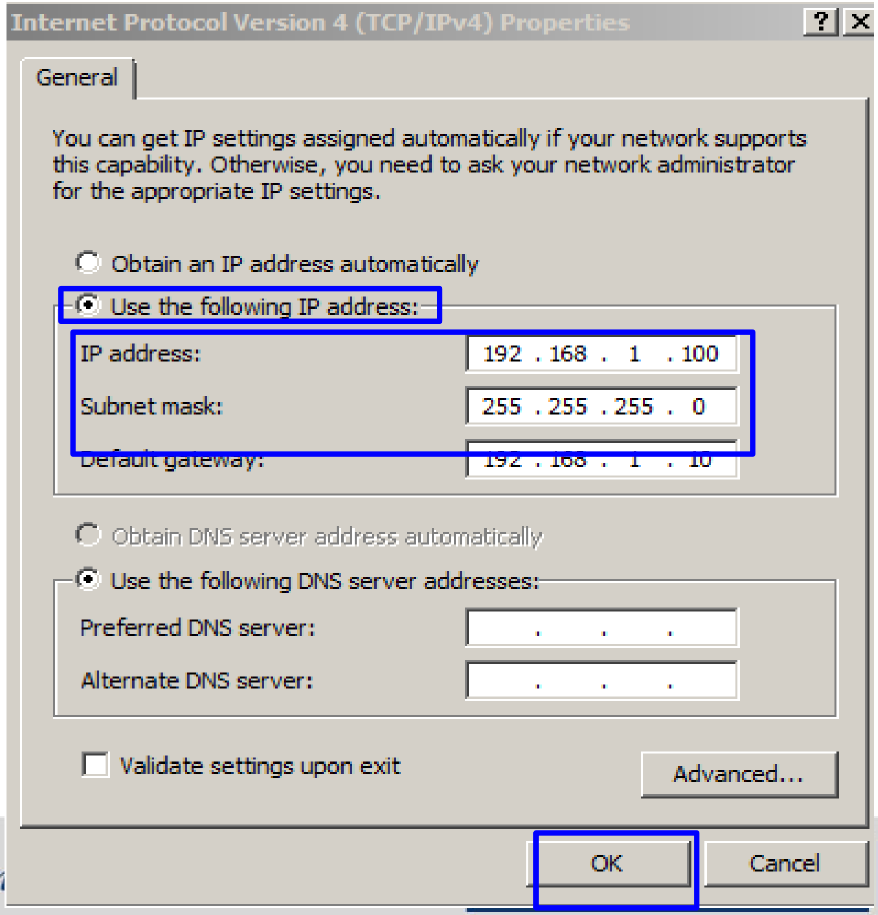
Response Size (decimal):

PC#1 & PC#2 in same subnet(2/7)

1. Click to manual set up PC#1& PC#2 IP address
2. Configure the IP address & subnet mask. Setup in the same local network with EKI-1221EIMB
3. Save to Exit

PC#1 : 192.168.1.100 ;

PC#2: 192.168.1.122;



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 10

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

PC#2 Set-up modsim tool (3/7)

Simulate End device to send out Modbus/TCP data

1st. Click "File" and "New"

2nd. Click "Connection", and select the "Modbus/TCP Svr"

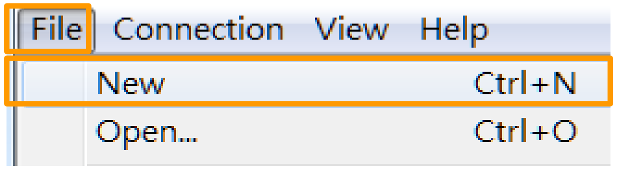
3rd. Select Modbus Service Port: 502

4th. Key in ***Device id:1, Address:001, Length:20, FC:3***

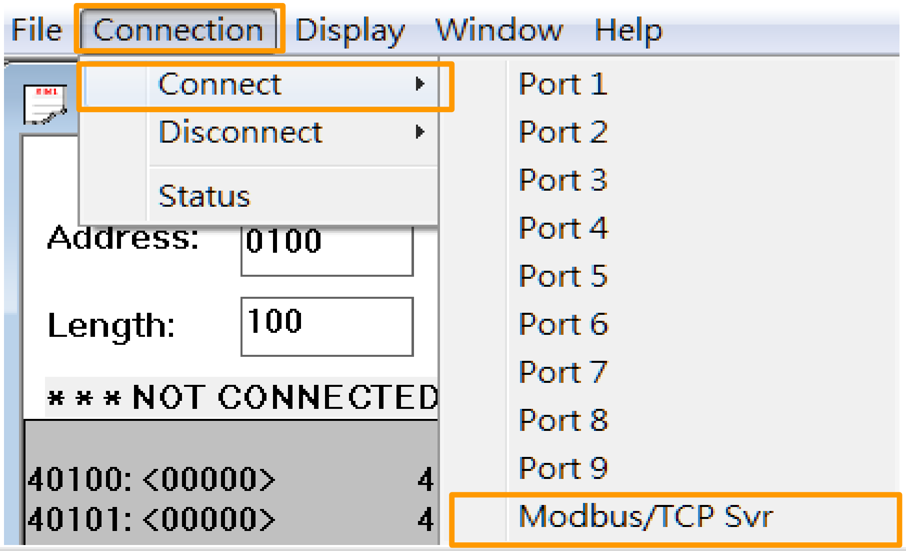
PC# 2

IP: 192.168.1.122

1st.



2nd.

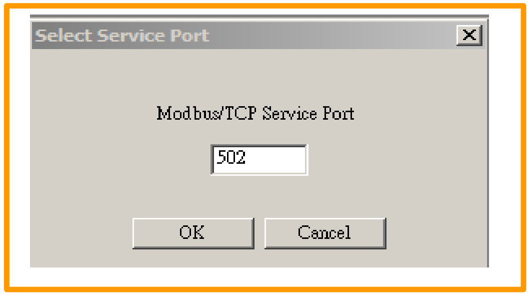


Address: 0100

Length: 100

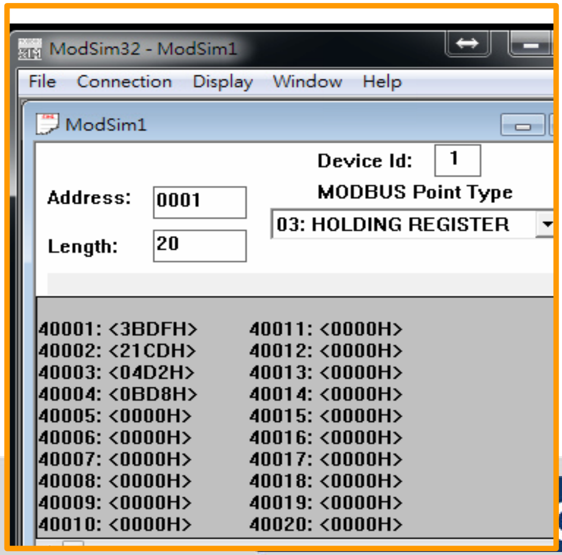
```
* * * NOT CONNECTED
40100: <00000>        4
40101: <00000>        4
```

3rd.



Modbus/TCP Service Port: 502

4th.



Device Id: 1

Address: 0001

Length: 20

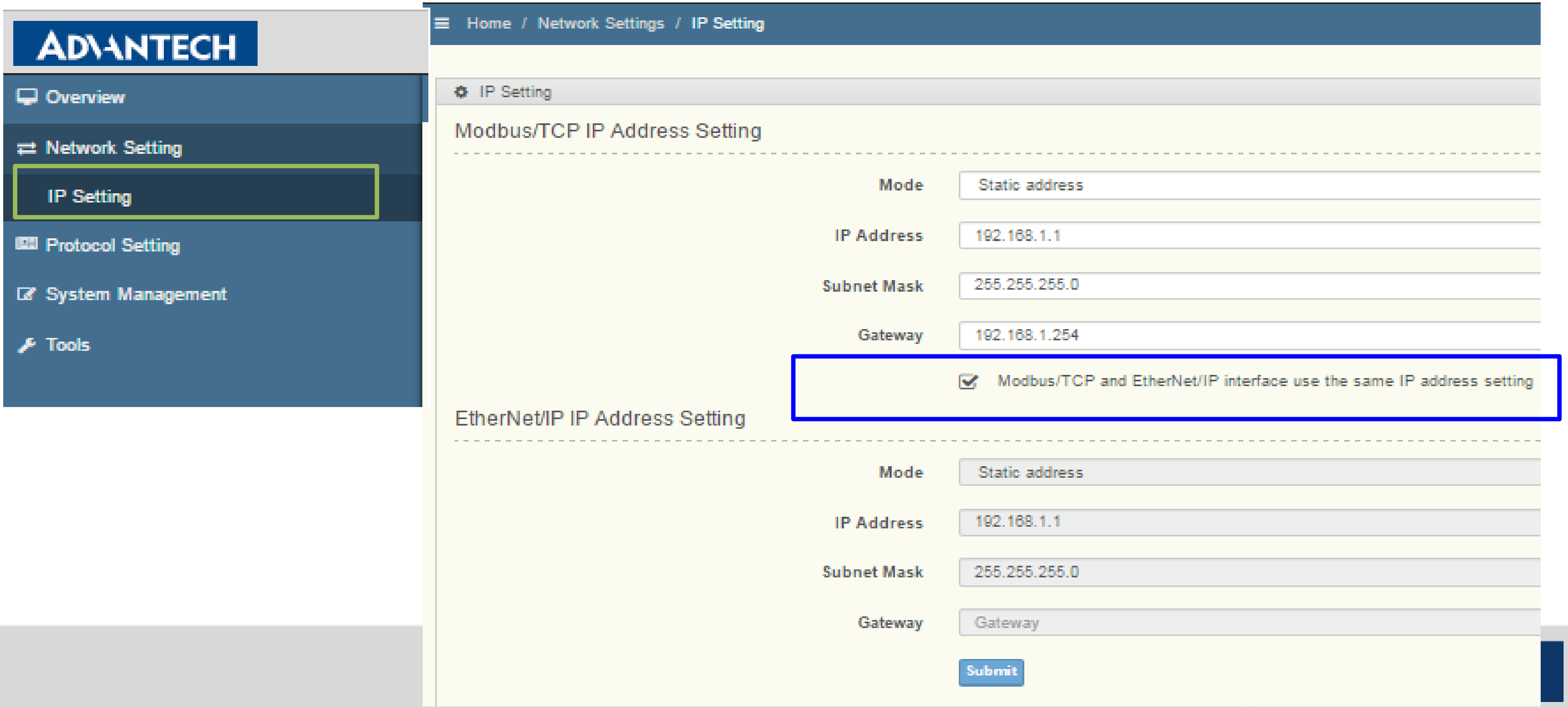
MODBUS Point Type: 03: HOLDING REGISTER

```
40001: <3BDFH>    40011: <0000H>
40002: <21CDH>    40012: <0000H>
40003: <04D2H>    40013: <0000H>
40004: <0BD8H>    40014: <0000H>
40005: <0000H>    40015: <0000H>
40006: <0000H>    40016: <0000H>
40007: <0000H>    40017: <0000H>
40008: <0000H>    40018: <0000H>
40009: <0000H>    40019: <0000H>
40010: <0000H>    40020: <0000H>
```

WEBGUI - Network Setting (4/7)

Set up IP Setting

- Click to bridge to same IP address (Ethernet#1) and PC#1 & PC#2 can login in the same subnet



Modbus/TCP IP Address Setting

Mode: Static address
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: 192.168.1.254

☑ Modbus/TCP and EtherNet/IP interface use the same IP address setting

EtherNet/IP IP Address Setting

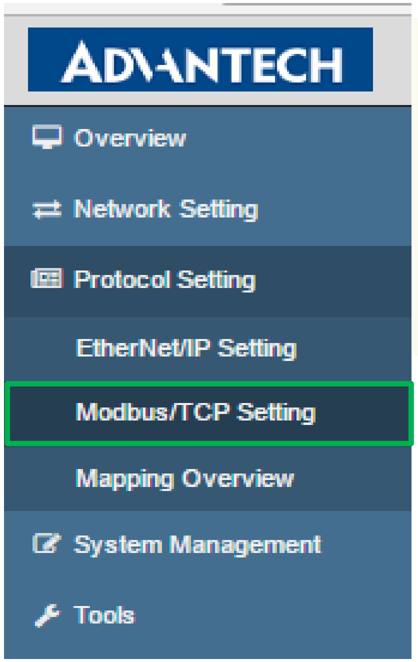
Mode: Static address
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0
Gateway: Gateway

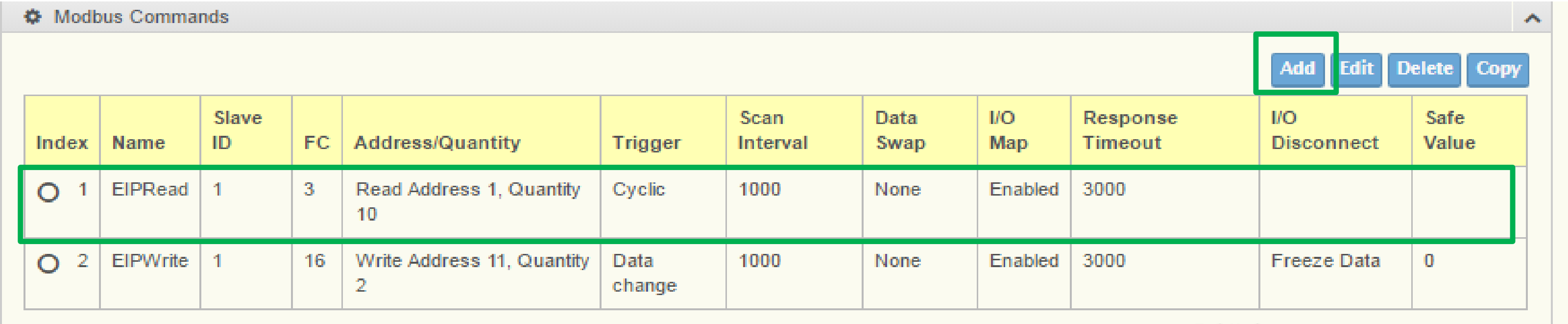
Ethernet/IP Mapping Setting (5/7)

- Modbus to Ethernet/IP total data buffer are 496 bytes.
  - Add modbus exception code would occupy 64 byte of input.
  - Add data status/code would occupy 2 byte of input/output

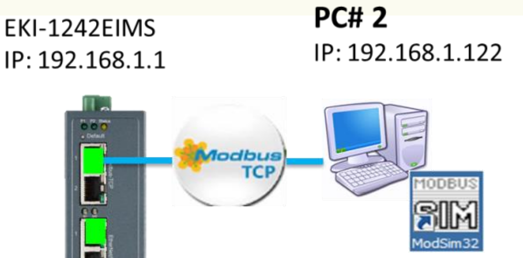
Modbus TCP/RTU Transaction (6/7)

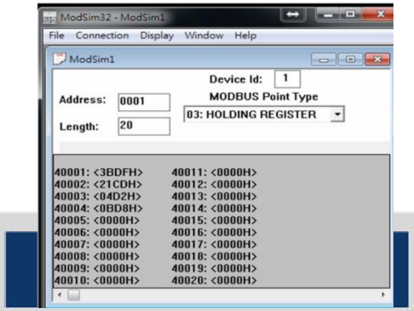
- ➢ Using Add button to add Modbus TCP transaction
  - Add one that can cycling Read Modbus TCP data





Index	Name	Slave ID	FC	Address/Quantity	Trigger	Scan Interval	Data Swap	I/O Map	Response Timeout	I/O Disconnect	Safe Value
○ 1	EIPRead	1	3	Read Address 1, Quantity 10	Cyclic	1000	None	Enabled	3000		
○ 2	EIPWrite	1	16	Write Address 11, Quantity 2	Data change	1000	None	Enabled	3000	Freeze Data	0





Device Id: 1

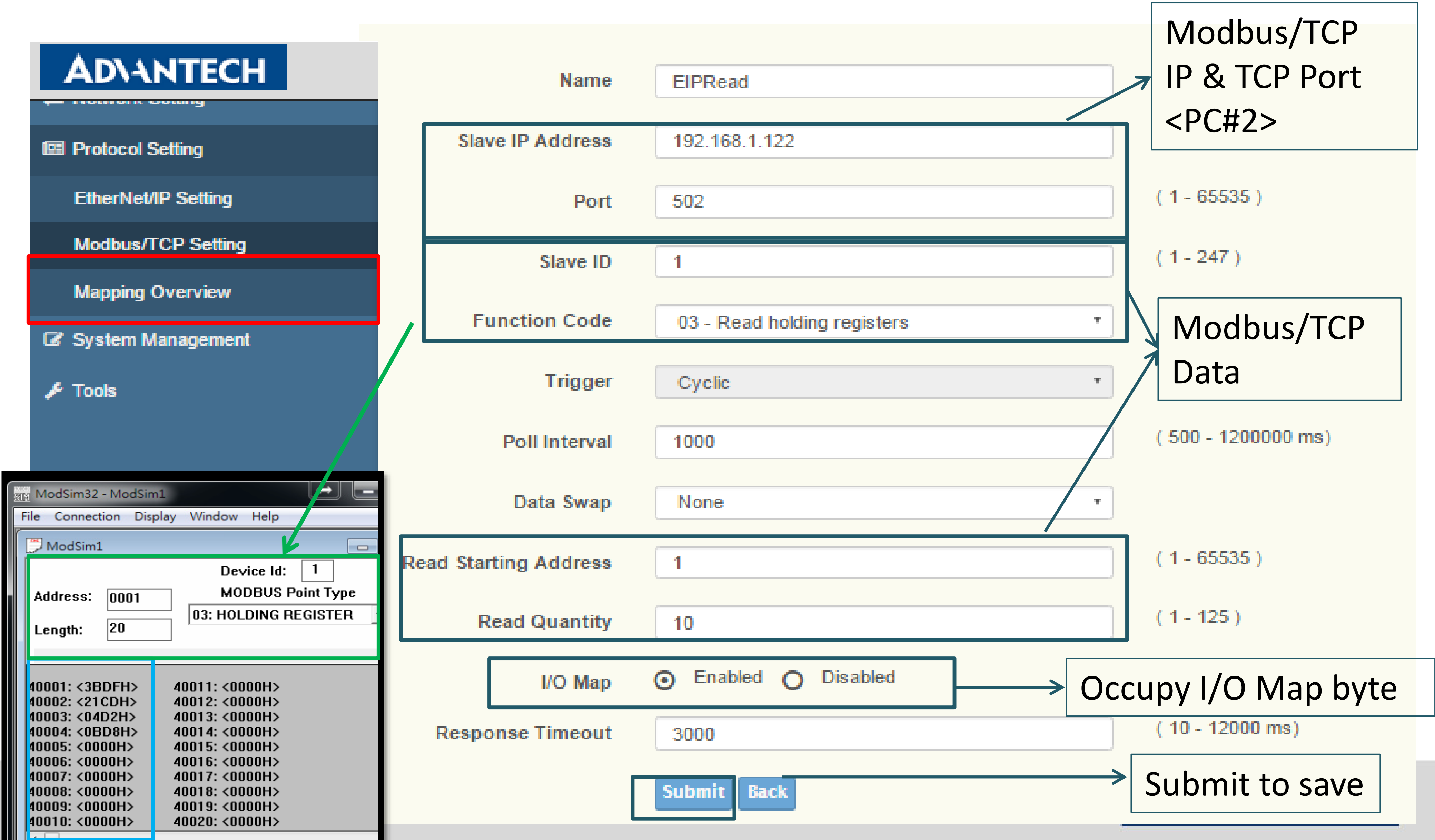
MODBUS Point Type: 03: HOLDING REGISTER

Address: 0001

Length: 20

```
40001: <3BDFH>      40011: <0000H>
40002: <21CDH>      40012: <0000H>
40003: <04D2H>      40013: <0000H>
40004: <0BD8H>      40014: <0000H>
40005: <0000H>      40015: <0000H>
40006: <0000H>      40016: <0000H>
40007: <0000H>      40017: <0000H>
40008: <0000H>      40018: <0000H>
40009: <0000H>      40019: <0000H>
40010: <0000H>      40020: <0000H>
```

Modbus/TCP Data Setting (7/7)



Name: EIPRead

Slave IP Address: 192.168.1.122

Port: 502 (1 - 65535)

Slave ID: 1 (1 - 247)

Function Code: 03 - Read holding registers

Trigger: Cyclic

Poll Interval: 1000 (500 - 1200000 ms)

Data Swap: None

Read Starting Address: 1 (1 - 65535)

Read Quantity: 10 (1 - 125)

I/O Map ● Enabled ○ Disabled

Response Timeout: 3000 (10 - 12000 ms)

Modbus/TCP
IP & TCP Port
<PC#2>

Modbus/TCP
Data

Occupy I/O Map byte

Submit to save

Device Id: 1

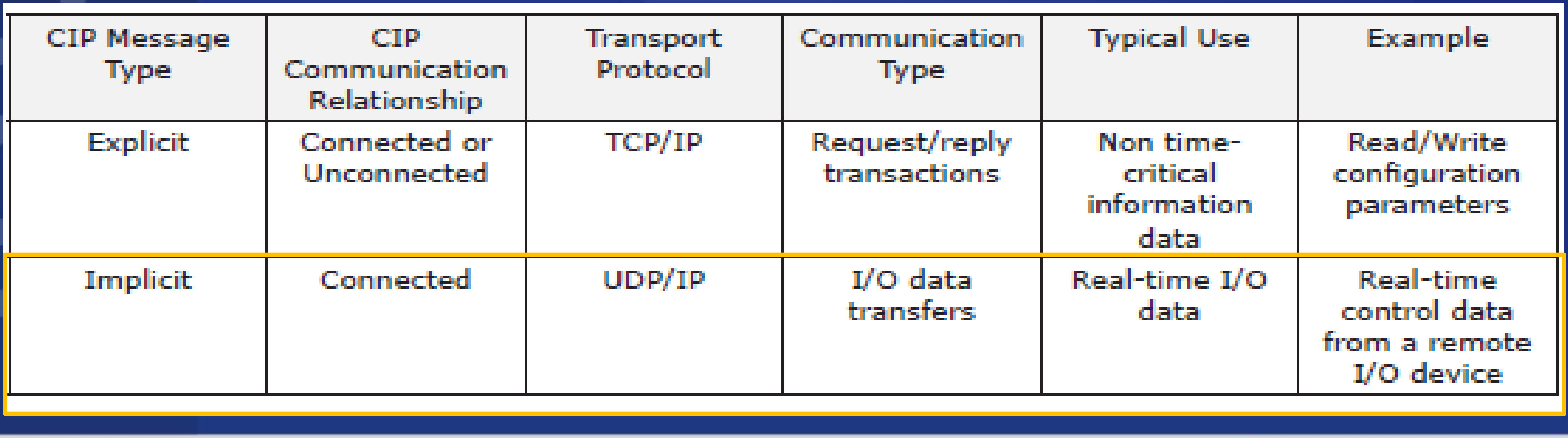
Address: 0001

Length: 20

MODBUS Point Type: 03: HOLDING REGISTER

```
40001: <3BDFH>    40011: <0000H>
40002: <21CDH>    40012: <0000H>
40003: <04D2H>    40013: <0000H>
40004: <0BD8H>    40014: <0000H>
40005: <0000H>    40015: <0000H>
40006: <0000H>    40016: <0000H>
40007: <0000H>    40017: <0000H>
40008: <0000H>    40018: <0000H>
40009: <0000H>    40019: <0000H>
40010: <0000H>    40020: <0000H>
```

Implicit Message to query I/O data



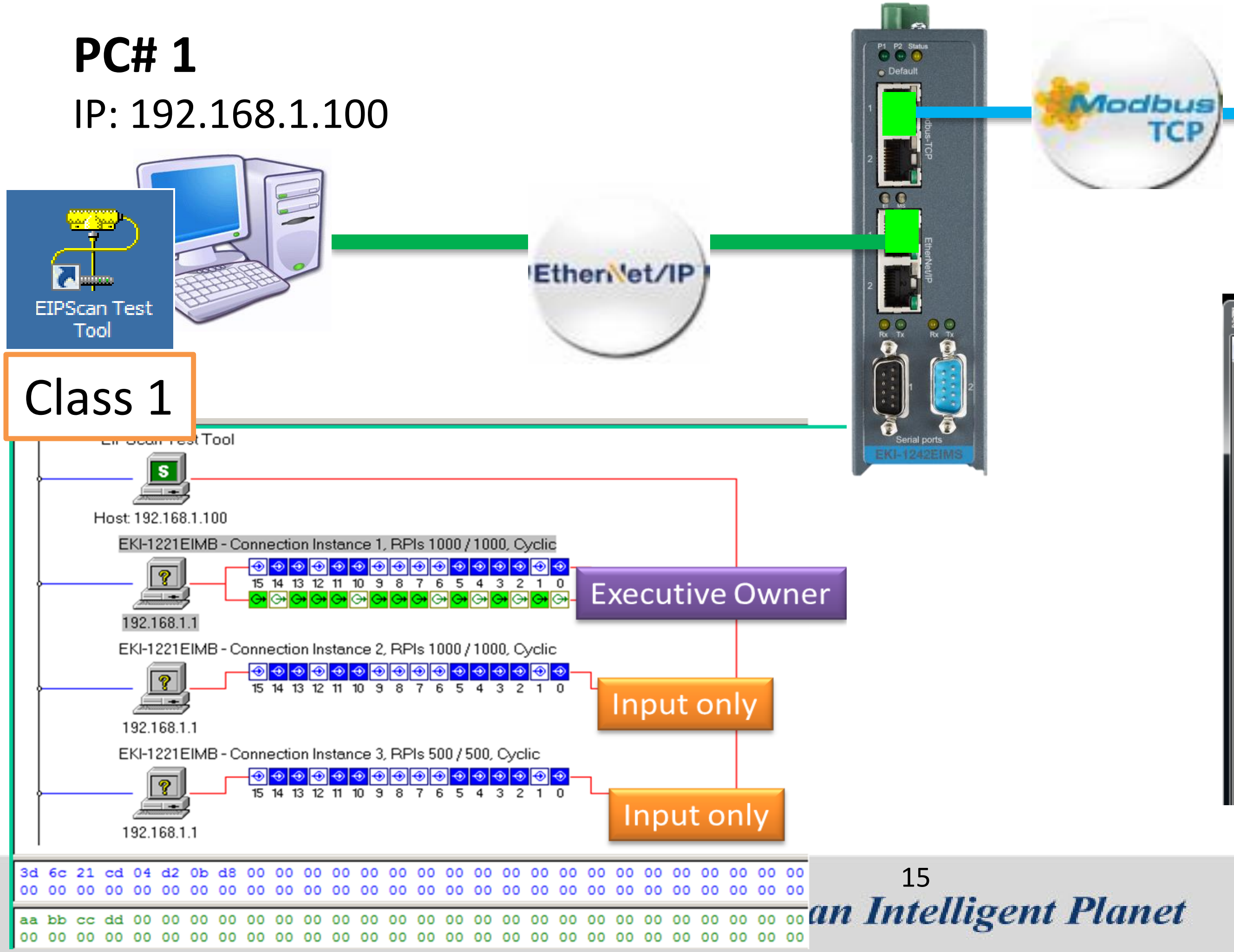
CIP Message Type	CIP Communication Relationship	Transport Protocol	Communication Type	Typical Use	Example
Explicit	Connected or Unconnected	TCP/IP	Request/reply transactions	Non time-critical information data	Read/Write configuration parameters
Implicit	Connected	UDP/IP	I/O data transfers	Real-time I/O data	Real-time control data from a remote I/O device

Network Topology

PC# 1
IP: 192.168.1.100

EKI-1242EIMS
IP: 192.168.1.1

PC# 2
IP: 192.168.1.122



Host 192.168.1.100

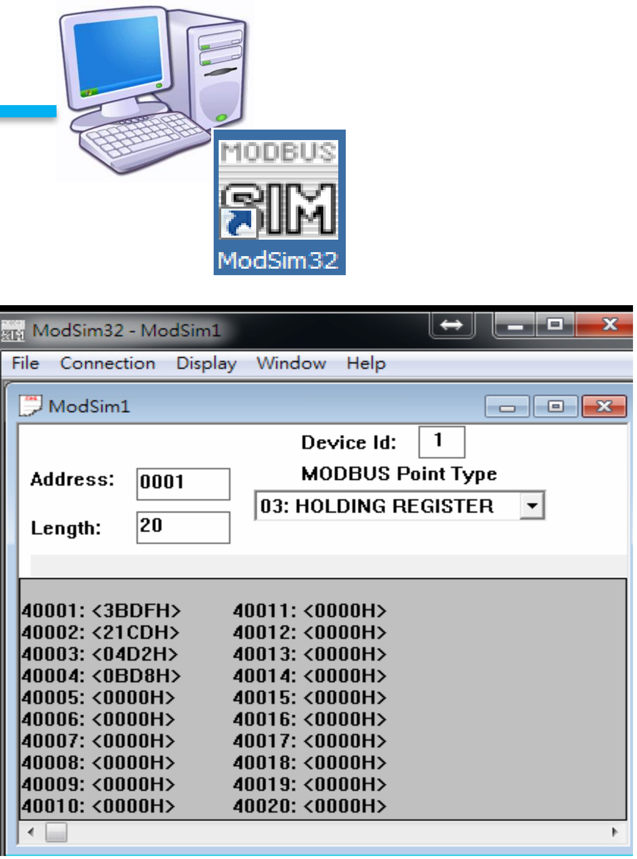
EKI-1221EIMB - Connection Instance 1, RPIs 1000 / 1000, Cyclic
192.168.1.1

EKI-1221EIMB - Connection Instance 2, RPIs 1000 / 1000, Cyclic
192.168.1.1

EKI-1221EIMB - Connection Instance 3, RPIs 500 / 500, Cyclic
192.168.1.1

```
3d 6c 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
aa bb cc dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



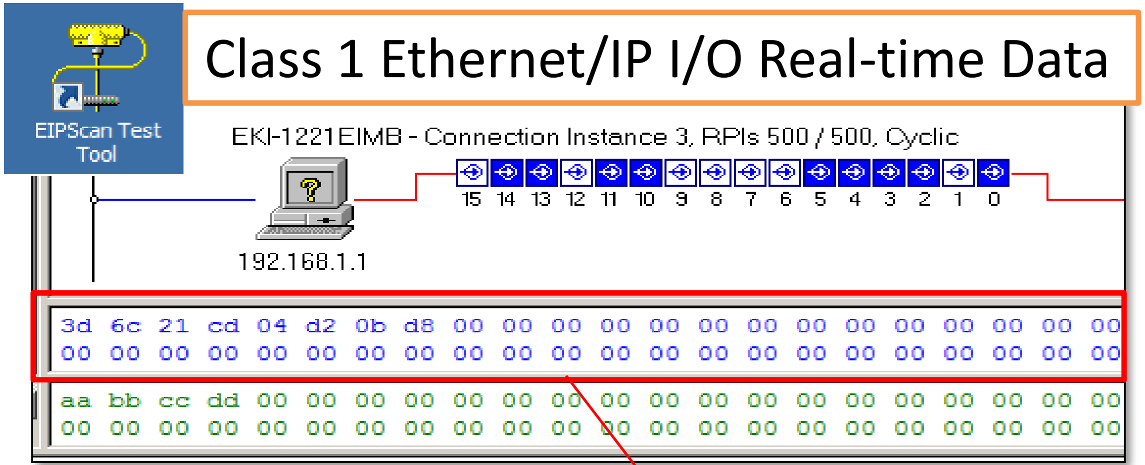
Device Id: 1
Address: 0001
Length: 20
MODBUS Point Type: 03: HOLDING REGISTER

```
40001: <3BDFH>     40011: <0000H>
40002: <21CDH>     40012: <0000H>
40003: <04D2H>     40013: <0000H>
40004: <0BD8H>     40014: <0000H>
40005: <0000H>     40015: <0000H>
40006: <0000H>     40016: <0000H>
40007: <0000H>     40017: <0000H>
40008: <0000H>     40018: <0000H>
40009: <0000H>     40019: <0000H>
40010: <0000H>     40020: <0000H>
```

PC#1 EIPSCAN - Real time Data View

- Class 1 : EIPSCAN data Real-time I/O Data view(384 bytes)

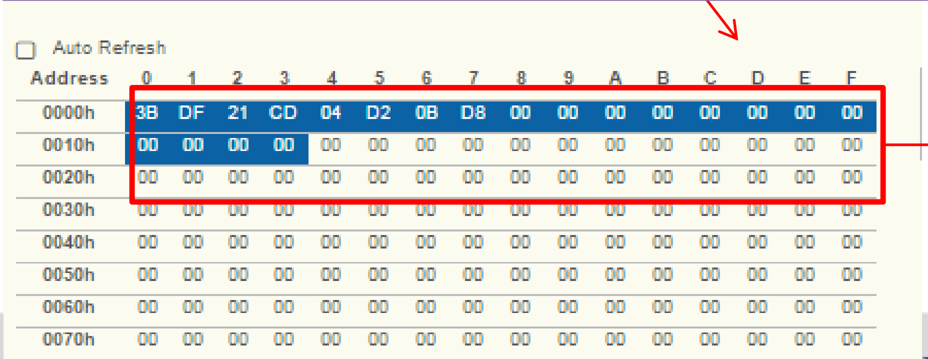
Class 1 Ethernet/IP I/O Real-time Data



```
3d 6c 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
aa bb cc dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

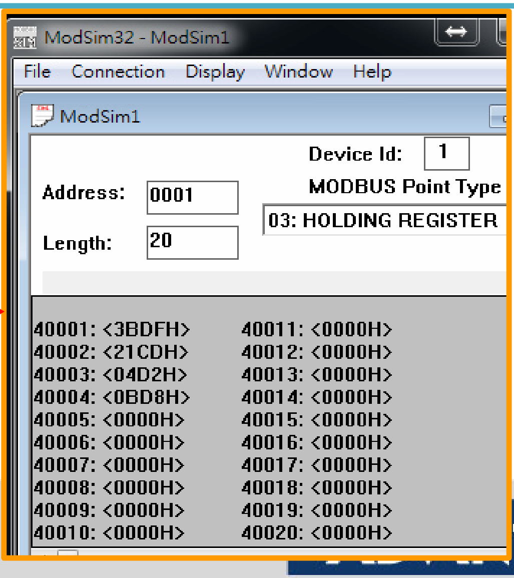
Modsim-
Simulator modbus slave data

WEBGUI - Real time Ethernet/IP I/O Data



☐ Auto Refresh

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h	3B	DF	21	CD	04	D2	0B	D8	00	00	00	00	00	00	00	00
0010h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0020h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0050h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

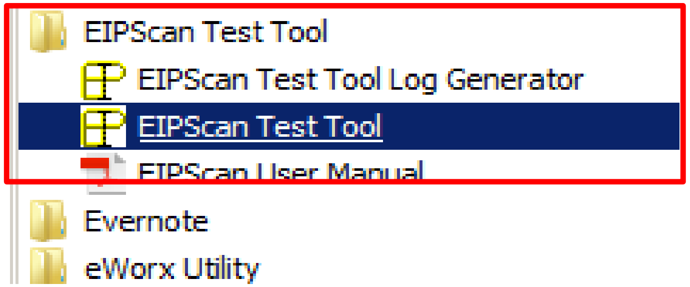


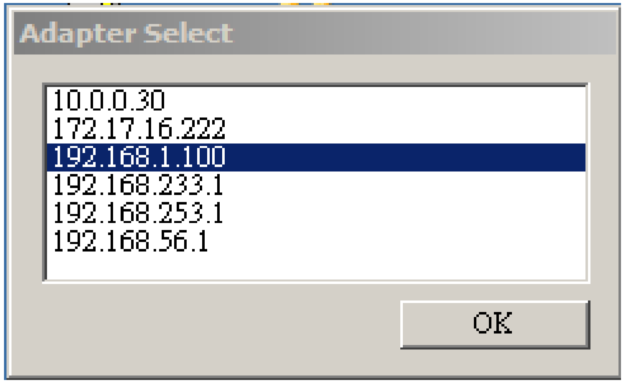
Device Id: 1
Address: 0001
MODBUS Point Type 03: HOLDING REGISTER
Length: 20

```
40001: <3BDFH>     40011: <0000H>
40002: <21CDH>     40012: <0000H>
40003: <04D2H>     40013: <0000H>
40004: <0BD8H>     40014: <0000H>
40005: <0000H>     40015: <0000H>
40006: <0000H>     40016: <0000H>
40007: <0000H>     40017: <0000H>
40008: <0000H>     40018: <0000H>
40009: <0000H>     40019: <0000H>
40010: <0000H>     40020: <0000H>
```

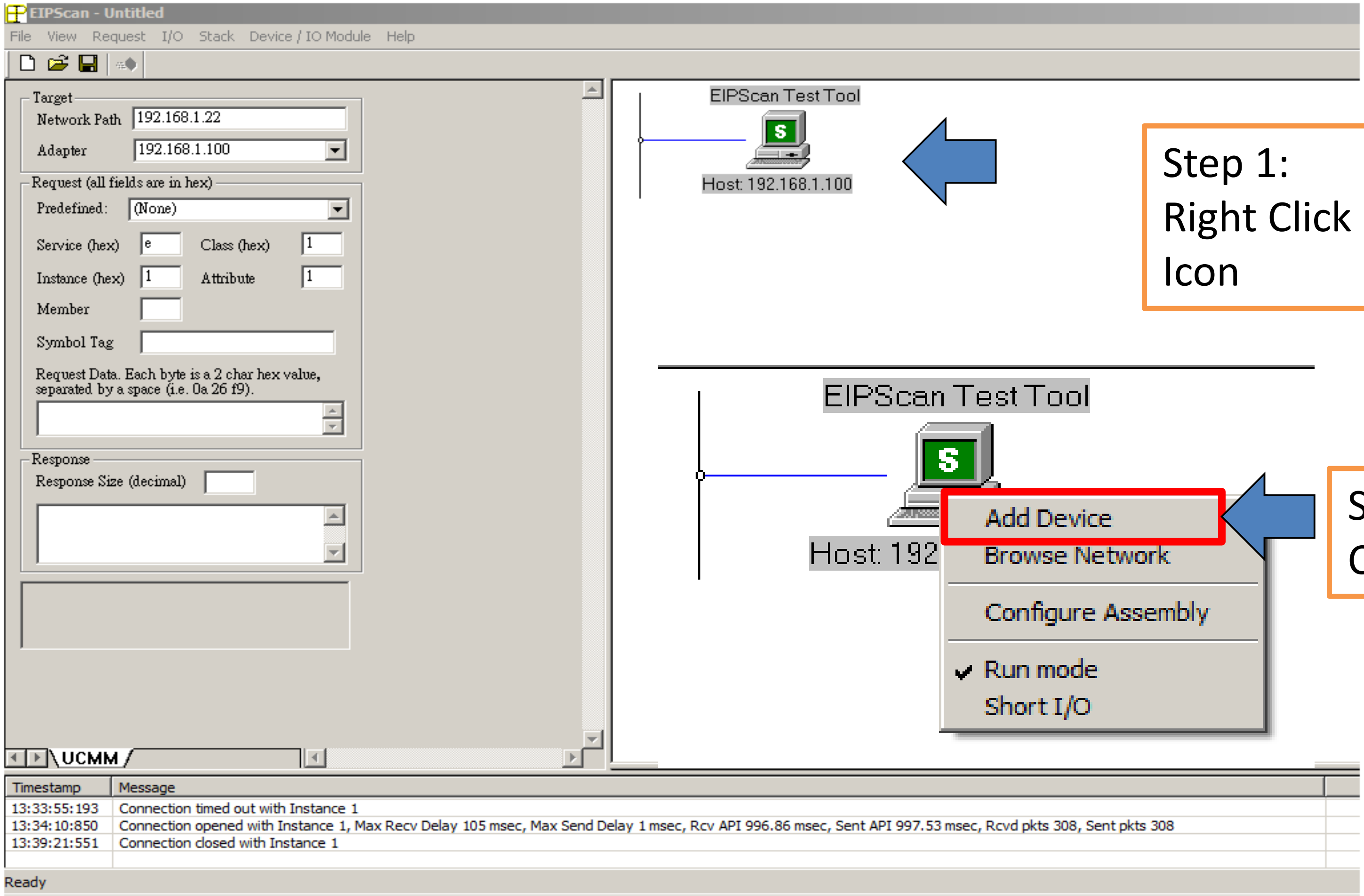
Start to Configure EIPSCAN (1/5)

- If you have more than one network card.
- That would show up the same subnet you would like to connect with EKI-1221IEIMB





Class 1 I/O Data- Set up *EIPScan* Tool (2/5)



Target
Network Path 192.168.1.22
Adapter 192.168.1.100

Request (all fields are in hex)
Predefined: (None)
Service (hex) e
Class (hex) 1
Instance (hex) 1
Attribute 1
Member
Symbol Tag
Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

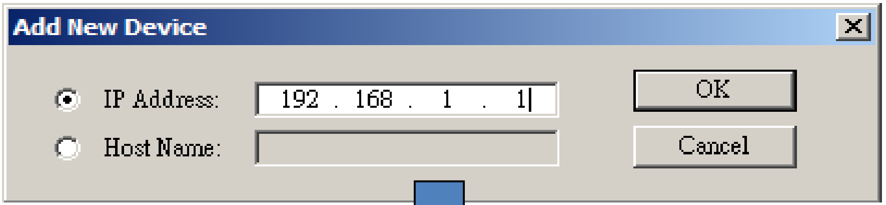
Response
Response Size (decimal)

```
Timestamp     Message
13:33:55:193  Connection timed out with Instance 1
13:34:10:850  Connection opened with Instance 1, Max Recv Delay 105 msec, Max Send Delay 1 msec, Rcv API 996.86 msec, Sent API 997.53 msec, Rcvd pkts 308, Sent pkts 308
13:39:21:551  Connection closed with Instance 1
```

Step 1:
Right Click Mouse in the Host PC Icon

Step 2:
Click the “Add Device”

Add EKI-1221IEIMB Device (3/5)

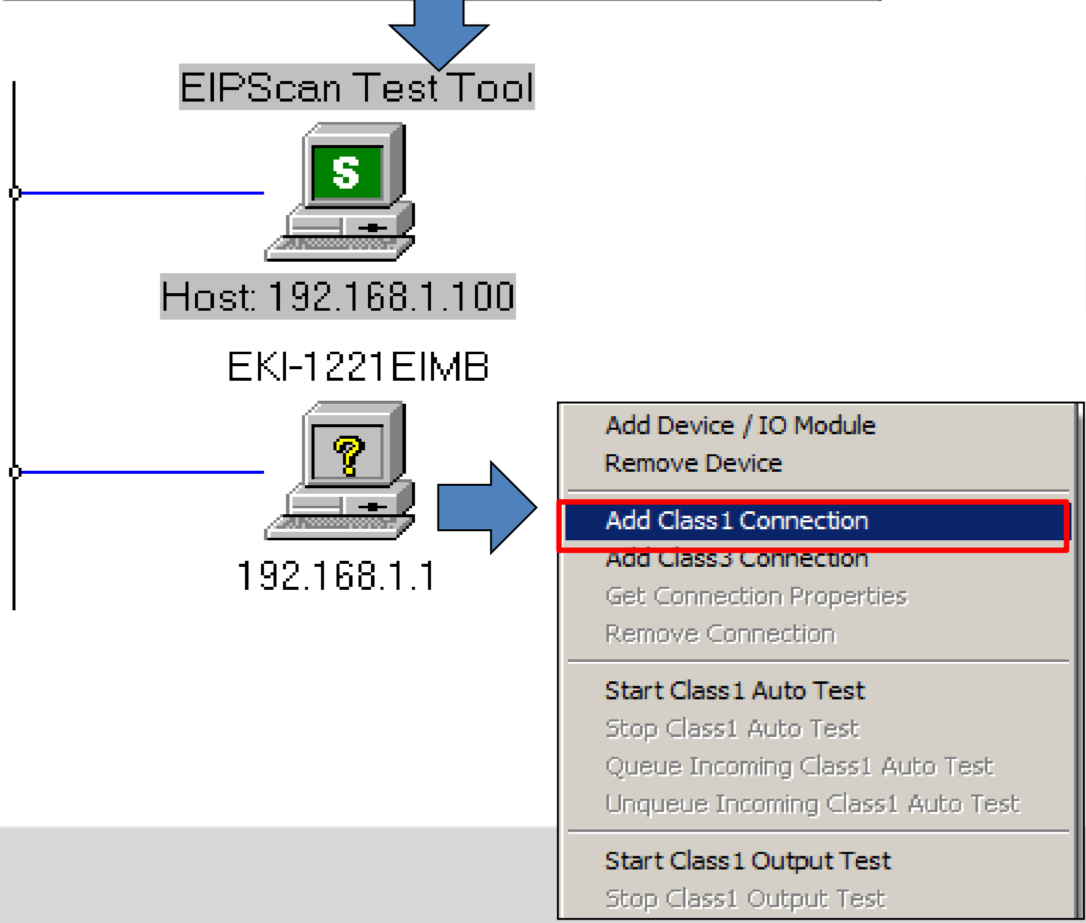


Add New Device

● IP Address: 192 . 168 . 1 . 1

○ Host Name:

Step 3: Key in EKI-1221EIMB IP address;
Using Default EKI-1221IEIMB IP for example

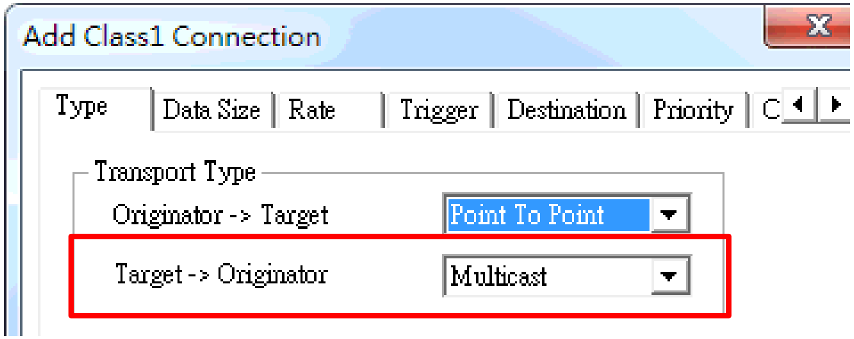


Step 4: you can see the EKI-1221EIMB Computer Icon

Step 5: In the EKI-1221IEIMB Icon. Left mouse
Click to “Add Class1 Connection”

EIPSCAN Parameter Setting (4/5)

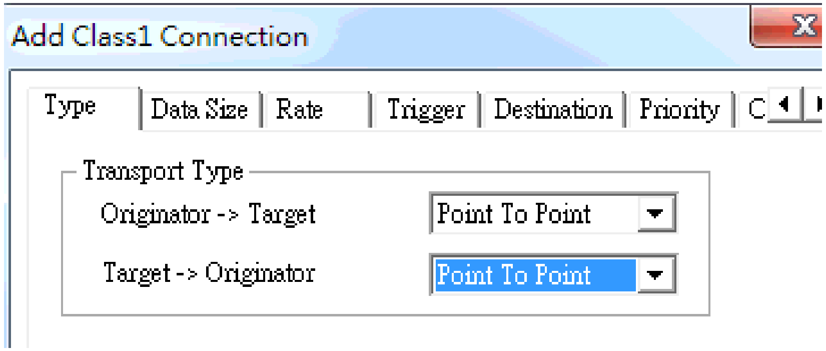
- A new dialogue window will now occur; it contains seven property pages used to set up the connection. In the first page it’s possible to select connection and transport type. To reduce the network load the setting for “Target -> Originator” have been changed from “Multicast” to “Point To Point”, the rest are left unchanged. Both setting is available for EKI-1242EIMS



Transport Type

Originator -> Target: Point To Point

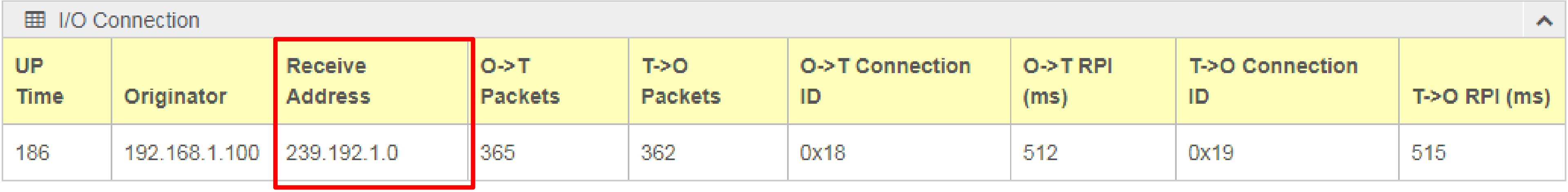
Target -> Originator: Multicast



Transport Type

Originator -> Target: Point To Point

Target -> Originator: Point To Point

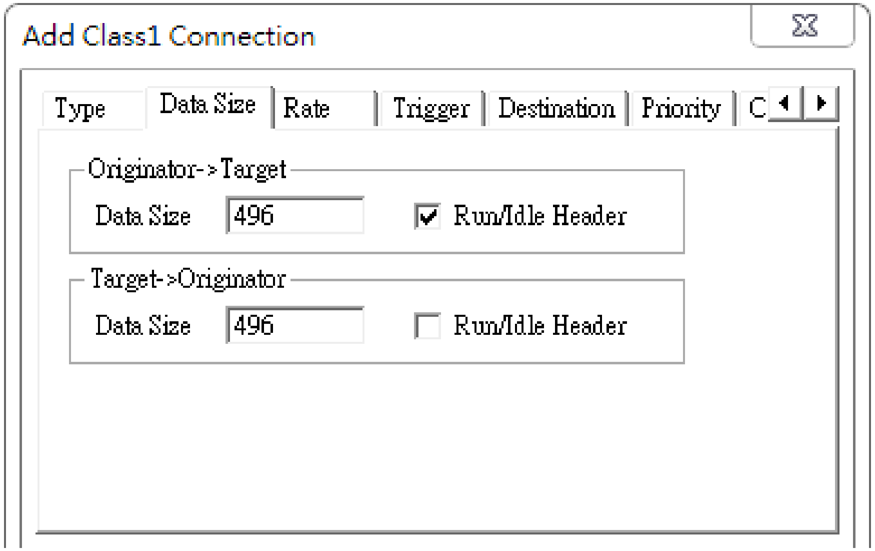


I/O Connection

UP Time	Originator	Receive Address	O->T Packets	T->O Packets	O->T Connection ID	O->T RPI (ms)	T->O Connection ID	T->O RPI (ms)
186	192.168.1.100	239.192.1.0	365	362	0x18	512	0x19	515

EIPSCAN Parameter Setting (4/5)

- The second tile contains the data sizes; here we use 496 bytes in each direction since this is how the module was initiated.

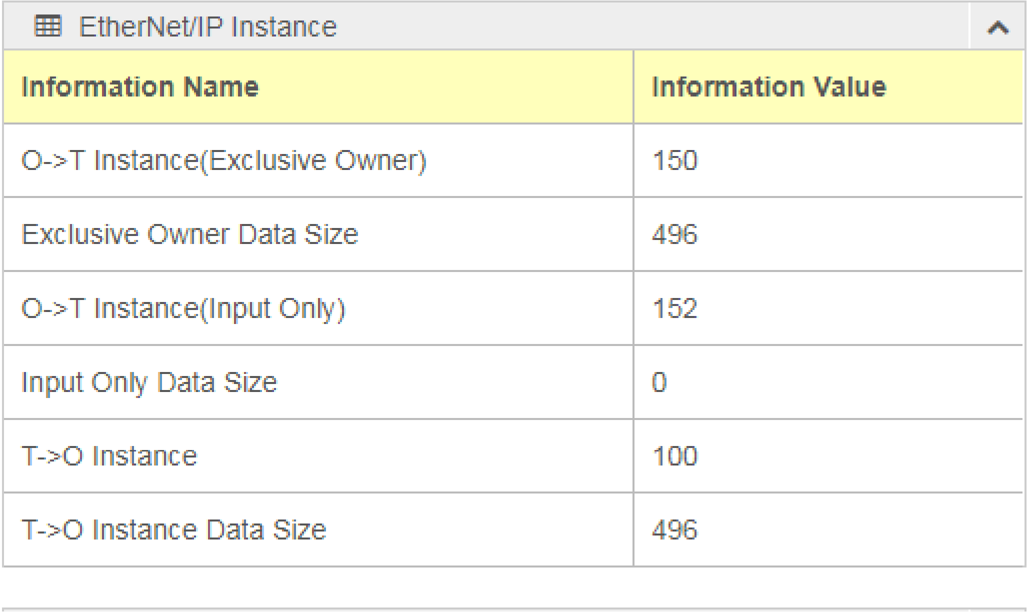


Originator->Target

Data Size: 496 ☑ Run/Idle Header

Target->Originator

Data Size: 496 ☐ Run/Idle Header

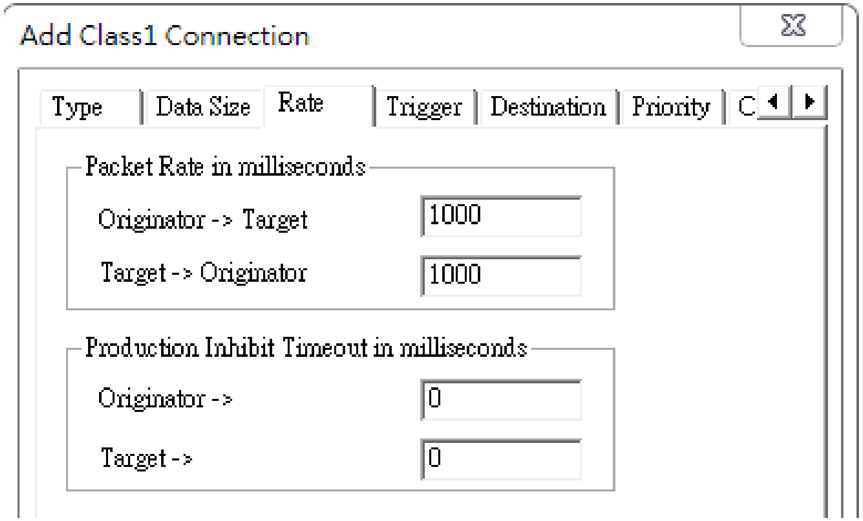


EtherNet/IP Instance

Information Name	Information Value
O->T Instance(Exclusive Owner)	150
Exclusive Owner Data Size	496
O->T Instance(Input Only)	152
Input Only Data Size	0
T->O Instance	100
T->O Instance Data Size	496

EIPSCAN Parameter Setting (4/5)

- The “Rate” tile holds the RPI (requested packet interval), this is how often data will be produced and consumed (in ms)
- In the “Trigger” tile the transport trigger and the timeout multiplier are selected. The EKI-1242EIMS Slave module only supports “Cyclic” triggers. The timeout are set to the default value of 16



Packet Rate in milliseconds

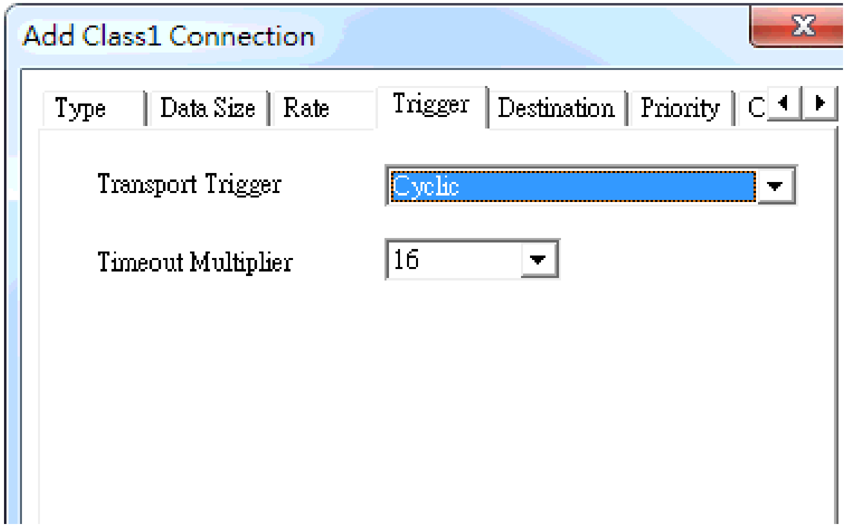
Originator -> Target: 1000

Target -> Originator: 1000

Production Inhibit Timeout in milliseconds

Originator ->: 0

Target ->: 0

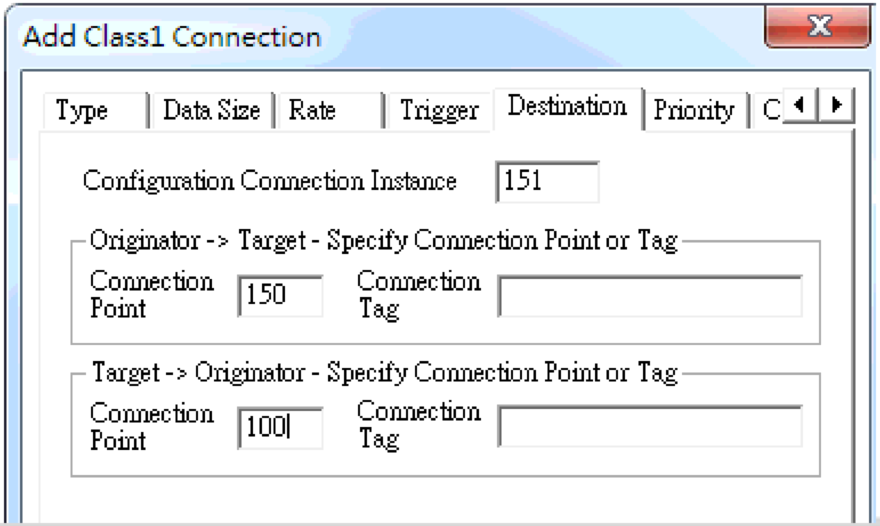


Transport Trigger: Cyclic

Timeout Multiplier: 16

EIPSCAN Parameter Setting (4/5)

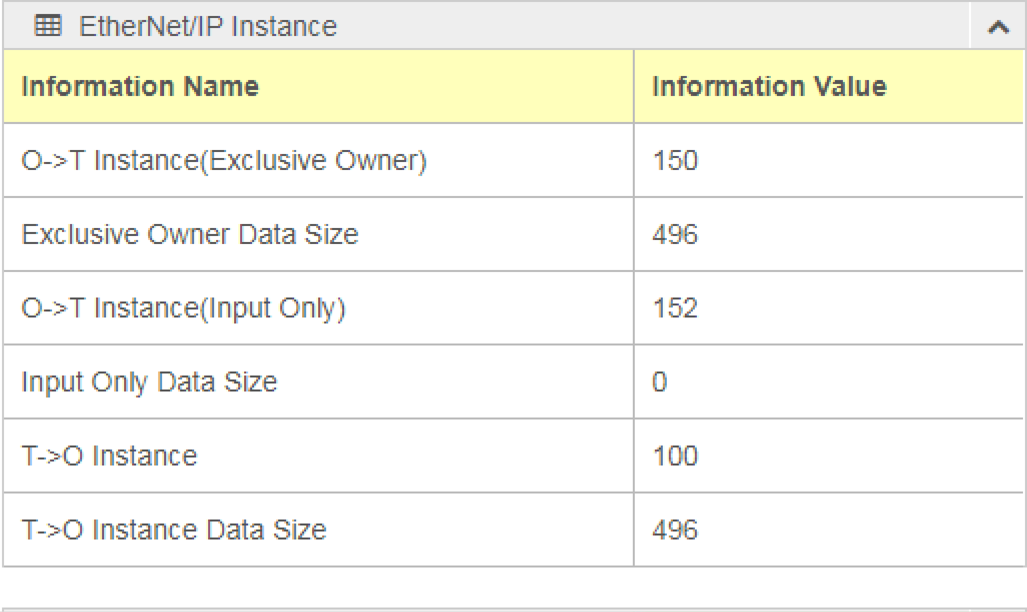
The “Destination” tile is used to set up the connection points in the Advantech EKI-1242EIMS Slave module. The EIPSCan Tool have its default display the correct connection points, make sure that the connection points are configured as below. Adjust the connection points if they do not match what is stated in the user manual or WEBGUI of EKI-1242EIMS for sure.



Configuration Connection Instance: 151

Originator -> Target - Specify Connection Point or Tag
Connection Point: 150
Connection Tag:

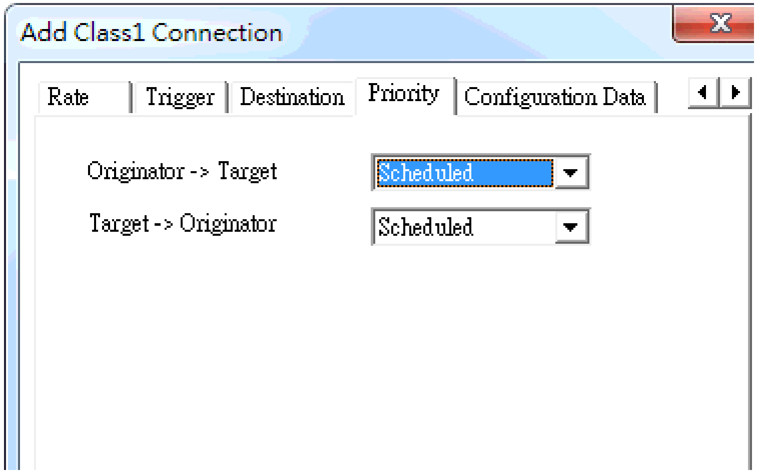
Target -> Originator - Specify Connection Point or Tag
Connection Point: 100
Connection Tag:



Information Name	Information Value
O->T Instance(Exclusive Owner)	150
Exclusive Owner Data Size	496
O->T Instance(Input Only)	152
Input Only Data Size	0
T->O Instance	100
T->O Instance Data Size	496

EIPSCAN Parameter Setting (4/5)

- In the “Priority” tile it is possible to set the priority of the connection, for the moment the EKI-1242EIMS only supports “Scheduled”. Now press “OK” and the connection will be opened.

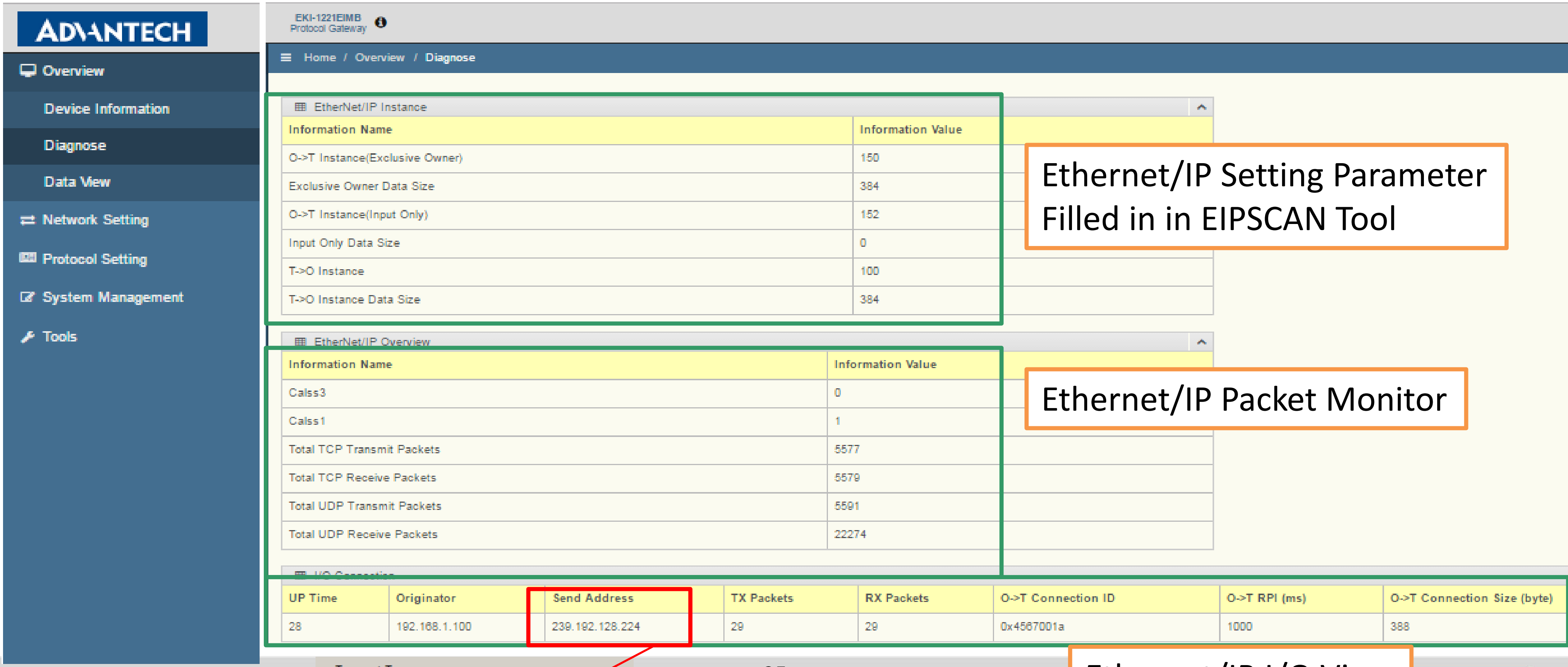


Originator -> Target: Scheduled

Target -> Originator: Scheduled

Ethernet/IP Parameter Diagnose(5/5)

- the Ethernet/IP Data Overview/ IO Connection



EtherNet/IP Instance

Information Name	Information Value
O->T Instance(Exclusive Owner)	150
Exclusive Owner Data Size	384
O->T Instance(Input Only)	152
Input Only Data Size	0
T->O Instance	100
T->O Instance Data Size	384

Ethernet/IP Setting Parameter Filled in in EIPSCAN Tool

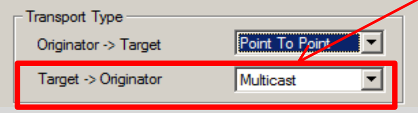
EtherNet/IP Overview

Information Name	Information Value
Calss3	0
Calss1	1
Total TCP Transmit Packets	5577
Total TCP Receive Packets	5579
Total UDP Transmit Packets	5591
Total UDP Receive Packets	22274

Ethernet/IP Packet Monitor

I/O Connection

UP Time	Originator	Send Address	TX Packets	RX Packets	O->T Connection ID	O->T RPI (ms)	O->T Connection Size (byte)
28	192.168.1.100	239.192.128.224	29	29	0x4567001a	1000	388



Transport Type

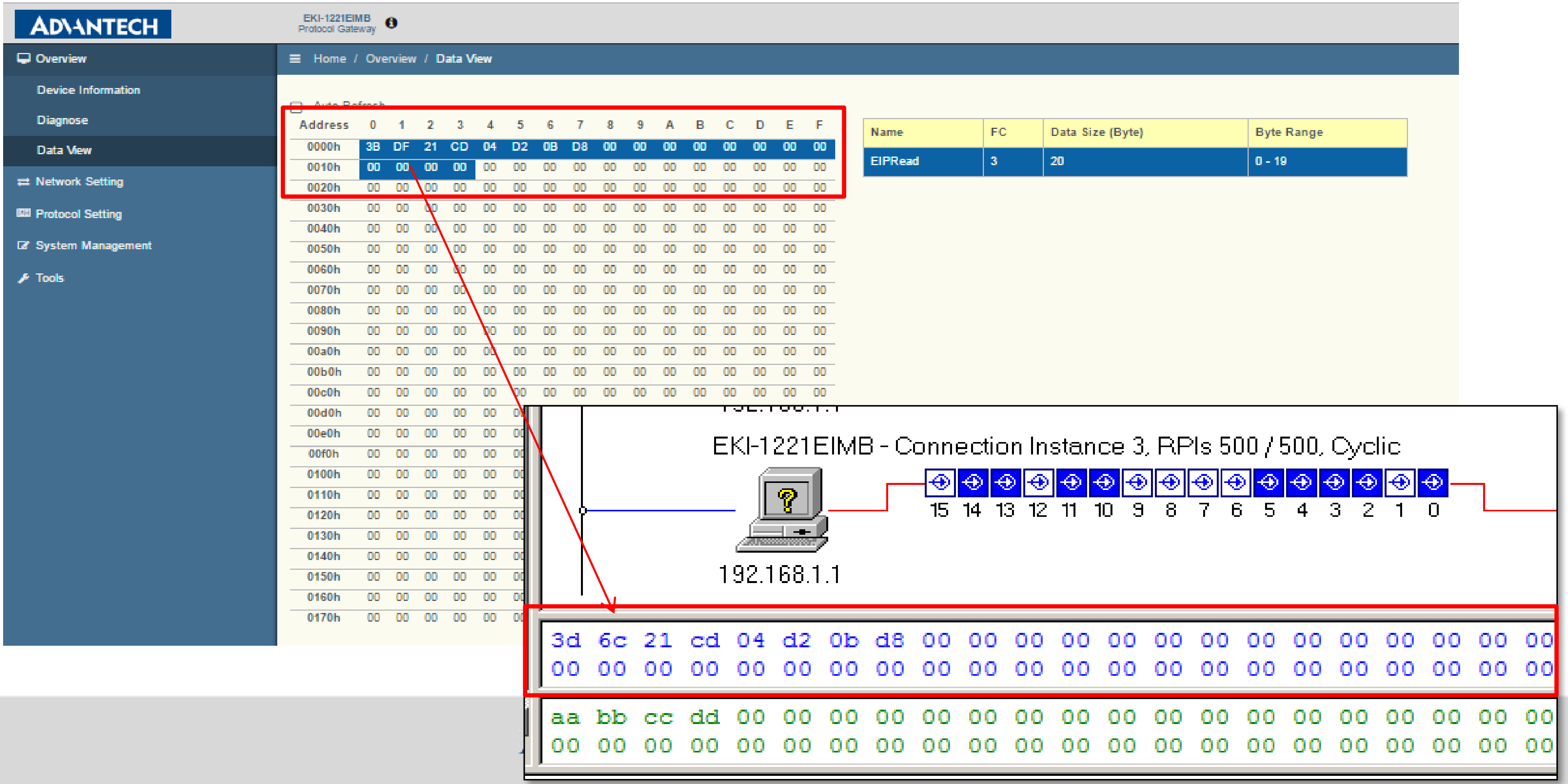
Originator -> Target: Point To Point

Target -> Originator: Multicast

Ethernet/IP I/O View

WEBGUI- Data View

- Compare with the Real time I/O Data *<EIPSCAN>* & Data View in WEBGUI



☐ Auto Refresh

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h	3B	DF	21	CD	04	D2	0B	D8	00	00	00	00	00	00	00	00
0010h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0020h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0050h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0090h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00a0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00b0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00c0h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00d0h	00	00	00	00	00											
00e0h	00	00	00	00	00											
00f0h	00	00	00	00	00											
0100h	00	00	00	00	00											
0110h	00	00	00	00	00											
0120h	00	00	00	00	00											
0130h	00	00	00	00	00											
0140h	00	00	00	00	00											
0150h	00	00	00	00	00											
0160h	00	00	00	00	00											
0170h	00	00	00	00	00											

Name	FC	Data Size (Byte)	Byte Range
EIPRead	3	20	0 - 19

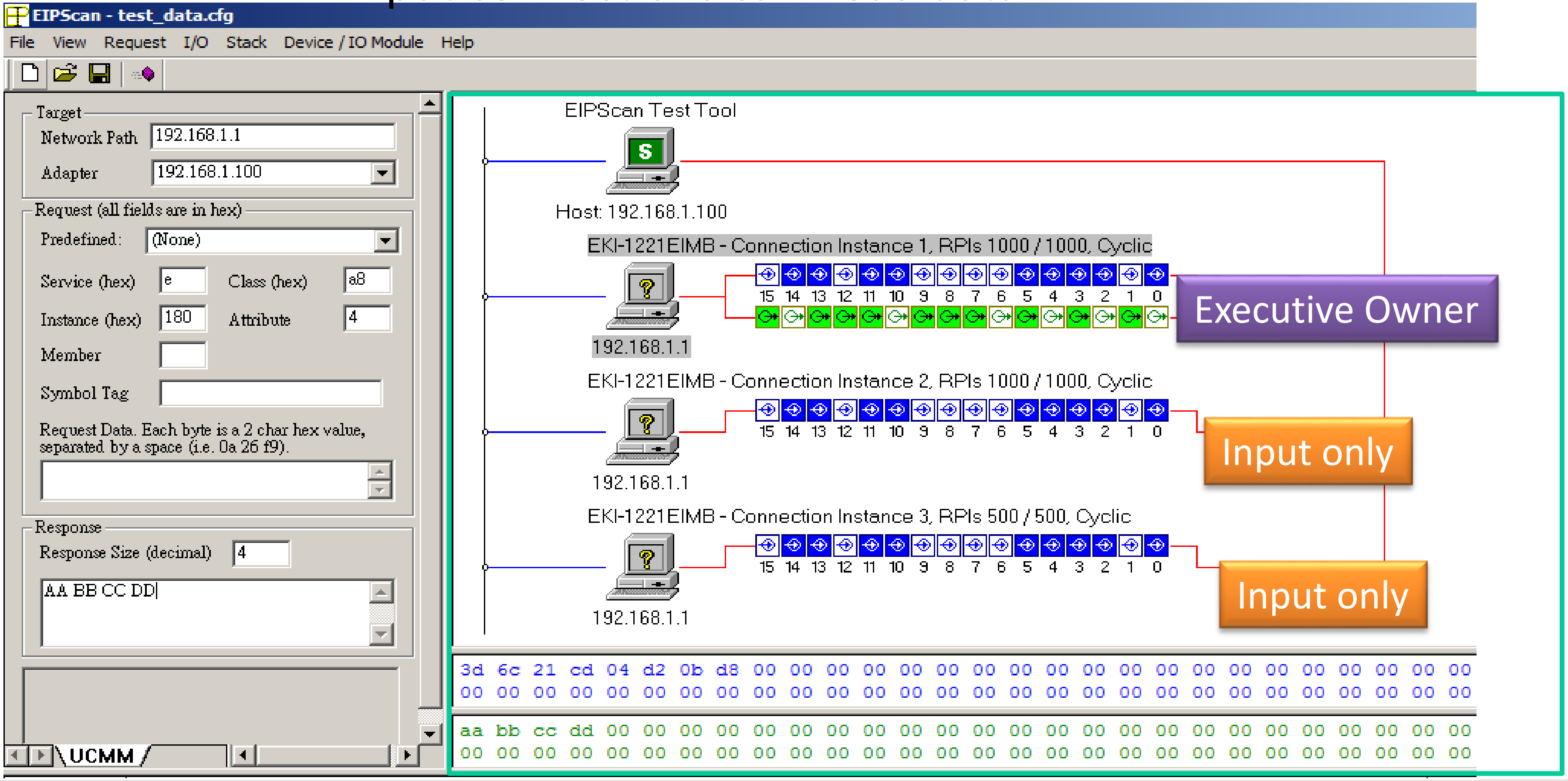
EKI-1221EIMB - Connection Instance 3, RPIs 500 / 500, Cyclic

```
3d 6c 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
aa bb cc dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Class 1-Implicit Message

Class 1 can support 1 Executive Owner can Read/Write
4 Input connections can Read data



Target
Network Path: 192.168.1.1
Adapter: 192.168.1.100

Request (all fields are in hex)
Predefined: (None)
Service (hex): e
Class (hex): a8
Instance (hex): 180
Attribute: 4
Member:
Symbol Tag:

Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

Response
Response Size (decimal): 4
AA BB CC DD

EIPScan Test Tool

Host: 192.168.1.100

EKI-1221EIMB - Connection Instance 1, RPIs 1000 / 1000, Cyclic
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
192.168.1.1

EKI-1221EIMB - Connection Instance 2, RPIs 1000 / 1000, Cyclic
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
192.168.1.1

EKI-1221EIMB - Connection Instance 3, RPIs 500 / 500, Cyclic
15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
192.168.1.1

```
3d 6c 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
aa bb cc dd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

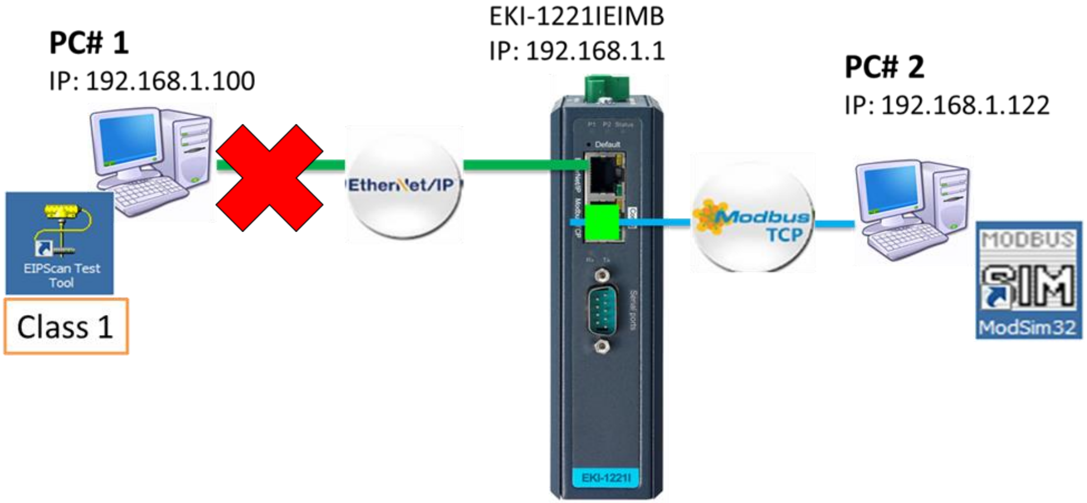
Executive Owner

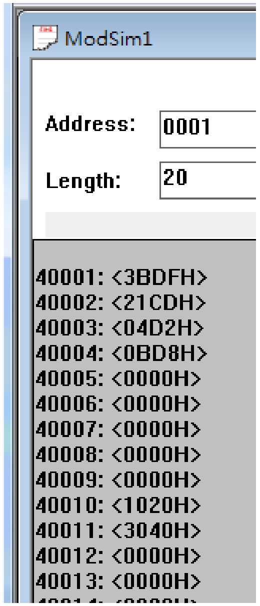
Input only

Input only

Safe value (1/2)

- If PLC is disconnect, EKI-1221IEIMB would send out safe value to end modbus device.

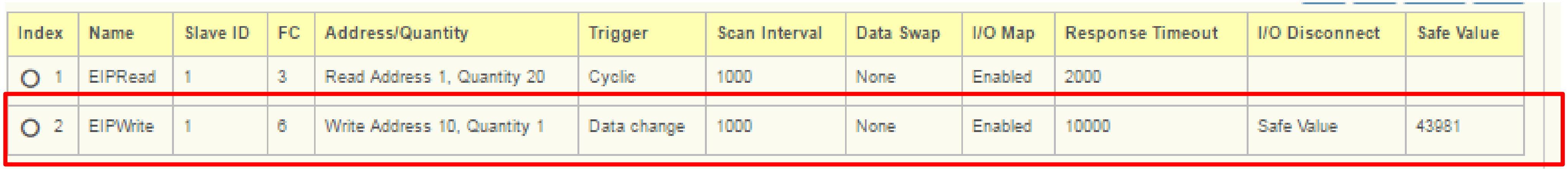




Address: 0001

Length: 20

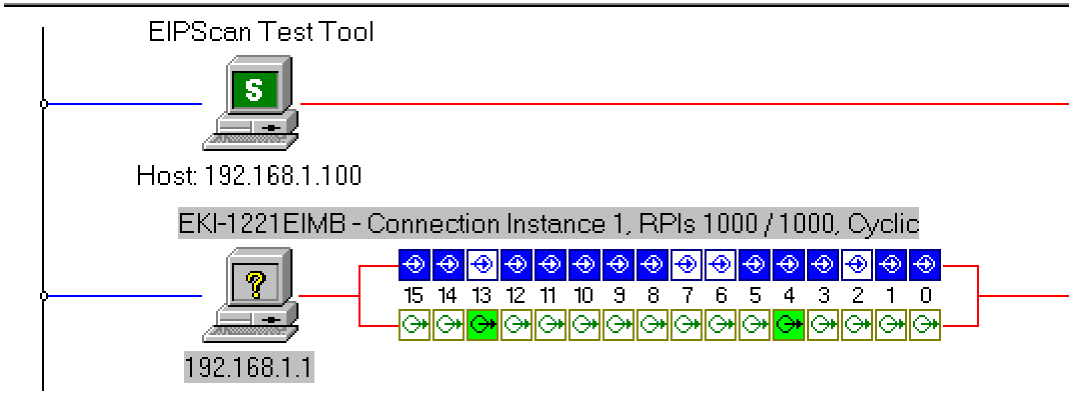
```
40001: <3BDFH>
40002: <21CDH>
40003: <04D2H>
40004: <0BD8H>
40005: <0000H>
40006: <0000H>
40007: <0000H>
40008: <0000H>
40009: <0000H>
40010: <1020H>
40011: <3040H>
40012: <0000H>
40013: <0000H>
```

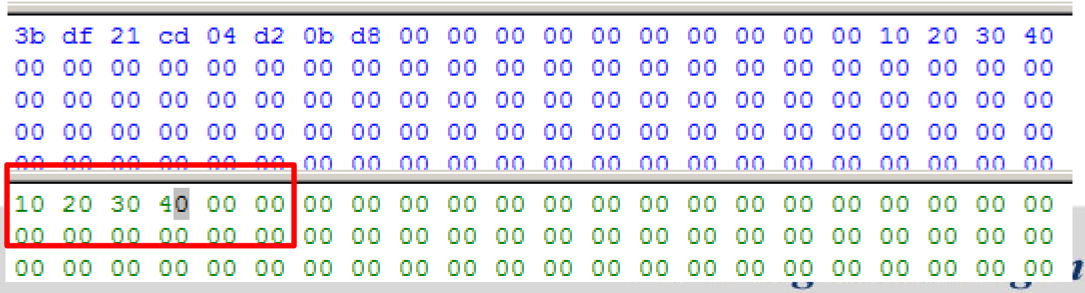


Index	Name	Slave ID	FC	Address/Quantity	Trigger	Scan Interval	Data Swap	I/O Map	Response Timeout	I/O Disconnect	Safe Value
○ 1	EIPRead	1	3	Read Address 1, Quantity 20	Cyclic	1000	None	Enabled	2000		
○ 2	EIPWrite	1	6	Write Address 10, Quantity 1	Data change	1000	None	Enabled	10000	Safe Value	43981

Safe value (2/2)

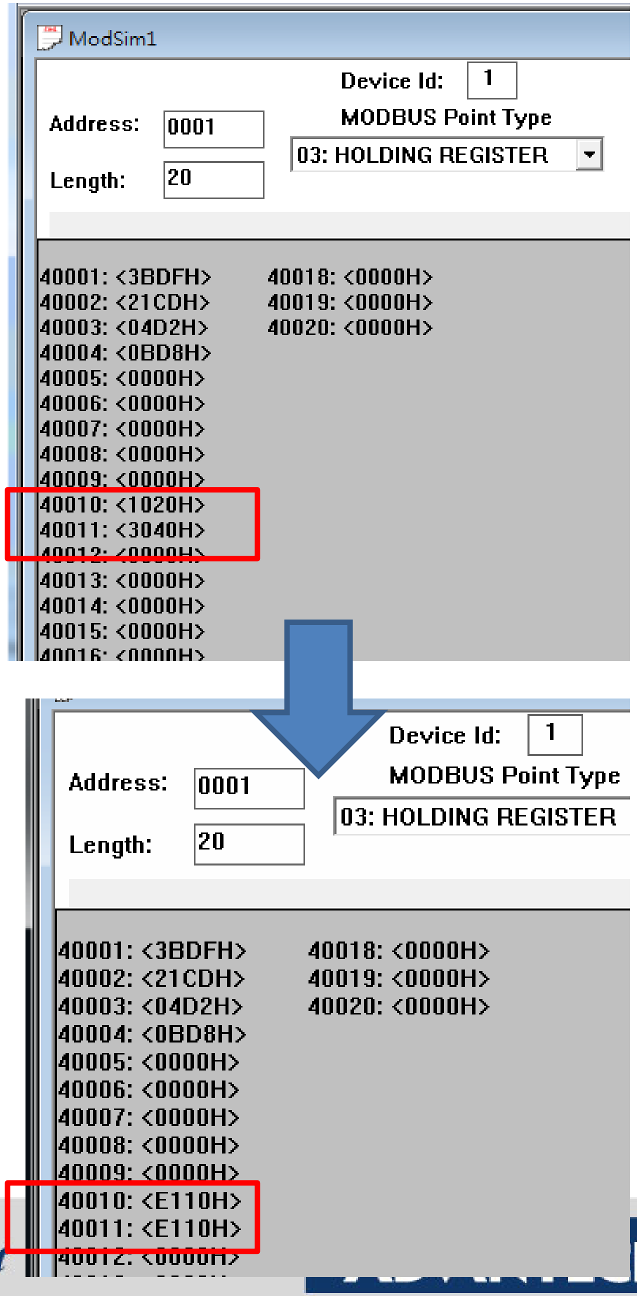
- Simulate when EIPSCAN disconnect and cannot send command data, EKI-1221IEIMB would send out safe value





```
3b df 21 cd 04 d2 0b d8 00 00 00 00 00 00 00 00 00 00 10 20 30 40
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

10 20 30 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



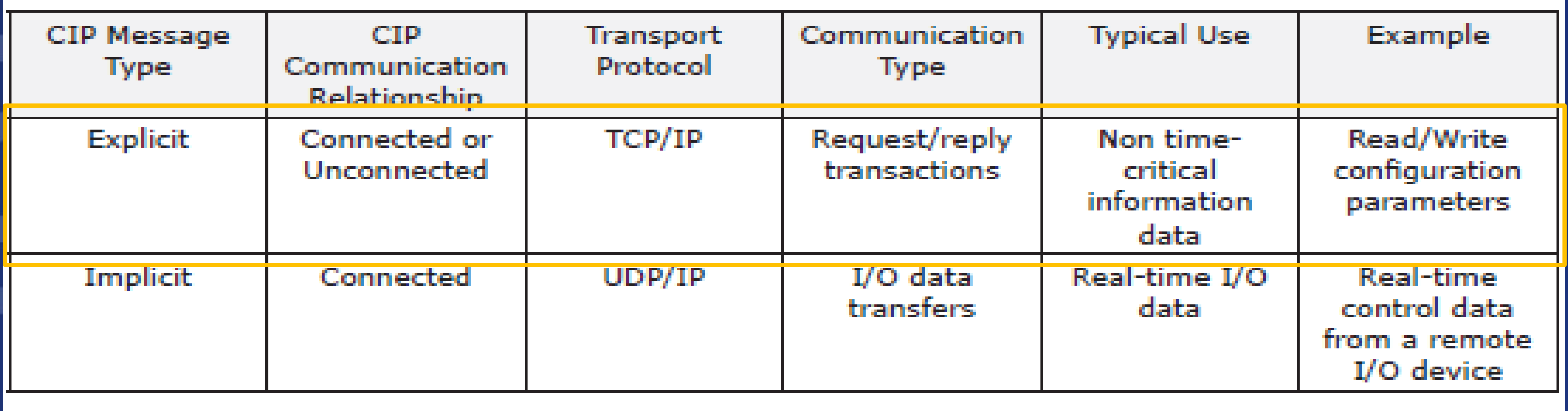
Device Id: 1
Address: 0001
MODBUS Point Type: 03: HOLDING REGISTER
Length: 20

```
40001: <3BDFH>     40018: <0000H>
40002: <21CDH>     40019: <0000H>
40003: <04D2H>     40020: <0000H>
40004: <0BD8H>
40005: <0000H>
40006: <0000H>
40007: <0000H>
40008: <0000H>
40009: <0000H>
40010: <1020H>
40011: <3040H>
40012: <0000H>
40013: <0000H>
40014: <0000H>
40015: <0000H>
40016: <0000H>
```

Device Id: 1
Address: 0001
MODBUS Point Type: 03: HOLDING REGISTER
Length: 20

```
40001: <3BDFH>     40018: <0000H>
40002: <21CDH>     40019: <0000H>
40003: <04D2H>     40020: <0000H>
40004: <0BD8H>
40005: <0000H>
40006: <0000H>
40007: <0000H>
40008: <0000H>
40009: <0000H>
40010: <E110H>
40011: <E110H>
40012: <0000H>
```

Explicit Message to Request/Reply transactions data

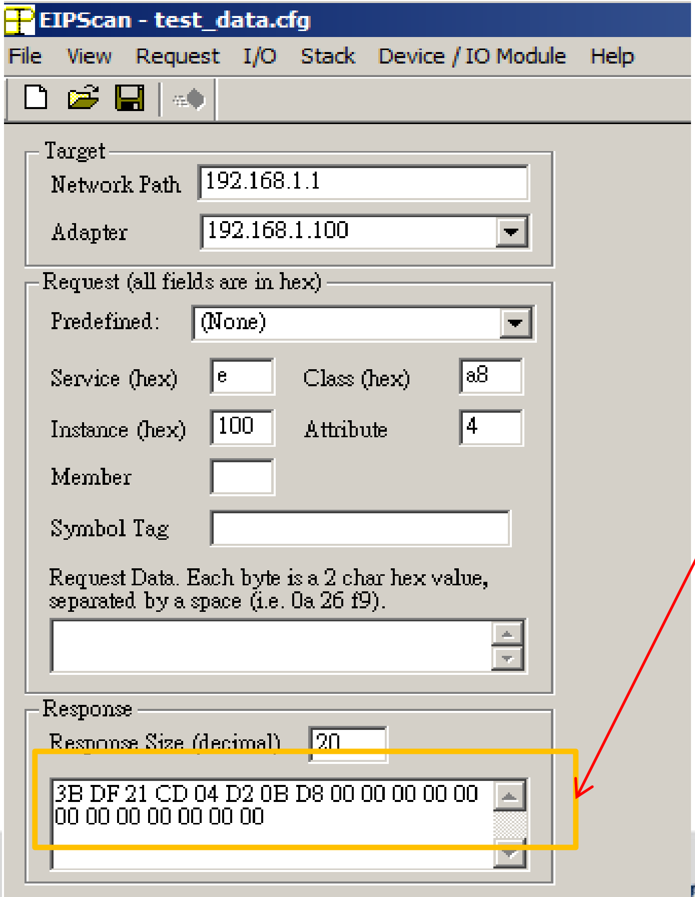


CIP Message Type	CIP Communication Relationship	Transport Protocol	Communication Type	Typical Use	Example
Explicit	Connected or Unconnected	TCP/IP	Request/reply transactions	Non time-critical information data	Read/Write configuration parameters
Implicit	Connected	UDP/IP	I/O data transfers	Real-time I/O data	Real-time control data from a remote I/O device

TCP Data Request

Target:

- Using Class 3 TCP transaction to get the EIPRead single data


EIPScan - test_data.cfg
File View Request I/O Stack Device / IO Module Help
Target
Request (all fields are in hex)
Response

Network Path 192.168.1.1

Adapter 192.168.1.100

Predefined: (None)

Service (hex) e

Class (hex) a8

Instance (hex) 100

Attribute 4

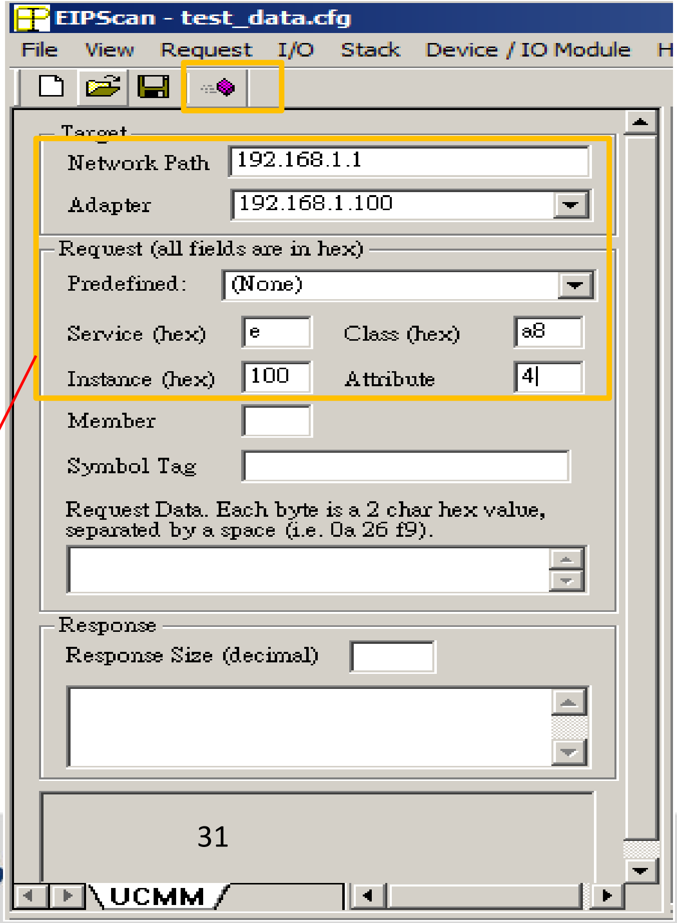
Member

Symbol Tag

Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

Response Size (decimal) 20

```
3B DF 21 CD 04 D2 0B D8 00 00 00 00 00
00 00 00 00 00 00 00
```


EIPScan - test_data.cfg
File View Request I/O Stack Device / IO Module H
Target
Request (all fields are in hex)
Response
UCMM

Network Path 192.168.1.1

Adapter 192.168.1.100

Predefined: (None)

Service (hex) e

Class (hex) a8

Instance (hex) 100

Attribute 4

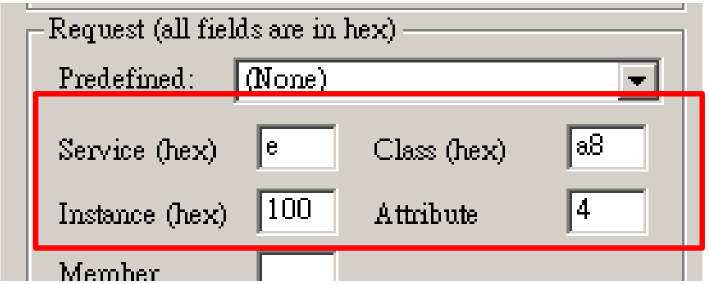
Member

Symbol Tag

Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

Response Size (decimal)

TCP Data Request (1/2)

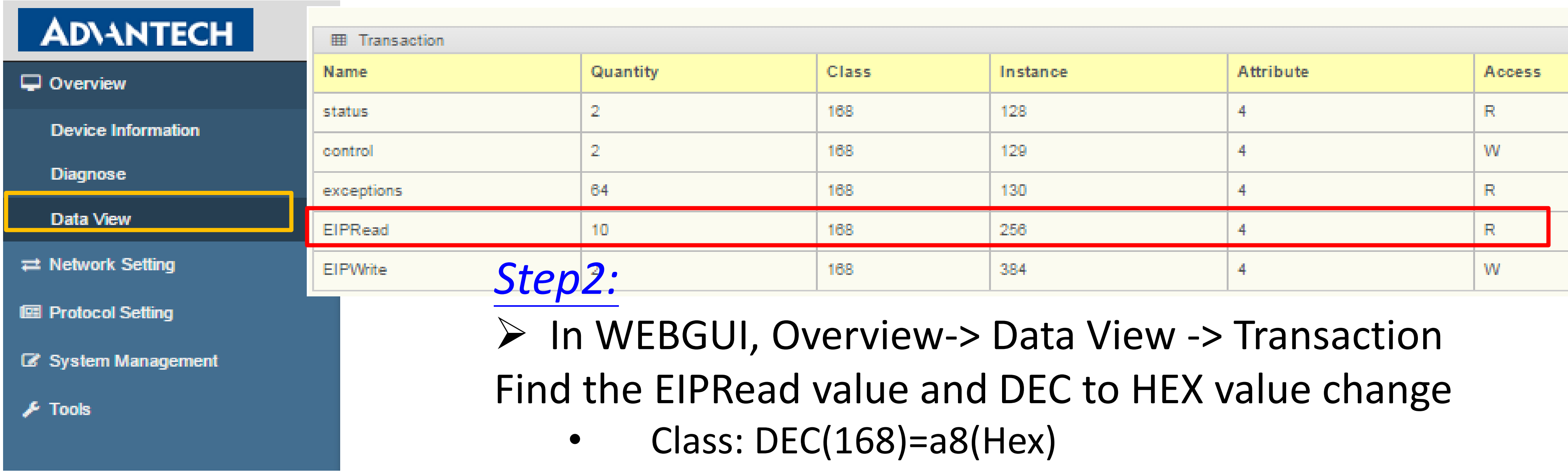


Request (all fields are in hex)

Predefined:	(None)		
Service (hex)	e	Class (hex)	a8
Instance (hex)	100	Attribute	4
Member			

Step1:

- In EIPSCAN Tool, Using TCP transaction to get the single data



Name	Quantity	Class	Instance	Attribute	Access
status	2	168	128	4	R
control	2	168	129	4	W
exceptions	64	168	130	4	R
EIPRead	10	168	256	4	R
EIPWrite	2	168	384	4	W

Step2:

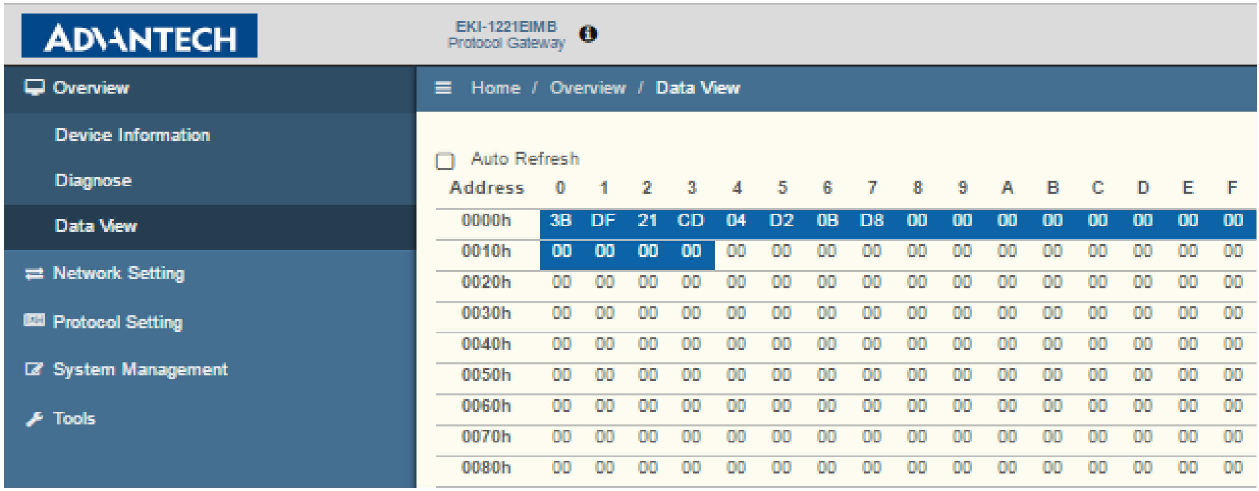
➢ In WEBGUI, Overview-> Data View -> Transaction Find the EIPRead value and DEC to HEX value change

- Class: DEC(168)=a8(Hex)
- Instance: DEC(256)=100(hex)

TCP Data Request (2/2)

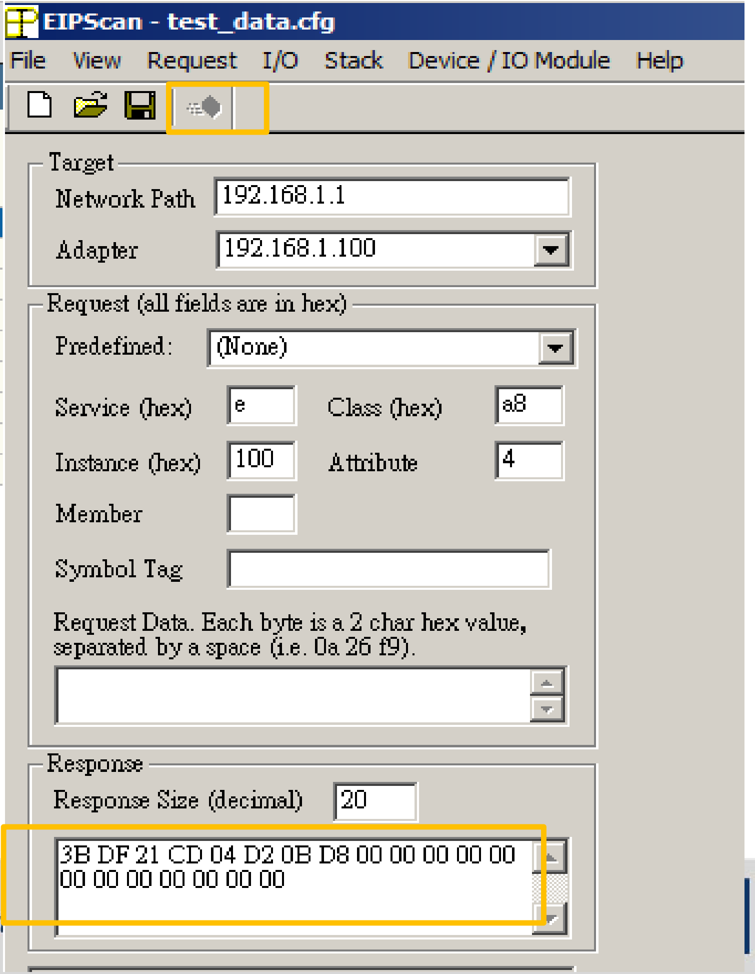
Step3:

- Compare with the single Transaction data & it can be seen in the Data View



☐ Auto Refresh

Address	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h	3B	DF	21	CD	04	D2	0B	D8	00	00	00	00	00	00	00	00
0010h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0020h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0040h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0050h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0060h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0070h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0080h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00



Target

Network Path: 192.168.1.1

Adapter: 192.168.1.100

Request (all fields are in hex)

Predefined: (None)

Service (hex): e

Class (hex): a8

Instance (hex): 100

Attribute: 4

Member:

Symbol Tag:

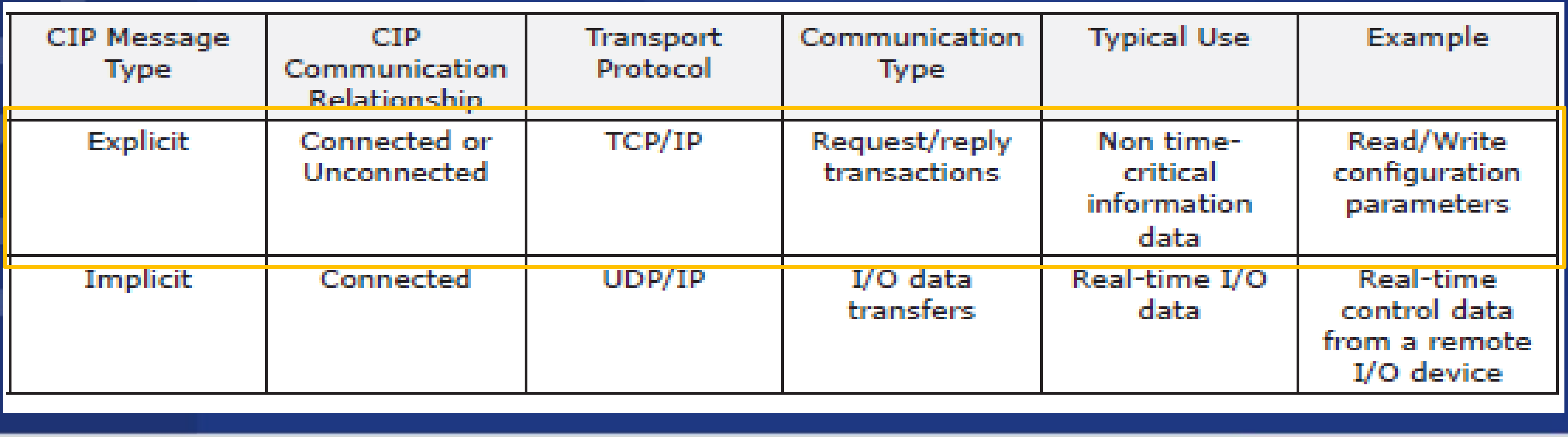
Request Data. Each byte is a 2 char hex value, separated by a space (i.e. 0a 26 f9).

Response

Response Size (decimal): 20

```
3B DF 21 CD 04 D2 0B D8 00 00 00 00 00
00 00 00 00 00 00 00
```

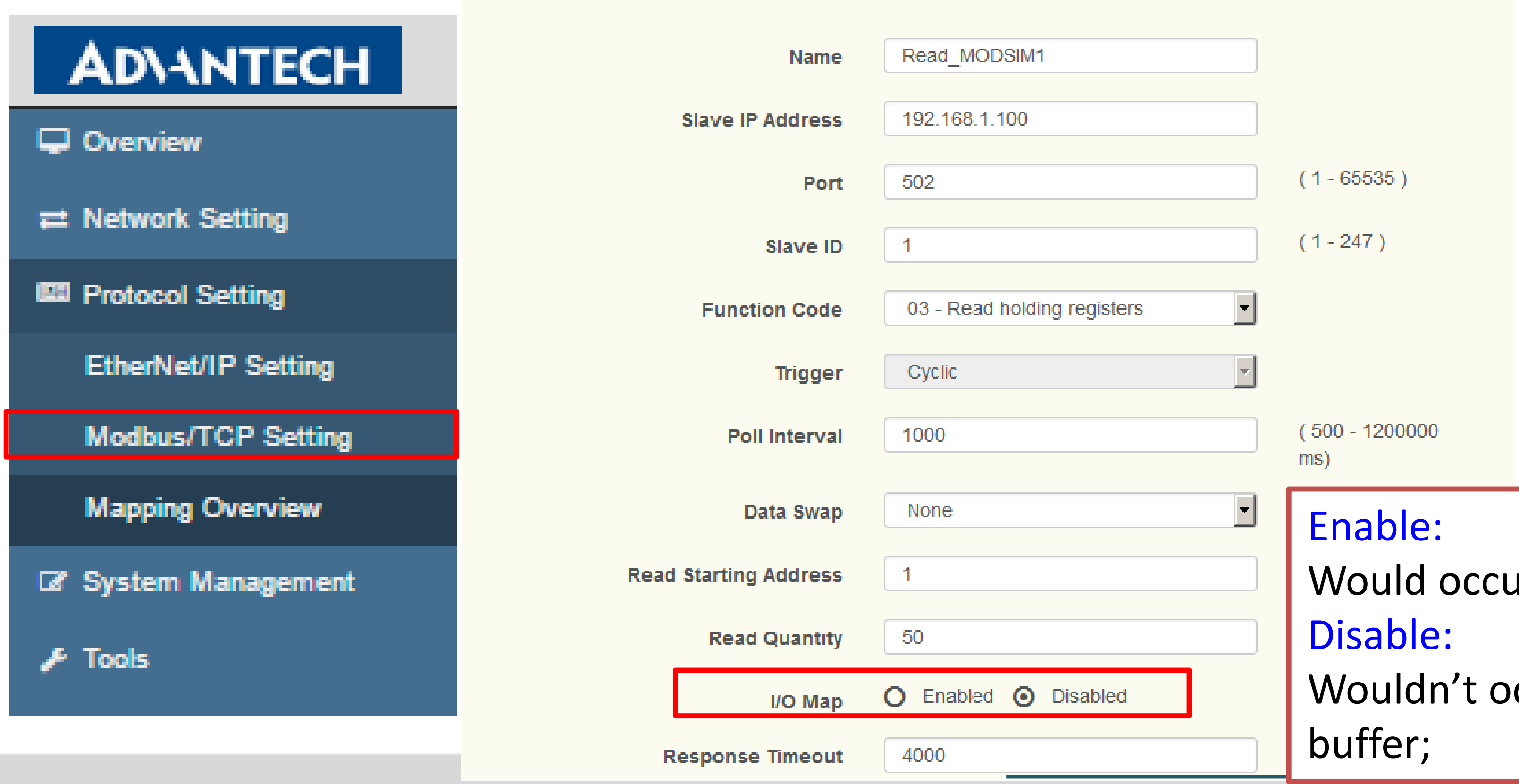
Without occupy I/O Map and query via Explicit message



CIP Message Type	CIP Communication Relationship	Transport Protocol	Communication Type	Typical Use	Example
Explicit	Connected or Unconnected	TCP/IP	Request/reply transactions	Non time-critical information data	Read/Write configuration parameters
Implicit	Connected	UDP/IP	I/O data transfers	Real-time I/O data	Real-time control data from a remote I/O device

Adding Modbus Polling Sessions

- Filled in the Modbus/TCP read/write data sessions you would like to query
- If you don’t want to occupy the I/O Map choose Disable <max total 384 bytes for read/write>

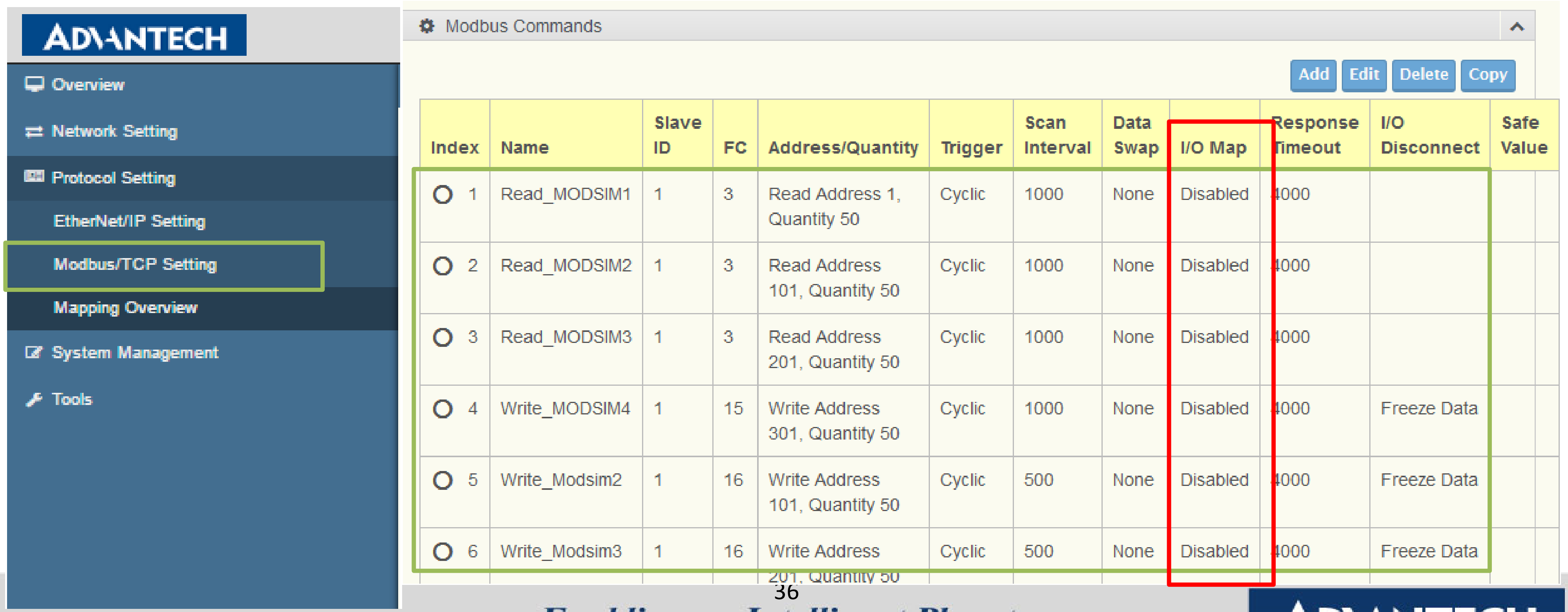


Name	Read_MODSIM1	
Slave IP Address	192.168.1.100	
Port	502	(1 - 65535)
Slave ID	1	(1 - 247)
Function Code	03 - Read holding registers	
Trigger	Cyclic	
Poll Interval	1000	(500 - 1200000 ms)
Data Swap	None	
Read Starting Address	1	
Read Quantity	50	
I/O Map	○ Enabled ● Disabled	
Response Timeout	4000	

Enable:
Would occupy total buffer;
Disable:
Wouldn’t occupy total buffer;

Modbus/TCP Polling Sessions

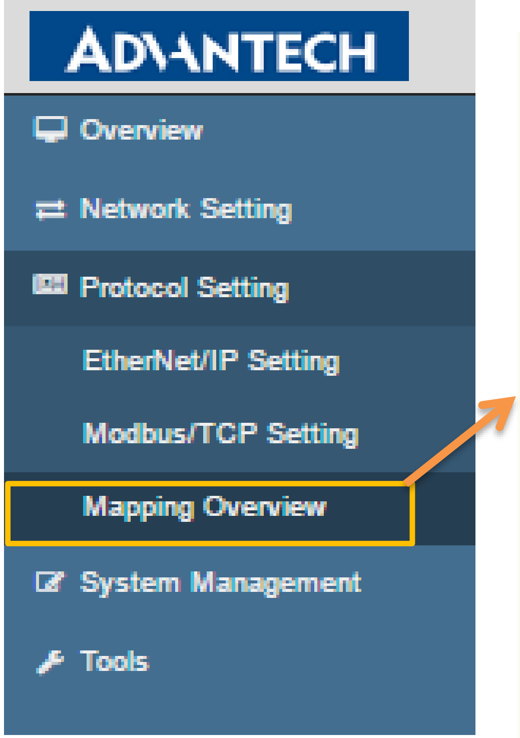
- Max can build 64 Modbus/TCP Sessions
- Max can occupy 384 read/write I/O Map
- Using Add/Edit/Delete/Copy to modify Modbus/TCP sessions

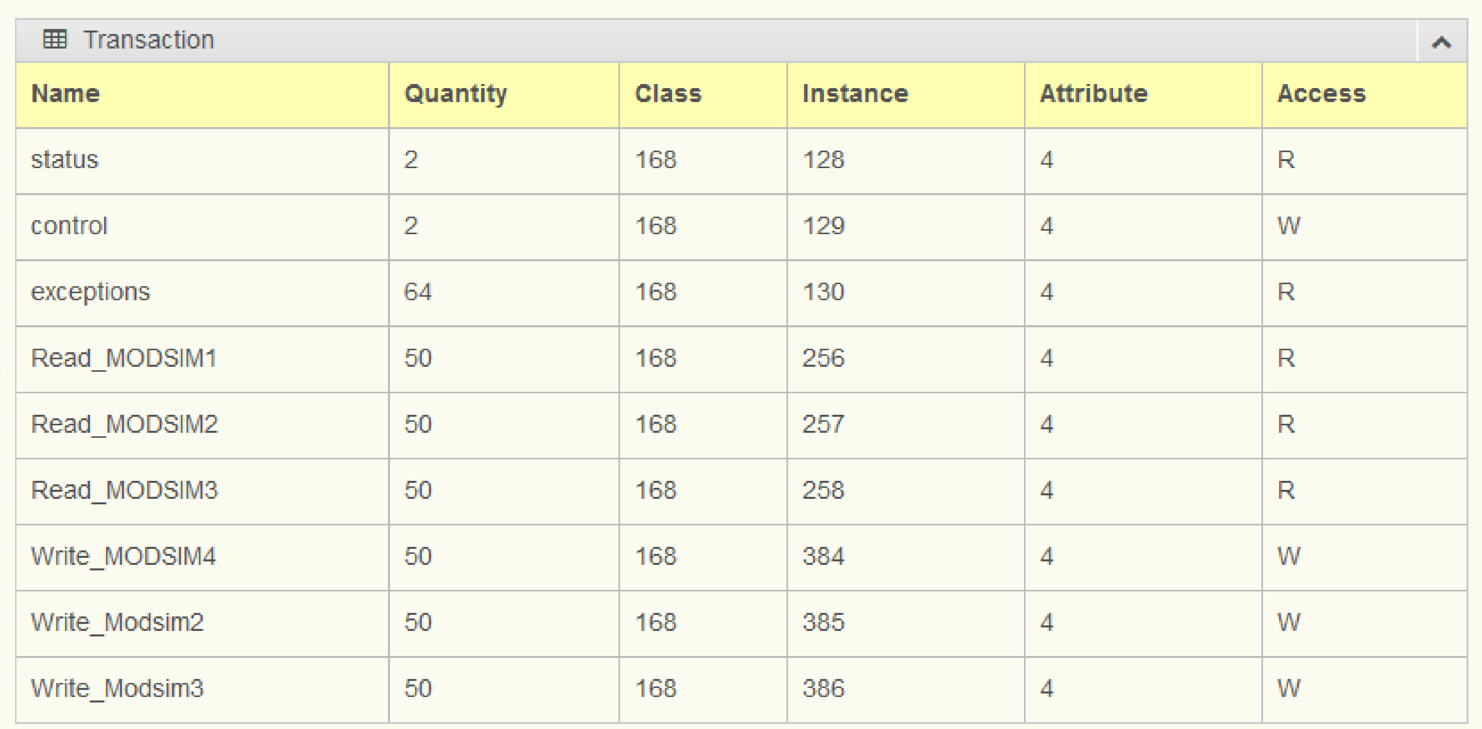


Index	Name	Slave ID	FC	Address/Quantity	Trigger	Scan Interval	Data Swap	I/O Map	Response Timeout	I/O Disconnect	Safe Value
○ 1	Read_MODSIM1	1	3	Read Address 1, Quantity 50	Cyclic	1000	None	Disabled	4000		
○ 2	Read_MODSIM2	1	3	Read Address 101, Quantity 50	Cyclic	1000	None	Disabled	4000		
○ 3	Read_MODSIM3	1	3	Read Address 201, Quantity 50	Cyclic	1000	None	Disabled	4000		
○ 4	Write_MODSIM4	1	15	Write Address 301, Quantity 50	Cyclic	1000	None	Disabled	4000	Freeze Data	
○ 5	Write_Modsim2	1	16	Write Address 101, Quantity 50	Cyclic	500	None	Disabled	4000	Freeze Data	
○ 6	Write_Modsim3	1	16	Write Address 201, Quantity 50	Cyclic	500	None	Disabled	4000	Freeze Data	

Mapping Overview Information

In the Mapping Overview, it would occupy the I/O data in the input/output part. And you can see the Transaction you would query by using explicit message





Name	Quantity	Class	Instance	Attribute	Access
status	2	168	128	4	R
control	2	168	129	4	W
exceptions	64	168	130	4	R
Read_MODSIM1	50	168	256	4	R
Read_MODSIM2	50	168	257	4	R
Read_MODSIM3	50	168	258	4	R
Write_MODSIM4	50	168	384	4	W
Write_Modsim2	50	168	385	4	W
Write_Modsim3	50	168	386	4	W

Enabling an Intelligent Planet