PYRAMIDSOLUTIONS

VISIONARY SOLUTIONS ▲ EXCEPTIONAL RESULTS

BridgeWay Ethernet to J1939 Gateway User Manual

Part No. AB7645
For Firmware Revision 2.07.01 and Later

Pyramid Solutions, Inc.
30200 Telegraph Road, Suite 440
Bingham Farms, MI 48025

www.pyramidsolutions.com | P: 248.549.1200 | F: 248.549.1400

Table of Contents

Warranty 7

Preface 9
- **Important User Information** 9
- **Related Documentation** 10

BridgeWay Module Description 11
- **Overview** 11
- **Theory of Operation** 12
- **J1939 Features** 13
- **Ethernet Features** 13
- **IT-Features** 14
- **System Requirements** 15
  - Required Hardware 15
  - Optional Hardware 15
  - Required Software 15
- **Hardware Description** 16

Installation 17
- **Installation and Operation Requirements** 17
- **Power and Network Connections** 18
- **Connecting Power** 19
- **Connecting J1939** 20
- **Connecting to Ethernet** 21
- **Configuration Port Connector** 21

Configuration 22
- **BridgeWay Configuration Tool (BWConfig)** 22
  - Installing the Tool 22
  - Connecting to the BridgeWay Module 23
  - Starting the Tool 23
  - BWConfig User Interface 24
- **Ethernet Network Configuration** 27
  - Setting the IP Address with BWConfig 27
  - Setting the IP Address with the Configuration Switch 29
  - Setting the IP Address Using DHCP/BootP 30
  - Setting the IP Address Using the Web Page 33
  - IP Address Initialization 35
- **J1939 Network Configuration** 37
  - Setting the J1939 NAME 39
- **J1939 I/O Configuration** 40
  - Inputs Versus Outputs 40
  - I/O Configuration Limits 40
  - Data Point Parameters 41
  - J1939 Diagnostic Tables 46

Example Application 48
- **Scenario #1 - EtherNet/IP** 48
- **Ethernet Network Configuration** 49

J1939 Network Configuration **49**
J1939 I/O Configuration **50**
Input Data Points 50
Output Data Points 52
Scenario #2 - Modbus/TCP **53**
Ethernet Network Configuration **54**
J1939 Network Configuration **54**
J1939 I/O Configuration **55**
Input Data Points 55
Output Data Points 57

EtherNet/IP Interface **58**
Product Features **58**
CIP Objects **58**
CIP Messaging **59**
I/O Messaging **60**
Assembly Objects and Connections **61**
Connection Points 61
Input Assembly 62
Output Assembly 63
Status Assembly 64
I/O Data Summary **66**
Using ControlLogix with the Gateway **68**

Modbus/TCP Interface **70**
Supported Commands **70**
Supported Exception Codes **71**
Modbus/TCP Addressing **72**
I/O Data Content **74**
Input Table 74
Output Table 75
Status Data Table 77
I/O Data Summary **79**
I/O Data Format **81**

J1939 Interface **82**
Address Management **82**
Single Configured Address 82
Multiple Configured Addresses 82
Address Loss 83
Invalid Addresses 83
Request for Address Claimed 83
Communications Methods **83**
Message Transmission **84**
Data Point to Message Relationship 84
Message Assembly 84
Automatic Transmission 85
Handling Request PGNs 86
Destination Addresses 86

Message Priority 86
Receiving Messages 87
Handled Messages 87
Input Table Update 87
Parameter Timeout Indication 88
Transport Protocol for Large Messages 89
Transmission of Large Messages 89
Reception of Large Messages 89
Limitations 89
J1939 Diagnostic Messages 90
Diagnostic Table Format 90
Bus-Off Reset Option 94
Option Disabled 94
Option Enabled 94
WARNING 94
Offline Detection 95
Online/Offline Status Indication 95
How Offline Detection Works 95
Offline Detection Message and Timer 96
Offline Detection with Offline Detection Message Disabled 97
Offline Detection with Offline Detection Message Enabled 97
J1939 Baud Rate 98

File System 99
File System Conventions 99
Case Sensitivity 99
Filename / Pathname length 99
File Size 99
Free space 99
Security 100
Normal mode 100
Administration Mode 101
Structure 102
Default Files 103
Virtual File System 104
System Files 104
Configuration Files 105
'ethcfg.cfg' 105
'ip_accs.cfg' 107
Password Files 109
'sys_pswd.cfg & ad_pswd.cfg' 109
'web_accs.cfg' 110
Other Files 111
'telwel.cfg' 111
Email files (email_1.cfg,email_2.cfg to email_10.cfg) 112
BridgeWay Web Page Files 115
'\index.htm' (Re-Direct Page) 115
'\web\index.htm' (Home Page) 115

'\web\BW_Settings.htm' (Settings) 115
'\web\IOAssemblyView.htm' (IOAssemblyView) 115
'\web\IOTableView.htm' (IOTableView) 115

IT Functionality 116
Default User Accounts 116
The FTP Server 117
Normal Mode / Normal User 117
Administration Mode / Admin User 117
The Telnet Server 117
Normal Mode / Normal User 117
Administration Mode / Admin User 117
General Commands 118
Diagnostic Commands 119
File System Operations 120
HTTP Server 123
Virtual Files 123
Security 124
SSI Functionality 124
Ethernet Address Display Functions 124
Store Function 128
Formatted Display 129
Formatted Input 134
Text Function 136
File Functions 137
String Functions 139
Email Client 141
SSI Includes in emails 141
Displaying I/O Data on a Web Page 142

Status and Diagnostics 143
BridgeWay LEDs 143
BridgeWay Status LED 143
J1939 Status LED 144
Ethernet Activity LED 144
Ethernet Link LED 144
Ethernet Module Status LED 145
Ethernet Network Status LED 145
J1939 Status Codes 147
J1939 General Status 147
J1939 Error Status 147
Diagnostic Web Pages 148
Status and Settings Web Page 148
I/O Assembly View Web Page 148
I/O Table View Web Page 148
Status Assembly 148

Specifications 149
Environmental Specifications 149

Temperature....149
EMC Directive Compliance....149
Electrical Specifications....149
DC Power....149
Mechanical Specifications....150
Mechanical Rating....150
DIN Rail Mount....150
Dimensions....150
I/O Data Sizes....151
J1939 Specifications....151
Message Types....151
Addressing....151
Transport Protocol Sessions....151
Connectors....152
Power....152
J1939....153
Ethernet RJ45....154
Configuration RS-232 9 Pin D-Subminiature....155
Support....156
Technical Product Assistance....156
Contact Information....156

Warranty

Pyramid Solutions warrants solely to the initial end-user buyer of this product that this product will, for one year after shipment by Pyramid Solutions (the "Warranty Period"), conform to Pyra- mid Solutions' written specifications for this product.

Pyramid Solutions' sole and exclusive obligation, and Buyer's sole remedy for failure of this prod- uct to conform to the above warranty, is, at the option of Pyramid Solutions, that Pyramid Solu- tions will repair or replace this product or refund the monies paid for this product. The purchaser must notify Pyramid Solutions of any nonconformity during the Warranty Period. In the case of replacement of a non-conforming product, the Warranty Period will be tolled beginning on the date upon which Pyramid Solutions receives the non-conforming product and will begin to run again when the purchaser of this product receives the repaired or replacement product.

The warranty will not apply if this product: (1) fails, malfunctions, or is damaged as a result of handling, installation, maintenance, removal, modification or repair other than as specified in Pyr- amid Solutions' then-current user manual or similar documentation; (2) suffers a casualty or is sub- jected to abuse (including electrostatic discharge) or improper use; (3) is altered or damaged so that Pyramid Solutions is unable to verify the defect with its normal test equipment; or (4) is not returned in the same or equivalent container in which it was shipped.

EXCEPT AS EXPRESSLY WARRANTED ABOVE, THIS PRODUCT IS SUPPLIED "AS IS" AND WITH ALL FAULTS. PYRAMID SOLUTIONS MAKES NO OTHER REPRESENTA- TIONS OR WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS PRODUCT AND PYRAMID SOLUTIONS EXPRESSLY DISCLAIMS ALL WARRANTIES AS TO ITS QUALITY, PERFORMANCE, MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

THE PURCHASER'S REMEDIES ARE EXPRESSLY LIMITED TO THE EXCLUSIVE REME- DIES STATED ABOVE. NEITHER PYRAMID SOLUTIONS NOR ANY DIRECT OR INDI- RECT SUPPLIER TO PYRAMID SOLUTIONS WILL BE LIABLE FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR PROFITS) ARISING OUT OF, RELATED TO, OR CAUSED, DIRECTLY OR INDIRECTLY BY, THE USE OR TRANSFER OF THIS PROD- UCT BY THE PURCHASER OF THIS PRODUCT OR ANY CUSTOMER OR SUCCESSOR HOLDER OF THIS PRODUCT, BY THE PERFORMANCE OR FAILURE TO PERFORM OF PYRAMID SOLUTIONS OR ANY DIRECT OR INDIRECT SUPPLIER TO PYRAMID SOLU- TIONS, OR IN ANY OTHER RESPECT, BY ANY OTHER ACT OR OMISSION OF PYRA- MID SOLUTIONS OR ANY DIRECT OR INDIRECT SUPPLIER TO PYRAMID SOLUTIONS, OR BY ANY OTHER CAUSE. IN NO EVENT WILL PYRAMID SOLUTIONS' OR ITS SUPPLIERS' TOTAL LIABILITY TO ANY PERSON FOR ANY CLAIM EXCEED THE SUM PAID TO PYRAMID SOLUTIONS FOR THE PRODUCT(S) GIVING RISE TO THE LIABILITY.

THESE LIMITATIONS APPLY REGARDLESS OF WHETHER PYRAMID SOLUTIONS OR ITS SUPPLIER(S) IS (ARE) OR WAS (WERE) AWARE OF THE POSSIBILITY OF ANY PARTICULAR DAMAGES AND REGARDLESS OF WHETHER ANY LIMITATION CAUSES A REMEDY TO FAIL OF ITS ESSENTIAL PURPOSE.

Preface

Important User Information

The data and illustrations found in this document are not binding. We reserve the right to modify our products in line with our policy of product development. The information in this document is subject to change and should not be considered as a commitment by Pyramid Solutions. Pyramid Solutions assumes no responsibil- ity for errors that may appear in this document

There are many applications of the BridgeWay module. Those responsible for the use of this device must satisfy themselves that all necessary steps have been taken to verify an application meets all performance and safety requirements including any applicable laws, regulations, codes, and standards.

The illustrations and samples in this guide are intended solely for the purpose of example. Pyramid Solutions does not assume responsibility or liability for actual use based upon the examples shown in this publication.

	**FAIL-SAFE OR CRITICAL OPERATIONS** This product is not designed, intended, authorized, or warranted to be suitable for use or resale as control equipment in, or for other applications related to, hazardous or potentially-hazardous environments or applications requiring high-availability or fail- safe performance, such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic con- trol, life support, public works, weapons systems, or any other application in which the failure of a product could lead to prop- erty damage, death, personal injury, or environmental damage.

Related Documentation

Document Name	Author	Web Page
EtherNet/IP Specification	ODVA	www.odva.org
Common Industrial Protocol (CIP)	ODVA	www.odva.org
Modbus Application Protocol Specification	Modbus-IDA	www.modbus.org
Modbus Messaging on TCP/IP Implementation Guide	Modbus-IDA	www.modbus.org
J1939 Recommended Practice	SAE	www.sae.org

Table 1-1 Related Documentation

BridgeWay Module Description

Overview

The BridgeWay Ethernet to J1939 Gateway allows you to monitor and control data on a J1939 heavy duty vehicle network from an Ethernet device. Data from J1939 messages are mapped to I/O table locations, making them accessible to the Ethernet network. The EtherNet/IP and Modbus/TCP protocols are supported. The BridgeWay acts as an EtherNet/IP Adapter, allowing J1939 data to be trans- ferred to an EtherNet/IP Scanner device using I/O or explicit messages. The module acts as a Modbus/TCP server, allowing J1939 data to be addressed as Modbus registers by a Modbus/TCP client device.

Examples of applications of the Ethernet to J1939 Gateway:

- An interface used on a diesel generator package to access engine parame- ters from a Programmable Logic Controller (PLC).
- An on-vehicle gateway used to interface the J1939 vehicle network to an on board industrial automation based control system.

Theory of Operation

The BridgeWay provides centralized data storage, the "PassageWay™", for data that is shared between the J1939 and Ethernet networks. Data is placed into the PassageWay by one network interface, allowing the data to be read through the other network interface.

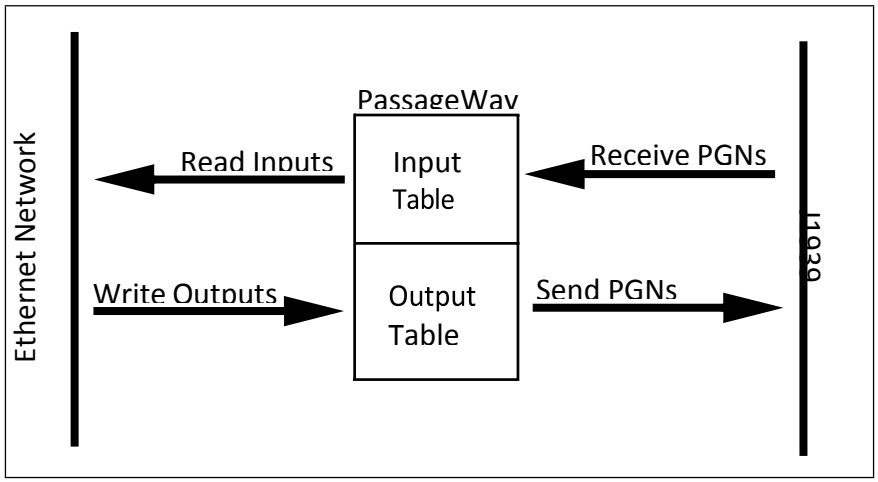


Figure 1-1 BridgeWay PassageWay Operation

The BridgeWay appears as a single device on either network using standard proto- col mechanisms. No special, or extended, protocol features are required of the devices on either network to read and write the data flowing through the Passage- Way; all cross-network activity is transparent to the devices on either network.

J1939 Features

- Transmission and reception of all types of fixed-length J1939 messages, including PDU1, PDU2, broadcast and destination specific.
- Monitoring of DM1 (active diagnostics) and DM2 (previously active diagnostics) messages.
- Complete network address management including address claim, protec- tion, and yield on higher priority conflict.
- Network address can be self-configurable over a range of addresses.
- J1939 Transport Protocol for transmission and reception of large mes- sages (9 - 1785 bytes). Both connection based (RTS/CTS) and broadcast (BAM) are supported.
- Configurable CAN bus-off reset option will reset the network interface and attempt to return to online when a CAN bus-off condition is detected.

Ethernet Features

- Supports the EtherNet/IP protocol, Adapter Class with I/O Server, and Message Server.
- Supports the Modbus/TCP protocol with up to 8 simultaneous connec- tions. Conforms to the Modbus/TCP specification 1.0.
- IP address configuration may be done using DHCP/Bootp, web page, or the BridgeWay Configuration Tool.

IT-Features

- The BridgeWay features a flexible file system with two security lev- els.The size available for user files is approximately 1.4 Mbyte.
- An FTP server provides easy file management using standard FTP clients.
- A Telnet server featuring a command line interface similar to the MSDOS™ environment.
- A flexible HTTP server (Web server) with Server Side Includes (SSI) functionality. These are commands to the web server embedded in the
- HTML code. This enables the user to access the IN/OUT area using a cus- tomizeable web page interface.
- Firmware updates of the BridgeWay using the RS232 port and Bridge- Way Configuration Tool.
- Email client capability.

System Requirements

The following hardware and software components are needed to use the Bridge- Way Ethernet to J1939 Gateway.

Required Hardware

BridgeWay module.
J1939 network connection.
Ethernet cabling.
PC or controller with access to the Ethernet network.
24 VDC power connection
PC with an RS-232 communications port or USB serial adapter to execute BridgeWay Configuration Tool (BWConfig).
RS-232 null-modem cable to connect PC running BWConfig to the BridgeWay.

Optional Hardware

DIN rail to mount the BridgeWay.

Required Software

BridgeWay Configuration Tool software (BWConfig) to configure the BridgeWay.
BWConfig requires that the PC be running Microsoft Windows 98, NT, 2000, or XP.

Hardware Description

All connections, whether power or fieldbus, to the BridgeWay are made on one end of the module. Phoenix-style connectors are provided for power and J1939 connections. An RJ-style connector is provided for Ethernet connection. There is a 9-pin D-Subminiature connector for the auxiliary RS-232 port that is used for device configuration. See “Installation” Page 2-1 for more details on the connec- tors.

There is an 8 position DIP switch on the end of the module that can be used to select a portion of a default IP address that may be used to permit an intranet con- nection. See “Ethernet Network Configuration” Page 3-6 for more details on con- figuring the IP address using the switches.

On the front of the BridgeWay module are 6 LEDs that are used for status indica- tion. These LEDs provide visual status for the overall module, the J1939 interface, and the Ethernet interface. See “BridgeWay LEDs” Page 10-1 for details on how the LEDs are used.

The back of the module has a DIN rail mount to allow the module to be mounted on a DIN rail.

Installation

Installation and Operation Requirements

- Power, input and output (I/O) wiring must be in accordance with Class 1, Division 2 wiring methods - article 501-4(b) of the National Electric Code, NFPA 70 and in accordance with local codes.
- **Warning - Explosion Hazard** - Substitution of components may impair suitabil- ity for Class 1, Division 2.
- **Warning - Explosion Hazard** - When in hazardous locations turn off power before replacing or wiring modules.
- **Warning - Explosion Hazard** - Do not disconnect equipment unless power has been switched off or the area is known to be nonhazardous.
- Terminal tightening torque must be between 5-7 lbs-in (0.5-0.8 Nm).
- For use in Class 2 circuits only.
- Suitable for surrounding temperature of 65 degrees C maximum.
- Use 60/75 C copper wire only.

Power and Network Connections

The power and network connections to the BridgeWay are made on the end of the module. Figure 2-1 indicates the location of each connector.

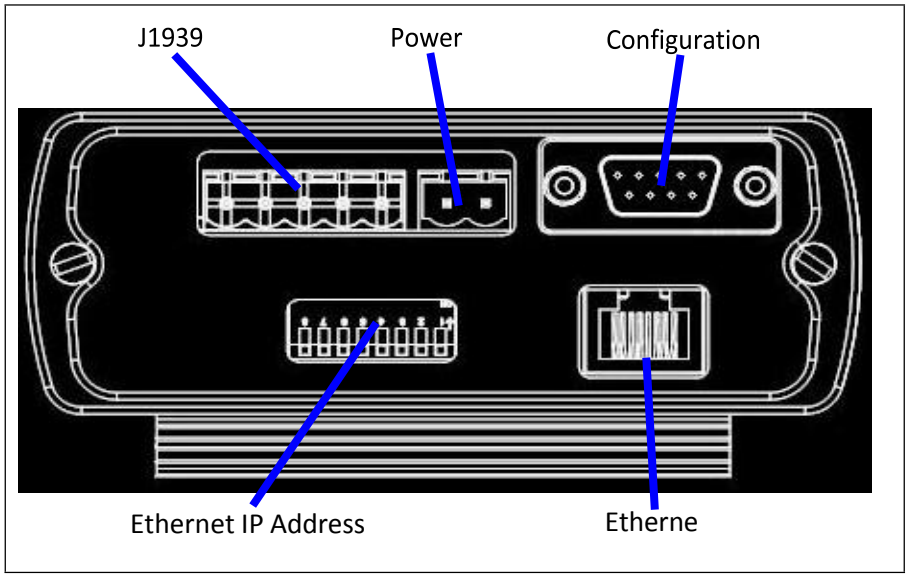


Figure 2-1 BridgeWay Power and Network Connections

Connecting Power

The power connection is a 2-pin terminal block located on the end of the module. The female terminal block connector is provided with the BridgeWay. Connec- tions to be made are illustrated in Figure 2-2.

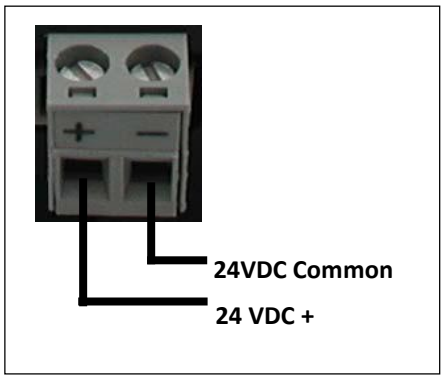


Figure 2-2 Power Connection

The BridgeWay requires 24 volts DC power. The module will start immediately when power is applied (There is no On/Off switch on the module).

Connecting J1939

The J1939 network connection is a 5-pin terminal block located next to the power connection on the end of the module. The female terminal block connector is pro- vided with the BridgeWay. Connections to be made are illustrated in Figure 2-3.

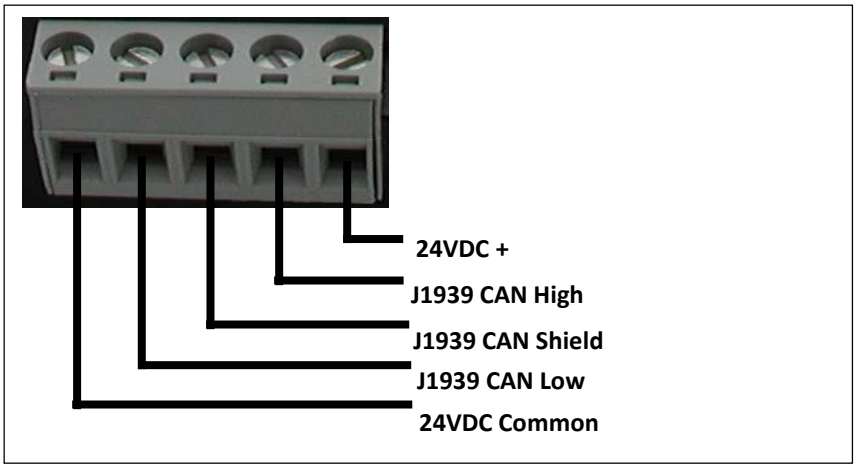


Figure 2-3 J1939 Connection

The CAN High and Low signal lines should be connected to the CAN High and Low connections respectively on all devices on the network. The signal lines should not be swapped on any device connections.

Note: The 24VDC terminals on pins 1 and 5 are physically connected to the power on the 2-pin power connector. The module may alternatively be powered from these pins.

Connecting to Ethernet

The Ethernet connection uses a standard RJ45 connector (not provided). This is plugged into the socket on the end of the module.

Configuration Port Connector

The configuration port is the 9-pin D-Subminiature female connector on the end of the BridgeWay. The connector has a standard RS-232 DTE pin configuration. The connections to be made as shown below.

Pin	Connection
2	Receive Data
3	Transmit Data
5	Signal Ground

The BridgeWay is connected to a PC for configuration using a null-modem cable. A null-modem cable has pins 2 and 3 swapped so that the PC's Transmit line is connected to the BridgeWay's Receive line, and the PC's Receive line is con- nected to the BridgeWay's Transmit line.

Note: The BridgeWay does not make use of the modem control signals specified for a DTE connector. Connecting the module through devices, such as isolation modules, which assume control of these lines may cause the BWConfig commu- nications to be unreliable.

Configuration

This chapter describes how the BridgeWay Ethernet to J1939 Gateway is config- ured using the BridgeWay Configuration Tool (BWConfig). Detailed descriptions of each configurable parameter in the gateway are provided as well as how they are set in the tool.

The next chapter walks the reader through the configuration of an example appli- cation to illustrate how the configurable parameters are used in a real-world appli- cation.

BridgeWay Configuration Tool (BWConfig)

The BridgeWay Configuration Tool allows you to configure the parameters asso- ciated with the Ethernet and J1939 network interfaces as well as to set up the con- tents and layout of the I/O table.

BWConfig is a Microsoft Windows application that communicates with a Bridge- Way over a standard RS-232 serial link using the PC serial port or USB serial adapter. BWConfig is compatible with Microsoft Windows 98, NT, 2000, and XP.

Installing the Tool

Install BWConfig from the CD by running *Setup.exe* which is found in the CD's root directory.

If you have downloaded BWConfig from the web site, unzip the downloaded file into a temporary directory and run *Setup.exe* which is found in the temporary directory.

Connecting to the BridgeWay Module

Connect the PC running BWConfig to the BridgeWay module using a standard Null-Modem (pins 2 and 3 swapped) serial cable between the PC serial port or USB adapter and the 9-pin D-Sub connector on the module. It does not matter which PC serial port you use, BWConfig will scan each available port and detect the connection automatically. No serial port configuration is required; BWConfig will automatically set the baud rate.

Starting the Tool

Launch BWConfig from the *BridgeWay Configuration* folder in the Windows Start Menu.

When BWConfig is started, it will attempt to locate a BridgeWay module on one of the PC serial ports. If a module is found, the status area of the tool will be updated to show the module type and status of the module that was located.

If a module is not connected to the PC, or is powered off, when the tool is started, the status area will indicate that no module was detected. Make sure that the mod- ule is powered and the connection is made, then press the Refresh button on the BWConfig tool bar; this will cause the tool to rescan the serial ports for a module.

BWConfig User Interface

The BridgeWay Configuration Tool's user interface is shown in Figure 3-1.

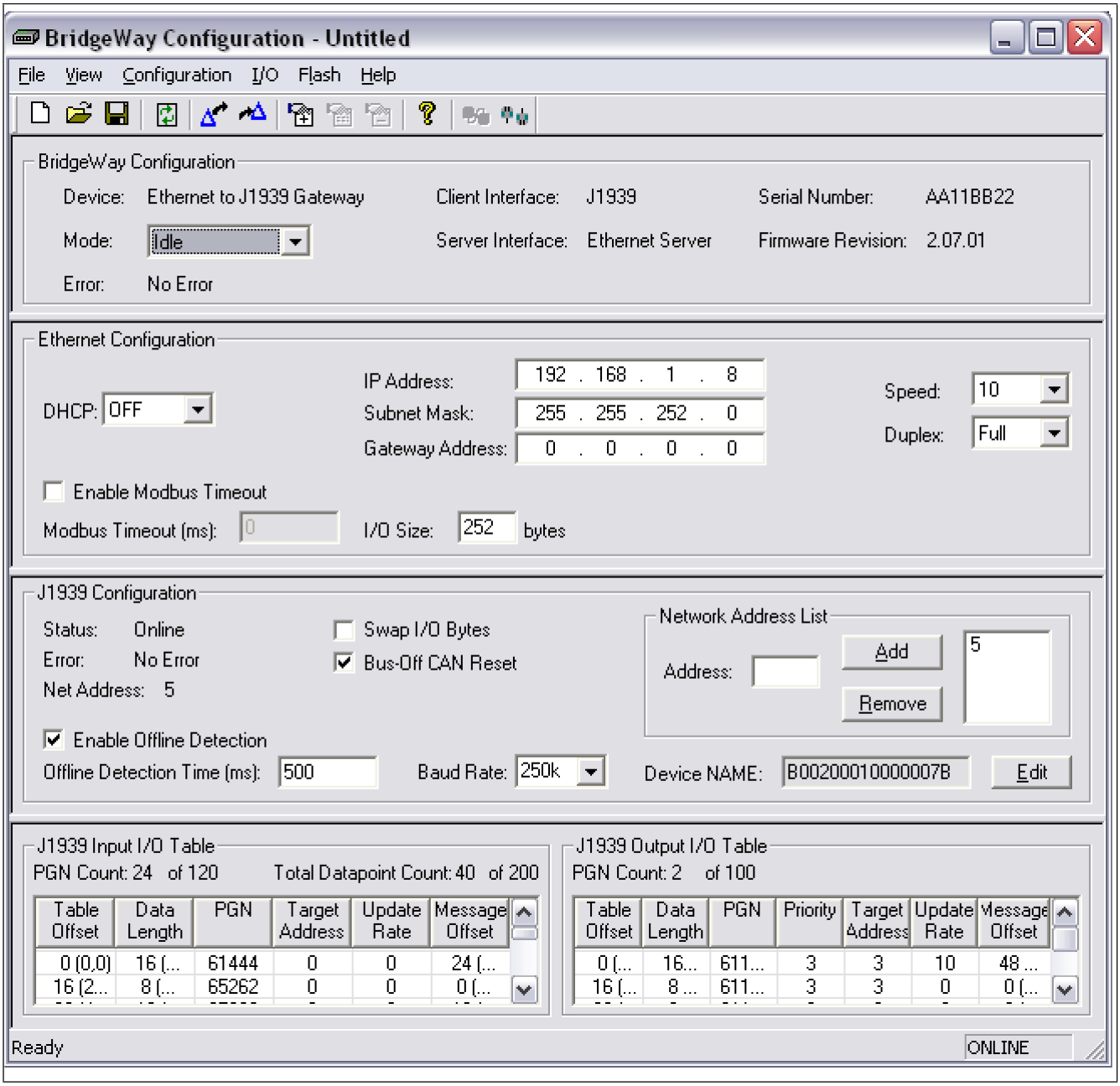


Figure 3-1 BWConfig User Interface

Display Panes

The BWConfig display is divided into 4 panes.

BridgeWay Configuration	Module type and status information about the BridgeWay module that was detected.
Ethernet Configuration	Configuration of Ethernet network parame- ters.
J1939 Configuration	Configuration of J1939 network parameters and status of the network interface.
J1939 I/O Configuration	Configuration of the content and layout of the I/O tables.

Tool Operations

The following operations are available through the BWConfig menus and tool bar.

New File	Create a new BridgeWay configuration for the selected type of module.
Open File	Open a previously saved BridgeWay configu- ration.
Save File	Save the current BridgeWay configuration to a file.
Refresh Device Status	Refresh the module identity and status infor- mation. This will update the current status information shown by the tool. This can also be used to start the detection process if a mod- ule has not been detected by the tool, or the connection has been changed to a different module.
Upload Configuration	Read the configuration that is currently stored in the BridgeWay module. This will overwrite any configuration that is displayed on the tool’s user interface.

Download Configuration	Send the configuration shown on the tool's user interface to the BridgeWay module.
Offline Configuration	Offline configuration will allow a configuration to be created and saved without being connected to a module.
Add I/O Point	Add a new input or output data point to the J1939 I/O configuration.
Edit I/O Point	Change the parameters associated with the selected input or output data point in the J1939 I/O configuration.
Remove I/O Point	Delete the selected input or output data point from the J1939 I/O configuration.
Flash Update	Perform a field upgrade of the BridgeWay module's firmware. **Note:** Care should be taken when upgrading firmware, an incomplete update could cause irreparable harm to the module.

Ethernet Network Configuration

Several methods may be used to set the IP Address. These methods include the BridgeWay Configuration Tool, IP Address Configuration Switch, DHCP/Bootp protocol, web browser, and the ARP protocol.

Setting the IP Address with BWConfig

The Ethernet network configuration contains the parameters used to control the behavior of the Ethernet network interface. The parameters are described in Table 3-1 below. Refer to Figure 3-1 to see how each parameter is displayed on the user interface.

Parameter	Description	Allowable Range
DHCP Enable	If DHCP is enabled, the module will receive its IP configuration from a DHCP server on the network. If no DHCP server is available, the module will revert to the last saved IP configuration.	On or Off
IP Address	The IP address the module will use on the Ethernet network. If DHCP is enabled, and a DHCP server is found, this address is ignored. If a DHCP server is not found, this address is used.	Valid IP address
Subnet Mask	The subnet mask the module will use on the Ethernet network. If DHCP is enabled, and a DHCP server is found, this mask is ignored. If a DHCP server is not found, this mask is used.	Valid IP sub-net mask
Gateway Address	The IP address of the gateway module on the network. If DHCP is enabled, and a DHCP server is found, this address is ignored. If a DHCP server is not found, this address is used.	Valid IP address
Network Speed	The speed that the module will communicate at on the Ethernet network. If the network speed is set to Auto, the module will auto-negotiate network speed.	10, 100, or Auto

Table 3-1 Ethernet Network Configuration Parameters

Parameter	Description	Allowable Range
Network Duplex	The duplex setting that the module will use to communicate on the Ethernet network. If the network duplex is set to Auto, the mod- ule will auto-negotiate duplex.	Half, Full, or Auto
Modbus Timeout	The Modbus Timeout option provides a means to detect the loss of the Modbus Scan- ner from the Ethernet network. If the option is enabled, and no Modbus requests are received within the configured timeout period, the module Run/Idle status will be set to Idle. **Important:** Do not enable the Modbus Timeout if an EtherNet/IP Scanner is used with the BridgeWay. The BridgeWay will be prohibited from entering Run mode if there is no Modbus messages.	0-65000ms
I/O Size	The I/O Size parameter provides the means to configure the maximum size of the Input and Output Assembly objects. This is useful when accessing the BridgeWay Assembly object using Class 3 or UCMM messages with mod- ules that do not support large assembly buffer sizes. The I/O size includes any status and command headers as well as the J1939 device data. See “I/O Data Summary” on page 5-9 for details. The actual output assembly size will be 4 bytes less than the I/O size configured. Again, refer to “I/O Data Summary” on page 5-9 for details. I/O table sizes below 500 truncate the input and output tables. Any J1939 device data that may be mapped beyond the configured I/O table size will not be transferred to Ethernet. Suggested maximum sizes for various Ether- Net/IP devices: MicroLogix 252 SLC 5/05 248 ControlLogix 500	4-500 bytes

Table 3-1 Ethernet Network Configuration Parameters

Setting the IP Address with the Configuration Switch

If DHCP/BootP is not enabled or a server is not found and the Configuration Switch is non zero, on power up the value of the switch is used to form an IP Address. The switch represents the binary value of the last byte in the 4 byte IP address. In this case it is *n*.

IP address: 192.168.1.*n*
Subnet mask: 255.255.255.0
Gateway address: 0.0.0.0 (No gateway set)

This is a private address and can only be used on a local intranet. In such a case a Web Browser such as Microsoft's Internet Explorer can be used to access the BridgeWay's web page which allows changing the IP Address, Subnet mask, and GateWay address settings.

Note: A non-zero DIP switch setting will override any other Ethernet configuration that is done.

DIP Switch Example

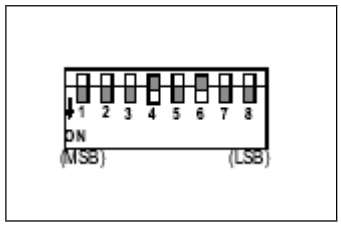


Figure 3-2 IP Configuration DIP Switch

The switches are set to 00010100 (20 decimal) (The switch position is shown in White in the diagram.)
The IP address of the module will be set to 192.168.1.20.

Note: The numbers on the switches on the IP configuration DIP switch do NOT correspond to bit locations in the address value. In fact, they are reversed. i.e. bit 0 is set by switch 8.

Setting the IP Address Using DHCP/BootP

When DHCP/BootP is enabled and a DHCP or BootP server is found, the IP address, Subnet mask, and Gateway address is automatically configured by the DHCP/BootP server. It can be enabled using BWConfig or the BridgeWay's Set- tings web page.

Note: The use of DHCP is the default configuration for the BridgeWay as shipped.

Setting the IP Address Using Address Resolution Protocol (ARP)
The module's IP address can be changed using the ARP command from a PC. The new IP address will be stored in non-volatile memory. ARP requires the module's Ethernet MAC Address that is printed on a label on the back of the module.

Note: ARP cannot be used to change the subnet mask and gateway address of the BridgeWay. These can be configured using the BridgeWay's Settings web page.

Switch all 8 switches of the IP Configuration DIP switch to the ON position.
Note: The ARP/Ping capability is disabled unless all switches are ON.

On a PC connected to the BridgeWay on Ethernet bring up an MS DOS™ win- dow and type:
arp -s <IP address> <MAC address>
The arp -s command will store the IP and MAC addresses in the PC's ARP table.

Next type:
ping <IP address>
When the Ping command is executed, the PC sends this information to the module using the MAC address. The module detects that it was addressed with the correct MAC address and adopts the IP address sent by the PC.

Next type:
arp -d <IP address>
The arp -d will remove the static route from the PC's ARP table.

Switch all 8 switches of the IP Configuration DIP switch to the OFF position to disable the feature.

This method can be used to reconfigure a module that has been previously config- ured, or even to reconfigure modules outside the host's subnet.

Arp/Ping Example:
The following commands will set the IP address of a BridgeWay with MAC address 00-30-11-02-00-5E to 65.106.34.252.
arp -s 65.106.34.252 00-30-11-02-00-5e ping 65.106.34.252
arp -d 65.106.34.252

Setting the IP Address Using the Web Page

The ethernet addresses can also be configured using the Status and Settings web page resident on the BridgeWay. The Status and Settings web page appears as shown below.

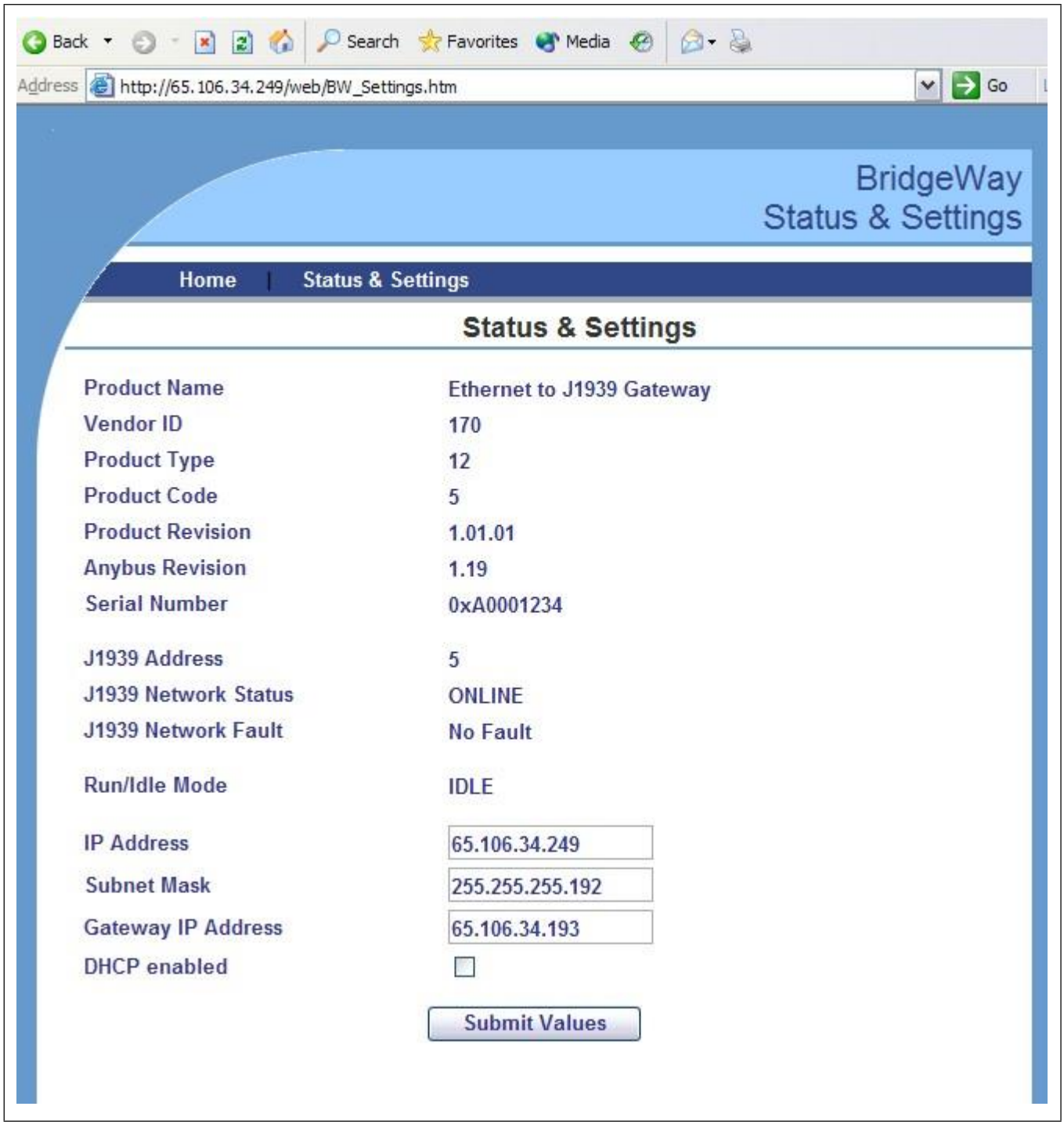


Figure 3-3 Status and Settings Web Page

The IP address, subnet mask, and default gateway address are displayed in the edit boxes on the web page. Changing any values and clicking the Submit Values button will set the addresses in the BridgeWay. Note that a power cycle or module reset is required for the changes to take effect.

Note: If your web browser is configured to cache web pages, it may appear that the BridgeWay has not changed address after you power cycle the module. Make sure that the browsers settings are configured to always reload pages. On Internet Explorer this is done in the Temporary Internet Files Settings dialog by selecting the “Every Visit” option for when the browser should check for page changes.

IP Address Initialization

The following flowchart describes how the IP configuration is determined when the BridgeWay is powered up.

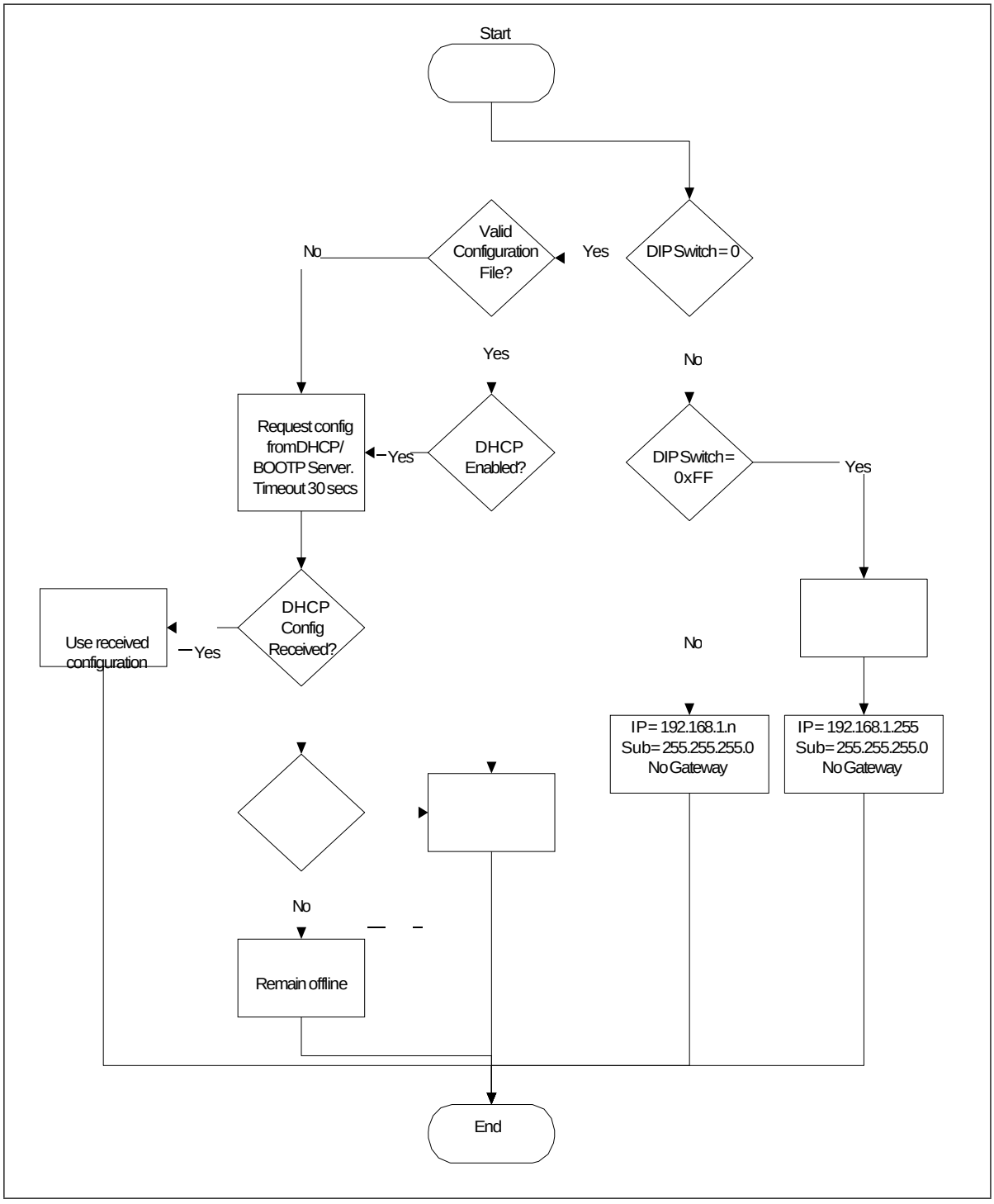


Figure 3-4 IP Configuration Initialization Sequence

J1939 Network Configuration

The J1939 network configuration contains the parameters used by the BridgeWay for J1939 address management and other network interface options. The parame- ters are described in Table 3-2 below. Refer to Figure 3-1 to see how each param- eter is displayed on the user interface.

Parameter	Description	Allowable Range
Device NAME	The J1939 NAME to be used by the module in address claim messages. Each J1939 module should have a unique NAME. See the section “Setting the J1939 NAME” below for details on how the NAME is config- ured.	See the J1939-81 specification.
Network Address List	The list of addresses that the module is able to use on the J1939 network. The module will only claim a single address at a time. This is the list of possible addresses that it can use if it is unable to claim the first address. See “Address Management” on page 7-1 for details on how the address list is used.	Each address must be in the range 0-253. Up to 10 addresses may be in the list.
Enable Bus-Off CAN Reset	If this option is enabled, the module will reset the CAN controller and attempt to go back online after a bus-off condition is detected. If the option is disabled, the module will remain offline after a bus-off condition until it is power cycled. **For most applications, this option should be left disabled.**	Enabled or Disabled

Table 3-2 J1939 Network Configuration Parameters

Parameter	Description	Allowable Range
Swap I/O Bytes	Enabling this option will cause the I/O data to be swapped on 16-bit word boundaries. This is useful if the Ethernet protocol being used is Modbus/TCP since it is a Big Endian network. If enabled, all data in the I/O table will be byte swapped on 16-bit word boundaries when transferred between J1939 and Ethernet. **Important:** Do not set the Swap I/O option if an EtherNet/IP Scanner is used with the BridgeWay. The BridgeWay will be pro- hibited from entering Run mode.	Enabled or Disabled
Offline Detection Time	Enabling the Offline Detection will allow the module to detect when it is not connected to the J1939 network when there is no Output PGN's configured. See "Offline Detection" on page 7-14 for a complete discussion.	1000ms to 60000ms when Enable d
Baud Rate	The J1939 baud rate may be set to either 250K or 500K baud. **Important:** The standard J1939 baud rate is 250K. Do not set the baud rate to a rate other then 250K unless you know for certain that the devices on the J1939 are communicat- ing at the other baud rate.	250K 500K

Table 3-2 J1939 Network Configuration Parameters

Setting the J1939 NAME

The J1939 Device NAME dialog is shown in Figure 3-5.

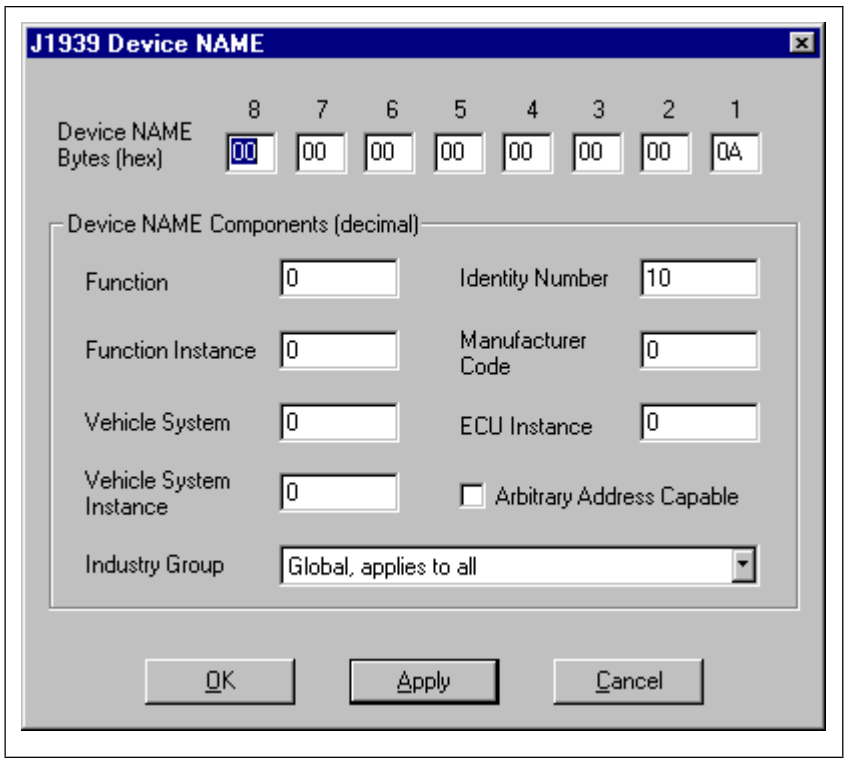


Figure 3-5 J1939 Device NAME Dialog

The NAME is a 64-bit value that must be unique for every module on a given J1939 network. The meaning and format of the data contained in the NAME value is defined in the J1939-81 specification.

The NAME value can be set 2 ways using the J1939 Device NAME dialog: directly or by component. To set the NAME value directly, simply type the desired value of each of the 8 bytes in hexadecimal using the top fields of the dia- log. Each component of the NAME value is broken out and displayed in the lower fields of the dialog; components can be edited individually using these fields.
Pressing the Apply button will update either set of fields to reflect the changes that were made.

Note: The J1939 interface is configured during BridgeWay initialization. If the network configuration is changed, the module must be power cycled before the changes will take effect.

J1939 I/O Configuration

The J1939 I/O configuration is used define the content and format of the J1939 device I/O tables. Data from J1939 messages that are to be monitored or transmit- ted are mapped to locations within the J1939 device Input or Output tables respec- tively. See “I/O Data Summary” on page 5-9 for an explanation of the association of the J1939 device data and the module’s I/O tables.

Inputs Versus Outputs

The J1939 device input table holds data that is collected from the J1939 network and can be read on the Ethernet network. Input data points are associated with data from messages that are received on the J1939 network.

The J1939 device output table holds data that is written by a device on the Ether- net network to be transmitted on the J1939 network. Output data points are associ- ated with data of messages that will be transmitted on the J1939 network.

I/O Configuration Limits

The I/O configuration is limited as follows:

496 bytes maximum in the J1939 device input table with an I/O Size setting of 500; I/O Size - 4 otherwise.
492 bytes maximum in the J1939 device output table with an I/O Size setting of 500; I/O Size - 8 otherwise.
200 total data points in the configuration. This is the combined number of input and ouput data points.
Up to 120 different PGN’s may be monitored by input data points Up to 100 different PGN’s may be transmitted by output data points

Data Point Parameters

Each data point defines a single piece of data in the either the J1939 device Input or Output table. The data point parameters are organized in columns in the J1939 I/O configuration editor, shown in Figure 3-6. Note that both Input and Output data points have the same parameters with the exception of the message priority; only the output data points have configurable message priority.

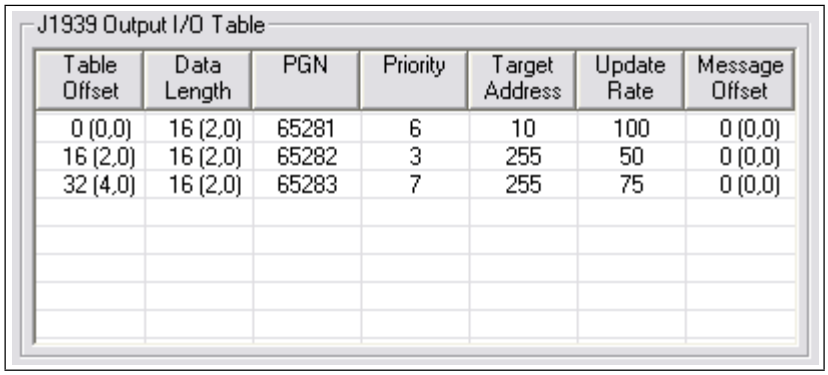


Figure 3-6 J1939 Data Point Configuration

The data point editing dialog is shown in Figure 3-7. This dialog is used to enter new, or edit existing data points in the I/O configuration Note that the output editor is shown; the input editor does not have the message priority parameter..

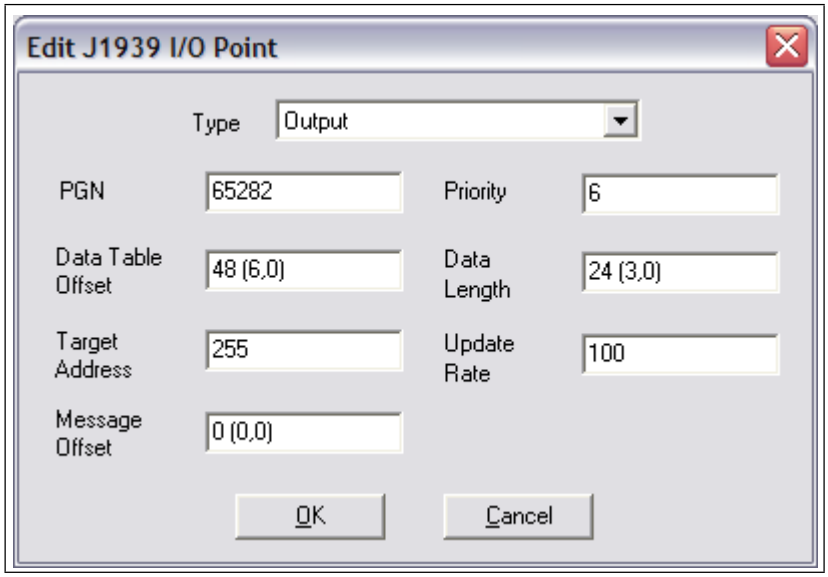


Figure 3-7 J1939 Data Point Editing Dialog

The parameters associated with I/O data points are described in Table 3-3.

Parameter	Description	Allowable Range
Table Offset	The offset into the J1939 device I/O data. If this is an input data point, the offset is into the Input data; if this is an output data point, the offset is into the Output data. The offset is in bits. It is displayed as both bits and the corresponding byte and bit, shown as (byte, bit). When entering this value in the editor: A sin- gle value will be interpreted as bits. 2 values separated by a comma or a period will be interpreted as a byte, bit combination. i.e. ‘16’ and ‘2,0’ are equivalent entries.	Input: 0-3999 bits 0-499 bytes Output: 0-3967 bits 0-495 bytes
Data Length	The amount of the data to be transferred between the J1939 device I/O data and the J1939 message data. The length is in bits. It is displayed as both bits and the corresponding byte and bit, shown as (byte, bit). When entering this value in the editor: A sin- gle value will be interpreted as bits. 2 values separated by a comma or a period will be interpreted as a byte, bit combination. i.e. ‘16’ and ‘2,0’ are equivalent entries.	1-14280 bits 0-1785 bytes
PGN	The J1939 PGN associated with this data point. If this is an input data point, the message data from messages received with this PGN will be transferred into the Input table. If this is an output data point, a message with this PGN will be built and transmitted using data from the Output table.	Any valid J1939 PGN

Table 3-3 J1939 I/O Data Point Parameters

Parameter	Description	Allowable Range
Priority	The J1939 message priority to be used when transmitting this message. If this is an output data point, this is the message priority that will be used when the message is produced on the J1939 network. If this is an input data point, this value is ignored. J1939 messages are screened by PGN and target address; the message priority is ignored. The default priority is 6.	0-7
Target Address	The J1939 network address associated with the data point. If this is an input data point, messages received must match both the PGN and source address to be used for this data point. If the Target Address is 255, any message with a matching PGN, regardless of source address will be accepted. If this is an output data point, the destination address of the transmitted message will be set to the Target Address. The message will be broadcast if the Target Address is set to 255.	0-253, 255

Table 3-3 J1939 I/O Data Point Parameters (Continued)

Parameter	Description	Allowable Range
Update Rate	The desired update rate for the data point in milliseconds. If this is in input data point, the data point is expected to be updated (a message received with matching PGN and address) within the configured Update Rate. If no update is received within the configured time, the mod- ule will request the data point's PGN by trans- mitting a Request PGN to the Target Address. If the Update Rate is set to 0, the PGN will never be requested. If the Update Rate is non-zero for an input point, and no update is received after an update period, the data associated with the PGN in the input table is set to 0xFF. If this is an output data point, this is the rate at which the associated message will be trans- mitted on the network. If the Update Rate is set to 0, the message will only be transmitted when a Request PGN is received for the con- figured PGN.	0-65535
Message Offset	The offset into the message data where the data associated with the data point begins. This is the location where data will be trans- ferred in and out of the message buffer. The offset is in bits. It is displayed as both bits and the corresponding byte and bit, shown as (byte, bit). When entering this value in the editor: A sin- gle value will be interpreted as bits. 2 values separated by a comma or a period will be interpreted as a byte, bit combination. i.e. '16' and '2,0' are equivalent entries.	0-14279 bits 0-1784 bytes

Table 3-3 J1939 I/O Data Point Parameters (Continued)

J1939 Diagnostic Tables

The BridgeWay has the ability to monitor the commonly used diagnostic mes- sages on J1939. The Active Diagnostics (DM1) and Previously Active Diagnos- tics (DM2) can be monitored by the BridgeWay. Configuring diagnostic table monitoring is done through the input data points in much the same manner as data PGN configuration. Figure 3-8 shows the data point editor dialog when a diagnos- tic type is selected.

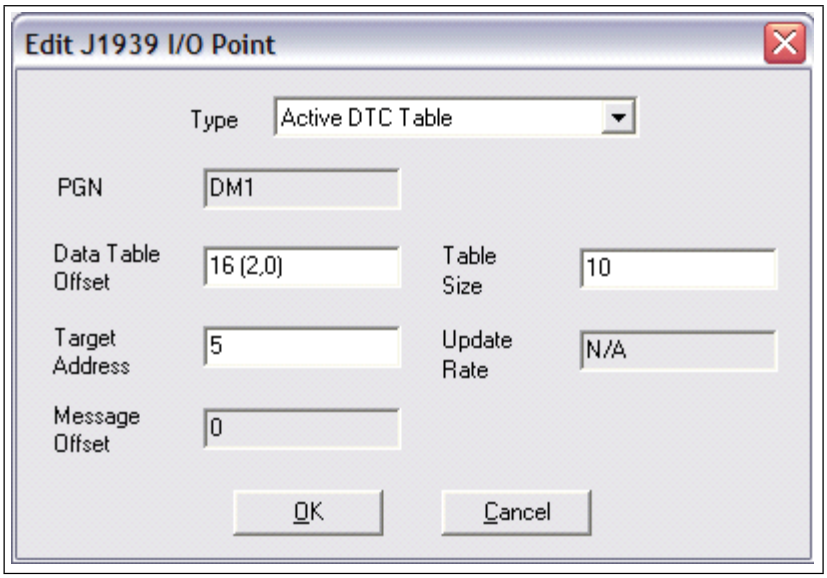


Figure 3-8 J1939 Data Point Editing Dialog for Diagnostics

Table 3-4 explains how the data point parameters are used when configuring a diagnostic table.

Parameter	Description	Allowable Range
Data Point Type	Set to Active DTC or Previously Active DTC to configure a diagnostic table.	Active DTC, Previously Active DTC
Table Offset	See Table 3-3.	
Table Size	The number of diagnostic entries this table can hold. This will be the maximum amount of diagnostics that can be placed into the table. If the J1939 diagnostic message from the device contains more diagnostics than fit in the table, only those that fit will be copied, and the high bit in the table header will be set to indicate that the table has overflowed. The table size is limited to 128 entries. Note that the total space occupied in the J1939 device input data will be (size * 4) + 2 bytes.	1-128
PGN	This will automatically be set to DM1 or DM2	DM1, DM2
Target Address	The J1939 address of the device from which this table is to monitor diagnostics.	0-253
Update Rate	See Table 3-3.	
Message Offset	This will automatically be set to 0	0

Table 3-4 Input Data Point Parameters for Diagnostic Tables

Note: See “J1939 Diagnostic Messages” on page 7-9 for details of the format of the diagnostic tables in the J1939 device input data.

Note: The J1939 I/O configuration is initialized at BridgeWay bootup and when- ever a new configuration is downloaded to the module from BWConfig. Any changes made to the I/O configuration will take place immediately after the con- figuration is downloaded to the module.

Example Application

Scenario #1 - EtherNet/IP

A system controller (PLC) on EtherNet/IP requires some data that is collected by an ECU and produced on J1939. There is also a piece of data that is determined by the system controller that would be beneficial for some of the ECUs that are on the J1939 network. Additionally, the active diagnostics for an ECU should be monitored by the controller.

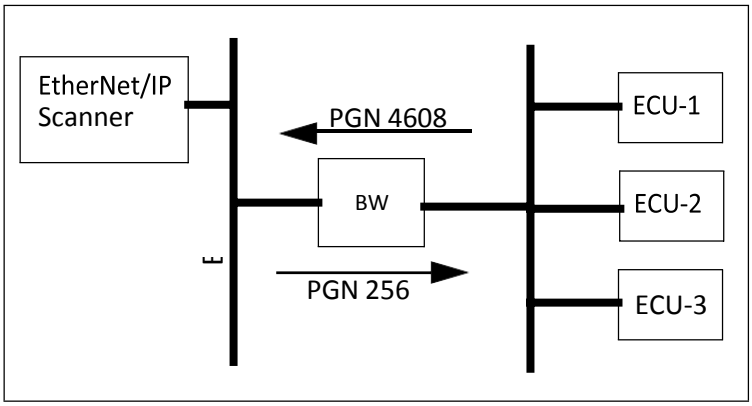


Figure 4-1 Example Application Network Diagram

The data required by the system controller is contained in the PGN 4608 message as 2 12-bit values. The values are packed into the first 3 bytes of the message as shown in Figure 4-2 below.

Bit Byte	7	6	5	4	3	2	1	0
0	Value #1 bits 0-7							
1	Value #2 bits 0-3				Value #1 bits 8-11			
3	Value #2 bits 4-11							

Figure 4-2 Example PGN 4608 Message Data Format

The data from the system controller is to be produced using PGN 256. The data is a 16-bit value and will be placed into the first 2 bytes of the message data.

Ethernet Network Configuration

The Ethernet network configuration dialog from BWConfig is shown in Figure 4-3. Refer to “Configuration” on page 3-1 for more details on BWConfig.

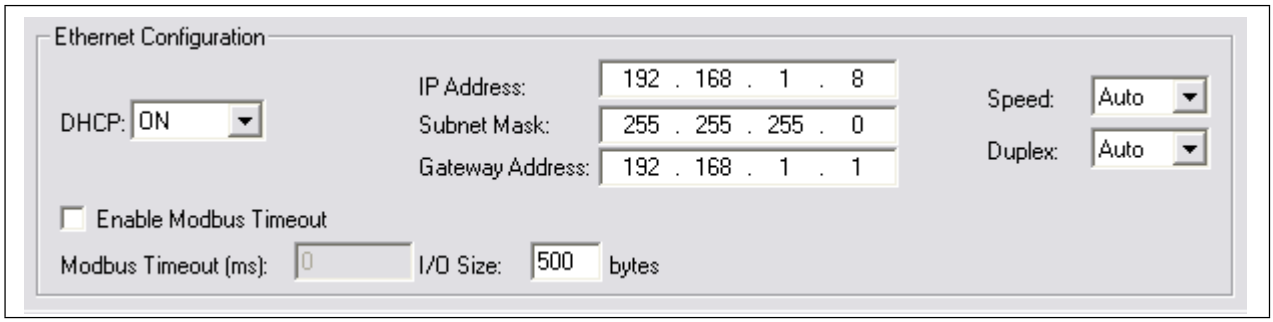


Figure 4-3 Example Ethernet Network Configuration

The Ethernet configuration has been set to auto-negotiate speed and duplex set- tings and retrieve the IP configuration from a DHCP server. If no DHCP server is found, the IP configuration will default to that shown in the dialog.

J1939 Network Configuration

The J1939 network configuration dialog from BWConfig is shown in Figure 4-4. Refer to “Configuration” on page 3-1 for more details on BWConfig.

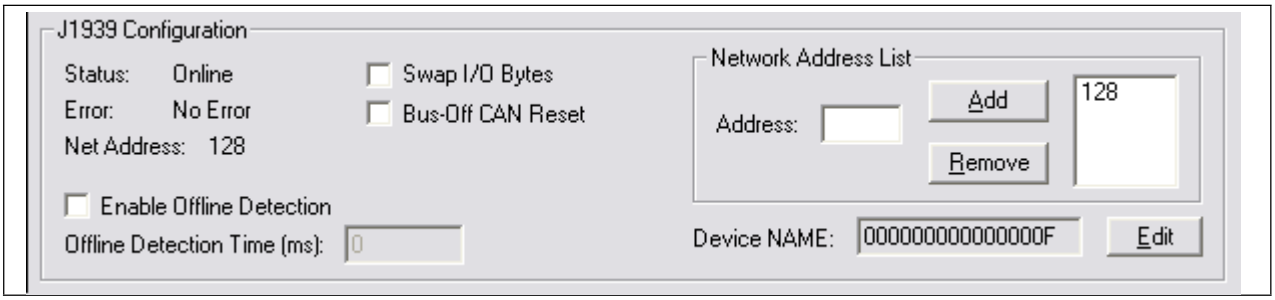


Figure 4-4 Example J1939 Network Configuration

The J1939 device NAME has been set to an arbitrary value for the purpose of this example. The NAME should be set according to the vendor and application where the module is being used based on the J1939 specification. The network address list is set to a single address of 128.

Since this example uses EtherNet/IP, I/O byte swapping has been turned off.

J1939 I/O Configuration

Input Data Points

The input data points are responsible for determining where in the J1939 device input data the J1939 data is to be placed.

It is desirable to be able to address the 2 values in our example as individual 16-bit words in the EtherNet/IP data. Since the values are packed into 3 bytes in the J1939 message, they need to be parsed out into 2 word locations in the J1939 device input data.

It has been determined that the diagnostic table should be located at an offset 100 bytes into the J1939 device input data, and contain up to 20 diagnostic entries.

The resulting J1939 input configuration from BWConfig is shown below.

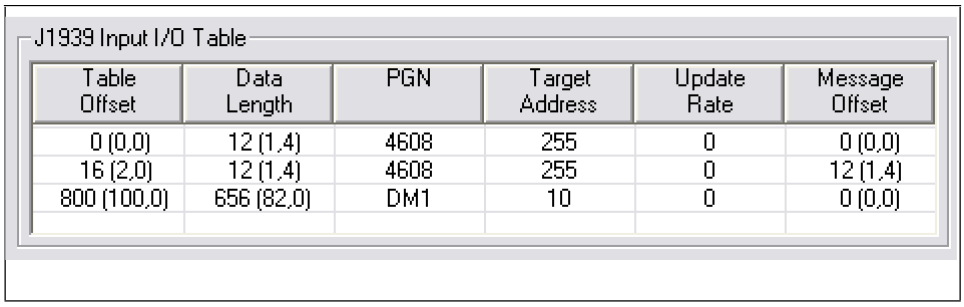


Figure 4-5 Example J1939 Input Configuration

2 data points have been defined, 1 for each value in the message. The first data point copies the first value (12 bits starting at the beginning of the message) into the first word of the J1939 device input table. The second data point copies the second value (12 bits starting 12 bits into the message) into the second word of the J1939 input table.

Both data points monitor the network for messages with PGN 4608 and any source address (Target Address 255 specifies “don’t care” source address).

The data point for the DM1 message was configured as shown in Figure 4-6.

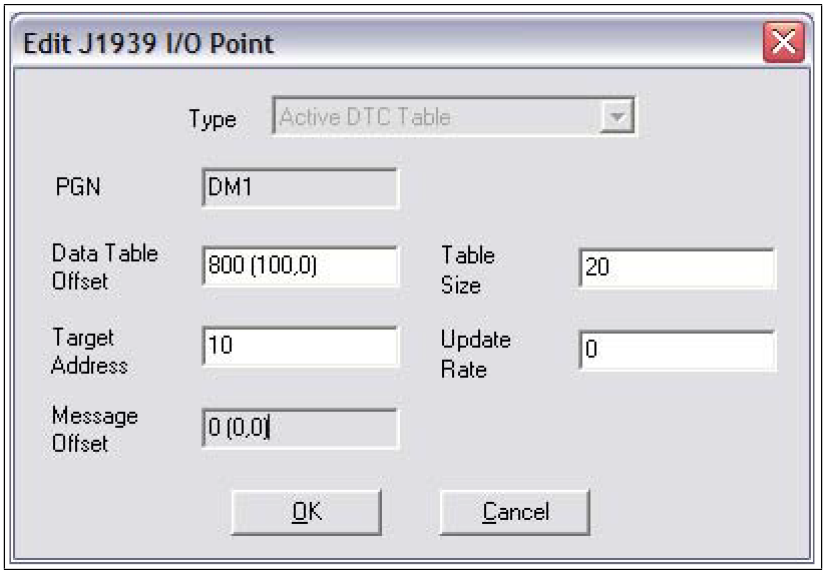


Figure 4-6 Example J1939 Diagnostic Data Point Configuration

Notice that the table length has been set to 20 entries. The target address specifies that the diagnostics of the ECM at address 10 are to be monitored by this data point. The diagnostic table will start at byte 100 of the J1939 device input data.

Output Data Points

The output data points determine what PGNs are going to be produced by the BridgeWay on J1939, and what the content of those PGN messages is going to be.

Since the example application only needs to produce 16 bits of data in a single PGN message, the resulting configuration is quite simple. It is shown in Figure 4- 7.

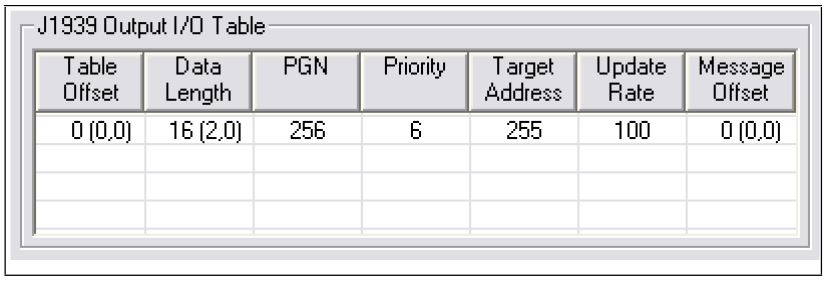


Figure 4-7 Example J1939 Output Configuration

The single data point specifies that 2 bytes of data from the beginning of the J1939 device output data is going to be copied into the first 2 bytes of the message. The message will be transmitted with a PGN of 256 and a priority of 6 every 100ms. The message will be broadcast (Target Address 255) so that it can be seen by everyone on the network.

Scenario #2 - Modbus/TCP

A system controller (PLC) on Modbus/TCP requires some data that is collected by an ECU on J1939. There is also a piece of data that is determined by the system controller that would be beneficial for some of the ECUs that are on the J1939 net- work. Additionally, the active diagnostics for an ECU should be monitored by the controller.

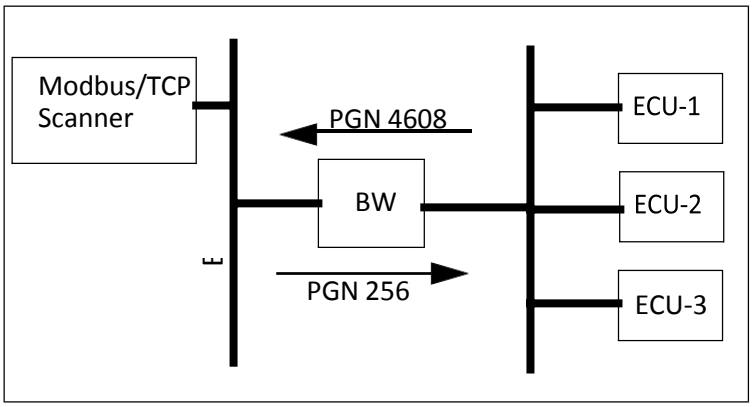


Figure 4-8 Example Application Network Diagram

The data required by the system controller is contained in the PGN 4608 message as 2 12-bit values. The values are packed into the first 3 bytes of the message as shown in Figure 4-9 below.

Bit Byte	7	6	5	4	3	2	1	0
0	Value #1 bits 0-7							
1	Value #2 bits 0-3				Value #1 bits 8-11			
3	Value #2 bits 4-11							

Figure 4-9 Example PGN 4608 Message Data Format

The data from the system controller is to be produced using PGN 256. The data is a 16-bit value and will be placed into the first 2 bytes of the message data.

Ethernet Network Configuration

The Ethernet network configuration dialog from BWConfig is shown in Figure 4-10. Refer to “Configuration” on page 3-1 for more details on BWConfig.

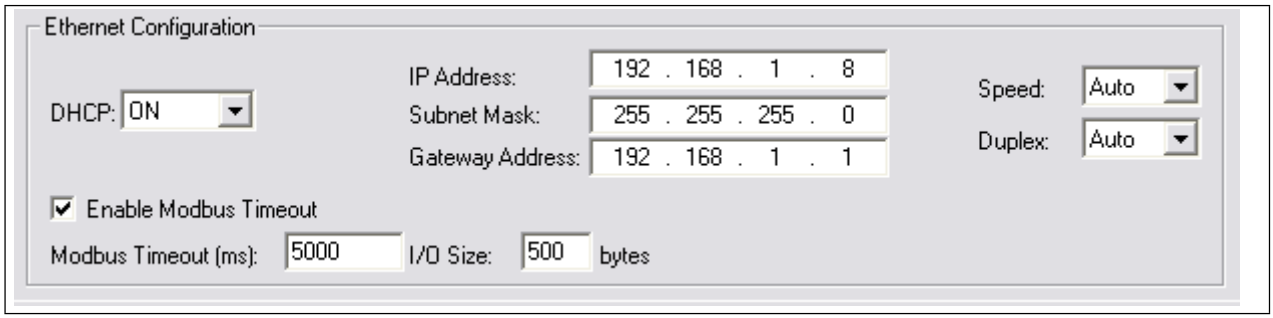


Figure 4-10 Example Ethernet Network Configuration

The Ethernet configuration has been set to auto-negotiate speed and duplex set- tings and retrieve the IP configuration from a DHCP server. If no DHCP server is found, the IP configuration will default to that shown in the dialog.

J1939 Network Configuration

The J1939 network configuration dialog from BWConfig is shown in Figure 4-11. Refer to “Configuration” on page 3-1 for more details on BWConfig.

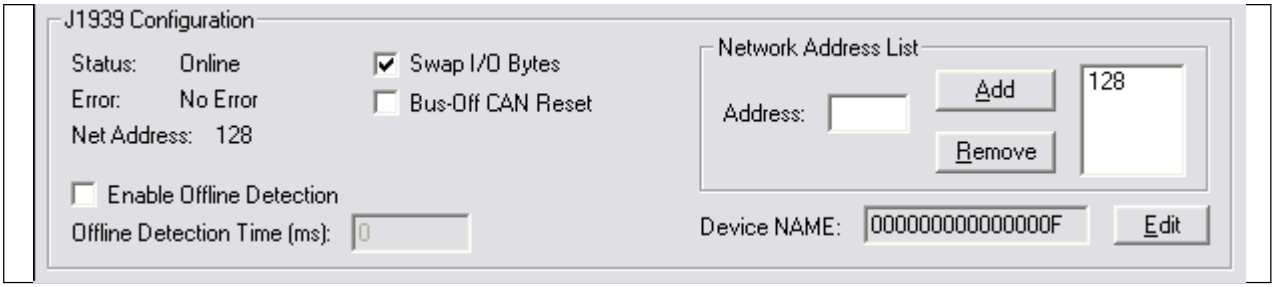


Figure 4-11 Example J1939 Network Configuration

The J1939 device NAME has been set to an arbitrary value for the purpose of this example. The NAME should be set according to the vendor and application where the module is being used based on the J1939 specification. The network address list is set to a single address of 128.

Since this example uses Modbus/TCP, I/O byte swapping has been enabled.

J1939 I/O Configuration

Input Data Points

The input data points are responsible for determining where in the J1939 device input data the J1939 data is to be placed. It is desirable to be able to address the 2 values in our example as individual registers in Modbus/TCP. Since the values are packed into 3 bytes in the J1939 message, they need to be parsed out into 2 regis- ter locations in the input data.

It has been determined that the diagnostic table should be located at an offset 50 words into the J1939 device input data, and contain up to 20 diagnostic entries.

Since Modbus registers are addressed as 16-bit words, each Modbus register occupies 2 bytes in the Input table. Placing values into Modbus registers requires that values be placed on even byte boundaries in the Input table (0, 2, 4,...).

The resulting J1939 input configuration from BWConfig is shown below.

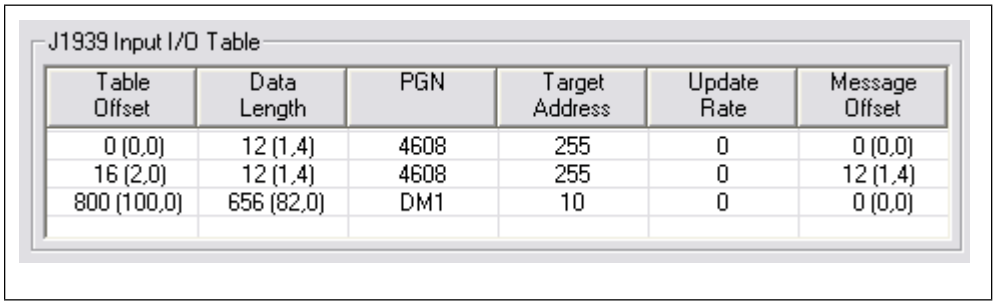


Figure 4-12 Example J1939 Input Configuration

2 data points have been defined, 1 for each value in the message. The first data point copies the first value (12 bits starting at the beginning of the message) into the first word of the J1939 device input data. The second data point copies the sec- ond value (12 bits starting 12 bits into the message) into the second word of the Input data.

Both data points monitor the network for messages with PGN 4608 and any source address (Target Address 255 specifies “don’t care” source address).

The resulting J1939 device input data provides the following Modbus/TCP Input Register addresses. Remember that there is a 2 register status header at Modbus Input Registers 1 and 2. (Modbus register numbers are defined as 1's offset)
0003 Value #1
0004 Value #2

The data point for the DM1 message was configured as shown in Figure 4-13.

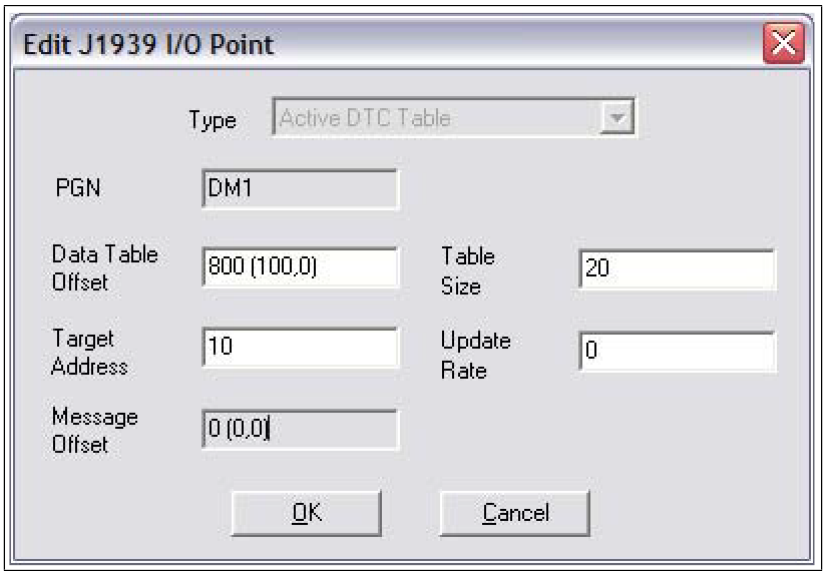


Figure 4-13 Example J1939 Diagnostic Data Point Configuration

Notice that the table length has been set to 20 entries. The target address specifies that the diagnostics of the ECM at address 10 are to be monitored by this data point. The diagnostic table will start at byte 100 of the J1939 device input data, this will set it at word 50 as desired.

This configuration will result in a diagnostic table for ECM 10 at Modbus Input Registers 0051-0092.

Output Data Points

The output data points determine what PGNs are going to be produced by the BridgeWay on J1939, and what the content of those PGN messages is going to be.

Since the example application only needs to produce 16 bits of data in a single PGN message, the resulting configuration is quite simple. It is shown in Figure 4- 14.

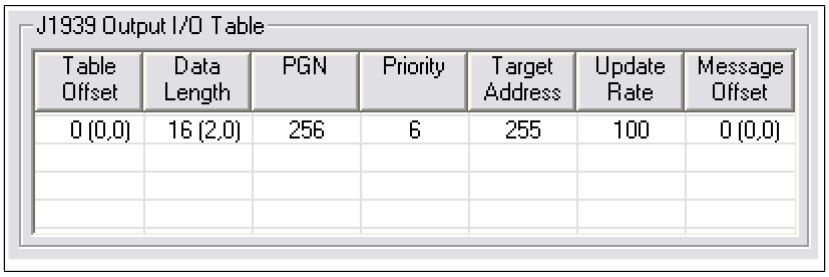


Figure 4-14 Example J1939 Output Configuration

The single data point specifies that 2 bytes of data from the beginning of the J1939 device output data is going to be copied into the first 2 bytes of the message. The message will be transmitted with a PGN of 256 and a priority of 6 every 100ms. The message will be broadcast (Target Address 255) so that it can be seen by everyone on the network.

The Modbus Holding Register address 1029 will be used by the system controller to set the data for the message. Remember that there are 4 registers worth of Run/ Idle and command headers starting at Holding Register address 1025.

EtherNet/IP Interface

EtherNet/IP is based on the Common Industrial Protocol (CIP), which is also the application layer for DeviceNet and ControlNet, to exchange data between nodes.

Product Features

The BridgeWay contains EtherNet/IP Adapter Class functionality. Being an I/O Server it can respond to requests for I/O messages but it does not generate such requests. The BridgeWay supports Message Server functionality. This means it can act as a target for messaging.

CIP Objects

CIP makes use of abstract object modeling to describe the communications of a product. Objects are well defined subsets of a device's functionality. They have functions that they perform called Services and data variables called Attributes. If more than one copy of an object is needed each copy is called an Instance. The BridgeWay contains the same objects as other modules that are based on the CIP protocol.

CIP Messaging

Two types of messaging are used. The regular or repeated transport of a specific set of data items is known as Implicit Messaging. Both parties agree in advance and allocate resources for the data being transported. The connection ID within the Implicit message defines the meaning of the data and establishes the transport rate and transport class. The term Implicit Messaging can be interchanged with the term I/O Messaging.

A one time transport of a data item where both parties do not know in advance what's being transferred is known as Explicit Messaging. Explicit messaging is used for point to point type messaging. The protocol of the message data describes (addresses) the data to be transferred. In object modeling the address is in terms of class number, instance number, and attribute number.

Messages can be sent as Connected or Unconnected. With Connected Messaging device resources are reserved in advance of data transfer and are dedicated and always available. Unconnected messaging provides a means for a device to send a request without establishing a connection prior to data transfer. This is accom- plished through the UCMM or UnConnected Message Manager of the EtherNet/ IP protocol. With UCMM all objects are accessible.

The BridgeWay will handle up to 64 concurrent unconnected transactions. Up to 16 class 3 (messaging) connections are supported.

All Explicit Messages have message data defined in a format called the Message Router Protocol Data Unit (MR_PDU). There are Requests and Responses.

The MR_PDU Request format includes a Service code, Path Size, Path, and data, if any, for the Service. The Path is an encoded series of bytes or Segments describ- ing the location of the data item involved in the transfer. The Logical Segment is most often used. It describes the Class, Instance, and Attribute of the data.

I/O Messaging

The BridgeWay allows an EtherNet/IP Scanner access to the I/O data tables. The data received from the J1939 network is collected in the Input Table (IN) of the BridgeWay and becomes the EtherNet/IP Input data to the EtherNet/IP scanner. EtherNet/IP Output data from the scanner is stored in the BridgeWay's Output Table (OUT) and transmitted on the J1939 network.

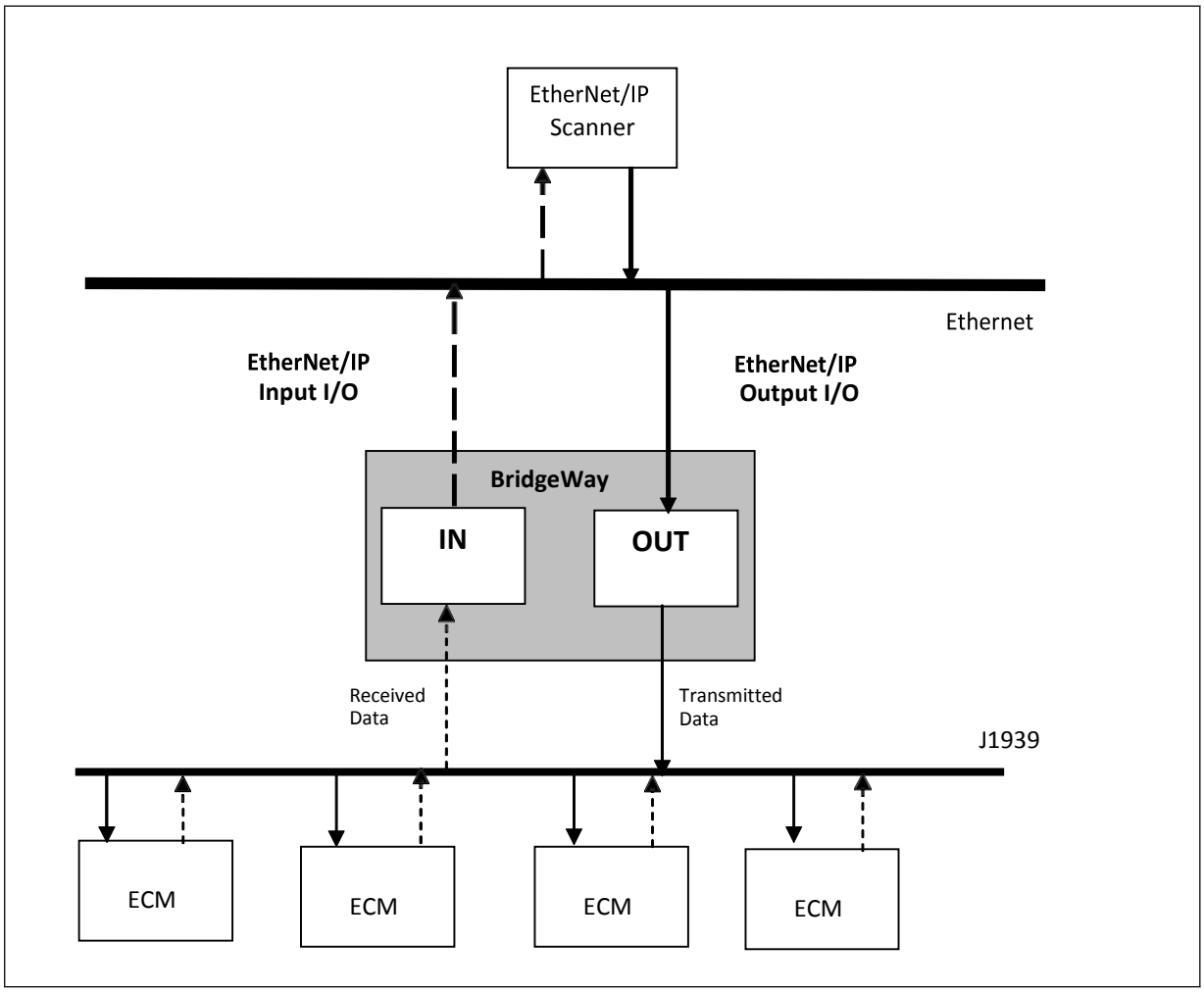


Figure 5-1 BridgeWay I/O Transfer

Assembly Objects and Connections

There are 3 Assembly Object instances accessible from EtherNet/IP: input, output and status. The input and output assemblies are linked to the input and output data tables. The status assembly provides current status information about the Bridge- Way.

The assembly instances associated with these 3 assemblies are listed below.

Assembly Instance	Description	Size in Bytes
100	Input	500 max
101	Status	12
150	Output	496 max

Table 5-1 EtherNet/IP Assembly Instances

Connection Points

Class 1 connections can be established to these assemblies using the connection points listed in Table 5-2.

Conn Point	Description	Size in Bytes	Use
198	Input-Only Heartbeat	0	Output connection point for input-only
199	Listen-Only Heartbeat	0	Output connection point for listen-only
100	Input	4-500	Input connection point.
101	Status	12	Input connection point.
150	Output	8-500	Output connection point.

Table 5-2 EtherNet/IP Connection Points

Connection sizes, when connecting to the input and output assemblies can be set according to the size of the configured I/O data tables configured plus the status and command words in the I/O assemblies. (see the assembly formats below) If a connection is created with a size larger than the configured I/O data table size, the extra data will be filled with 0.

Input Assembly

The input assembly contains a 32-bit status register followed by the J1939 device input data.

Byte Offset	Size in Bytes	Description
0	4	Status register.
4	Up to	J1939 device input data.

Table 5-3 Input Assembly Format

The J1939 device input data format and content is determined by the input data point configuration created with BWConfig. The data appears in the table as it is mapped from the J1939 messages. The J1939 device input data in the assembly is 496 bytes long; however, only the size of the configured input data table will be used, the remaining space will be filled with 0.

The status register is a bit string with the following bit definitions.

Bit	Description
0	BridgeWay is in Run mode. (Cleared if in Idle mode.)
1	BridgeWay is online on the J1939 network.
2	J1939 network interface fault.
3-31	Not used.

Table 5-4 Input Status Register Bit Definitions

Output Assembly

The output assembly contains a 32-bit command register followed by the J1939 device output data.

Byte Offset	Size in Bytes	Description
0	4	Command register.
4	Up to 492	J1939 device output data.

Table 5-5 Output Assembly Format

The J1939 device output data format and content is determined by the output data point configuration created with BWConfig. The data appears in the table as it is mapped to the J1939 messages. The J1939 device output data in the assembly is 492 bytes long; however, only the size configured for the output data table will be used, the remaining space will be ignored.

Note: EtherNet/IP I/O connections append a 32-bit Run/Idle register at the front of the output data. The actual output data transferred in the I/O connection includes this extra 4 bytes at the front of the output assembly described above.

The Command register is a bit string with the following bit definitions.

Bit	Description
0	Local Run Mode. Used in conjunction with the System Run Mode bit in the Run/Idle register to determine the run mode of the BridgeWay. Both bits must be set for the BridgeWay to be in Run mode; otherwise the module will be in Idle mode.
1	Reset Faults. Resets the J1939 network interface faults.
2	Not used.
3	Not used.
4	Reset the BridgeWay module.
5-31	Not used.

Table 5-6 Output Command Register Bit Definitions

Status Assembly

The status assembly is a collection of status and diagnostic information for the BridgeWay J1939 interface. The information in the assembly is updated once a second.

Note: All information in the status assembly is stored in little endian format. The least significant byte of multi-byte values is stored first.

Byte Offse	Size in	Data Type	Name	Description
0	2	UINT	J1939 Interface Status	The current status of the J1939 interface. The following values are defined: 0x8000 Offline 0x8001 Online 0x8002 Initializing
2	2	16-bit bit string	J1939 Interface Faults	The current fault status of the J1939 interface. See the bit definitions below.
4	2	UINT	CAN Error Counter	The number of CAN errors that have been accumulated. This counter is reset by the fault reset command bit.
6	2	UINT	CAN Bus-Off Counter	The number of CAN bus-off errors that have occurred. This counter is reset by the fault reset command bit.
8	2	UINT	CAN Overrun Counter	The number of CAN receive overrun errors that have occurred. This counter is reset by the fault reset
10	2	N/A	Reserved	Reserved

Table 5-7 Status Assembly Format

The J1939 Interface Faults word in the Status Assembly is a bit string with the following bit definitions.

Bit	Description
0	Address Claim Failed. The module was unable to claim the configured address and go online.
1	CAN Network Warning. The CAN controller has detected a large number of CAN errors. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
2	CAN Bus-Off. The CAN interface is currently bus- off. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
3	CAN Data Overrun. The CAN controller has detected a receive packet overrun. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
4	J1939 Transport Protocol Error. The protocol stack has detected an error with a transport protocol (large fragmented) message. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
5	J1939 Receive Queue Overflow. The J1939 receive queue has overflowed. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
6	J1939 Transmit Queue Overflow. The J1939 transmit queue has overflowed. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
7-15	Not used.

Table 5-8 J1939 Interface Fault Register Bit Definitions

I/O Data Summary

The following diagram illustrates how the various components of the input data are used to create the input assembly and connection data accessible from Ether- Net/IP.

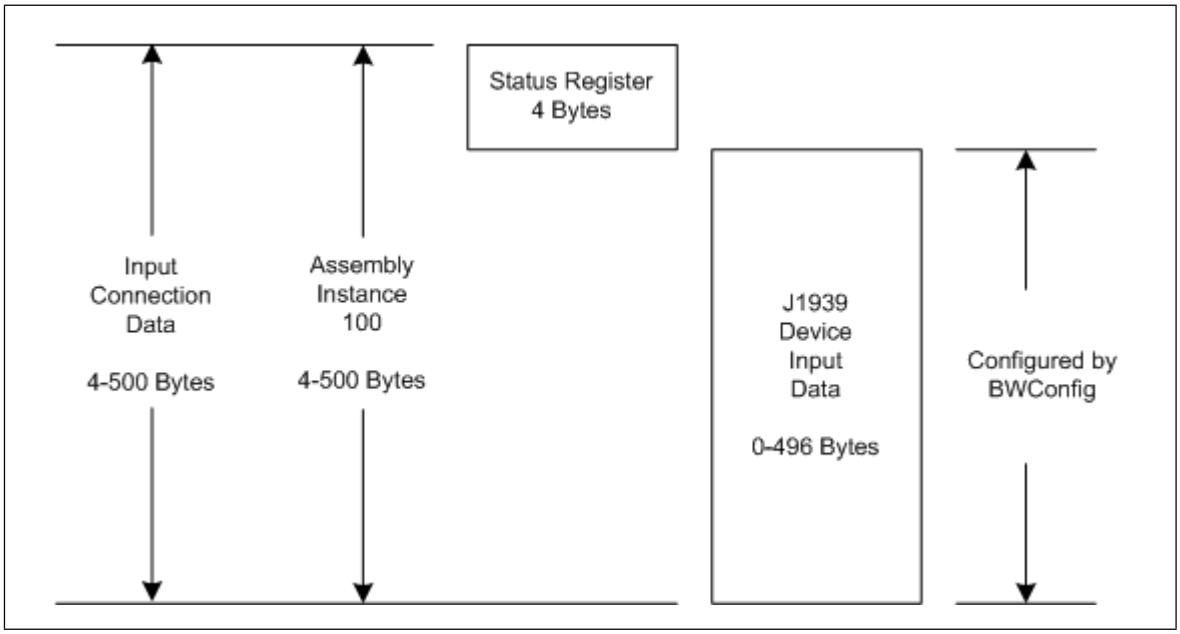


Figure 5-2 Input Data Association

The following diagram illustrates how the various components of the output data are used to create the output assembly and connection data accessible from Ether- Net/IP.

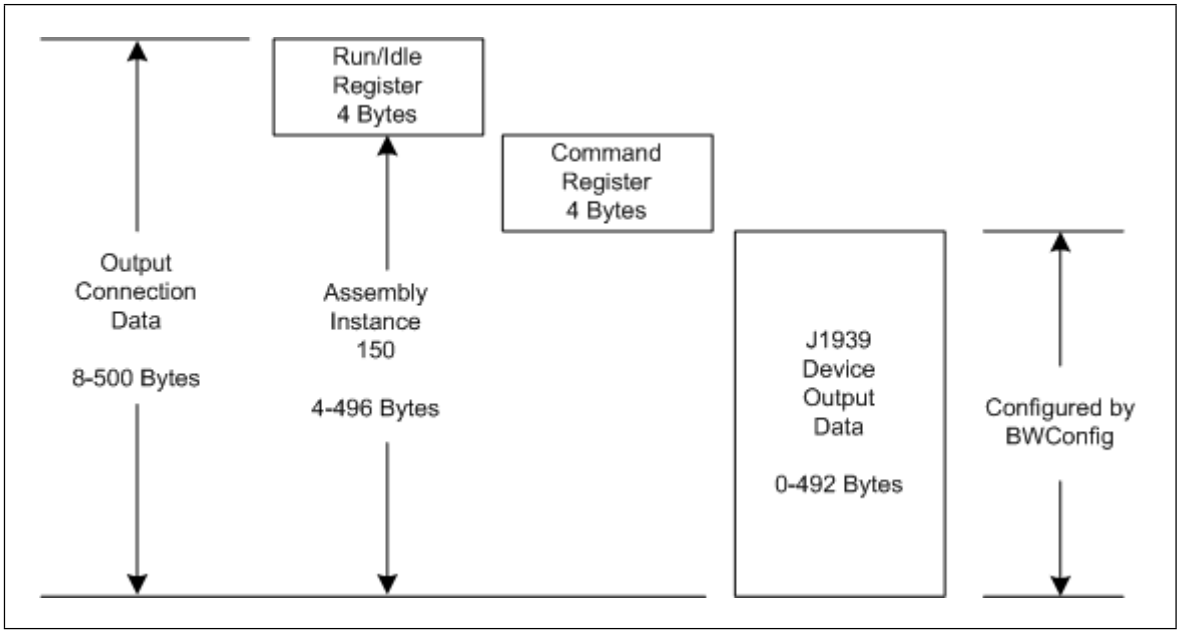


Figure 5-3 Output Data Association

Using ControlLogix with the Gateway

When configuring I/O connections between a Rockwell Automation Control- Logix EtherNet/IP scanner and the BridgeWay, the Generic EtherNet/IP device type should be used.

The Run/Idle register is automatically inserted at the front of the output data and the application has no control over its use. The System Run Mode bit is set according to the Run/Program mode of the controller.

The output size must be set to the configured J1939 output table size plus 4 bytes for the command register (up to a maximum of 496 bytes inclusive). The Run/ Idle header is automatically added by the controller and does not come into play in the size. The input size must be set to the configured J1939 input table size plus 4 bytes for the input status register (up to a maximum of 500 bytes inclusive).

The status assembly may also be monitored by configuring the generic device using a “with status” comm format. Note that although the status assembly size is 12 bytes, only the first 10 bytes contain information. The status connection size for the various connection types are:

SINT with Status	12 bytes		
INT with Status	6 words (16-bit)	DINT with Status	3 dwords (32-bit)

The BridgeWay does not support a configuration assembly. The configuration instance in the device configuration may be set to any number since it will be ignored. Set the configuration assembly size to 0.

The figure below shows a typical ControlLogix device configuration.

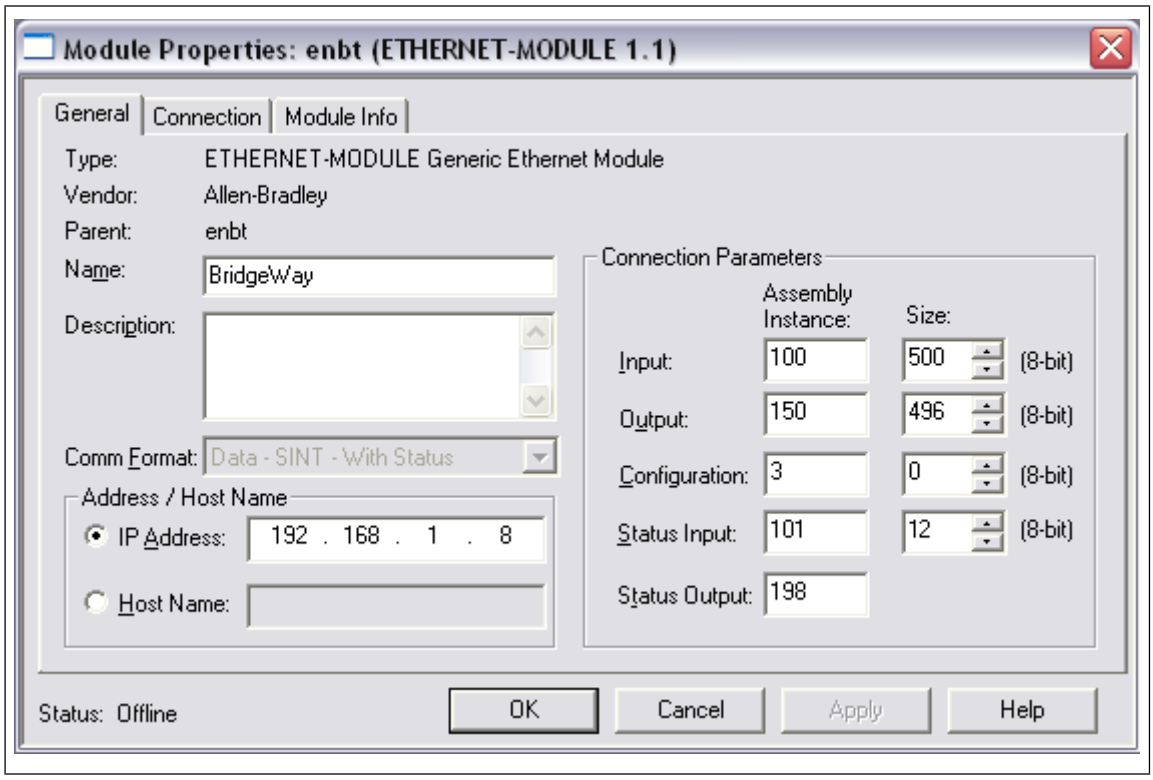


Figure 5-4 ControlLogix Configuration

Modbus/TCP Interface

The BridgeWay supports Modbus/TCP commands. The implementation of the Modbus/TCP server is done according to the Modbus/TCP specification 1.0. All commands according to class 0 and class 1 are implemented and a subset of the class 2 commands.

The module can handle 8 simultaneous connections.

Supported Commands

The following Modbus/TCP commands are supported by the BridgeWay.

Function Code	Function Name	Class	Affects	Address Method
1	Read Coils	1	IN/OUT	Bit
2	Read Input Discrete	1	IN/OUT	Bit
3	Read Multiple Registers	0	IN/OUT	Word
4	Read Input Registers	1	IN/OUT	Word
5	Write Coil	1	OUT	Bit
6	Write Single Register	1	OUT	Word
15	Force Multiple Coils	2	OUT	Bit
16	Force Multiple Registers	0	OUT	Word
22	Mask Write Registers	2	OUT	
23	Read/Write Registers	2	IN/OUT	

Table 6-1 Modbus Commands

Supported Exception Codes

An exception code is returned in the response when the BridgeWay is unable to service the Modbus request that was received. The following exception codes will be used by the BridgeWay.

Exception Code	Name	Description
01	Illegal Func-tion	The module does not support the function code in the query
02	Illegal Data address	The data address received in the query is out- side the initialized memory area
03	Illegal Data Value	The data in the request is illegal

Table 6-2 Exception Codes

Modbus/TCP Addressing

The BridgeWay's Input (IN) and Output (OUT) areas are set to a maximum size of 500 bytes each (or less depending on the I/O size parameter setting). The Status assembly area is 10 bytes. When accessing these areas, with Modbus commands, the addressing is done according to the following tables.

Note: Input Status and Coil bits are mapped MSB first. i.e. Coil 1 corresponds bit 15 of the associated register.

Input Register	Input Status Bit Address									
	15	14	13	12	11	10	9	...	1	0
1	1	2	3	4	5	6	7	...	15	16
2	17	18	19	20	21	22	23	...	31	32
.....										
250	3985	3986	3987	3988	3989	3990	3991	...	3999	4000

Table 6-3 Input Addressing

Holding Register	Coil Bit Address									
	15	14	13	12	11	10	9	...	1	0
1025	1638	1638	1638	1638	16389	1639	16391	...	16399	16400
1026	1640	1640	1640	1640	16405	1640	16407	...	16415	16416
...										
1274	2036 9	2037 0	2037 1	2037 2	20373	2037 4	20375	...	20383	20384

Table 6-4 Output Addressing

Input Register	Input Status Bit Address									
	15	14	13	12	11	10	9	...	1	0
257	4097	4098	4099	4100	410	4102	410	...	4111	411
258	4113	4114	4115	4116	411	4118	411	...	4127	412
...										
261	4161	4162	4163	4164	416 5	4166	416 7	...	4175	417 6

Table 6-5 Status Addressing

Bit Addressing Examples

- To reference the first bit of the Input Table use Input Status bit address 16.
- To reference the 15th bit of the Input Table use Input Status bit address 2
- To reference the first bit of the Output Table use Coil bit address 16400.
- To reference the 15th bit of the Output Table use Coil bit address 16386.

Word Addressing Examples

- To reference the first word of the Input Table use Input Register address 1.
- To reference the 10th word of the Input Table use Input Register address 10
- To reference the first word of the Output Table use Holding Register address 1025.
- To reference the 100th word of the Output Table use Holding Register address 1124.

I/O Data Content

Input Table

The input table contains a 32-bit status register followed by the J1939 device input data.

Modbus Input Register	Size in Words	Description
1	2	Status register.
3	Up to	J1939 device input data.

Table 6-6 Input Table Format

The J1939 device input data format and content is determined by the input data point configuration created with BWConfig. The data appears in the table as it is mapped from the J1939 messages. The J1939 device input data in the assembly is 248 bytes long; however, only the size of the configured input data table will be used, the remaining space will be filled with 0.

The status register is a bit string with the following bit definitions.

Bit	Description
0	BridgeWay is in Run mode. (Cleared if in Idle mode.)
1	BridgeWay is online on the J1939 network.
2	J1939 network interface fault.
3-31	Not used.

Table 6-7 Input Status Register Bit Definitions

Output Table

The output table contains a 32-bit command register followed by the J1939 device output data.

Modbus Holding	Size in Words	Description
1025	2	System Run/Idle register
1027	2	Command register.
1029	Up to	J1939 device output data.

Table 6-8 Output Table Format

The J1939 device output data format and content is determined by the output data point configuration created with BWConfig. The data appears in the table as it is mapped to the J1939 messages. The J1939 device output data in the assembly is 492 bytes long; however, only the size configured for the output data table will be used, the remaining space will be ignored.

The System Run/Idle register is a bit string with the following bit definitions.

Bit	Description
0	System Run Mode. Used in conjunction with the Local Run Mode bit in the Command register to determine the run mode of the BridgeWay. Both bits must be set for the BridgeWay to be in Run mode; otherwise the module will be in Idle mode.
1-31	Not used.

Table 6-9 System Run/Idle Register Bit Definitions

The Command register is a bit string with the following bit definitions.

Bit	Description
0	Local Run Mode. Used in conjunction with the System Run Mode bit in the Run/Idle register to determine the run mode of the BridgeWay. Both bits must be set for the BridgeWay to be in Run mode; otherwise the module will be in Idle mode.
1	Reset Faults. Resets the J1939 network interface faults.
2	Not used.
3	Not used.
4	Reset the BridgeWay module.
5-31	Not used.

Table 6-10 Output Command Register Bit Definitions

Status Data Table

The status data table is a collection of status and diagnostic information for the BridgeWay J1939 interface. The information in the assembly is updated approximately once a second.

Modbus Input Register	Size in Words	Data Type	Name	Description
257	1	UINT	J1939 Interface Status	The current status of the J1939 inter- face. The following values are defined: 0x8000 Offline 0x8001 Online 0x8002 Initializing
258	1	16-bit bit string	J1939 Interface Faults	The current fault status of the J1939 interface. See the bit definitions below.
259	1	UINT	CAN Error Counter	The number of CAN errors that have been accumulated. This counter is reset by the fault reset
260	1	UINT	CAN Bus-Off Counter	The number of CAN bus-off errors that have occurred. This counter is reset by the fault reset command bit.
261	1	UINT	CAN Overrun Counter	The number of CAN receive overrun errors that have occurred. This counter is reset by the fault reset
262	1	N/A	Reserved	Reserved

Table 6-11 Status Data Format

The J1939 Interface Faults word in the Status Assembly is a bit string with the following bit definitions.

Bit	Description
0	Address Claim Failed. The module was unable to claim the configured address and go online.
1	CAN Network Warning. The CAN controller has detected a large number of CAN errors. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
2	CAN Bus-Off. The CAN interface is currently bus- off. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
3	CAN Data Overrun. The CAN controller has detected a receive packet overrun. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
4	J1939 Transport Protocol Error. The protocol stack has detected an error with a transport protocol (large fragmented) message. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
5	J1939 Receive Queue Overflow. The J1939 receive queue has overflowed. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
6	J1939 Transmit Queue Overflow. The J1939 transmit queue has overflowed. This is a sticky bit; it will not be cleared until a Clear Fault command has been issued.
7-15	Not used.

Table 6-12 J1939 Interface Fault Register Bit Definitions

I/O Data Summary

The following diagram illustrates how the various components of the input data are used to create the input assembly and connection data accessible from Mod- bus/TCP.

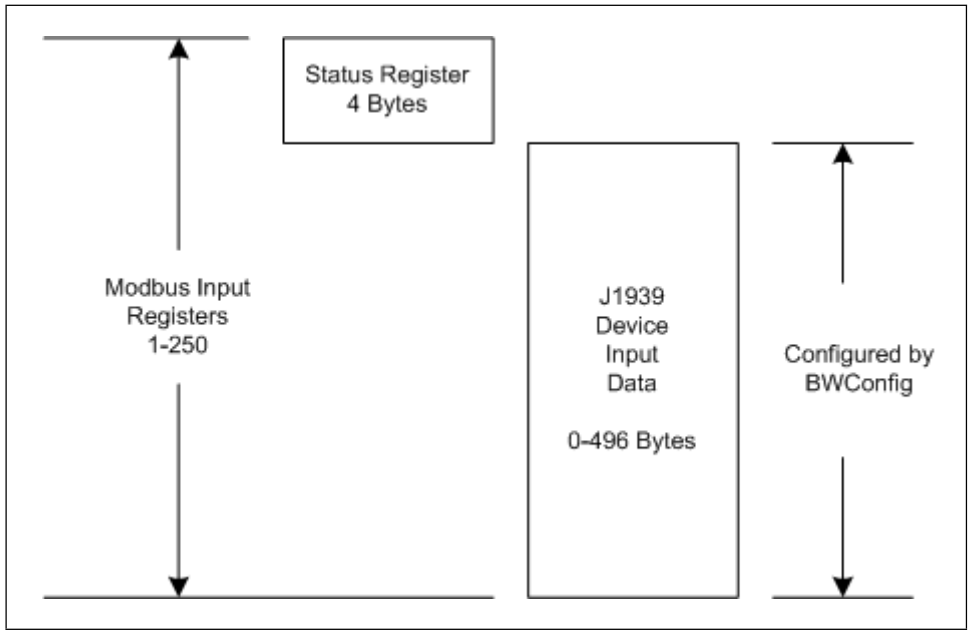


Figure 6-1 Input Data Association

The following diagram illustrates how the various components of the output data are used to create the output assembly and connection data accessible from Mod- bus/TCP.

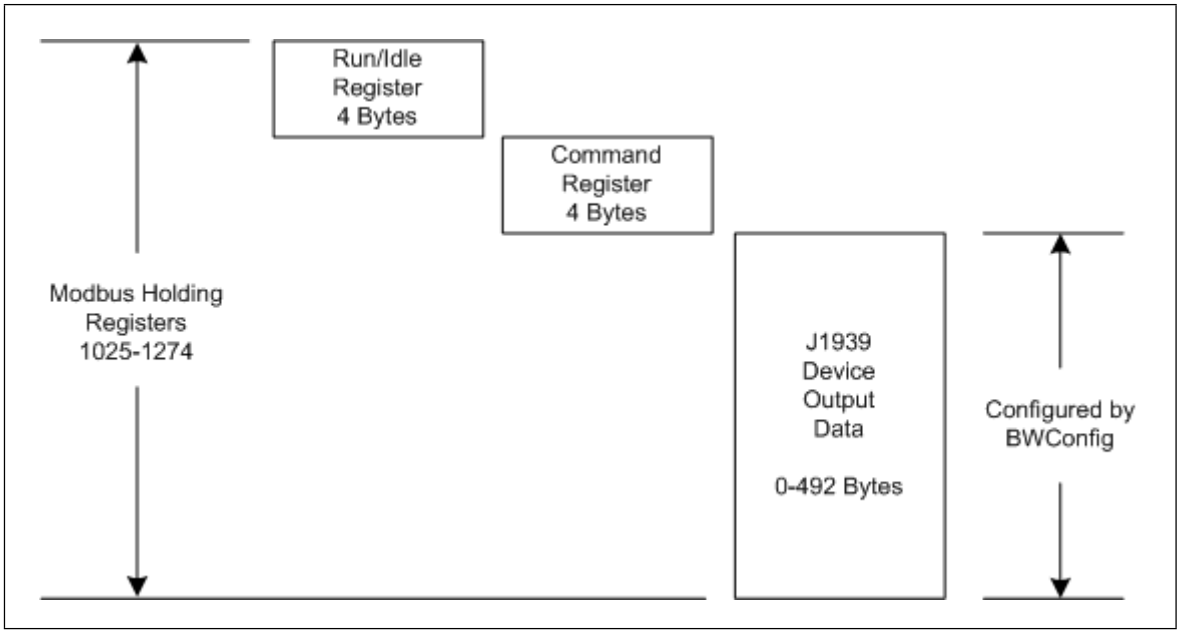


Figure 6-2 Output Data Association

I/O Data Format

The BridgeWay transfers I/O data between Modbus/TCP and J1939 without regard to data content or format. Due to this, the user is responsible for making sure that the devices on either network understand the format of the data.

J1939 is a little endian protocol; values are transmitted least significant byte first. Hence, all data in the I/O tables is assumed, by the J1939 nodes, to be stored as lit- tle endian.

Modbus/TCP is a big endian protocol; values are transmitted most significant byte first.

The Swap I/O Bytes option in the J1939 Network Configuration pane of BWCon- fig will swap the bytes of each 16-bit word in the I/O data tables. This will aid in the transformation between the big and little endian networks. However, care must be taken to assure that data is mapped to 16-bit work boundaries in order for this feature to be fully effective.

J1939 Interface

Address Management

The BridgeWay address management is responsible for bringing the module online on the J1939 network with a unique network address in accordance to the J1939-81 specification. The address management will claim a configured address, if possible, and protect it against lower priority contending address claims. If a configured address is unable to be uniquely claimed, or is lost due to a higher pri- ority contending claim, the module will be taken offline.

This manual will not discuss the address management protocol in detail; readers should reference the J1939-81 specification for complete details. The scope of this section is to explain how the configuration of the address list affects address man- agement.

Single Configured Address

If a single address is configured in the address list, the module will attempt to claim that address. If the configured address is successfully claimed, the module will join the J1939 network using that address. If the address cannot be claimed, the module remains offline.

Multiple Configured Addresses

If more than one address is configured in the address list, the module will attempt to claim addresses in the order they appear in the list until it is either successful, or it runs out of addresses. Once an address is successfully claimed, the module will join the J1939 network using that address. If an address cannot be claimed, the module moves to the next address in the list and attempts to claim that address. If no addresses in the list can be claimed, the module remains offline.

Address Loss

If the module loses its current network address to a higher priority contending address claim, it will cease all network activity using that address. If the address list is configured with a single address, the module will remain offline after an address loss. If the address list has multiple addresses, the module will attempt to claim the next address on the list. If no addresses in the list can be successfully claimed, the module will remain offline.

Invalid Addresses

If the address configured is invalid (outside of the range 0-253), the module will remain offline and not attempt an address claim.

Request for Address Claimed

The BridgeWay will respond to a Request for the Address Claimed PGN (0x00EE00) sent both destination specific and broadcast. The response is depen- dent on the current address management state, and is discussed below.

If the module has successfully claimed an address and is online, the response will be an Address Claimed message with the current address.
If the module is offline because it has lost its address to a higher priority claim and cannot successfully claim another address, the response will be a Cannot Claim Address message.
If the module is in the process of attempting to claim an address, it will not respond to the request.
If the module is offline because it has not yet attempted to claim an address, or the configured address is invalid, it will not respond to the request.

Communications Methods

The J1939 network interface supports reception and transmission of the following J1939 message types in accordance to the J1939-21 specification.

- PDU1 destination specific
- PDU1 broadcast
- PDU2 (broadcast)

Message Transmission

Messages are transmitted on the J1939 network according to the J1939 output configuration. Messages are assembled from data in the Output table and trans- mitted on a cyclic time basis, or in response to a request for the associated PGN.

Data Point to Message Relationship

Output data points with the same PGN and Target Address collectively define a single message to be transmitted on the network.

Message Assembly

Messages are assembled according to the output data points configured for the associated PGN and Target Address. Data is copied from the Output table to the message buffer based on the sizes and offsets of all output data points configured with the PGN and Target Address.

All bits in the message buffer that are not set from the Output table (ranges in the buffer that are not referenced by output data points) are set to 1.

The message length is set according to the size of the data point with the largest message offset. The length is rounded out to the nearest byte.

Note: Message length is strictly determined by the output data point configura- tion for a given message. The BridgeWay does not know the required data length for all possible PGN's. The output data point configuration must provide a data point that will specify the end of the message to ensure that the correct size mes- sage is assembled.

Automatic Transmission

Messages are transmitted automatically based on the Update Time parameter in the output data points associated with the message. The smallest, non-zero Update Time of all data points associated with the message will be used.

If the Update Time is configured as 0, no automatic transmission will occur for the message. The only way that a message configured in this way will be transmit- ted is if a request is received for the associated PGN.

Automatic transmission for a message will occur Update Time milliseconds after the last transmission of the message, regardless of whether the last transmission was automatic or a response to a request PGN.

Handling Request PGNs

Requests received that reference a PGN in an output data point will cause a message transmission of that message. The message will be assembled and transmitted immediately in response to the request, regardless of the timing of the automatic transmission.

Requests received that reference a PGN not configured in an output data point will cause a NAK response if the request was destination specific. Broadcast requests for non-configured PGNs will be ignored.

Destination Addresses

The destination address used for message transmission is dependant on the associated output data point configuration or the request message, whichever caused the transmission. The rules for destination addressing follow.

If the message PGN is a PDU2 type, all PDU2 messages are broadcast by definition.
If the transmission is automatic and the Target Address set to 255, the message will be broadcast.
If the transmission is automatic and the Target Address is not 255, the message will be destination specific to the Target Address.
If the transmission is due to a request and the request was destination spe- cific, the message will be destination specific to the source address of the request.
If the transmission is due to a request and the request was broadcast, the message will be broadcast.

Message Priority

The priority of the message being transmitted is set to the priority configured in the Output Data Point. By specification, the default priority of J1939 messages is 6.

Important: Care should be taken when changing the priority of messages to a value other than 6 as it may affect the performance of other traffic on the J1939 network.

Receiving Messages

Handled Messages

The following J1939 messages are handled by the BridgeWay when they are received from the network.

Address Claimed messages are handled by address management. See “Address Management” on page 7-1.
Request for Address Claimed messages are handled by address manage- ment. See “Address Management” on page 7-1.
Request messages referencing PGNs configured in output data points trig- ger message transmission for the associated message. See “Message Transmission” on page 7-3.
Messages with PGNs and source addresses matching configured input data points trigger an Input table update. See “Input Table Update” below.

Input Table Update

Messages received with a PGN and source address matching that configured for an input data point will be parsed according to the configured data points.

Input data points are combined according to PGN and Target Address. All input data points with matching PGN and Target Address are combined to define the handling for a given message.

If the Target Address is configured as 255, all incoming messages with a match- ing PGN will be parsed using the data point, regardless of source address. If the Target Address is not 255, received messages must match both the PGN and source address in order to be handled by the input data point. Received messages are handled by all input data points that meet these rules; a given message may be processed by more than one input data point.

If a received message passes an input data point’s matching test, the data from its message buffer is copied to the Input table according to the data point configura- tion. Data of the configured length is copied from the configured message buffer offset to the configured Input table offset.

Parameter Timeout Indication

Parameter timeout indication has been provided to allow the Modbus controller to determine if a device on the J1939 network has gone inactive.

Input data points configured with a non-zero update rate will indicate a timeout when the associated message is not received within the configured update rate.

The timeout indication is all bits in input table data for the input data point set to 1. This will effect all input data points associated with the PGN/Target Address. The result appears as if a message was received which contained 0xFF for all data bytes in the message.

Note: The timeout indication (all bits set to 1) will also be used for input data points with non-zero update rates whenever an offline status is detected.

Transport Protocol for Large Messages

The previous sections discussed message handling generically, ignoring message sizes. Messages with buffer sizes of 8 bytes or less can be directly sent and received on J1939. However, messages with buffer sizes greater than 8 bytes must be fragmented, transmitted, and reassembled using the J1939 transport protocol. This section will not discuss the details of the transport protocol, readers should reference the J1939-21 specification; this document will provide a description of when and how the transport protocol is used by the BridgeWay.

Transmission of Large Messages

Messages larger than 8 bytes in length will be sent using transport protocol. If the destination address is 255, the message will be broadcast using BAM (Broadcast Announce Message) mechanisms. If the message is destination specific, a connec- tion will be opened with the destination node and the message sent using RTS/ CTS (Request To Send/Clear To Send) mechanisms. For a complete discussion of BAM and RTS/CTS refer to the J1939-21 specification.

Reception of Large Messages

The BridgeWay will receive large messages that are broadcast using BAM or sent to the module using RTS/CTS. Once a complete message is received and reassem- bled, it is processed generically as described in the previous sections.

Limitations

The current implementation of the transport protocol in the BridgeWay is limited as described below.

Only a single outgoing transport protocol session is active at a time, regardless of whether the message is transmitted using BAM or RTS/ CTS. Large messages are queued for transmission and transmitted in the order in which they are queued.

The module supports up to 35 concurrent incoming transport protocol ses- sions. The concurrent sessions may be any mixture of BAM and RTS/ CTS sessions. Additional BAM sessions will be ignored and RTS connec- tion requests will be denied once the limit is reached.

J1939 Diagnostic Messages

The DM1 (active diagnostics) and DM2 (previously active diagnostics) are the 2 most commonly used J1939 diagnostic messages. The BridgeWay includes sup- port for these 2 message types.

Using BWConfig, the user is able to configure an active or previously active diag- nostic table (or both) for a given J1939 device. The BridgeWay will update the tables based on the contents of DM1 or DM2 messages produced on J1939 by the device, and provide read access to the tables on Ethernet.

This section will describe how the diagnostic tables are handled. See “J1939 Diagnostic Tables” on page 3-23 for configuration details.

Diagnostic Table Format

The active and previously active diagnostic tables have the same format. The for- mat consists of a table header followed by a list of table entries.

Table Header

The table header is a 16-bit word and provides an indication of the number of diagnostic entries that are currently in the table. It also contains the current J1939 lamp status information. The table header content is described below.

Bit	Description
0-1	J1939 Protect lamp status.
2-3	J1939 Amber Warning lamp status.
4-5	J1939 Red Stop lamp status.
6-7	J1939 Malfunction lamp status.
8-14	Entry count. The current number of entries in the table.
15	Table overflow indication.

Table 7-1 J1939 Diagnostic Table Header Content

Table Entry
Each entry in the table contains information for a single diagnostic (J1939 SPN/ FMI). Each table entry is 4 bytes with bit fields as described in the tables below.

The J1939 SPN value may be encoded differently in the diagnostic message received from the ECU. Due to an early vagueness in the J1939-73 specification, there is not a definite means to tell how the SPN is encoded. ECU's that follow the current specification will set the SPN Conversion Method flag to 0 and will encode the SPN value in a specific way. ECU's that follow the early specification will set the Conversion Method flag to 1; however, there are 3 ways that the SPN may be encoded in this case.

The BridgeWay module, as of v2.03.01 provides the value of the Conversion Method in the diagnostic table entries. If the Conversion Method is set to 1, the user should refer to the ECU vendor to determine how the SPN is encoded.

The tables below illustrate how the SPN is stored in the diagnostic table entry for each type of SPN encoding described in the J1939-73 specification.

SPN Conversion Method 0:

Word	Byte	Bits	Description
0	0	0-2	J1939 SPN bits 16-18.
		3-7	J1939 FMI.
	1	0-6	Occurrence count.
		7	SPN Conversion Method (set to 0)
1	2	0-7	J1939 SPN bits 0-7
	3	0-7	J1939 SPN bits 8-15

Table 7-2 Diagnostic Table Entry Content for SPN Conversion Method 0

SPN Conversion Method 1 - Encoding version 1 - The least significant bits with the FMI and the upper 16 bits in Big Endian order.

Word	Byte	Bits	Description
0	0	0-2	J1939 SPN bits 0-2
		3-7	J1939 FMI.
	1	0-6	Occurrence count.
		7	SPN Conversion Method (set to 1)
1	2	0-7	J1939 SPN bits 11-18
	3	0-7	J1939 SPN bits 3-10

Table 7-3 Diagnostic Table Entry Content for SPN Conversion Method 1, Version 1

SPN Conversion Method 1 - Encoding version 2 - The least significant bits with the FMI and the upper 16 bits in Little Endian order.

Word	Byte	Bits	Description
0	0	0-2	J1939 SPN bits 0-2
		3-7	J1939 FMI.
	1	0-6	Occurrence count.
		7	SPN Conversion Method (set to 0)
1	2	0-7	J1939 SPN bits 3-10
	3	0-7	J1939 SPN bits 11-18

Table 7-4 Diagnostic Table Entry Content for SPN Conversion Method 1, Version 2

SPN Conversion Method 1 - Encoding version 3 - The most significant bits with the FMI and the lower 16 bits in Little Endian order.

Word	Byte	Bits	Description
0	0	0-2	J1939 SPN bits 16-18.
		3-7	J1939 FMI.
	1	0-6	Occurrence count.
		7	SPN Conversion Method (set to 0)
1	2	0-7	J1939 SPN bits 0-7
	3	0-7	J1939 SPN bits 8-15

Table 7-5 Diagnostic Table Entry Content for SPN Conversion Method 1, Version 3

Bus-Off Reset Option

The bus-off reset option allows the BridgeWay to be configured to attempt to come back online after it has been knocked offline due to excessive CAN errors.

Option Disabled

If the bus-off reset option is disabled, the BridgeWay will remain offline after a bus-off condition is detected; it will not participate in any J1939 network activity. The only way to bring the module back online is to power cycle the module.

Option Enabled

If the bus-off reset option is enabled, the BridgeWay will re-initialize the CAN controller after a bus-off condition is detected. Once the controller is reinitialized, the module will attempt to go online and resume network activity on the J1939 network.

WARNING

It is suggested that the bus-off reset option be disabled for most applications. Severe network problems can arise if the option is enabled and the BridgeWay module is the node that is causing the CAN errors.

Important: THIS OPTION SHOULD NEVER BE ENABLED WHEN THE MODULE IS USED ON A CONTROL NETWORK OF ANY KIND! IT SHOULD BE RESERVED FOR MONITORING NETWORKS.

Offline Detection

The BridgeWay is able to detect whenever it is not connected to the J1939 net- work or when it is the only device on the network (lonely). In either case the module is not able to transmit or receive J1939 messages.

Online/Offline Status Indication

There is a variety of means to determine whether the BridgeWay is online on the J1939 network.

J1939 Status LED	See “J1939 Status LED” on page 10-2.
Input Status Register	Bit 1 of the Input Status Register in the Input Assembly indicates online status. If the bit is set the module is online. If the bit is cleared the module is offline. See “Input Status Register Bit Definitions” on page 5-5 for EtherNet/IP or “Input Status Register Bit Definitions” on page 6-5 for Modbus/TCP.
Status Assembly	Bit 0 of the J1939 Interface Status register in the Status Assembly indicates whether the module is online. If the bit is set the module is online. If the bit is cleared the module is offline. See “Status Assembly” on page 5-7 for EtherNet/IP or “Status Data Table” on page 6-8 for Mod- bus/TCP.
BridgeWay Con- figruation Tool	The BridgeWay Configuration Tool indicates the online and offline status in the J1939 Configuration pane.

Table 7-6 Online/Offline Status Indications

How Offline Detection Works

The BridgeWay is considered “offline” when it is not able to successfully transmit messages on the J1939 network. In order to successfully transmit a message the module must receive an acknowlegement on the CAN network; if no acknowlege- ment is received for a transmitted message the module is then considered offline. This condition may occur when the module is not connected to the network, or if it is the only node on the network (lonely).

Important: At least one other node besides the BridgeWay module must be present on the J1939 network in order for the BridgeWay to go online.

Offline Detection Message and Timer

Since the BridgeWay uses message transmission to determine whether it is online, if there are no data points configured in the Output Table, the module must transmit a special message, the Offline Detection Message, to test for online status. The Offline Detection Message uses PGN 61184 (EF00h) with the source and destination address both set to the address of the BridgeWay.

The Offline Detection Message may be enabled or disabled in the configuration. When the message is enabled, the Offline Detection Time determines how often the Offline Detection Message will be sent. This effectively determines the time within which an offline condition will be detected. If the application requies that the offline status be detected quickly the time should be set to a smaller value; if the application does not require quick detection the time may be set to a larger value.

Note: The offline detection mechanism is always active regardless of whether the BridgeWay is in Run or Idle mode. The module will transmit Offline Detection Messages when it is in Idle mode. This ensures that the online status being reported is always correct.

Important: If periodic transmission of PGN 61184 could cause adverse affects in the network application, make sure to disable the Offline Detection in the configuration.

Important: The Offline Detection Time should be set as large as the application will allow. Although setting the time to a small value will provide quicker detection of an offline condition, there is a trade-off in that the Offline Detection Message is being transmitted more often.
This trade-off could affect the performance of the BridgeWay and of the J1939 network overall.

Offline Detection with Offline Detection Message Disabled

When the Offline Detection Message feature in the configuration is disabled offline detection will be performed on the messages transmitted by the output data points. An offline condition will be detected whenever an output message is transmitted. If the output data point transmission rate is large, an offline condition that occurs between transmissions will be detected at the next transmission. If no output data points are configured an offline condition will not be detected.

Offline Detection with Offline Detection Message Enabled

When the Offline Detection Message feature in the configuration is enabled offline detection will be performed on the messages transmitted by the output data points as well as the Offline Detection Message. As described above, an offline condition will be detected whenever an output message is transmitted. If the Offline Detection Time is less than the output message transmission rate, the Out- put Detection Message will be transmitted between output data point messages to increase the rate at which an offline condition will be detected. If output data point messages are transmitted at a faster rate than the Offline Detection Time, the Offline Detection Message will not be transmitted

J1939 Baud Rate

The BridgeWay is capable of supporting communication baud rates on the J1939 network of 250K and 500K baud. The correct baud rate must be configured through the BWConfig Baud Rate option in the J1939 Configuration pane.

Important: The standard baud rate for J1939 is 250K baud. Do not set the baud rate to 500K baud unless you are certain that all devices on the network are communicating at 500K baud.

Important: Configuring the module with the incorrect baud rate may cause other devices on the network to experience bus-off faults.

File System

The files system is a fixed-size storage area with a hierarchical directory structure. Any data, user or application can be stored in files within the file system. Files can be grouped in directories for readability.

The file system features two security levels. Depending on security level, different users can have access to different files and directories. The file system is accessi- ble via FTP, Telnet, and HTTP.

File System Conventions

Case Sensitivity

The file system is case sensitive. This means that the file 'pyramid.txt' is not identical to the file 'Pyramid.TXT'.

Filename / Pathname length

Filenames can be a maximum of 48 characters long. Pathnames can be 256 characters in total, filename included.

File Size

The file size is not restricted. Naturally, a file cannot be larger than the available space, see below.

Free space

There is approximately 1 MB available for user files.

Security

The file system features two security levels: Administration and Normal. In Administration mode, the user has full access to the file system through FTP and Telnet. This enables the user to access areas of the file system that are restricted or inaccessible in Normal mode. Normal mode is recommended for normal operation, so that web pages and other settings are protected. Administration mode is intended for product development.

The security level can be set individually for each login.

Files within the file system can be protected from web access through username/ password authorization, see “Password Files” on page 8-11 and “‘web_accs.cfg’” on page 8-12. It is also possible to configure which IP addresses and what proto- cols that are allowed to connect to the module, see “‘ip_accs.cfg’” on page 8-9.

Normal mode

The BridgeWay contains a default admin password (“ad_pswd.cfg”) file so when the module is first powered it operates in normal mode (See “Default User Accounts” on page 9-1). If a valid admin password file (see “Password Files” on page 8-11) is not found, the module will default operations to Administration mode.

In normal mode the FTP and Telnet services are only enabled if there is a subdi- rectory called “\user”. When a normal user connects via FTP or Telnet, this direc- tory will be their root directory. The user will not be able to access files outside this directory and its subdirectories (administrator files).

In normal mode the BridgeWay provides user/password protection for FTP and Telnet with a file called “sys_pswd.cfg” in the directory “\user\pswd”. Files in this directory cannot be accessed by a web browser. A default “sys_pswd.cfg” file is provided. The default file provides a guest user access to FTP and Telnet. This user has username “guest” and password “guest”.

To prevent unauthorized access this should be changed as soon as possible. This can be done by changing the username or password. The Administrator can access this file to add or remove users or change passwords.

If a user logs into Telnet or FTP using a username/password combination found in the admin password file (see “Password Files” on page 8-11) he will gain access to the entire system.

Administration Mode

At power up the BridgeWay contains a default admin password file (See “Default User Accounts” on page 9-1.) A user can login as an administrator by using the username “admin” and password “admin”.

To prevent unauthorized access this should be changed as soon as possible. This can be done by changing the username or password.

If no admin password file (see “Password Files” on page 8-11) is found the mod- ule operates in Administration mode. The user has full access to the file system via FTP or Telnet. ***No login is needed for Telnet, and the FTP server accepts any username/password combination.***

Structure

The figure below illustrates the structure of the file system, where the system files are located, and which areas that can be accessed by normal/admin users.

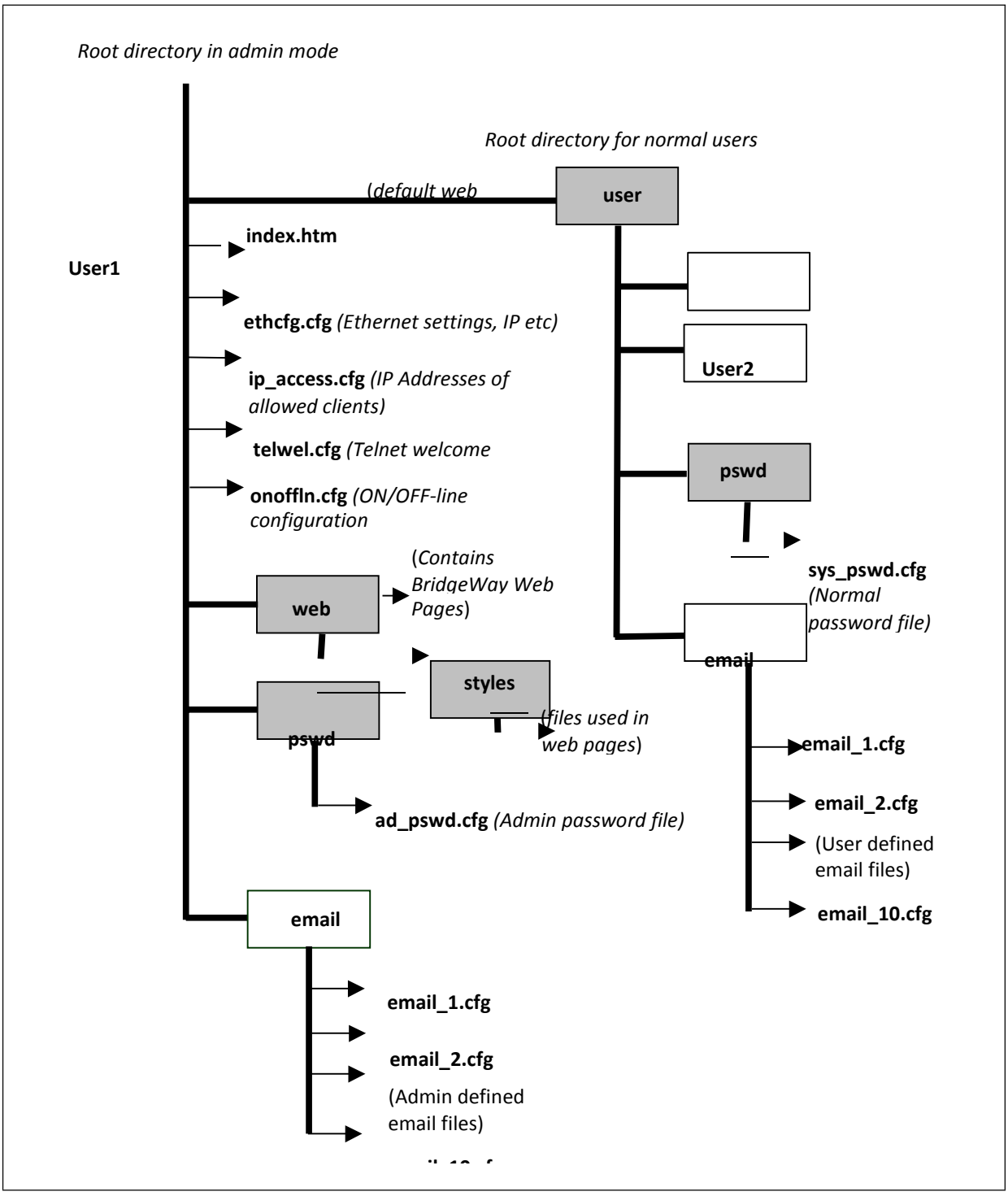


Figure 8-1 File System Directory Structure

Default Files

The following directories are already created on the BridgeWay when first pow- ered;

\pswd,
\user,
\web,
\web\styles,
\user\pswd.

The following files are also on the BridgeWay;

\pswd\ad_pswd.cfg,
\telwel.cfg,
\ethcfg.cfg,
\index.htm
\user\pswd\sys_pswd.cfg.

These files can be edited as needed. Each file is discussed below. The BridgeWay power must be recycled for any changes to take effect.

Virtual File System

The module contains a virtual file system, a set of files used to build the default configuration web page. These are hidden files. The files can be replaced or dis- abled, but not erased. A file with the same name in the file system replaces the file in the virtual file system until it is removed.

The virtual file system contains the following files: index.htm
config.htm configform.htm store.htm logo.gif configuration.gif boarder.bg.gif boarder_m_bg.gif

The BridgeWay contains an “index.htm” file replacing its virtual file counterpart to provide a link to the BridgeWay’s Home page.

System Files

The module uses these files for configuration purposes. The system files are ASCII files and can be edited with any text editor. Depending on security settings, the files may be inaccessible for normal users.

Note: These files shall not be used to store any user or application data.

Configuration Files

'ethcfg.cfg'

This file contains the network configuration and is read by the module at start up. The settings in this file are affected by SSI commands.

The components and format of the file is shown below: [IP address] IP address
10.10.12.212

[Subnet mask] Subnet mask 255.255.255.0

[Gateway address] Gateway address 0.0.0.0

[SMTP address] SMTP address – This must be configured in
0.0.0.0 order to send emails

[SMTP username] The user name required by the SMTP server. Do not
username include this parameter if the server does not require
a username and password.

[SMTP password] The password required by the SMTP server. Do not
password include this parameter if the server does not require a username
and password.

[DNS1 address] Needed to be able to resolve host names. 0.0.0.0

[DNS2 address] Needed to be able to resolve host names. 0.0.0.0

[Domain name] The default domain name for not fully qualified domain
host names.

[DHCP/BOOTP] DHCP/BootP 'ON'-Enabled, 'OFF'-Disabled OFF

[Speed] Speed ‘Auto’ Autonegotiation will be used
Auto ’100’ Forces the module at 100mbits ‘10’ Forces the module at 10mbits

[Duplex] Duplex ‘Auto’ Autonegotiation will be used
Auto ’Full’ Forces the module to operate only at full duplex. ’Half’ Forces the module to operate only at half duplex.

The contents of this file can be redirected by placing the line ‘[File path]’ on the first row, and a file path on the second.

Example:
[File path]
\user\eth_settings.cfg
In this example, the settings described above will be loaded from the file ‘user\eth_settings.cfg’.

This permits normal users to access the network configuration settings.

Note: The module needs to be restarted for changes in this file to have affect.

‘ip_accs.cfg’

It is possible to configure which IP addresses and what protocols that are allowed to connect to the module. This information is stored in the file ‘\ip_accs.cfg’. The file contains one or several of the headers below.

[Web]
[FTP]
[Telnet] [Modbus/TCP] [Ethernet/IP] [All]

Under each header the allowed IP addresses are written. The wildcard ‘*’ can be used to allow series of IP addresses. If a protocol header is not given, the system will use the configuration set under the header ‘All’. If the ‘All’ header is not given, the protocol will not accept any connections.

Example:
[Web] 10.10.12.*
10.10.13.* [FTP] 10.10.12.*
[Telnet] 10.10.12.*
[All]
..*.*

The above example will allow all IP addresses beginning with 10.10.12 to access all protocols in the module. IP numbers beginning with 10.10.13 will not be able to access the FTP and Telnet servers. The Modbus/TCP and EtherNet/IP servers will accept connections from any IP address. The contents of this file can be redirected by placing the line '[File path]' on the first row, and a file path on the second.

Example:
[File path]
\my_settings\ip_access_rights.cfg
In this example, the settings described above will be loaded from the file '\my_settings\ip_access_rights.cfg'.

Note: The module has to be restarted in order for any changes in this file to have affect.

Password Files

'sys_pswd.cfg & ad_pswd.cfg'
These files contain user / password information for users in normal mode ('sys_pswd.cfg') and administration mode ('ad_pswd.cfg'). The files shall be located in '\user\pswd' and '\pswd' respectively.

These directories are protected from web browser access.

The file format is the following: User1:password1 User2:password2
...
UserN:passwordN

Example:
JohnQ:Password
In this example, the username is 'JohnQ', and the password is 'Password'.

If no ':' is present, the password will be equal to the username.

Example:
BillH
In this example, both username and password will be 'BillH'.

‘web_accs.cfg’

Files within the file system can be protected from web access through username/password protection. To put username/password protection to files, a file called ‘web_accs.cfg’ must be located in the same directory as the files to protect. If this file is available, all files within that directory and its subdirectories will be protected. Multiples of these password files may be present in the system, giving different users access to different files and directories.

The file format is the same as for the ‘ad_pswd.cfg’ and ‘sys_pswd.cfg’ files, except that the optional parameter ‘Auth Name’ can be added. The value of this parameter will be presented in the login window as the “Realm”. If it is not given, the requested file/pathname will be presented instead.

Example:

User:Password [Auth Name] (Message goes here)

The contents of this file can be redirected by placing the line ‘[File path]’ on the first row, followed by a list of password files.

Example:

[File path]
\user\pswd\my_passwords\web_pswd.cfg
\user\pswd\my_passwords\more_pswd.cfg
In this example, the accepted user/passwords will be loaded from the files ‘\user\pswd\my_passwords\web_pswd.cfg’ and ‘\user\pswd\my_passwords\more_pswd.cfg’

If any errors in the format of these files is detected the user/password protection will be ignored.

Other Files

'telwel.cfg'

The default Telnet welcome message can be changed by creating this file. It shall contain the new welcome message in ASCII form.

The contents of this file can be redirected by placing the line '[File path]' on the first row, and a file path on the second.

Example:

[File path]
\my_settings\telnet_welcome_message.txt
In this example, the welcome message will be loaded from the file '\my_settings\telnet_welcome_message.txt'.

Email files (email_1.cfg,email_2.cfg to email_10.cfg)

These files contain predefined email messages and information on how and when to send them. It is possible to have a maximum of 10 admin defined email files and 10 user defined email files. The files must be named 'email_1.cfg'... 'email_10.cfg', and placed in the folders '\email' and '\user\email' respectively. If the SMTP server is not configured the email will not be sent (See "'ethcfg.cfg'" on page 8-7).

The file must have the following format. [Register]
Area, Offset, Type

[Register Match]
Match Value, Mask, Match Operand

[To]
Recipient(s)

[From] Sender

[Subject] Subject Line

[Headers] Extra Headers

[Message] Message Body

Parameter	Values	Descriptio
Area	IN OUT	Source area in Input/Output
Offset	a hexadeci-mal (0xN) or decimal	Source Offset in Input/Output
Type	byte wor d	Source data type
Matc h Value	a hexadeci-mal (0xN) or	Value to compare with source value.
Mask	a hexadeci-mal (0xN) or	A logical “AND” is performed on the source data using this Mask before com- paring with the Match Value
Match Operan d	< = >	How the data is compared with the Match Value
Recipient(s)	text (colon	Destination email address(es)
Sender	text	Sender email address
Subject	text (only 1 line)	email subject
Extra Head-ers	text	Optional. It may be useful to send HTML email
Messag e Body	text	Message

Table 8-1 Email Parameters

Example

```
[Register]
IN, 0x0003, byte        A byte is read from the Input area at location 3.


[Register match]
0x20, 0x7F, >   Mask Input byte with 0x7F,
if result greater than 0x20 send email.
[To]
support@your_company.com [From] YourDevice@your_network.com

[Subject] Status

[Message]
Data out of range
```

BridgeWay Web Page Files

The BridgeWay contains several web pages in HTML files to allow changing the default configuration settings and displaying DeviceNet status. Information dis- played on these pages are updated every 2.5 seconds.

NOTE: These web pages require that your browser support Java. Recent versions of Microsoft Internet Explorer do not support Java by default. The Microsoft Vir- tual Machine for Internet Explorer may be downloaded from Microsoft's web site at http://v4.windowsupdate.microsoft.com/en/default.asp.

The files associated with the web pages are in the \web directory and correspond- ing support files are located in \web\styles.

'\index.htm' (Re-Direct Page)
The '\index.htm' file replaces the virtual file index.htm and provides an entry screen with a link to the BridgeWay's Home page in the \web subdirectory.

'\web\index.htm' (Home Page)
The '\web\index.htm' file provides an information screen with links to other web pages in the \web subdirectory. This is considered the BridgeWay's Home page.

'\web\BW_Settings.htm' (Settings)
Click on the "Settings" link to display a web page allowing ethernet address set- tings to be re-configured including the subnet mask, gateway address, IP address, and DHCP enable.

'\web\IOAssemblyView.htm' (IOAssemblyView)
Click on the "IOAssemblyView" link to display a web page providing the current values in the first 20 words of the Input and Output data from an EtherNet/IP per- spective. The current module status is also displayed on this page.

'\web\IOTableView.htm' (IOTableView)
Click on the "IOTableView" link to display a web page providing the current val- ues in the first 20 registers of the Input and Output data from a Modbus/TCP per- spective. The current module status is also displayed on this page.

IT Functionality

The module features common IT functionality such as an HTTP server, FTP server, an Email client, and a Telnet server. This provides easy file management and the possibility to customize the module to provide user-friendly access to parameters.

Also, the module can be configured to report selected information via Email using the Email client.

Default User Accounts

The BridgeWay contains two user accounts on initial power up. One account is for Administration mode (username=admin, password=admin). One account is for a normal user (username=guest, password=guest).

To prevent unauthorized access this should be changed as soon as possible. This can be done by changing the username or password. The Administrator can access the Password files to add or remove users or change passwords. (See files “‘sys_pswd.cfg & ad_pswd.cfg’” on page 8-11).

The FTP Server

It is possible to upload/download files to/from the file system using a standard FTP client. Depending on security settings, different parts of the file system can be accessed by the user:

Normal Mode / Normal User
The user must login using a valid username/password combination. The root directory will be the '\user' directory unless the user has admin permission, see below.

Administration Mode / Admin User
The admin user has unrestricted access to the file system.

The Telnet Server

Through a Telnet client, the user can access the file system using a command line interface similar to MS-DOS™.

Normal Mode / Normal User
The user must login using a valid username/password combination. The root directory will be the '\user' directory unless the user has admin permission, see below.

Administration Mode / Admin User
The user must supply a valid admin user/password combination either during login or by using the command 'admin' in order to get admin permission.
The admin user has full access to the file system. The root directory will be "\" and no files or folders will be hidden.

General Commands

admin
Usage:

admin

Provided that the user can supply a valid admin username/password combination, this command enables admin access in normal mode. This command has no affect in administration mode.

help
Usage:

help [general|diagnostic|filesystem]

General commands:
help - Help with menus
version - Display version information exit - Exit station program
Also try 'help general|diagnostic|filesystem'

version
Usage:

version

This command will display version information, serial number and MAC Address of the module.

exit
Usage:

exit

This command closes the Telnet session.

Diagnostic Commands

The following commands can be viewed by the command ‘help diagnostic’

arps
Usage:

arps

Display ARP stats and table

iface
Usage:

iface

Display net interface stats

sockets
Usage:
sockets

Display socket list

routes
Usage:

routes

Display IP route table

File System Operations

For commands where filenames, directory names or paths shall be given as an argument the names can be written directly or within quotes. For names including spaces the filenames must be surrounded by quotes. It is also possible to use relative pathnames using ‘.’, ‘\’ and’.’.

dir
Usage:

dir [path]

Lists the contents of a directory. If no path is given, the content of the current directory is listed.

md
Usage:

md [[path][directory name]]

Creates a directory. If no path is given, the directory is created in the current directory.

rd
Usage:

rd [[path][directory name]]

Removes a directory. The directory can only be removed if it is empty.

cd
Usage:

cd [path]

Changes current directory.

format
Usage:

format

Formats the file system. This is a privileged command and can only be called in administration mode.

del
Usage:

del [[path][filename]]

Deletes a file.

ren
Usage:

ren [[path][old name]] [[path][new name]]

Renames a file or directory.

move
Usage:

move [[source path][source file]] [[destination path]]

This command moves a file or directory from the source location to a specified destination.

copy
Usage:

copy [[source path][source file]] [[destination path]]

This command creates a copy of the source file at a specified location.

type
Usage:

type [[path][filename]]

Types the contents of a file.

mkfile
Usage:

mkfile [[path][filename]]

Creates an empty file.

append
Usage:
append [[path][filename]] [“The line to append”]

Appends a line to a file.

df
Usage:
df

Displays file system information.

HTTP Server

The module features a complete HTTP (web) server with Server Side Include (SSI) functionality. Server Side Includes are commands to the web server embed- ded in the HTML code. When the web server encounters the commands, the com- mand is executed and the results of the command are inserted into the web page. SSI commands allow easy access to the IN and OUT data areas of the BridgeWay module. It is possible to upload web pages to the module, giving access to data in the memory of the module using a customizable interface.

Virtual Files

The module contains a set of virtual files that can be used when building a web page for configuration of network parameters. These virtual files can be overwrit- ten (not erased) by placing files with the same name in the root of the file system.

By using this feature it is, for example, possible replace a logo by uploading a new logo named '\logo.gif'. It is also possible to make links from a web page to the virtual configuration page. In that case the link shall point to '\config.htm'.

The available virtual files are:
index.htm - Shows the contents of config.htm
config.htm - Configuration frame page configform.htm - Configuration form page configform2.htm - Configuration form page store.htm - Configuration store page
logo.gif - Logo
configuration.gif - Configuration picture boarder_bg.gif - Picture
boarder_m_bg.gif - Picture

Security

All files except the files in the directories “\user\pswd\”, “\pswd\” and files named ‘web_accs.cfg’ can be viewed by default. Other directories can be protected by placing a file called ‘web_accs.cfg’(see “Password Files” on page 8-11) in the directory to protect. The file contains a list of users that are allowed to browse that directory.

Also, it is possible to configure which IP addresses are allowed to connect to the web sever, “‘ip_accs.cfg’” on page 8-9.

SSI Functionality

SSI functionality makes it possible to make web pages interact with module data. e.g. Changing the data in the OUT area of the module. It is also possible to include SSI functions in emails (see “SSI Includes in emails” on page 9-25). The follow- ing are the available SSI functions.

Ethernet Address Display Functions

DisplayIP
This function returns the currently used IP address.

Syntax:

```
<?--#exec cmd_argument=’DisplayIP’-->
```

DisplayMacId
This function returns the MAC ID in the format xx:xx:xx:xx:xx:xx.

Syntax:

```
<?--#exec cmd_argument=’DisplayMacId’-->
```

DisplaySubnet
This function returns the currently used Subnet mask.

Syntax:
<?--#exec cmd:argument=’DisplaySubnet’-->

DisplayGateway
This function returns the currently used Gateway address.

Syntax:
<?--#exec cmd_argument=’DisplayGateway’-->

DisplayDhcpState
This function returns whether DHCP/BootP is enabled or disabled.

Syntax:

<?--#exec cmd_argument=’DisplayDhcpState(
“Output when ON”, “Output when OFF”)’-->

DisplayEmailServer
This function returns the current SMTP server address.

Syntax:
<?--#exec cmd_argument=’DisplayEmailServer’-->

DisplayDNS1
This function returns the address of the primary DNS server.

Syntax:

<?--#exec cmd_argument='DisplayDNS1'-->

DisplayDNS2
This function returns the address of the secondary DNS server.

Syntax:

<?--#exec cmd_argument='DisplayDNS2'-->

DisplayHostName
This function returns the host name.

Syntax:

<?--#exec cmd_argument='DisplayHostName'-->

DisplayDomainName
This function returns the default domain name.

Syntax:

<?--#exec cmd_argument='DisplayDomainName'-->

DisplaySMTPUser
This function returns the username used for SMTP authentication.

Syntax:

<?--#exec cmd_argument='DisplaySMTPUser'-->

DisplaySMTPPswd
This function returns the password used for SMTP authentication.

Syntax:

<?--#exec cmd_argument='DisplaySMTPPswd'-->

Store Function

StoreEtnConfig
This SSI function stores a passed IP configuration to FLASH.

Syntax:

<?--#exec cmd_argument='StoreEtnConfig'-->

Include this line in a HTML page and pass a form with new IP settings to it.

Accepted fields in form:

SetIp SetSubnet SetGateway SetEmailServer
SetDhcpState - value "on" or "off"

Default output:

Invalid IP address! Invalid Subnet mask! Invalid Gateway address!
Invalid IP address or Subnet mask! Invalid Email Server IP address!
Configuration stored correctly. Invalid DHCP state!
Failed to store the configuration!

For information about how to change the SSI output, please see "Changing SSI Output" on page 9-23.

Formatted Display

printf
This SSI function includes a formatted string, which may contain data from the Input (IN) Output (OUT) area, on a web page. The formatting of the string is equal to the standard C function printf().

Syntax:

```
<?--#exec cmd_argument='printf(
"String to write", Arg1, Arg2,..., ArgN)'-->
```

Like the standard C function printf() the "String to write" for this SSI function contains two types of objects: Ordinary characters, which are copied to the output stream, and conversion specifications, each of which causes conversion and printing of the next successive argument to printf. Each conversion specification begins with the character "%" and ends with a conversion character.

Between the “%” and the conversion character there may be the following modifiers:

Modifier	Description
-	Specifies left adjustment of the converted argument in its field.
+	Specifies that the number will always be printed with a sign.
space	If the first character is not a sign, a space will be prefixed.
0	Specifies padding to the field with leading zeroes.
#	Specifies an alternate output form. For o, the first digit will be zero. For x or X, 0x or 0X will be prefixed to a non-zero result. For e, E, f, g and G, the output will always have a decimal point; for g and G, trailing zeros will not be removed.
width	A number specifying a minimum field width. The converted argument will be printed in a field at least this wide, and wider if necessary. If the converted argument has fewer characters than the field width it will be padded on the left (or right, if left adjustment has been requested) to make up the field width. The padding character is normally space, but can be 0 if the zero pad- ding flag is present.
precision	A number, the precision, that specifies the maximum number of characters to be printed from a string, or the number of digits to be printed after the decimal point for e, E, or F conversions, or the number of significant digits for g or G conversion, or the minimum number of digits to be printed for an integer (leading 0s will be added to make up the necessary
.	A period, which separates the field width from the precision.
h	A length modifier. “h” Indicates that the corresponding argument is to be printed as a short or unsigned short.
l or L	A length modifier. “L” or “l” indicates that the argument is along or unsigned long.

Table 9-1 printf Modifiers

The conversion characters and their meaning are shown below. If the character after the “%” is not conversion character, the behavior is undefined.

Charac- ter	Argument Type	Converted To
d, i	Byte,Short	Signed Decimal Notation
o	Byte,Short	Unsigned Octal Notation (without a leading zero)
x,X	Byte,Short	Unsigned hexadecimal notation (without a lead- ing 0x or 0X)
u	Byte,Short	Unsigned decimal notation
c	Byte,Short	Single character, after conversion to unsigned char
s	char *	Characters from the string are printed until a “\0” is reached or until the number of characters indi- cated by the precision have been printed
f	Long	Decimal notation of the form [-] m.dddddde+ -xx or [-]m.ddddddE+-xx where the number of d’s is specified by the precision. The default precision is 6; a precision of 0 suppresses the decimal point.
e,E	Long	Decimal notation of the form [-] m.dddddde+ -xx or [-]m.ddddddE+-xx where the number of d’s is specified by the precision. The default precision is 6; a precision of 0 suppresses the decimal point.
g,G	Long	“%e” or “%E” is used if the exponent is less than -4 or greater than or equal to the precision; other- wise “%f” is used. Trailing zeroes and trailing decimal point are not printed.
%		Print a “%”

Table 9-2 printf Conversion Characters

The arguments that can be passed to the SSI function *printf* are:

Argument	Description
InReadSByte(offset)	Reads a signed byte from position offset in the Input (IN) area
InReadUByte(offset)	Reads a unsigned byte from position offset in the IN area
InReadSWord(offset)	Reads a signed word (short) from position offset in the IN area
InReadUWord(offset)	Reads a unsigned word (short) from position offset in the IN area
InReadSLong(offset)	Reads a signed longword (long) from position offset in the IN area
InReadULong(offset)	Reads an unsigned longword (long) from position offset in the IN area
InreadString(offset)	Reads a string (char*) byte from position offset in the IN area
InReadFloat(offset)	Reads a floating point (float) value from position offset in the IN area
OutReadSByte(offset)	Reads a signed byte from position offset in the OUT area
OutReadUByte(offset)	Reads a unsigned byte from position offset in the OUT area
OutReadSWord(offset)	Reads a signed word (short) from position offset in the OUT area
OutReadUWord(offset)	Reads a unsigned word (short) from position offset in the OUT area
OutReadSLong(offset)	Reads a signed longword (long) from position offset in the OUTarea
OutReadULong(offset)	Reads an unsigned longword (long) from position offset in the OUT area
OutReadString(offset)	Reads a string (char*) byte from position offset in the OUT area
OutReadFloat(offset)	Reads a floating point (float) value from position offset in the OUT area

Table 9-3 SSI Functions to Read Data

Note: The I/O data accessed by the web page is in the same format as the data accessed via the Ethernet network via EtherNet/IP or Modbus/TCP. The web server operates in a big endian environment. Some data may have to be manipu- lated to account for byte ordering when displaying it on a web page depending on the configuration of the Swap I/O Bytes parameter in the Ethernet configuration.

Formatted Input

scanf
This SSI function reads a string passed from an object in a HTML form, interprets the string according to the specification in format, and stores the result in the Out- put (OUT) area according to the passed arguments. The formatting of the string is equal to the standard C function call scanf().

Syntax:

<?--#exec cmd_argument='scanf(ObjName, format, Arg1,..., ArgN), ErrVal1,..., ErrvalN'-->

ObjName The name of the object with the passed data string format Specifies how the passed string shall be formatted
Arg*n* Specifies where to write the data
ErrVal*n* Optional; specifies the value/string to write in case of an error.

Character	Input Data and Argument Type
d	Decimal number; byte, short
i	Number, byte, short. The number may be in octal (leading 0(zero)) or hexadecimal (leading 0x or 0X)
o	Octal number (with or without leading zero); byte, short
u	Unsigned decimal number; unsigned byte, unsigned short
x	Hexadecimal number (with or without leading 0x or 0X); byte, short
c	Characters; char*. The next input characters (default 1) are placed at the indicated spot. The normal skip over white space is suppressed; to read the next non-white space character, use "%1s"
s	Character string (not quoted); char*, pointing to an array of char- acters large enough for the string and a terminating "\0" that will be added.
e, f, g	Floating-point number with optional sign, optional decimal point and optional exponent; float
%	Literal "%"; no assignment is made.

Table 9-4 scanf Formats

The conversion characters d, i, o, u and x may be preceded by the letter “l” to indicate that a pointer to ‘long’ appears in the argument list rather than a ‘byte’ or a ‘short’

The arguments that can be passed to the SSI function scanf are:

Argument	Description
OutWriteByte(offset)	Writes a byte to position *offset* in the OUT area
OutWriteWord(offset)	Writes a word (short) to position *offset* in the OUT area
OutWriteLong(offset)	Writes a long to position *offset* in the OUT area
OutWriteString(offset)	Writes a string to position *offset* in the OUT area
OutWriteFloat(offset)	Writes a floating point (float) value to position *offset* in the OUT area

Table 9-5 SSI Functions to Write Data

Default output: Write succeeded Write failed

For information about how to change the SSI Output, see “Changing SSI Output” on page 9-23“.

Note: The I/O data accessed by the web page is in the same format as the data accessed via the Ethernet network via EtherNet/IP or Modbus/TCP. The web server operates in a big endian environment. Some data may have to be manipu- lated to account for byte ordering when displaying it on a web page depending on the configuration of the Swap I/O Bytes parameter in the Ethernet configuration.

Text Function

GetText
This SSI function gets the text from an object and stores it in the OUT area.

Syntax:

```
<?--#exec cmd arbgument='GetText(
"ObjName", OutWriteString (offset), n)'-->
```

offset specifies the offset from the beginning of the OUT area. n (optional) specifies maximum number of characters to read

Default output:
Success - Write succeeded Failure - Write failed

File Functions

IncludeFile
This SSI function includes the contents of a file on a web page.

Syntax:
<?--#exec cmd_argument='IncludeFile(Filename)'-->

Default output:
Success - <File contents>
Failure - Failed to open <filename>

SaveToFile
This SSI function saves the contents of a passed form to a file. The passed name/ value pair will be written to the file "File name" separated by the "Separator" string. The contents can either be Appended to the file or overwrite the current content of the file.

Syntax:

<?--#exec cmd_argument='SaveToFile(
"File name", "Separator", [Append|Overwrite])'-->

Default output:
Success - Form saved to file Failure - Failed to save form

SaveDataToFile
This SSI function saves the data of a passed form to a file. The Object Name parameter is optional and, if specified, only the data from that object will be stored. If no object is specified, the data from all objects in the form will be stored. The contents can either be Appended to the file or Overwrite the current contents of the file.

Syntax:

```
<?--#exec cmd_argument='SaveDataToFile(
"File name", "Object name", [Append|Overwrite])'-->
```

Default output:
Success - Form data saved to file Failure - Failed to save form data

String Functions

Changing SSI Output
There are two methods of changing the output strings from SSI functions:
Changing SSI output defaults by creating a file called “\ssi_str.cfg” con- taining the output strings for all SSI functions in the system.

Temporary changing the SSI output by calling the SSI function “SsiOut- put()”.

SSI Output string file
If the file “\ssi_str.cfg” is found in the file system and the file is correct according to the specification below, the SSI functions will use the output strings specified in this file instead of the default strings.

The file has the following format: [StoreEtnConfig]
Success: “String to use on success”
Invalid IP: “String to use when the IP address is invalid” Invalid Subnet: “String to use when the Subnet mask is invalid”
Invalid Gateway: “String to use when the Gateway address is invalid” Invalid Email server: “String to use when the SMTP address is invalid”
Invalid IP or Subnet: “String to use when the IP address and Subnet mask does not match”
Save Error: “String to use when storage fails”
Invalid DHCP state: “String to use when the DHCP state is invalid”

[scanf]
Success: “String to use on success” Failure: “String to use on failure”

[IncludeFile]
Failure: “String to use when failure” To include filename “%s” can be included to the string once

[SaveToFile]
Success: “String to use on success”
Failure: “String to use on failure” To include filename “%s” can be included to the string once.

[GetText]
Success: “String to use on success” Failure: “String to use on failure”

The contents of this file can be redirected by placing the line [File path] on the first row, and the actual file path on the second row.

Temporary SSI Output change
The SSI output for the next called SSI function can be changed with the SSI function “SsiOutput()” The next called SSI function will use the output according to this call. Thereafter the SSI functions use the default outputs or the outputs according to the file ‘\ssi_str.cfg’. The maximum size of a string is 128 bytes.

Syntax:

```
<?--#exec cmd_argument=’SsiOutput(
“Success string”, “Failure string”)’-->
```

Example:

This example shows how to change the output strings for a scanf SSI call.

```
<?--#exec cmd_argument=’SsiOutput (“Parameter1 updated”, “Error”)’-->
<?--#exec cmd_argument=”scanf(“Parameter1”, “%d”, OutWriteByte(0))’-->
```

Email Client

It is possible to send predefined email messages to predefined receivers triggered by an event in the IN/OUT area. This area is scanned 2 times a second. The IP address to a SMTP (mail) server and any required username and password must be configured (See“‘ethcfg.cfg’” on page 8-7). It is possible to have 10 user defined, and 10 admin defined emails triggered on different events. These shall be placed in directories “\user\email” for user configurable emails and “\email” for non-user configurable emails. See “Email files (email_1.cfg,email_2.cfg to email_10.cfg)” on page 8-14.

SSI Includes in emails

For predefined emails it possible to include data. This is performed in the same way data is added to web pages using SSI functions. The supported SSI functions for emails include:

DisplayIP
DisplayMACID
DisplaySubnet
DisplayGateway
DisplayDNS1
DisplayDNS2
DisplayHostName
DisplayDomainName
DisplayEmailServer
DisplayDHCPState
DisplaySMTPUser
DisplaySMTPPswd
printf
IncludeFile
SsiOutput

Displaying I/O Data on a Web Page

The following is an example of an HTML file that when uploaded to the module displays in hex the second byte of data from the IN table and the third byte of data of the OUT table using the SSI “printf” command.

```
<html>
<head>
<title>Ethernet to DeviceNet BridgeWay</title>
</head>
<body>
<center>
</h1>
<?--#exec cmd_argument='printf(“IN 2 = 0x%2X”,InReadUByte(2))'-->
<?--#exec cmd_argument='printf(“OUT 3 = 0x%2X”,OutReadUByte(3))'-->
</body>
</html>
```

Status and Diagnostics

BridgeWay LEDs

There is a group of LED indicators on the front of the BridgeWay that is used to annunciate the current status of the module and the network interfaces. The layout of the LEDs is shown in Figure 10-1.

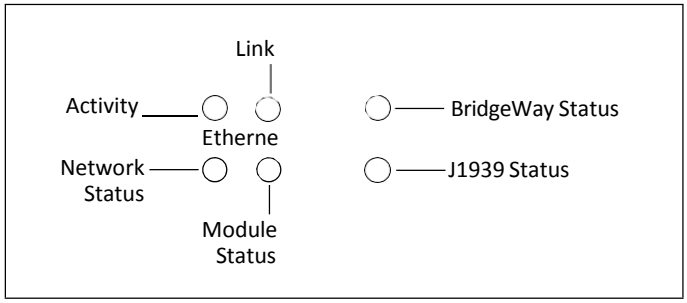


Figure 10-1 BridgeWay LEDs

BridgeWay Status LED

State	Summary	Description
Flashing Green	Idle	Module is in Idle mode.
Solid Green	Run	Module is in Run mode.
Solid Orange	Hardware Initialization	The LED will be in this state immedi-ately after power is applied.
Flashing Red/Green	Error	A major, unrecoverable fault has been detected.
Red, Green, Orange Alternate	Self Test	A self test of the module is in progress.

Table 10-1 BridgeWay Status LED States

Major unrecoverable faults are indicated by a series of green and red flashes. If the BridgeWay Status LED is flashing red and green for an extended period of time, count the number of red and green flashes and call technical support.

J1939 Status LED

State	Summary	Description
Flashing Green	Initializing / Offline	The J1939 network interface is cur- rently being initialized and is waiting to come online. The module is not par- ticipating in J1939 traffic.
Solid Green	Online	A J1939 network address has been suc- cessfully claimed and the module is online and active.
Flashing Red/Green	Online with Faults	The module is online and active on the J1939 network, but faults have been detected. Check the J1939 status codes to determine the cause of the
Solid Red	Offline	The module is not participating in the J1939 network.
Flashing Red	Offline with Faults	The module is not participating in the J1939 network and faults have been detected. Check the J1939 status codes to determine the cause of the

Table 10-2 J1939 Status LED States

Ethernet Activity LED

The Ethernet Activity LED flashes green as Ethernet packets are received or transmitted.

Ethernet Link LED

The Ethernet Link LED indicates that the module is connected to an Ethernet net- work. The LED will display solid green if there is a valid physical link.

Ethernet Module Status LED

State	Summary	Description
Off	No Power	Not powered
Solid Green	Normal	The module is controlled by an Ether- Net/IP scanner in Run mode.
Flashing Green	Standby	The module is not controlled by a scanner in Run mode. Note that this is the normal state when using Modbus/ TCP masters.
Solid Red	Unrecover - able fault	A fault the requires user intervention has been detected. Correct the problem and reset the BridgeWay.
Flashing Red	Recoverabl e fault.	A fault that can be corrected and does not require a BridgeWay reset has been detected.
Red,Green Alternate	Self Test	A self test of the module is in progress.

Table 10-3 Ethernet Module Status LED States

Ethernet Network Status LED

State	Summary	Description
Off	No Power	The module has no power or no IP address assigned.
Solid Green	Network OK and commu-	There is at least one EtherNet/IP con- nection. *(Not affected by Modbus/TCP connections.)*
Flashing Green	Network OK	There are no active connections. *(Not affected by Modbus/TCP*
Solid Red	Address con- flict	The module's IP address is already in use by another module.
Flashing Red	Connectio n Time-out	One or more of the connections in which this module is the target has timed out. This state is only left if all timed out connections are re-estab- lished or if the module is reset.

Red,Green Alternate	Self Test	A self test of the module is in progress.

Table 10-4 Ethernet Network Status LED States

J1939 Status Codes

The status codes for the J1939 interface are displayed by the BridgeWay Configu- ration Tool in the network configuration pane associated with the J1939 network. There are 2 status codes: a general status, and an error status. The general status is displayed as a textual status. The error status codes are bit strings, so the values are displayed in hexadecimal format to make them easier to decipher.

J1939 General Status

Value	Description
Offline	The module is not participating in J1939 network activity.
Online	The module is online and participating in J1939 network activ- ity.

Table 10-5 J1939 General Status Values

J1939 Error Status

Bit	Description
0	The address claim has failed. The BridgeWay was unable to claim a unique J1939 network address and join network activity.
1	The CAN error counter has exceeded its warning limits at least one time since bootup or the last fault reset.
2	The CAN controller has reported a bus-off condition at least one time since bootup or the last fault reset.
3	A CAN receive overrun condition was detected at least one time since bootup or the last fault reset.
4	A J1939 transport protocol error has occurred at least one time since bootup or the last fault reset.
5	A receive message queue has overflowed at least one time since bootup or the last fault reset.
6	A transmit message queue has overflowed at least one time since bootup or the last fault reset.
7-15	Not used.

Table 10-6 J1939 Error Status Bit Definitions

Diagnostic Web Pages

Status and Settings Web Page

The Status and Settings page displays the BridgeWay identification information, current status, and IP configuration. The IP configuration can be changed from this page. The module status is updated approximately every 2.5 seconds.

I/O Assembly View Web Page

The I/O Assembly page displays the current values that are in the input and output assemblies from the perspective of EtherNet/IP. The data values are updated approximately every 2.5 seconds.

I/O Table View Web Page

The I/O Table page displays the current values that are in the input and output tables from the perspective of Modbus/TCP registers. The data values are updated approximately every 2.5 seconds.

Status Assembly

The status assembly is an assembly object instance that is accessible from Ether- Net/IP both explicitly and using an I/O connection. The status assembly contains current status and diagnostic information pertaining to the BridgeWay's J1939 interface. See "Status Assembly" on page 5-7 for complete details of the format and content of the assembly for EtherNet/IP. See "Status Data Table" on page 6- 8 for details of the format and content of the data for Modbus/TCP.

Specifications

Environmental Specifications

Temperature

Operating: 0 to 70 degrees Celsius
Non-Operating: -25 to 85 degrees Celsius

EMC Directive Compliance

This product is tested to meet the Council Directive 89/336/EC Electromagnetic Compatibility (EMC) by applying the following standards, in whole or in part, documented in a technical construction file:

- EN50081-2-EMC Generic Emission Standard, Part 2 - Industrial Envi- ronment
- EN50082-2-EMC Generic Immunity Standard, Part 2 - Industrial Envi- ronment

This product is intended for use in an industrial environment.

Electrical Specifications

DC Power

Operating voltage: 12-30v DC.
Current Requirements: 130-140 mA at 24 VDC.

Mechanical Specifications

Mechanical Rating

IP20/NEMA 1

DIN Rail Mount

The BridgeWay connects to a DIN 3 rail.

Dimensions

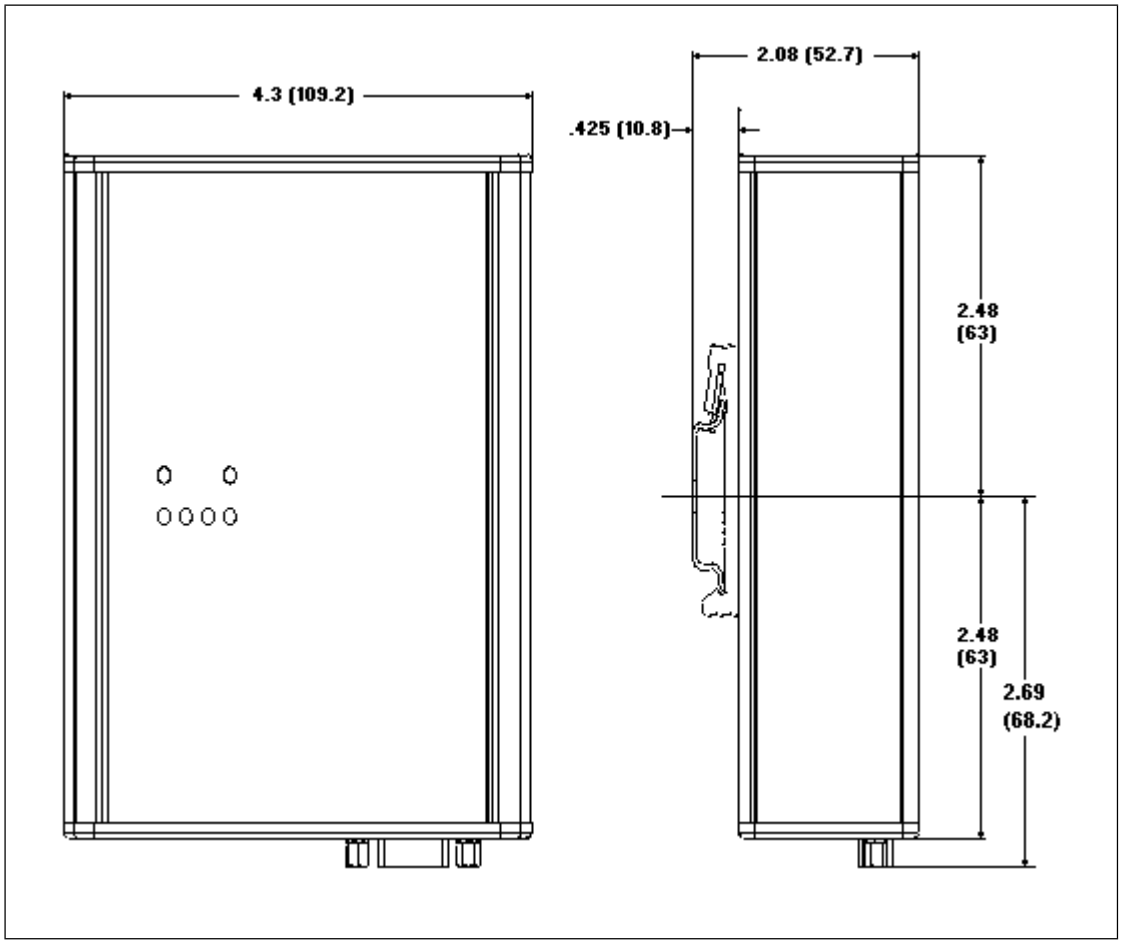


Figure 11-1 BridgeWay Mechanical Dimensions

I/O Data Sizes

Maximum 500 bytes input including the status register Maximum 496 bytes output including the command register 12 bytes of status data 200 total data points (input plus output)

Up to 120 different PGN's may be monitored by input data points Up to 100 different PGN's may be transmitted by output data points Up to 20 data points may be mapped for a single PGN

J1939 Specifications

Message Types

Supports transmission and reception of the following message types:

PDU1 destination specific
PDU1 broadcast
PDU2

Addressing

Claims and protects a single configurable address. Self-configurable using a list of addresses.

Transport Protocol Sessions

Support of J1939 transport protocol for large messages with the following limitations:

Single outgoing session (either BAM or RTS/CTS).
35 concurrent incoming sessions (any mixture of BAM and RTS/CTS).

Connectors

Power

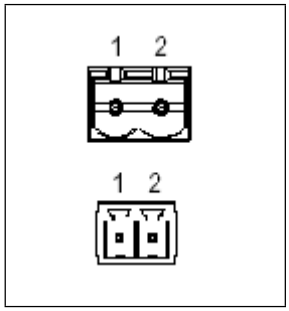


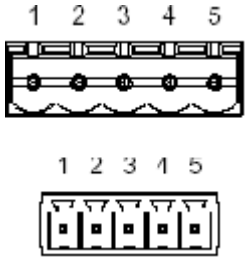
Figure 12-1 Power Connector

Pin	Connection
1	24 VDC +
2	24 VDC Common

Table 12-1 Power Connector Pin Definitions

Use Phoenix connector part number MSTB 2,5/2-ST-5,08 ABGY

J1939



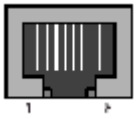
Pin	Signal
1	24 VDC Common
2	CAN Low
3	Shield
4	CAN High
5	24 VDC +

Table 12-2 J1939 Connector Pin Definitions

Use Phoenix connector part number MSTB 2,5/5-ST-5,08-ABGYAU.

Note: The 24VDC connections on the J1939 and Power connectors are physically connected internally. The module may be powered from either set of pins.

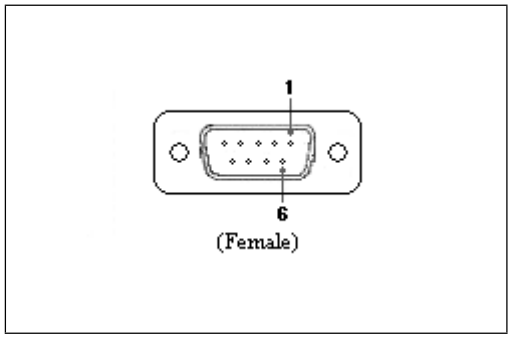
Ethernet RJ45



Pin	Signal
1	TD+
2	TD-
3	RD+
4	Termination
5	Termination
6	RD-
7	Termination
8	Termination

Table 12-3 RJ45 Pinout

Configuration RS-232 9 Pin D-Subminiature



Pin	Signal
1	NC
2	Receive
3	Transmit
4	NC
5	Signal Ground
6	NC
7	NC
8	NC
9	NC

Table 12-4 RS232 9 Pin

Support

Technical Product Assistance

If you require BridgeWay product technical support by phone:

Call 248-549-1200
Dial 0 for the Operator
Ask for BridgeWay Support

If you require support by email:

Email: productsupport@pyramidsolutions.com
Subject: “AB7645 Support Request”
Provide a detailed explanation of your question or issue in the email text.

You can also obtain AB7645 files and information online at the following URL:
http://pyramidsolutions.com/support/network-connectivity-support/

Contact Information

Pyramid Solutions, Inc.
302000 Telegraph Road
Suite 440
Bingham Farms, Michigan 48025

Phone: 1-248-549-1200
Toll free: 1-888-PYRASOL
Fax: 1-248-549-1400
Website: www.pyramidsolutions.com