DNP3 Router

User Manual

A-DNP3R

Document No. D109-010
10/2019
Revision 1.26

aparian

CONTENTS

1. Preface 6
1.1. Introduction to the DNP3 Router 6
1.2. Features 6
1.3. Architecture 8
1.4. Additional Information 11
1.5. Support 11
2. Installation 13
2.1. Module Layout 13
2.2. Module Mounting 15
2.3. Power 16
2.4. RS232 Port 16
2.5. Ethernet Port 16
3. Setup 17
3.1. Install Configuration Software 17
3.2. Network Parameters 17
3.3. Creating a New Project 21
3.4. DNP3 parameters 23
3.5. Message Routing 34
3.5.1. Reactive Tag (Outstation) Mode 34
3.5.2. Scheduled Tag (Master) Mode 39
3.5.3. Unscheduled Mode 44
3.6. DNP3 Events 44
3.6.1. Reactive Mode (DNP3 Outstation) 44
3.6.2. Scheduled Mode (DNP3 Master) 47
3.7. Outstation Repeaters 49
3.8. Module Download 52
3.9. RSLogix 5000 Configuration 54
3.9.1. Studio 5000 Configuration (Version 20+) 54
3.9.2. RSLogix 5000 Configuration (Pre-Version 20) 58
4. Logix Operation 63
4.1. Message Routing 63

4.2. RSLogix 5000 assemblies 63
4.2.1. Input Assembly 64
4.2.2. Output Assembly 65
4.3. Unscheduled Messaging 65
4.3.1. Example 69
5. DNP3 Operation 71
5.1. General 71
5.2. Analog/Binary Output Commands 73
5.2.1. Receiving Output Commands 75
5.2.2. Sending Output Commands 75
5.2.3. Control Relay Output Block (CROB) Parameters 76
5.3. Counter Freeze Commands 77
5.4. DNP3 Events – Unsolicited Responses 78
5.4.1. Outstation Event Configuration 78
5.4.2. Master Event Unloading 80
5.5. Report-By-Exception 82
5.6. Outstation Time Needed 83
6. Security 86
6.1. Key Updates 87
6.1.1. Local Key Update 87
6.1.2. Remote Key Update 90
7. Diagnostics 95
7.1. LEDs 95
7.2. Module Status Monitoring in Slate 96
7.3. DNP3 Packet Capture 105
7.4. Module Event Log 108
7.5. Web Server 109
8. Technical Specifications 110
8.1. Dimensions 110
8.2. Electrical 111
8.3. Ethernet 111
8.4. Serial Port 112
8.5. DNP3 112

8.6. DNP3 Secure Authentication....113
8.7. Certifications....114
A. Appendix – DNP3 reference....115
A.1. DNP3 Functions....115
A.2. DNP3 Groups....116
A.3. Supported DNP3 Group Variations....118
A.4. DNP3 Qualifier Code....119
A.5. DNP3 Event Status Flags....121
Index....123

Revision History

Revision	Date	Comment
1.0	29 May 2015	Initial document
1.1	26 June 2015	Add Scheduled mode Tag map status
1.2	14 July 2015	Add note that a maximum of 230 bytes can be transferred per mapped item when in Scheduled Tag Mode.
1.3	24 July 2015	Indication of serial data and stop bits supported
1.4	25 August 2015	Add UL Listed mark
1.5	30 September 2015	Add support for EtherNet/IP retry statistics and configuration
1.6	13 May 2016	Add ODVA Conformance mark
1.7	26 June 2016	Updated temperature range
1.8	11 August 2016	Added RoHS2 compliant to certifications
1.9	8 September 2016	Updated Reactive Mode to support DNP3 Events Support Group and Variations to DNP3 Conformance Level 3 Support for DNP3 Device Attributes
1.10	20 January 2017	Update new master event features Create sections for unsolicited operation
1.11	21 February 2017	Added support for unsolicited connection creation in Outstation mode. Added the ability to change the TCP connection timeouts in Master or Outstation mode.
1.12	10 March 2017	Added support for Logix triggered outstation Event Logging.
1.13	23 May 2017	Add support for two additional interface modes.

		Add RCM Conformance mark.
1.14	8 September 2017	Added support for Rockwell's Micro820 and Micro850 controllers.
1.15	15 September 2017	Added option in Slate configuration to link CSQ of unsolicited to that of aggressive mode.
1.16	5 October 2017	Added UL Class 1 Division 2
1.17	15 October 2017	Added remotely changing of DNP3 update key Added new parameters to security
1.18	23 November 2017	Added support for repeater functionality in Outstation
1.19	29 January 2018	Added support for read/write of 8-bit unsigned integers. Update unscheduled message instruction size.
1.20	14 February 2018	Updated supported DNP3 Group/Variation table
1.21	21 June 2018	Update Unscheduled mode supporting Secure Authentication
1.22	16 August 2018	Add CROB parameter definition
1.23	3 October 2018	Added 64bit alignment option for Master Added CIP message to force Outstation to set Time Needed DNP3 indicator
1.24	15 December 2018	Added TCP Retry and Timeout Added Max Application Segment Added Outstation Max Event Unload Count Added Outstation Max Events per group
1.25	15 February 2019	Added TCP ACK Wait option Reduced Max Application Segment to 4096 from 8192 Increased the Max Unload Count for events in Reactive Mode to 250
1.26	21 October 2019	Added parameter to allow user to select the qualifier to be used for Unsolicited Responses when in Reactive (Outstation mode).

1. PREFACE

1.1. INTRODUCTION TO THE DNP3 ROUTER

This manual describes the installation, operation, and diagnostics of the Aparian DNP3 Router. The DNP3 Router provides intelligent data routing between EtherNet/IP and DNP3 (serial, Ethernet UDP, or Ethernet TCP). The DNP3 Router allows the user to integrate DNP3 devices over a secure link into a Rockwell Logix platform (e.g. ControlLogix or CompactLogix) with minimal effort.

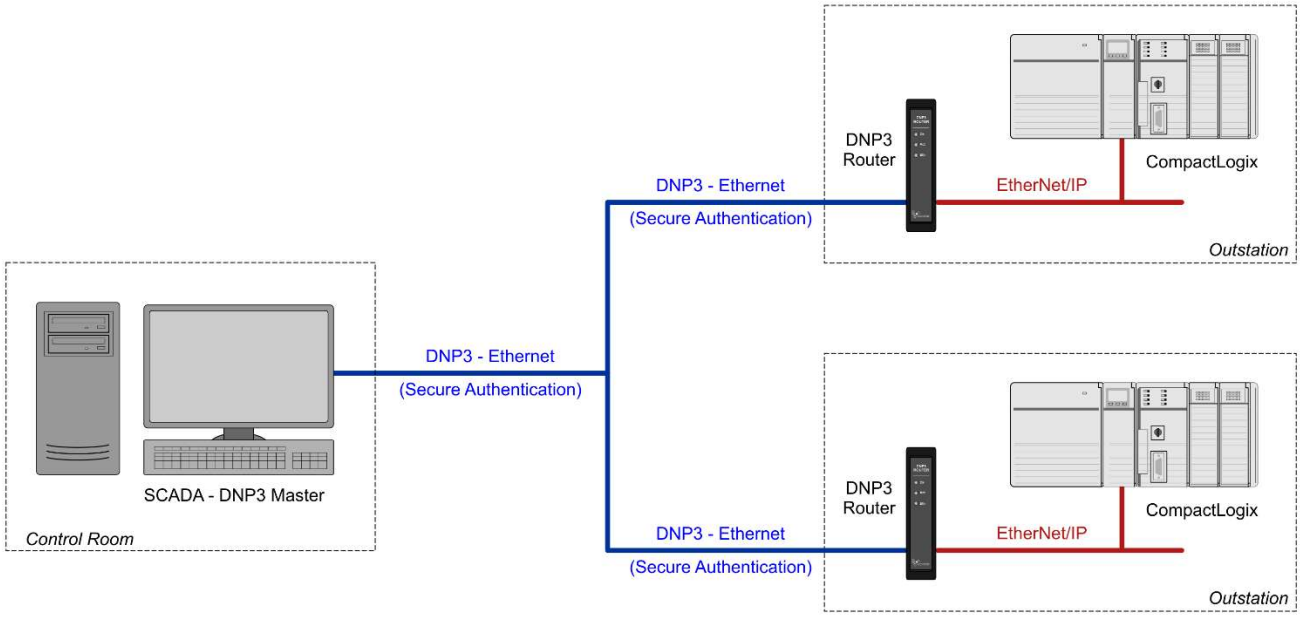


Figure 1.1. – Typical Setup

1.2. FEATURES

The DNP3 Router is able to transfer data from various DNP3 devices to a maximum of three Logix controllers. The module operates in one of three modes, simplifying the configuration for all applications.

Mode	Description	Message Initiator
Reactive Tag	The DNP3 Router will convert DNP3 messages to Logix controller tag reads or tag writes. (DNP3 Outstation)	Remote Device
Scheduled Tag	The DNP3 Router transfers data between a DNP3 device and a number of Logix tags, using a preconfigured scheduled. (DNP3 Master)	DNP3 Router

	No Logix or remote device configuration is required.	
Unscheduled	The DNP3 Router transfers messages received from a Logix Message Instruction. (DNP3 Master)	Logix (Msg)

Table 1.1. – Modes of Operation

The DNP3 Router is configured using the Aparian Slate application. This program can be downloaded from www.aparian.com free of charge. Slate offers various configuration methods, including a controller tag browser.

Hereafter the DNP3 Router will be referred to as the **module**.

The module can operate in both a Logix "owned" and standalone mode. With a Logix connection the input and output assemblies will provide additional diagnostics information which will be available in the Logix controller environment.

The DNP3 Router allows the user to integrate DNP3 devices into a Logix system with minimal effort. No copying or mapping of data in the Logix controller is required as the DNP3 Router writes directly into Logix tags.

The DNP3 Router also provides DNP3 Secure Authentication 5 which enables the user to connect DNP3 devices to a Logix platform securely. The module also provides a range of statistics and traffic analyser to help fault find any problems.

The DNP3 Router supports DNP3 on three ports which can be configured from the Slate environment; Serial, Ethernet TCP, or Ethernet UDP.

Previously complicated data mapping is made easy by precompiled UDTs which converts the various DNP3 data formats into sensible data in the Logix environment.

The DNP3 Router also supports repeater functionality in Outstation mode allowing the user to have infield configurable repeaters in radio network applications.

The module uses isolated RS232 for DNP3 serial communication providing better noise immunity. The RS232 port also uses a terminal block for convenient installation.

A built-in webserver provides detailed diagnostics of system configuration and operation, including the display of DNP3 operation and communication statistics, without the need for any additional software.

1.3. ARCHITECTURE

The figure below provides an example of the typical network setup in reactive mode.

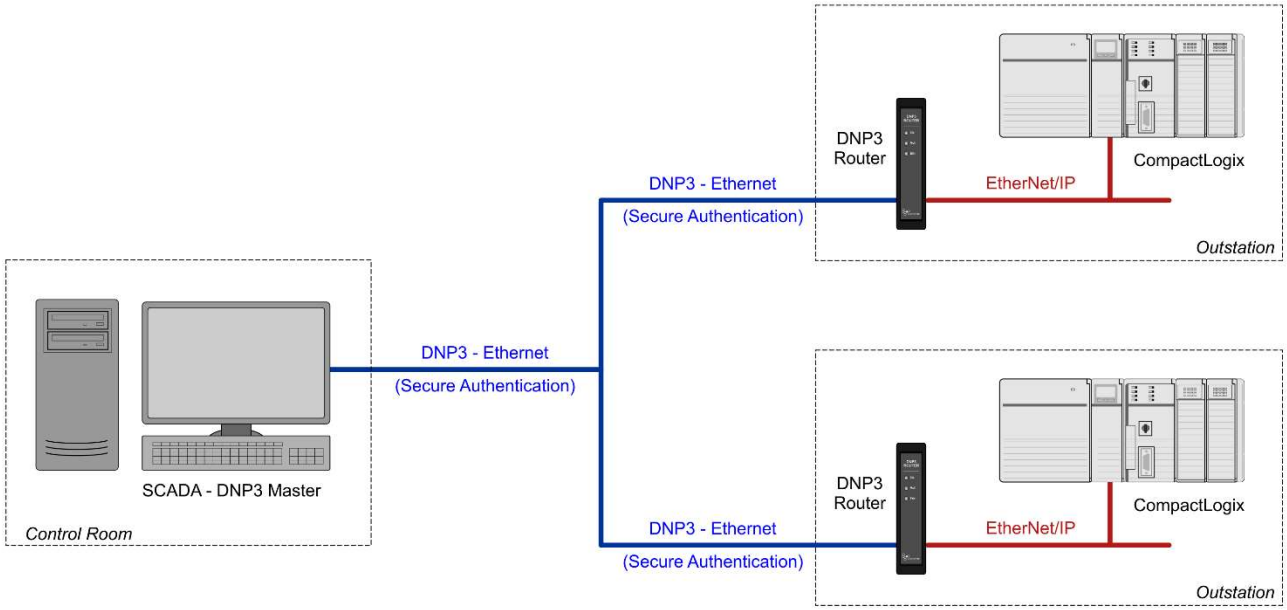


Figure 1.2. - Example of a typical network setup in reactive mode

By converting and redirecting serial DNP3 messages from legacy devices to EtherNet/IP, the module provides an interface for data exchange to Allen-Bradley ControlLogix and CompactLogix platforms. This enables user to replace legacy devices and systems with minimal effort and downtime.

The DNP3 Router allows a Logix platform to seamlessly integrate into a DNP3 network with Reactive Tag Mode. The module will route DNP3 message directly to Logix tags with no need for additional ladder code.

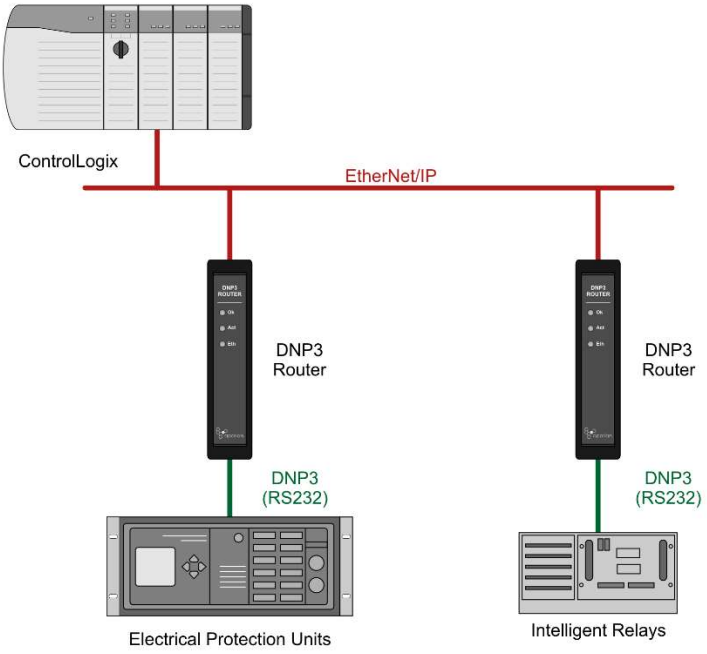


Figure 1.3. - Example of a typical network setup in scheduled/unscheduled mode

Systems that rely on a central ControlLogix communicating to a number of remote DNP3 devices, (e.g. Eletrical Protection Units or Intelligent Relays), may find the DNP3 Router useful when operating in Scheduled Tag Mode as shown in the image above. The module will exchange data between the DNP3 device and Logix platform at a configured interval without any need for additional coding or mapping.

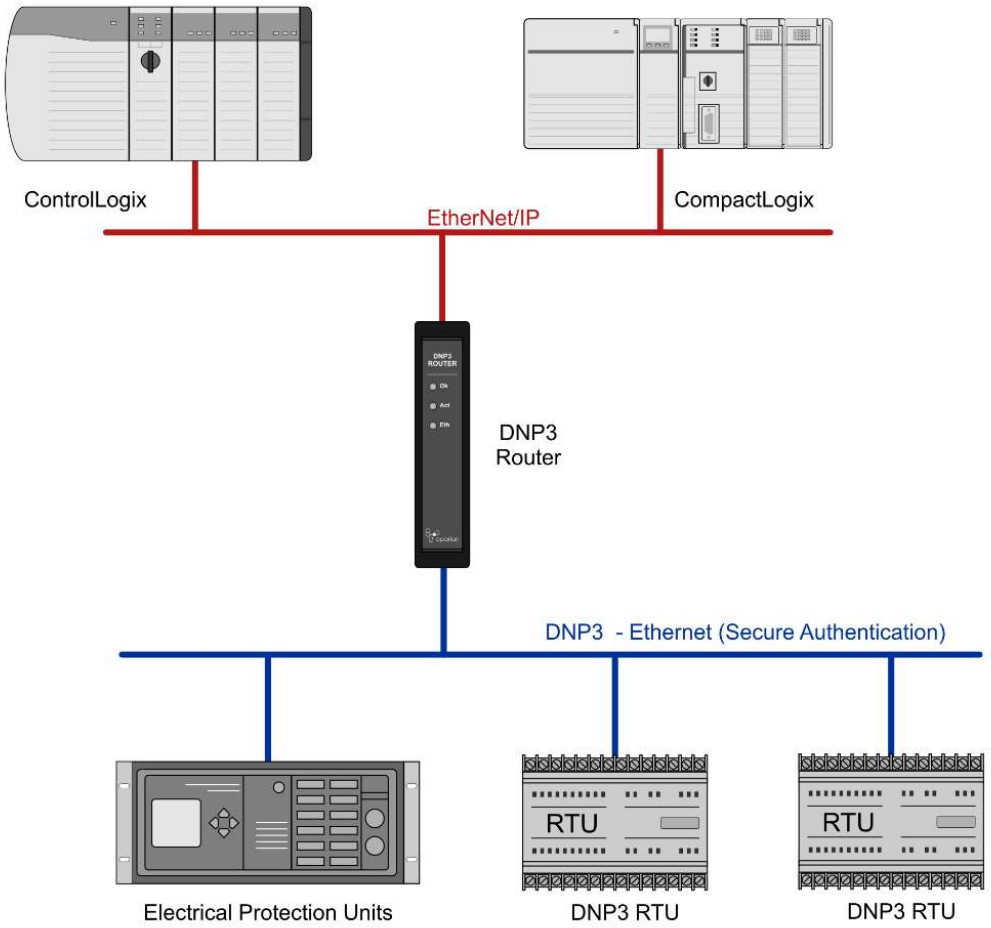


Figure 1.4. – Example of a typical network setup when using secure authentication

The DNP3 Router also provides the latest DNP3 Secure Authentication 5 standard which allows for secure authentication across the DNP3 network (Serial or Ethernet). The need for network security is essential to utility installations and operations to prevent unwanted attacks from outsiders. The DNP3 Router allows the user to configure the type and level of security needed with minimal effort.

The DNP3 Router also allows the user to implement repeaters into a radio network architecture when the DNP3 Master cannot see all the outstations (see below). The DNP3 Router in Outstation mode can be configured to repeater certain messages as well as route messages to other DNP3 Routers over Ethernet.

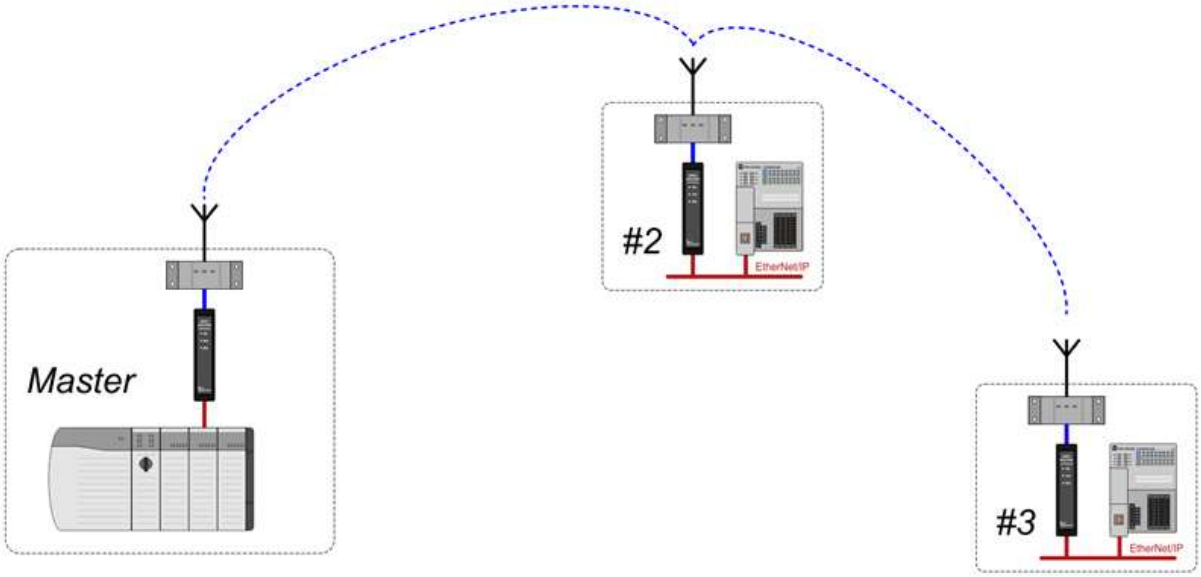


Figure 1.5. – Example of using the DNP3 Router as a repeater

1.4. ADDITIONAL INFORMATION

The following documents contain additional information that can assist the user with the module installation and operation.

Resource	Link
Slate Installation	http://www.aparian.com/software/slate
DNP3 Router User Manual DNP3 Router Datasheet Example Code & UDTs	http://www.aparian.com/products/dnp3router
Ethernet wiring standard	www.cisco.com/c/en/us/td/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig/Connectors.html
CIP Routing	The CIP Networks Library, Volume 1, Appendix C:Data Management
DNP3	http://www.dnp.org

Table 1.2. - Additional Information

1.5. SUPPORT

Technical support is provided via the Web (in the form of user manuals, FAQ, datasheets etc.) to assist with installation, operation, and diagnostics.

For additional support the user can use either of the following:

Resource	Link
Contact Us web link	www.aparian.com/contact-us
Support email	support@aparian.com

Table 1.3. – Support Details

2. INSTALLATION

2.1. MODULE LAYOUT

The module has three ports at the bottom of the enclosure as shown in the figure below. The ports are used for Ethernet, RS232 serial, and power. The power port uses a three-way connector which is used for the DC power supply positive and negative (or ground) voltage as well as the earth connection.

The RS232 port uses a four-way connector. This provides connection for the communication transmit (TX), receive (RX), and ground (GND) conductors. The fourth connection (earth) is used for shielding the cable in high noise environments.

The Ethernet cable must be wired according to industry standards which can be found in the additional information section of this document.

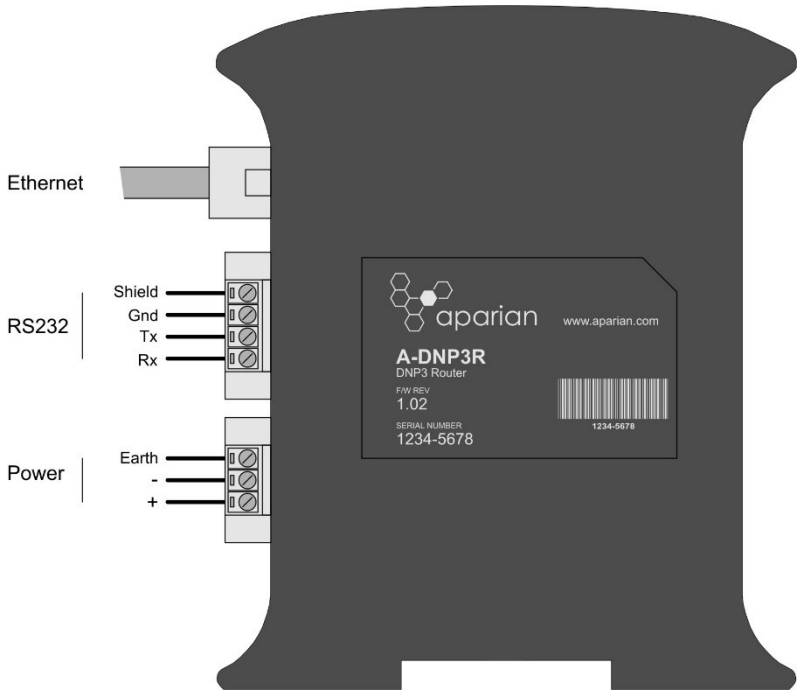


Figure 2.1. – DNP3 Router side and bottom view

The module provides three diagnostic LEDs as shown in the front view figure below. These LEDs are used to provide information regarding the module system operation, the Ethernet interface, and the auxiliary communication interface (RS232).



Figure 2.2. – DNP3 Router front and top view

The module provides four DIP switches at the top of the enclosure as shown in the top view figure above.

DIP Switch	Description
DIP Switch 1	Used to force the module into “Safe Mode”. When in “Safe Mode” the module will not load the application firmware and will wait for new firmware to be downloaded. This should only be used in the rare occasion when a firmware update was interrupted at a critical stage.
DIP Switch 2	This will force the module into DHCP mode which is useful when the user has forgotten the IP address of the module.
DIP Switch 3	Reserved
DIP Switch 4	Reserved

Table 2.1. - DIP Switch Settings

2.2. MODULE MOUNTING

The module provides a DIN rail clip to mount onto a 35mm DIN rail.

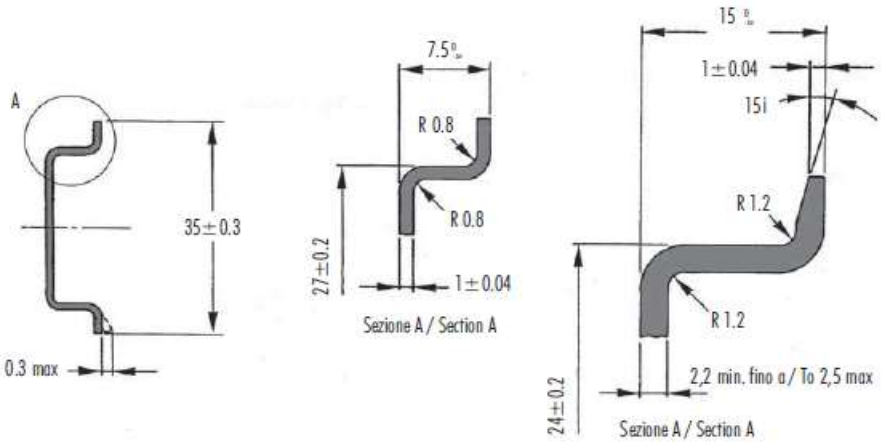


Figure 2.3 - DIN rail specification

The DIN rail clip is mounted on the bottom of the module at the back as shown in the figure below. Use a flat screw driver to pull the clip downward. This will enable the user to mount the module onto the DIN rail. Once the module is mounted onto the DIN rail the clip must be pushed upwards to lock the module onto the DIN rail.



Figure 2.4 - DIN rail mouting

2.3. POWER

A three way power connector is used to connect Power+, Power– (GND), and earth. The module requires an input voltage of 10 – 28Vdc. **Refer** to the technical specifications section in this document.

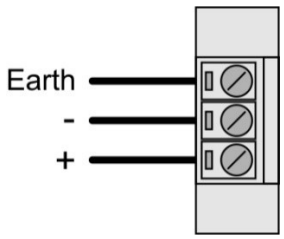


Figure 2.5 - Power connector

2.4. RS232 PORT

The four way RS232 connector is used to connect the transmit (TX), receive (RX), and GND conductors for serial communication. The shield terminal can be used for shielded cable in high noise environments.

NOTE: The shield of the RS232 port is internally connected to the power connector earth. Thus when using a shield it is important to connect the Earth terminal on the power connector to a clean earth. Failing to do this can lower the signal quality of the RS232 communication.

NOTE: When using a shielded cable, it is important that only one end of the shield is connected to earth to avoid current loops. It is recommended to connect the shield to the DNP3 Router module, and not to the other DNP3 device.

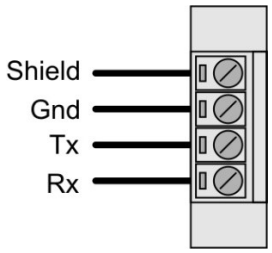


Figure 2.6 - RS232 connector

2.5. ETHERNET PORT

The Ethernet connector should be wired according to industry standards. **Refer** to the additional information section in this document for further details.

3. SETUP

3.1. INSTALL CONFIGURATION SOFTWARE

All the network setup and configuration of the module is achieved by means of the Aparian Slate device configuration environment. This software can be downloaded from http://www.aparian.com/software/slate.

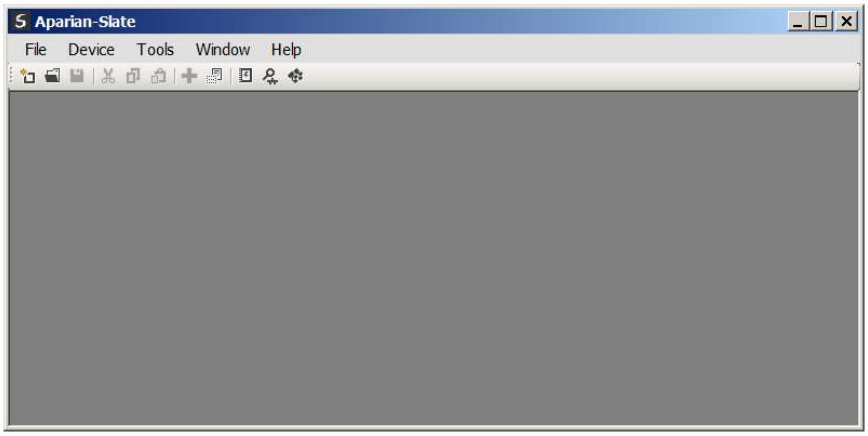


Figure 3.1. - Aparian Slate Environment

3.2. NETWORK PARAMETERS

The module will have DHCP (Dynamic Host Configuration Protocol) enabled as factory default. Thus a DHCP server must be used to provide the module with the required network parameters (IP address, subnet mask, etc.). There are a number of DHCP utilities available, however it is recommended that the DHCP server in Slate be used.

Within the Slate environment, the DHCP server can be found under the Tools menu.

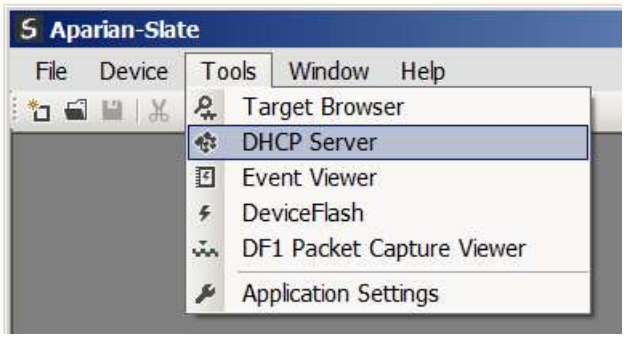


Figure 3.2. - Selecting DHCP Server

Once opened, the DHCP server will listen on all available network adapters for DHCP requests and display their corresponding MAC addresses.

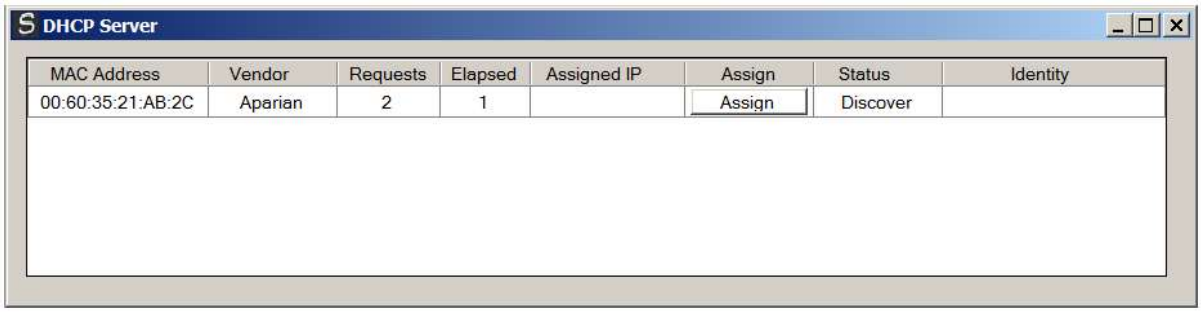


Figure 3.3. - DHCP Server

NOTE: If the DHCP requests are not displayed in the DHCP Server it may be due to the local PC's firewall. During installation the necessary firewall rules are automatically created for the Windows firewall. Another possibility is that another DHCP Server is operational on the network and it has assigned the IP address.

To assign an IP address, click on the corresponding "Assign" button. The IP Address Assignment window will open.

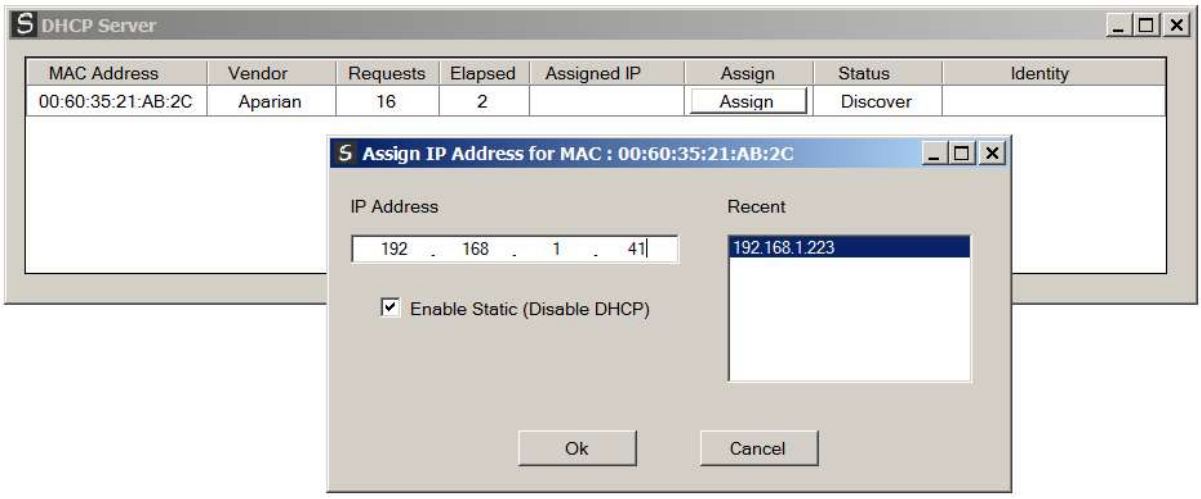


Figure 3.4. - Assigning IP Address

The required IP address can then be either entered, or a recently used IP address can be selected by clicking on an item in the Recent List.

If the "Enable Static" checkbox is checked, then the IP address will be set to static after the IP assignment, thereby disabling future DHCP requests.

Once the IP address window has been accepted, the DHCP server will automatically assign the IP address to the module and then read the Identity object Product name from the device.

The successful assignment of the IP address by the device is indicated by the green background of the associated row.

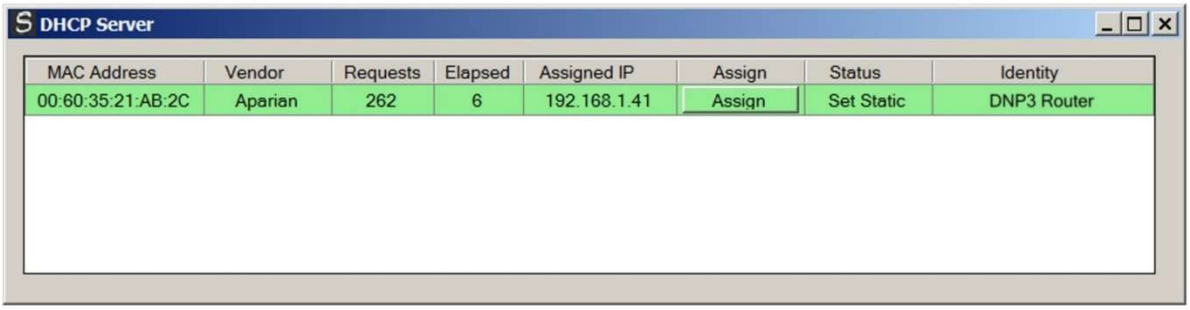


Figure 3.5. - Successful IP address assignment

It is possible to force the module back into DHCP mode by powering up the device with DIP switch 2 set to the On position.

A new IP address can then be assigned by repeating the previous steps.

NOTE: It is important to return DIP switch 2 back to Off position, to avoid the module returning to a DHCP mode after the power is cycled again.

If the module's DIP switch 2 is in the On position during the address assignment, the user will be warned by the following message.



Figure 3.6. - Force DHCP warning

In addition to the setting the IP address, a number of other network parameters can be set during the DHCP process. These settings can be viewed and edited in Slate's Application Settings, in the DHCP Server tab.

Once the DHCP process has been completed, the network settings can be set using the Ethernet Port Configuration via the Target Browser.

The Target Browser can be accessed under the Tools menu.

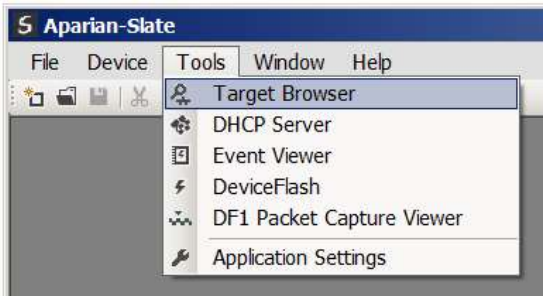


Figure 3.7. - Selecting the Target Browser

The Target Browser automatically scans the Ethernet network for EtherNet/IP devices.

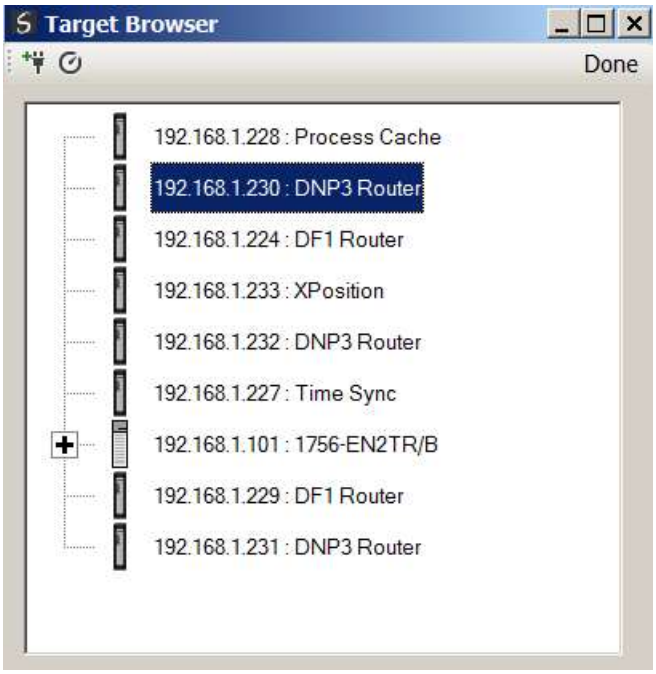


Figure 3.8. - Target Browser

Right-clicking on a device, reveals the context menu, including the Port Configuration option.

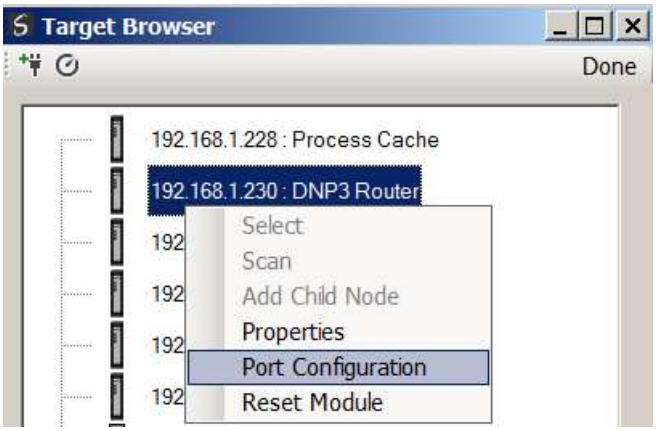


Figure 3.9. - Selecting Port Configuration

All the relevant Ethernet port configuration parameters can be modified using the Port Configuration window.

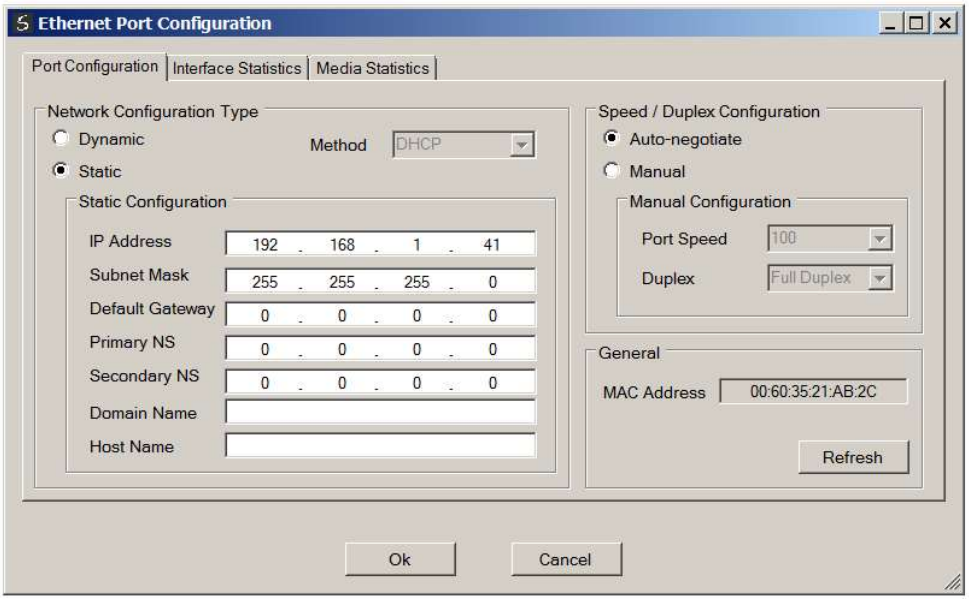


Figure 3.10. - Port Configuration

Alternatively, these parameters can be modified using Rockwell Automation's RSLinx software.

3.3. CREATING A NEW PROJECT

Before the user can configure the module, a new Slate project must be created. Under the File menu, select New.

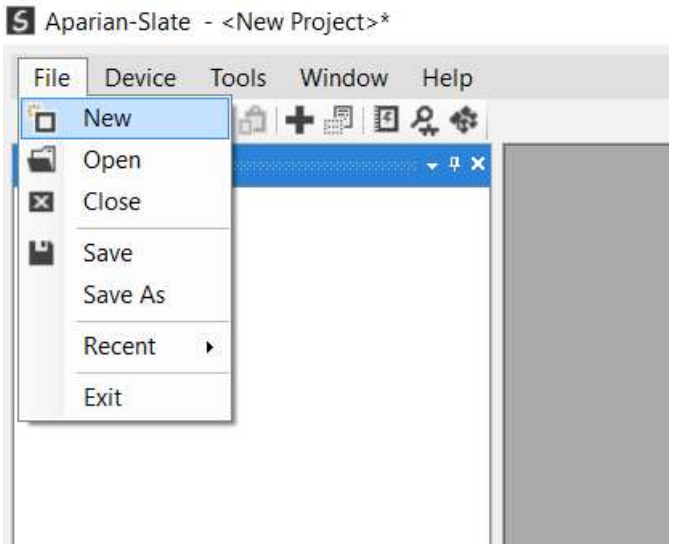


Figure 3.11. - Creating a new project

A Slate project will be created, showing the Project Explorer tree view. To save the project use the Save option under the File menu.

A new device can now be added by selecting Add under the Device menu.

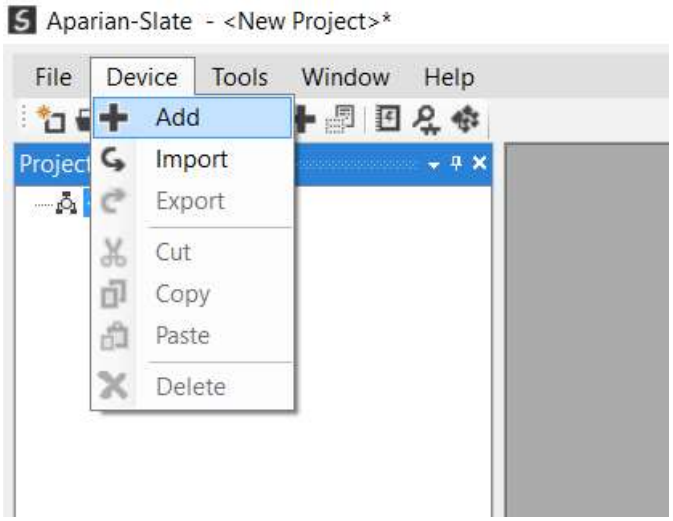


Figure 3.12. - Adding a new device

In the Add New Device window select the DNP3 Router, and click the Ok button.

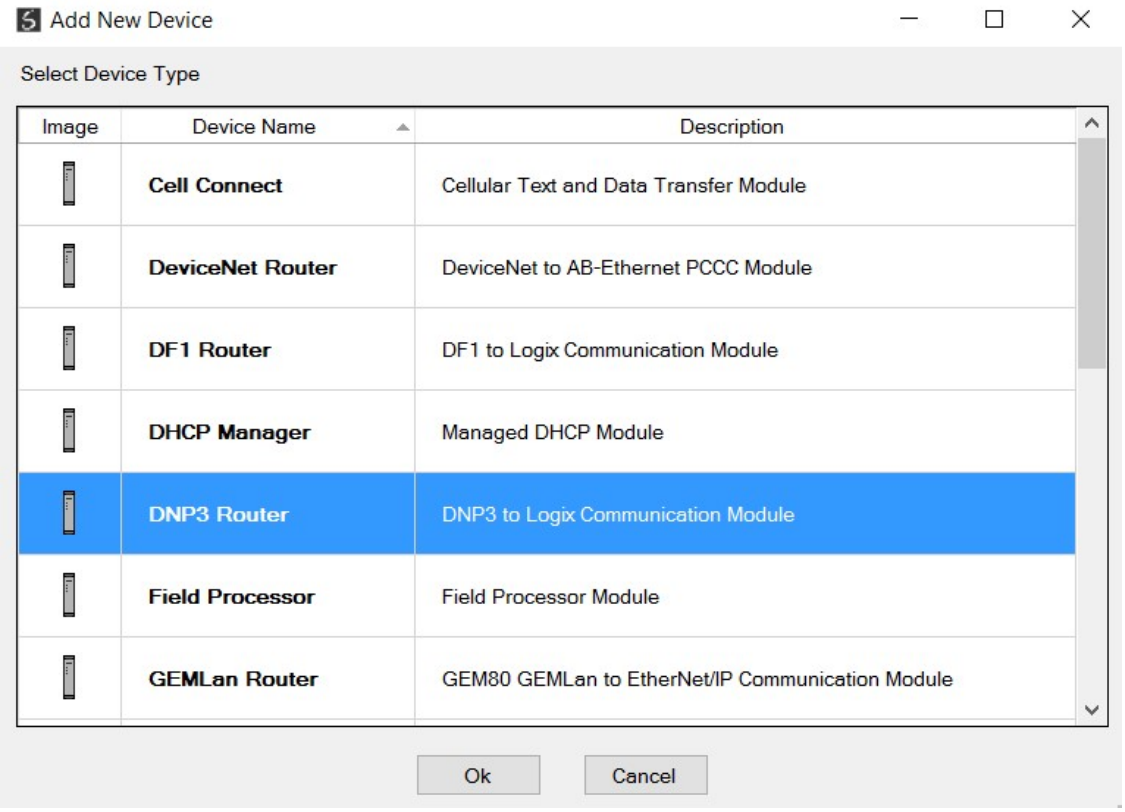


Figure 3.13 – Selecting a new DNP3 Router

The device will appear in the Project Explorer tree as shown below, and its configuration window opened.

The device configuration window can be reopened by either double clicking the module in the Project Explorer tree or right-clicking the module and selecting *Configuration*.

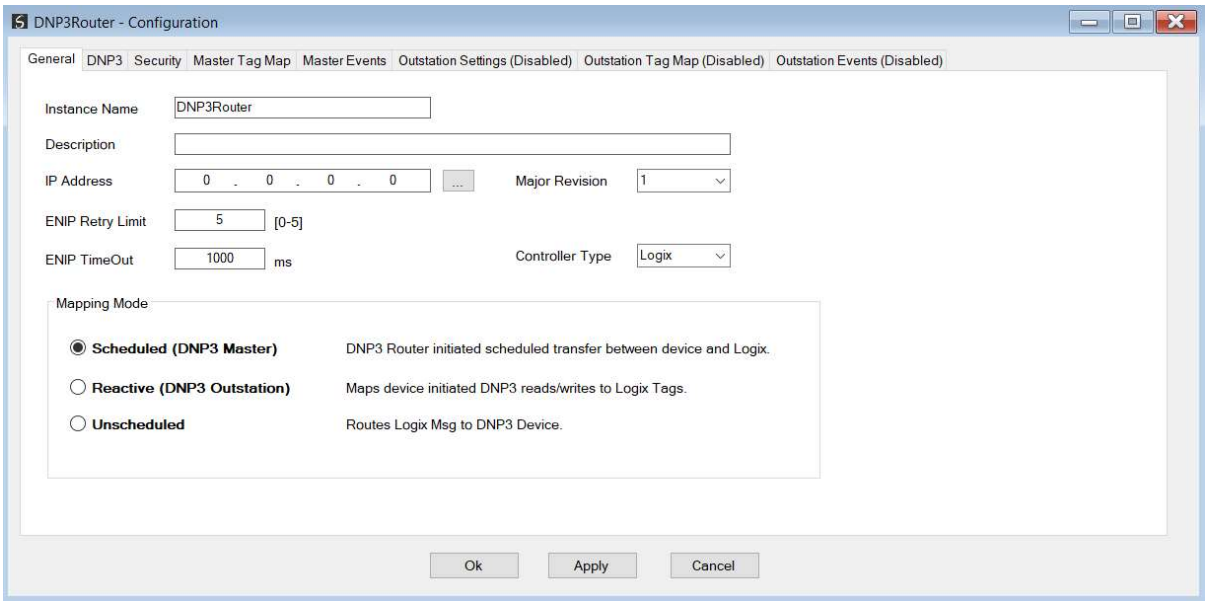


Figure 3.14. – DNP3 Router configuration

Refer to the additional information section in this document for Slate's installation and operation documentation.

3.4. DNP3 PARAMETERS

The DNP3 parameters will be configured by Slate. **Refer** to the additional information section for documentation and installation links for Aparian Slate. The DNP3 parameter configuration consists of a general configuration, security configuration as well as a serial configuration. When downloading this configuration into the module it will be saved in non-volatile memory that persists when the module is powered down.



NOTE: When a firmware upgrade is performed, the module will clear all DNP3 configuration and routing maps.

The general configuration consists of the following parameters:

Parameter	Description
Instance Name	This parameter is a user defined name to identify between various DNP3 Routers.

Description	This parameter is used to provide a more detail description of the application for the module.
Major Revision	The major revision of the module
Mapping Mode	The mapping mode will determine how the DNP3 messages are routed. In Reactive Tag mode the module will automatically route the DNP3 message and function to the correct Logix tag. In this mode, the DNP3 Router will map the DNP3 request to the preconfigured tag. DNP3 communication in this mode is initiated by the remote DNP3 device. In Scheduled Tag mode, the DNP3 Router will initiate the exchange between the remote DNP3 device and Logix. Either by reading data from a DNP3 device and writing it into a preconfigured Logix tag or vice versa. DNP3 communication in this mode is initiated by the DNP3 Router. In Unscheduled mode the DNP3 Router routes Logix messages to the remote DNP3 device and returns the result. There is little configuration required in the DNP3 Router as the routing information is configured by Logix for each message transaction. DNP3 communication in this mode is initiated by Logix. Refer to the message routing section of the document for a details explanation of the routing operation.
ENIP Retry Limit	The amount of EtherNet/IP retries the module will make once no response was received from the Logix Controller.
ENIP Timeout	The time in milliseconds after which a retry is sent. Once the first retry is sent the next retry will be sent after the same amount of time. This will repeat until the ENIP Retry Limit is reached.
Controller Type	The DNP3 Router can communicate to either a Rockwell Automation Logix based controller or a Rockwell Automation Micro820/850 controller. The user can select either **Logix** or **Micro800** for the controller type. Refer to the Micro800 Application Note for further information regarding the setup and operation of the DNP3 Router with the Micro820/850 controllers.

Table 3.1 - General configuration parameters

The general configuration is shown in the figure below. The DNP3 general configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration*.

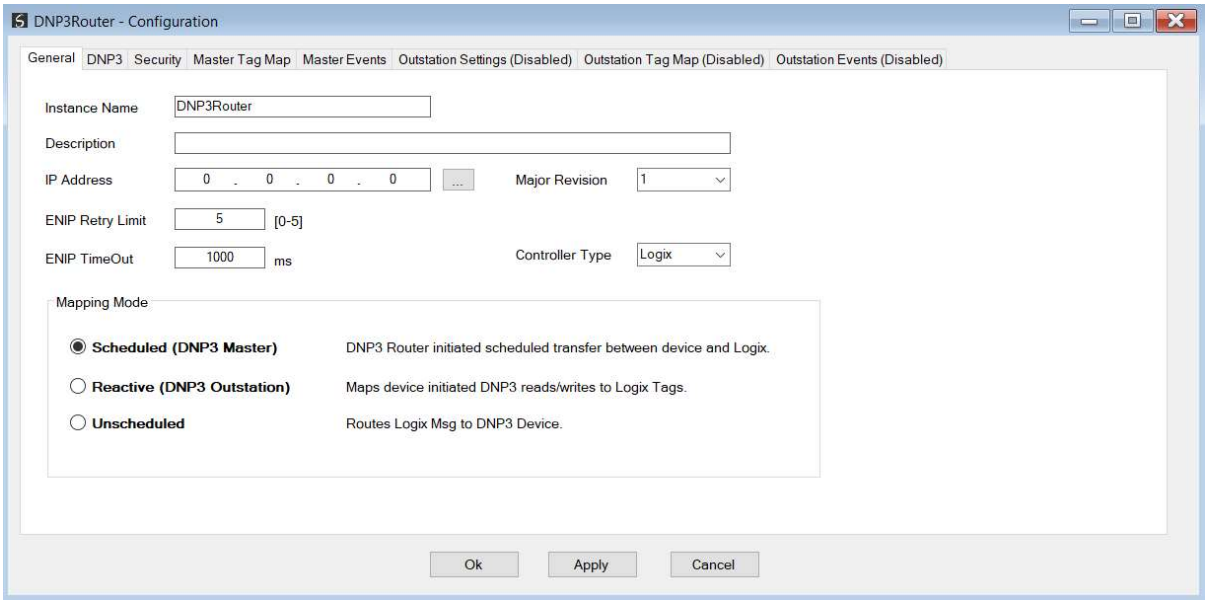


Figure 3.15. - General Configuration

The DNP3 configuration consists of the following parameters:

Parameter	Description
Protocol	The DNP3 Router can interface to the DNP3 device(s) on either serial, Ethernet TCP, or Ethernet UDP.
Retry Limit	The retry limit determines how many times the module must retry the message exchange before failing it.
Timeout	The timeout is used to determine the interval between retries when a message exchange has failed.
Reply Msg Wait	The reply message wait is the minimum delay before the DNP3 reply is transmitted to the DNP3 device.
Confirm Delay	In Scheduled Mode, this is the amount of time the execution of the next scheduled mapped item is delayed after a confirm message has been sent to an Outstation. This is useful in low bandwidth network where repeaters are used, or unsolicited responses are received.
Inter-Mapping Delay	In Scheduled Mode, this is the time delay between executing consecutive mapped items. This is useful in low bandwidth network where repeaters are used, or unsolicited responses are received.
Node Address	The node address is only configurable in Unscheduled mode. In all other modes, the node address is dynamically changed to suite the required mapping.
BAUD Rate	The BAUD rate will configure at what speed the data is sent across the RS232 serial network. The module provides the following speeds: 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200
Parity	The parity parameter will configure the parity of the module's RS232 serial port. The module allows for Even, Odd, or None parity setting.

Socket Timeout	When using DNP3 TCP the user has the ability to set the timeout of the TCP socket that will be used (in Master and Outstation mode). This will allow for unsolicited communication over the same TCP sockets from the DNP3 Master over an extended period of time. This value defaults to 120s.
Unsolicited Connection Creation	When using DNP3 TCP the DNP3 Router (in Outstation mode) has the ability to create a TCP connection to the DNP3 Master when unsolicited responses must be sent. This will allow for unsolicited communication without the need to worry about TCP socket timeouts. **NOTE:** Certain DNP3 Masters will not allow a DNP3 Outstation to create a TCP connection on the DNP3 Master.
Max Application Segment	The maximum application segment size that will be sent per response. For example, if the DNP3 response is 1000 bytes in size and the application segment max is 500, then the DNP3 Router will send an application segment of 500 bytes and request a confirm. Once the confirm has been received from the DNP3 Master the next 500 bytes of application data will be sent.
TCP Retry Timeout	If the DNP3 Router (with Protocol TCP) has sent a request or a response to another node and no TCP ACK has been received after the retry timeout, then the TCP layer will be sent again.
TCP Retry Limit	This parameter is the number of TCP retries that will be sent before the response is flagged as failed.
TCP ACK Wait	Enabling this parameter will force the DNP3 Router to buffer all outgoing TCP messages (in DNP3 Reactive mode – outstation) to be used for retrying when one of the packets was dropped by the DNP3 Master.

Table 3.2 – DNP3 configuration parameters

NOTE: In bad communication areas or applications, it is recommended to set the Max Application Segment size lower. This will result in a higher probability of packets successfully arriving at the destination address because of the packet confirmation.

NOTE: In bad communication areas or applications, the TCP retry (when using TCP protocol) can help with responses that are lost due to intermittent communication.

The DNP3 configuration is shown in the figure below. The DNP3 configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration.* Once in the configuration window, select the second tab at the top *DNP3*.

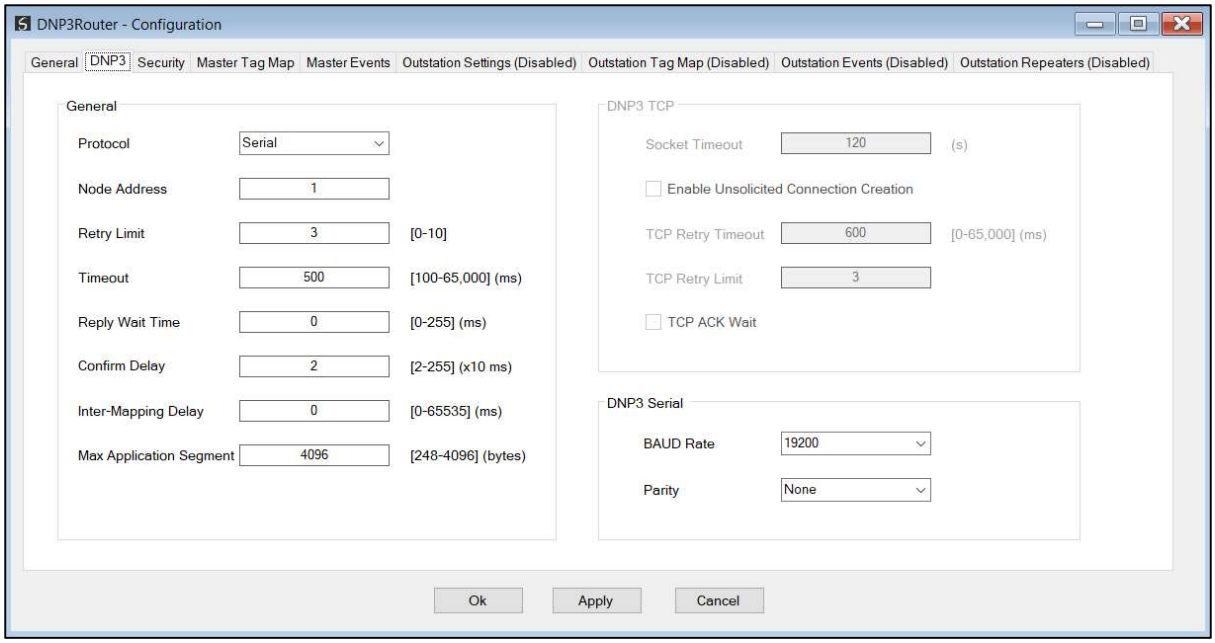


Figure 3.16. – DNP3 Configuration

NOTE: The DNP3 Router supports 8 data bits and 1 stop bit.

The Security configuration consists of the following parameters:

Parameter	Description
Enable Security	DNP3 Secure Authentication can be enabled or disabled. When enabled there will be no exchange of data (for critical functions).
Key Change Method	This setting determines the method by which security keys are exchanged between two devices. Currently the DNP3 Router only supports the Pre-Shared Key method. When using this method both devices need to have update keys entered by means outside the DNP3 protocol. **NOTE:** There are two options to be selected with the Key Change Method. **Pre-Shared Key** This is normal operation and the Update Keys will have to be changed locally for each DNP3 Router. **Pre-Shared Key – Allow Remote Update** This option allows the user to remotely change the update key over the DNP3 Network. See the Security section for more details regarding this.
MAC Algorithm	The MAC algorithm is used to encrypt the challenge data for secure authentication. DNP3 allows for various encryption standards in different formats to be used for secure authentication: HMAC SHA-1 encryption (4 octets – serial) – for legacy support HMAC SHA-1 encryption (8 octets – serial) HMAC SHA-1 encryption (10 octets – networked)

	HMAC SHA-256 encryption (8 octets – serial) HMAC SHA-256 encryption (16 octets – networked) AES-GMAC (12 octets)
Key Wrap Algorithm	DNP3 uses various keys for secure authentication. The keys that are used for data exchange and called the session keys and these keys may be updated frequently. To exchange the session keys between two DNP3 devices the update key (refer to the Secure Authentication section for further detail) is used to encrypt the data and session keys before exchanging it between parties. DNP3 allows for two standards to encrypt the session keys: AES-128 Key Wrap AES-256 Key Wrap
Aggressive Mode	To reduce the bandwidth used for secure authentication the user can select aggressive mode which allows the message initiator to anticipate and provide the required authentication in the request message. Thus from a network point of view there is a two message exchange for secure authentication compared to the normal four message exchange for secure authentication.
Link Unsolicited and Aggressive Mode CSQ	Ensure that the Challenge Sequence Numbers (CSQ) of unsolicited requests and Aggressive Mode requests are the same.
Secure Optional Critical Functions	When secure authentication is enabled there are various mandatory and optional application functions that must be authenticated before data can be exchanged. The optional functions can be selected in the box. Mandatory functions, e.g. Operate, are therefore not included in the options list.
Allow Unsecure Key Download	When this option is selected the user will be able to change the Update and Transfer Keys (unsecure) using a Logix MSG instruction. See the Security section for more details regarding this.
Session Key Change Interval	This is the time (in minutes) when the DNP3 Router, in Master mode, is forced to update the session keys.

Table 3.3 – Security configuration parameters



NOTE: For further information regarding the security settings refer to the Security section.

The security configuration is shown in the figure below. The DNP3 Security configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration.* Once in the configuration window, select the second tab at the top *Security*.



NOTE: The actual pre-shared key cannot be included in the configuration. It can only be written to the DNP3 Router when online via the Status window.

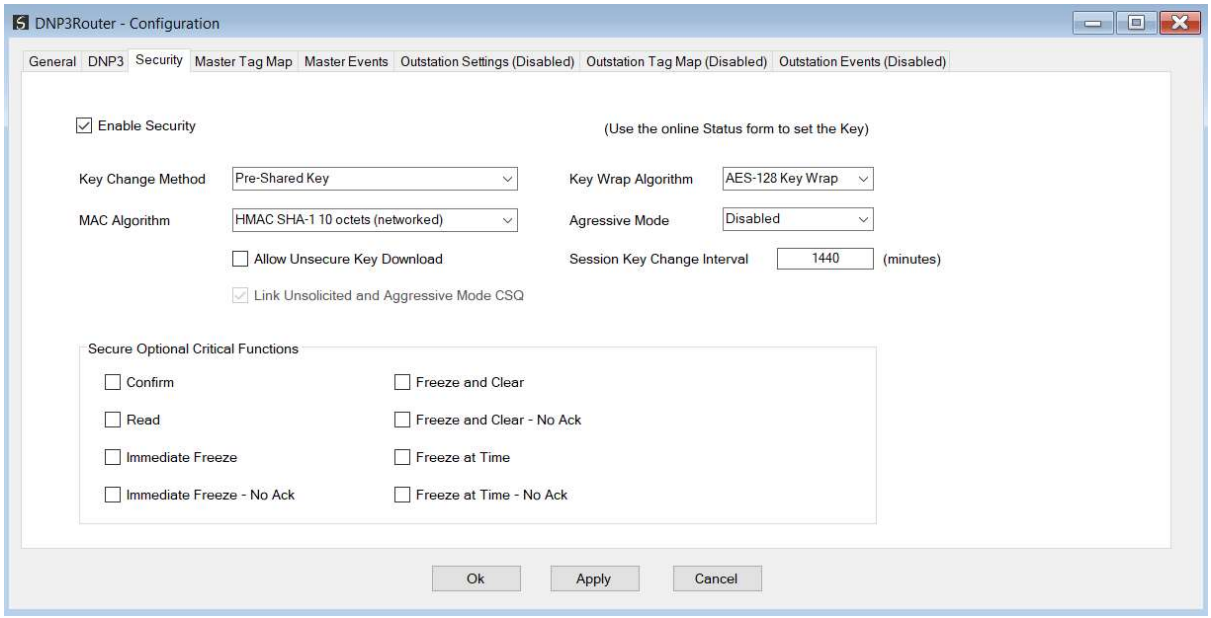


Figure 3.17 - Security configuration

The Master Events configuration consists of the following parameters:

Parameter	Description
Event Unload Mode	When the DNP3 Router is set in Scheduled (Master) Mode it can unload Events from DNP3 Outstations in one of two ways: **Class Mode** Events will be unloaded by class (e.g. class 1, 2, 3). Class mode supports both polled and unsolicited events. Selecting *Class Mode* for the Event Unload Mode will enable the Event Classes configuration on the setup form. **Group Mode** In this mode Events will be unloaded by group (e.g. Group 32 Analog Inputs Events). Each group will be individually polled for new events for each Outstation. Unsolicited events are not supported in this mode. Selecting *Group Mode* for the Event Unload Mode will enable the Event Groups configuration on the setup form
Logix Controller	When the DNP3 Router (in Master mode) receives events (by polling or by unsolicited reporting) it will be unloaded into a Logix Event buffer array. The Logix Controller parameter is the controller selected from the Master Tag Map controller list which the DNP3 Router will use to update the events received.
Logix Event Buffer Tag	When the DNP3 Router (in Master mode) receives events (by polling or by unsolicited reporting) it will be unloaded into a Logix Event buffer array. The Logix Event Buffer Tag parameter is the Logix Tag selected from the selected Logix Controller which the DNP3 Router will use to update the events received. **NOTE**: This tag type must be an array of the buffer event UDT. See section 5.4

Logix 64-bit Alignment	If **Logix v27+** is being used, then the user will need to select this option to ensure the events are unloaded correctly to Logix. Failing to do this will result in Events not being written to Logix.
Buffer Size	The size of the Events Array defined in the Logix controller.  **NOTE**: This value must not exceed the Logix controller tag array size. If this is the case the unloading of events to the Logix controller will not operate correctly.
Unload Count	This parameter is the maximum number of evens that will be uploaded per poll. This value is between 1 and 10.
Poll Rate	The rate (in seconds) at which the DNP3 Router polls for events from either classes (e.g. Class 1) or groups (e.g. Group 32 Analog Inputs).
Event Classes	When the Event Unload Mode is *Class Mode* then the user can select how each event Class must operate. The following options are available: **None** This group will not be queried or allowed to unload events with unsolicited responses. **Poll** The event class will be polled for events at the poll rate. **Unsolicited** The DNP3 Router will enable Unsolicited Responses for that specific class for each DNP3 Outstation. This will allow the DNP3 Outstation to send new events as they are generated rather than being polled (reducing network traffic).
Event Groups	The groups are polled for events at the poll rate selected.

Table 3.4 – Master Events configuration parameters

The Master Events configuration is shown in the figure below. The DNP3 Master Events configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration*.

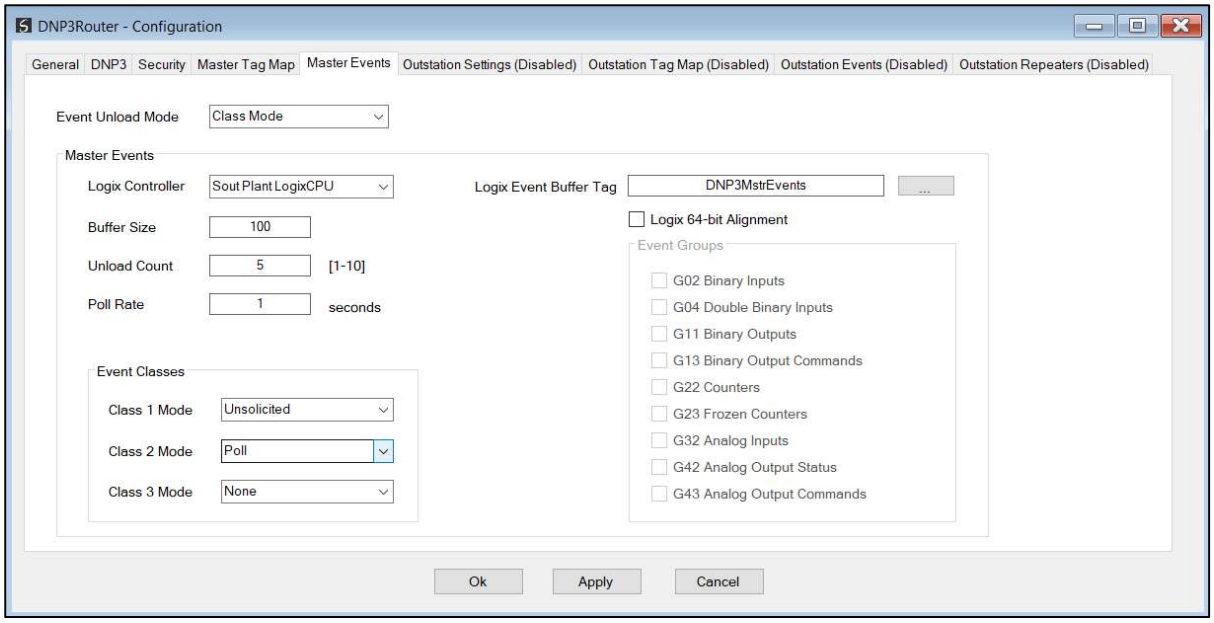


Figure 3.18 – Master Events configuration

The Outstation Settings Attributes configuration consists of the following parameters:

Parameter	Description
Enable Master Filter	The DNP3 Router (in Outstation Mode) can have a DNP3 Master allowed list. This can help reducing risks of unauthorized DNP3 Masters exchanging data with the DNP3 Outstation. It also allows the DNP3 Router to switch between DNP3 Masters (if a DNP3 Master were to go offline) when sending Unsolicited Responses. Should the DNP3 Master currently being used for unsolicited responses were to go offline, the DNP3 Router will go through the list to find the next DNP3 Master which can receive unsolicited responses. **NOTE**: The DNP3 Masters in the list are listed from highest priority to lowest (where the highest priority DNP3 Master is at the top). Should a DNP3 Master with a higher priority reconnect, then the DNP3 Router will redirect its Unsolicited responses to that DNP3 Master. The following criteria can be used to allow a DNP3 Master: **IP Address** This is IP Address of the allowed DNP3 Master. (Note that this field is only available with Ethernet communication e.g. TCP or UDP). **Node Address** The Node Address of the allowed master.
Location Name	This parameter is a name or code given where the device is installed by the user.
ID Code	This parameter is the code or number given to the device by the end user.
Device Name	This parameter is the name given to the device by the end user.

Product Name/Model	This parameter is the device manufacturer's product name and model
Manufacturer's Name	This parameter is the name of the device manufacturer.
Software Version	This attribute is the version code of the manufacturer's device software.
Hardware Version	This attribute is the version code of the manufacturer's device hardware.
Serial Number	This attribute is the serial number assigned by the device manufacturer.

Table 3.5 – Outstation Settings parameters

The Outstation Device Attributes can be setup to make the DNP3 Router look like any DNP3 Outstation. The Outstation Settings configuration is shown in the figure below. The DNP3 Outstation Settings configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration*.

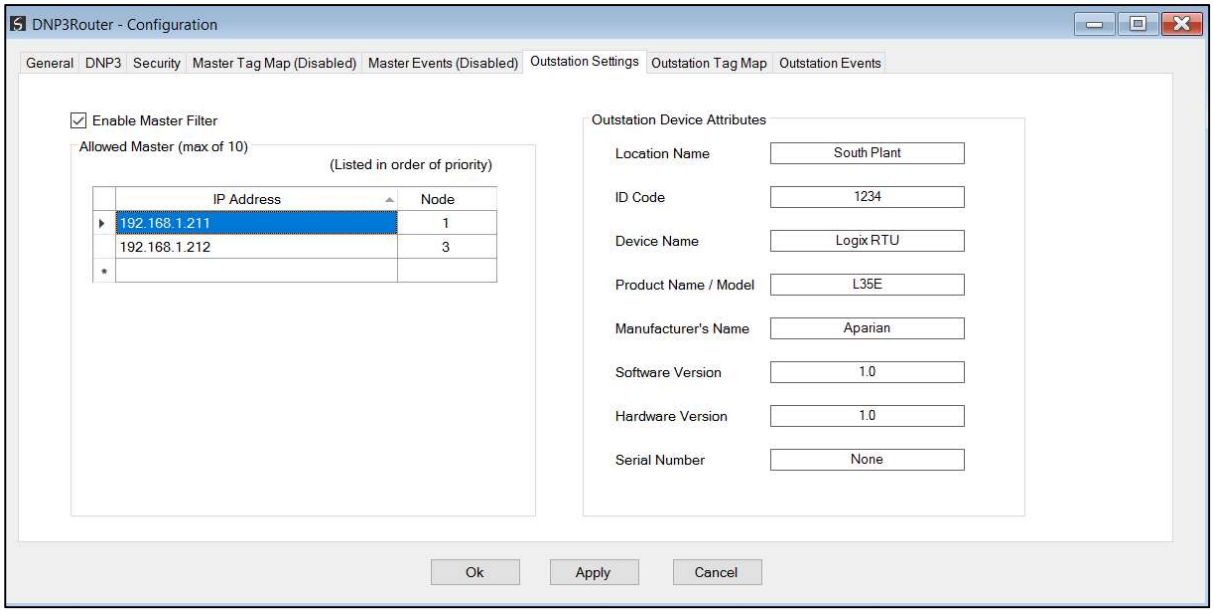


Figure 3.19. – Outstation Settings Configuration

The Outstation Events configuration consists of the following parameters:

Parameter	**Description**
Unsolicited Response Qualifier	This parameter allows the user to select which qualifier must be used when sending Unsolicited Responses. **Default** The qualifier will be 2-byte Prefix and 1-byte Object Count. **1 byte Prefix / 1 byte Count** The qualifier will be 1-byte Prefix and 1-byte Object Count. **2 byte Prefix / 1 byte Count** The qualifier will be 2-byte Prefix and 1-byte Object Count.

	2 byte Prefix / 2 byte Count The qualifier will be 2-byte Prefix and 2-byte Object Count.
Unsolicited Event Trigger	The Event triggers can be used by the DNP3 Router (in Outstation Mode) to limit the amount of individual unsolicited responses sent to the DNP3 Master. To reduce traffic the user can set limits, one of which must be reached, before an unsolicited response is sent. The follow criteria can be used: **Max Count** This is the number of events that must be buffered by the DNP3 Router (in Outstation Mode) before an unsolicited response is sent (when enabled by the DNP3 Master). The minimum is 1, implying every event received is sent immediately to the DNP3 Master. **Max Time** The maximum time parameter is used to send an unsolicited response when there have been events buffered for a preconfigured amount of time. If the Max Time is set to 10s then if there are events in the event buffer for longer than 10s the DNP3 Router will send the events currently in the event buffer.
Outstation Default Event Classes	Each DNP3 Group which has the ability to log events must be assigned an Event Class. The user can select either Class 1, 2, or 3. This will be used when events are being unloaded based on the DNP3 Event Class requested.
Max Unload Count	The maximum number of events that will be returned per event class per request.
Max Event / Group	The maximum number of events that will be logged for a specific DNP3 Group. This will default to 100,000.

Table 3.6 – Outstation Events parameters

The Outstation Events configuration is shown in the figure below. The DNP3 Outstation Events configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration*.

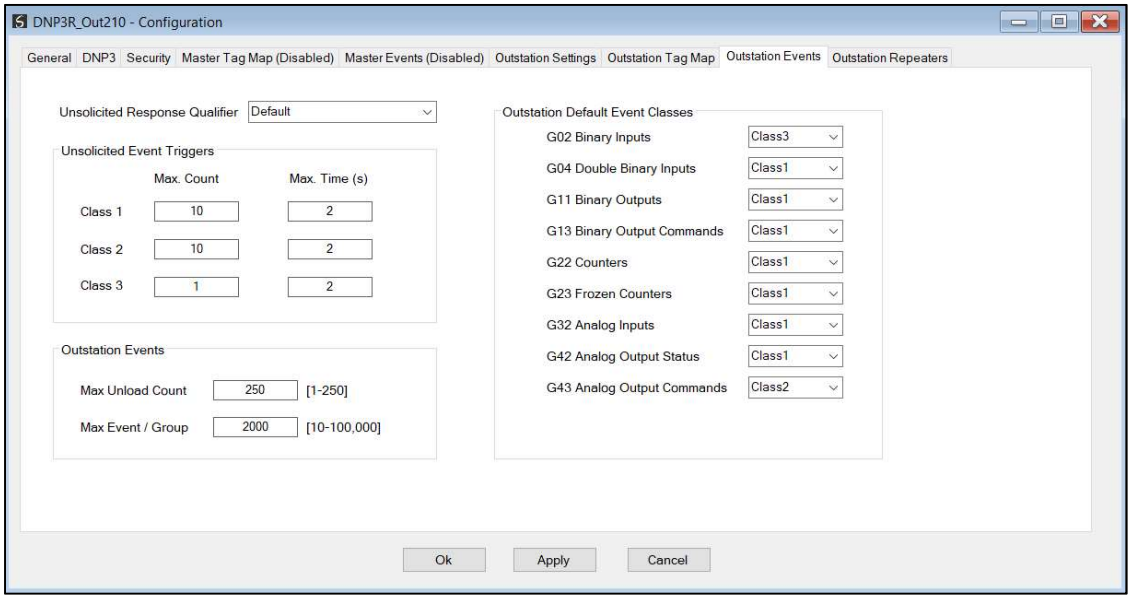


Figure 3.20. – Outstation Events Configuration

3.5. MESSAGE ROUTING

The module can be configured to route DNP3 data in one of three modes:

- Reactive Tag (Outstation) mode
- Schedule Tag (Master) mode
- Unscheduled mode

3.5.1. REACTIVE TAG (OUTSTATION) MODE

The Reactive Tag routing mode allows mapping of virtual Data Files to Logix tags across multiple controllers. In this mode the DNP3 Router will redirect a DNP3 message to a Logix controller at a preconfigured path.

Thus the routing of the DNP3 group, variation, and range to a Logix Controller tag is managed by the DNP3 Router. In the Reactive Tag mode the DNP3 Router can operate completely independently from the Logix controller by directly reading and writing to Logix tags.

NOTE: In Reactive Tag mode only Read, Write, Select, Operate, Direct-Operate, Direct-Operate-No-Response, and Secure Authentication functions will be supported.

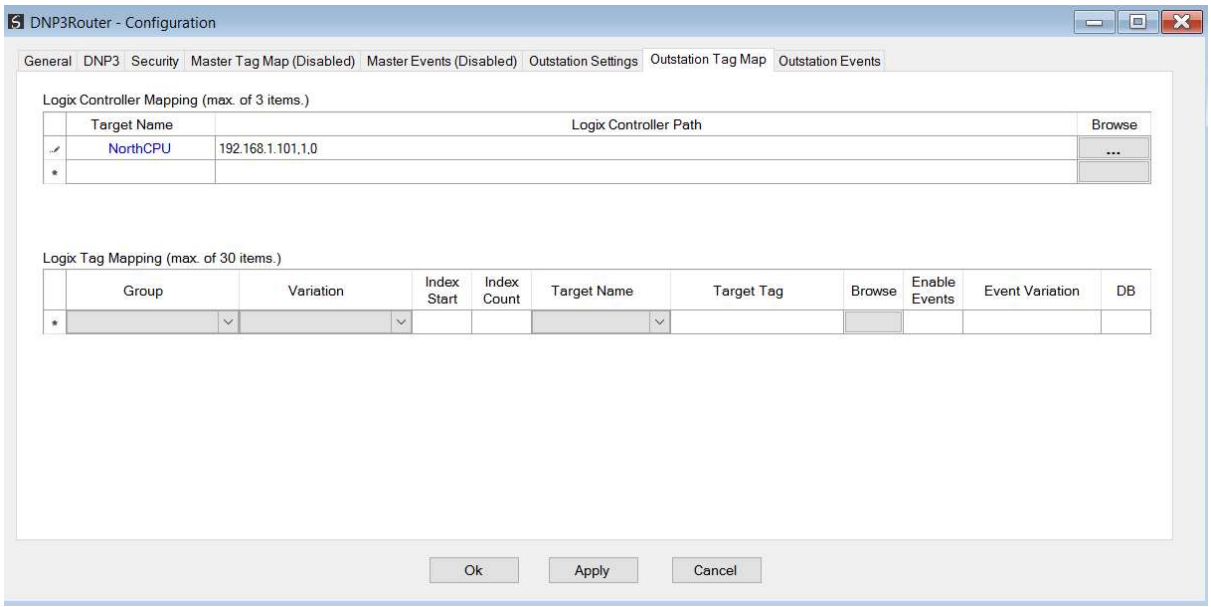


Figure 3.21. - Reactive Tag mode configuration

The Reactive Tag mode is configured in two steps. First the user must create a Target Name (CIP path to the destination Logix controller) which will be used to link the DNP3 group, variation, and range to the destination Logix tag.

The Logix controller paths can either be entered manually or the user can browse to them by clicking the Browse button. The Target Browser will open and automatically scan for all available EtherNet/IP devices.

If the Ethernet/IP module is a bridge module, it can be expanded by right-clicking on the module and selecting the Scan option.

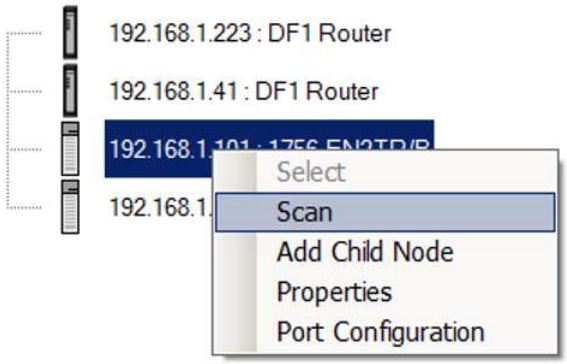


Figure 3.22. - Scanning node in the Target Browser

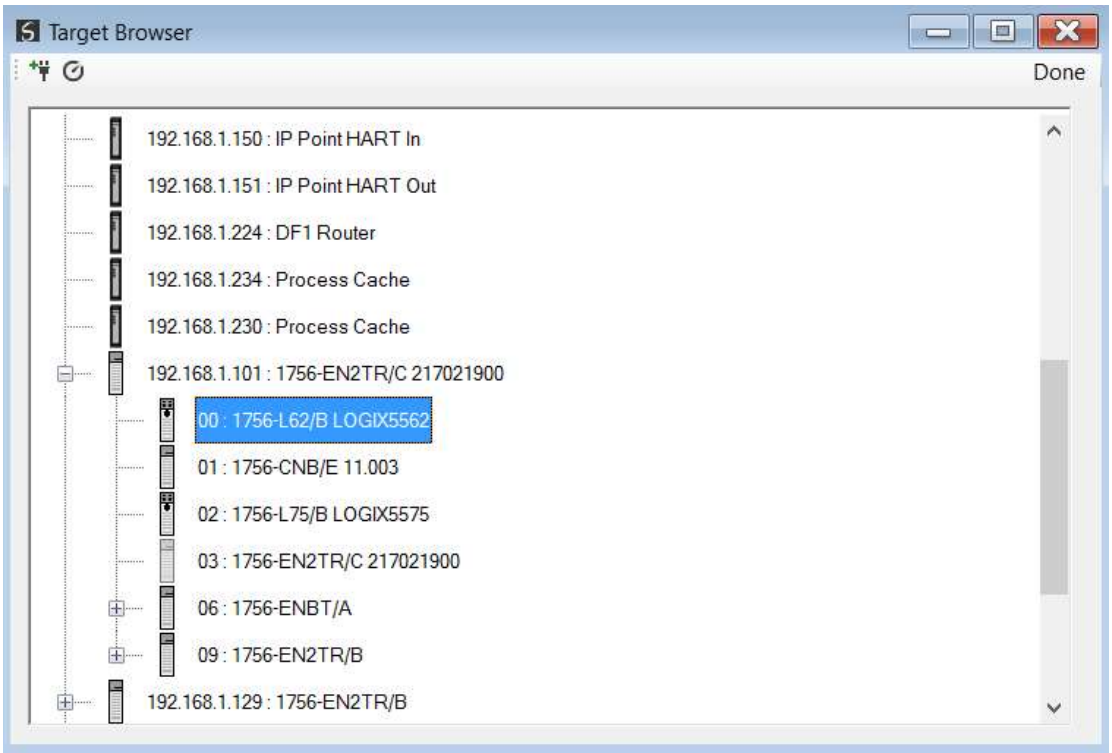


Figure 3.23. - Target Browser selection

The required Logix controller can then be chosen by selecting it and clicking the Ok button, or by double-clicking on the controller module.

A maximum number of 3 controller mapping entries can be added.

The second part of the Reactive Tag mode is to configure the link between a DNP3 group, variation, and range combination to a Logix tag. This will allow the DNP3 message initiator to effectively write to, or read from, a Logix tag using traditional DNP3 functions (e.g. Select/Operate).

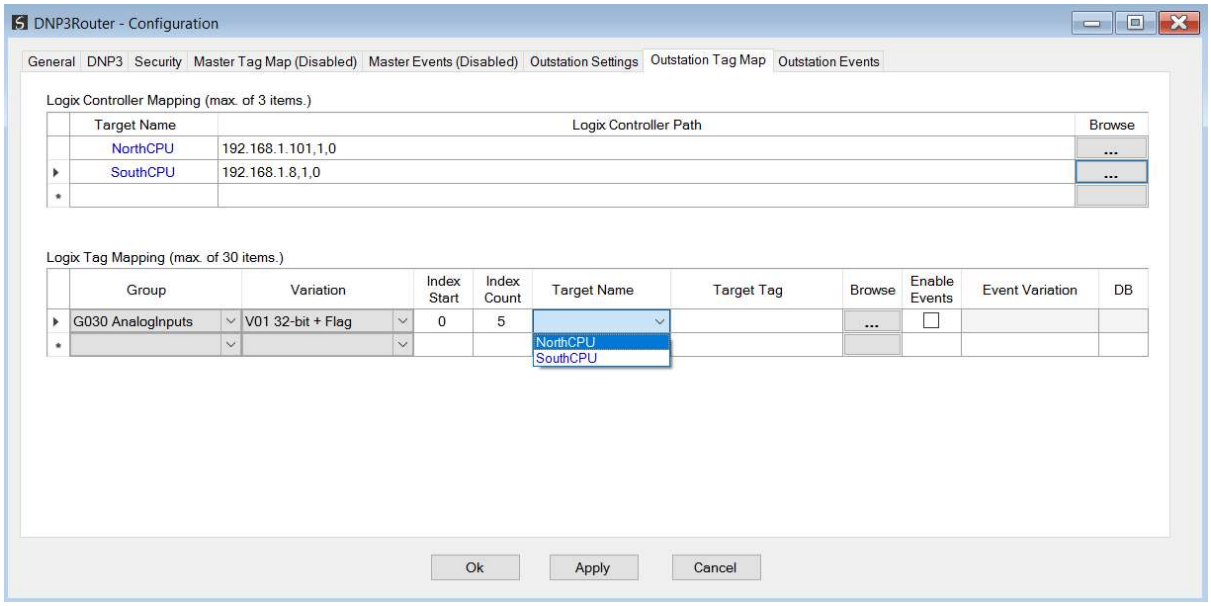


Figure 3.24. – Reactive Tag Mapping

DNP3 allows the user to select from a range of different formats (called variations) for each group. This will allow the user to access additional information for a specific group (e.g. timestamp, status, etc.). For this reason, the user must use or match the example UDTs provided (see the additional information section) to access the all data in the Logix controller.



NOTE: The example UDTs provided must be used to map the data in the Logix Controller when DNP3 variations are chosen which allow for additional information, that is, non-standard Logix atomic data types. If these UDTs are not used the user risks using the exchanged data incorrectly. Refer to the DNP3 Logix Mapping section for further information.

Next the range of data to be accessed must be specified. This is done by selecting a start index as well as the index count which is the number of elements that the user needs to access.

Below is an example of the target tag selection. The Target Tag can be either entered manually or selected using the Tag Browser in Slate. The Tag Browser requires the controller to be available on the network.

To browse to the tag, click on the Browse button. The Tag Browser will open and scan all the tags inside that controller. If the controller has been recently scanned in this Slate session, then a cached version of the tags will be displayed. A rescan of the tags can be triggered by selecting the Refresh button in the Tag Browser's toolbar.

Only tags of a relevant type will be enabled, guiding the user to select a suitable tag.

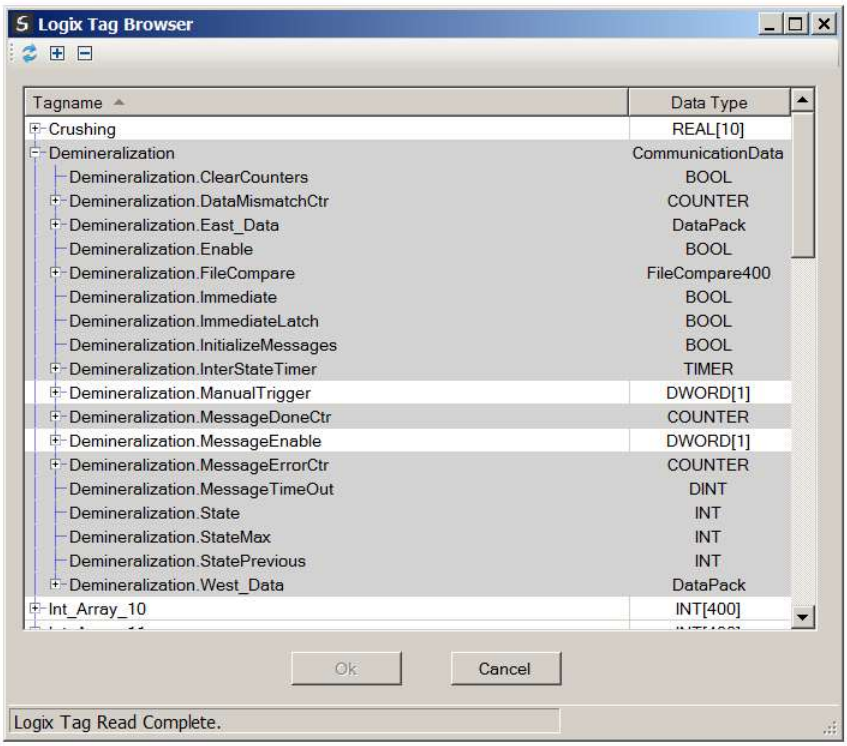


Figure 3.25. – Tag Browser tag selection

The figure below is an example of how DNP3 messages are routed to the Logix tags using the Reactive Tag Map mode.

NOTE: It is the user's responsibility to ensure that the Logix tag datatype/UDT and size matches that of the DNP3 message requests. Failing to do this can cause unexpected results and communication faults.
A list of recommended data types for each Group – Variant combination is listed in Appendix A.

Logix Controller Mapping (max. of 3 items.)

Target Name	Logix Controller Path	Browse
NorthCPU	192.168.1.101,1,0	...
SouthCPU	192.168.1.8,1,0	...

Logix Tag Mapping (max. of 20 items.)

Group	Variation	Index Start	Index Count	Target Name	Target Tag	Browse
G030 AnalogInputs	V03 32-bit No Flag	0	5	NorthCPU	PowerStatus	...
G001 BinaryInputs	V01 Packed	0	20	SouthCPU	RelayStatus	...

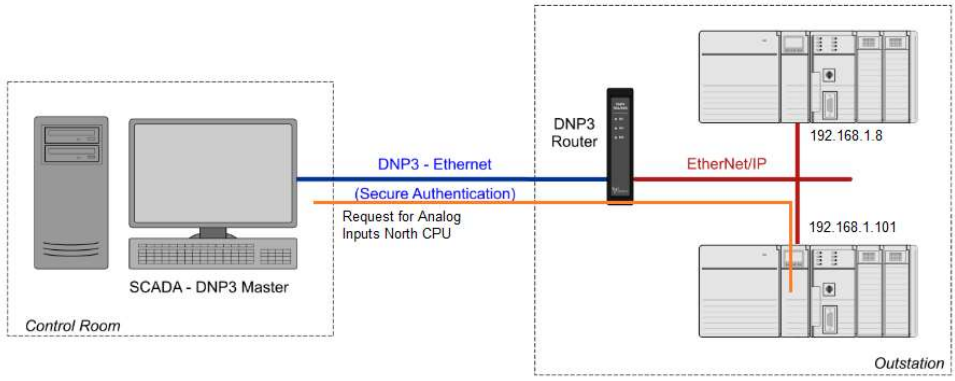


Figure 3.26 - Reactive Tag mode configuration in Slate (example route 1)

Logix Controller Mapping (max. of 3 items.)

Target Name	Logix Controller Path	Browse
NorthCPU	192.168.1.101,1,0	...
SouthCPU	192.168.1.8,1,0	...

Logix Tag Mapping (max. of 20 items.)

Group	Variation	Index Start	Index Count	Target Name	Target Tag	Browse
G030 AnalogInputs	V03 32-bit No Flag	0	5	NorthCPU	PowerStatus	...
G001 BinaryInputs	V01 Packed	0	20	SouthCPU	RelayStatus	...

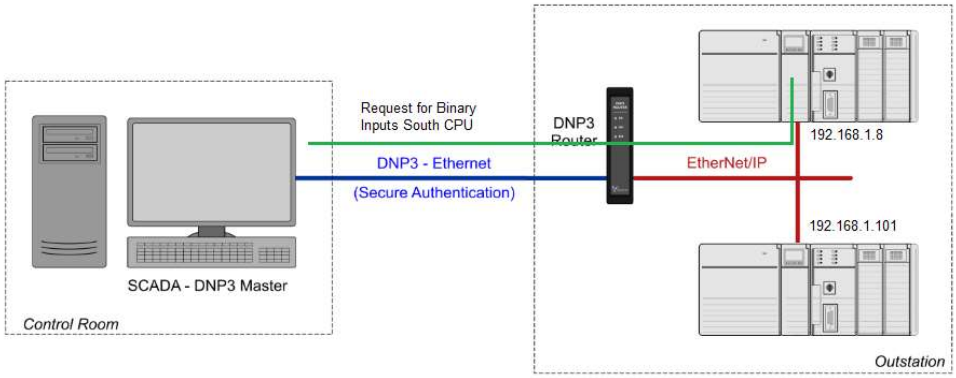


Figure 3.27 - Reactive Tag mode configuration in Slate (example route 2)

When using operate commands the user will always need a tag for the operate command as well as a tag for the status. For example, when using Binary Commands (switching a binary

value on or off) the Binary Control Group 12 will need to be used. This group is an operate-only group and does not contain or hold any value. The value received via the Command Group must then be copied to the Status Group 10 in the Logix controller (as shown in the diagram below). This is a read only group and is used by the DNP3 Master to monitor the status and actual value of the outputs. The same must be done for Analog Output Commands and Status Groups. See the example ***DNP3OutstationExample*** project.

Logix Tag Mapping (max. of 30 items.)

	Group	Variation	Index Start	Index Count	Target Name	Target Tag	Browse	Enable Events	Event Variation	DB
▸	G010 BinaryOutputs	V02 Output Status +...	0	10	NorthCPU	DNP3G10V02	...	☐		
	G012 BinaryOutput...	V01 CROB	0	10	NorthCPU	DNP3G12V01	...	☐		
	G040 AnalogOutput...	V03 Single Float + Fl...	0	10	NorthCPU	DNP3G40V03	...	☐		
	G041 AnalogOutputs	V03 Single Float	0	10	NorthCPU	DNP3G41V03	...	☐		
*										

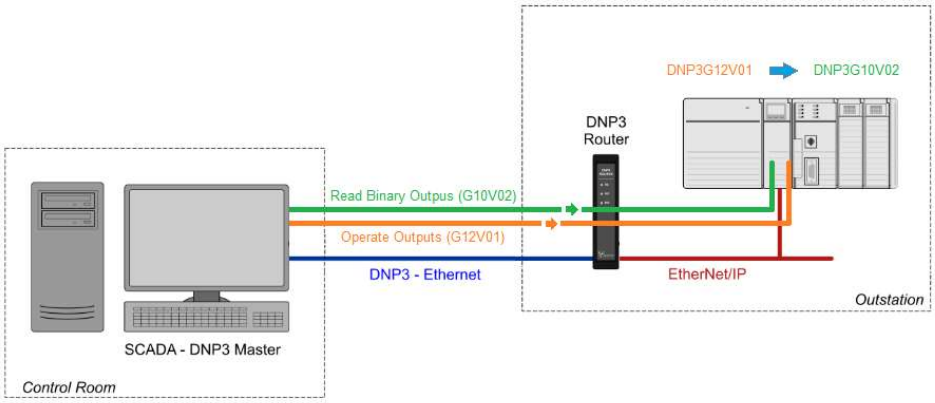


Figure 3.28 – DNP3 Commands configuration and operation

3.5.2. Scheduled Tag (Master) Mode

The Scheduled Tag routing mode transfers data between DNP3 devices and Logix controllers. Unlike the Reactive tag mode, the DNP3 Router when in the Scheduled Tag mode initiates the messaging.

In this mode the DNP3 Router transfers data between a Logix controller and DNP3 devices without any configuration or programming required in either the DNP3 device or the Logix controller. The data will be exchanged at a fixed interval which is configured in Slate.

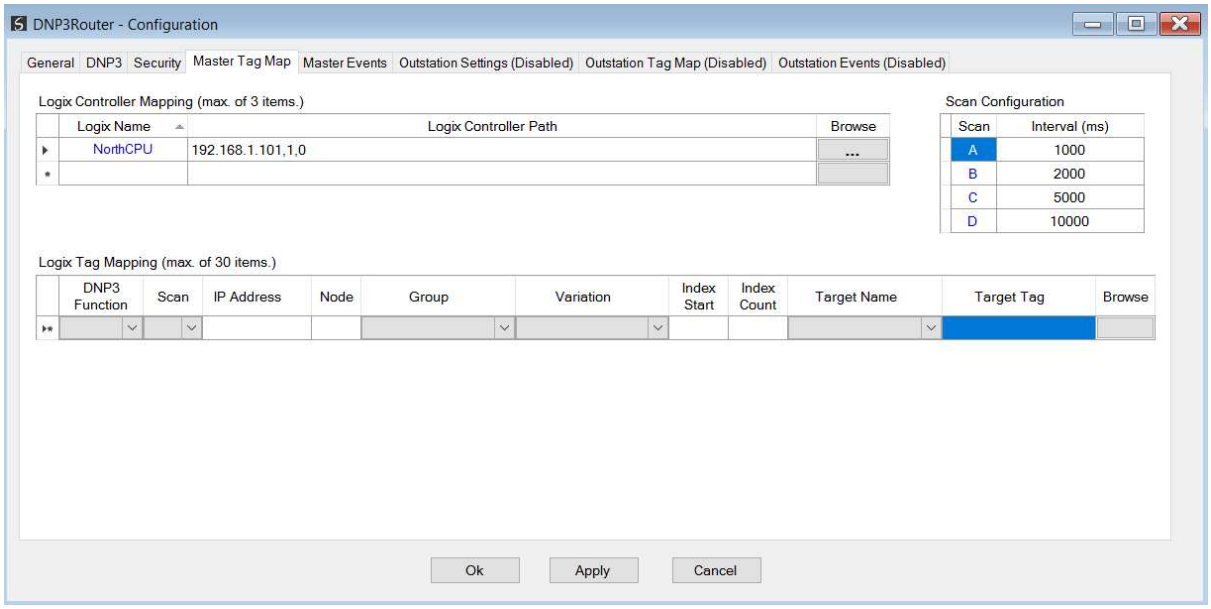


Figure 3.29. - Scheduled Tag configuration

The Schedule Tag mode is configured in three steps. First the user must create a Target Name (CIP path to the destination Logix controller) which will be used to link the DNP3 group, variation, and range to the destination Logix tag.

The Logix controller paths can either be entered manually or the user can browse to them by clicking the Browse button. The Target Browser will open and automatically scan for all available EtherNet/IP devices.

If the Ethernet/IP module is a bridge module, it can be expanded by right-clicking on the module and selecting the Scan option.

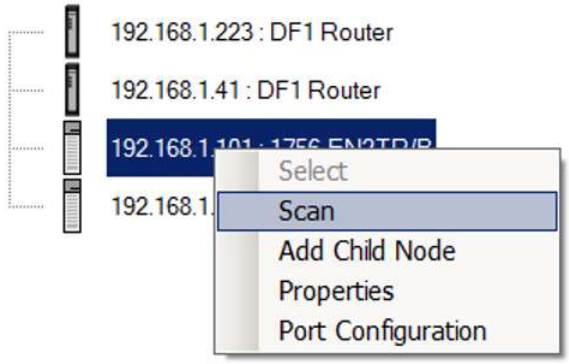


Figure 3.30. - Scanning node in the Target Browser

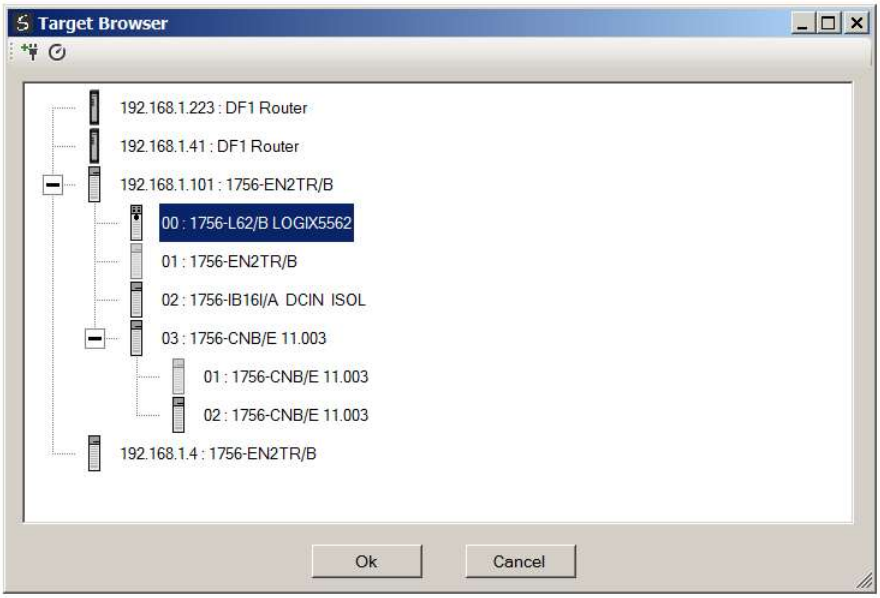


Figure 3.31. - Target Browser selection

The required Logix controller can then be chosen by selecting it and clicking the Ok button, or by double-clicking on the controller module.

A maximum number of 3 controller mapping entries can be added.

NOTE: A maximum of 230 bytes can be exchanged per mapped item when running in Scheduled Tag Mode. Thus if the user needs to exchange 130 x 32bit values from/to the Scheduled Tag DNP3 Router three mapped items will be required. The first and second mapped items can each transfer a maximum of 57 x 32bit values (228 bytes) whilst the third mapped item just needs to transfer the last 16 x 32bit values. This is shown in the figure below:

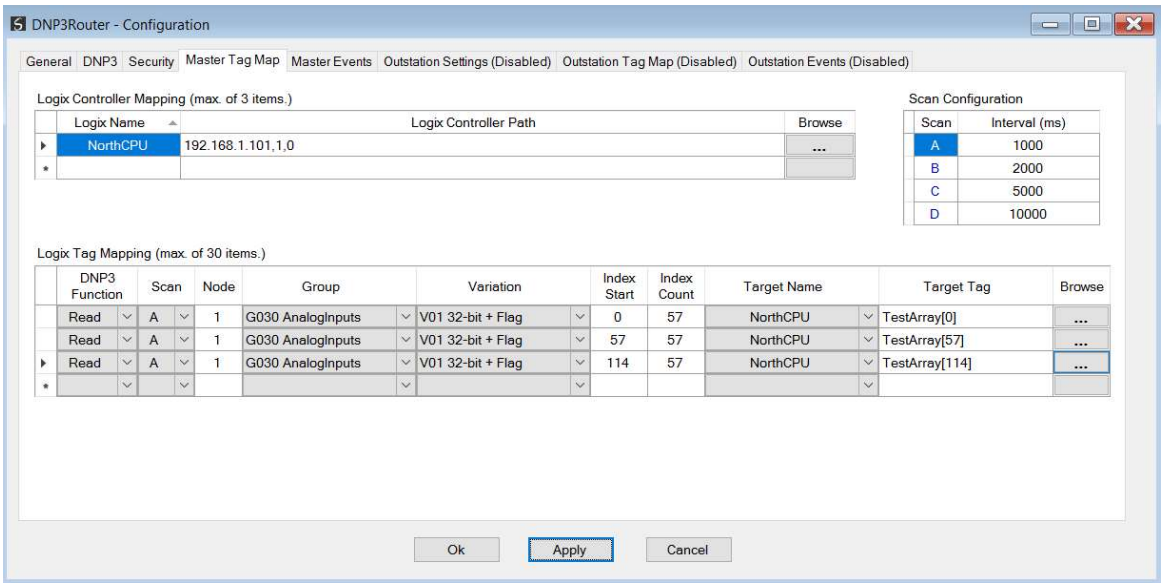


Figure 3.32. – Data exchange of arrays greater than 230 bytes

The second part of the Scheduled Tag mode setup is to configure the scan intervals. The scan intervals allow different data items to be transferred at different rates. There are 4 scan classes, viz. A, B, C and D. The intervals for each can be adjusted by entering the scan time in milliseconds. The interval must be between 200 milliseconds and 60 seconds.

The third part of the Scheduled Tag mode setup is to configure the link between a DNP3 group, variation, and range combination to a Logix tag, and the associated action and scan required.

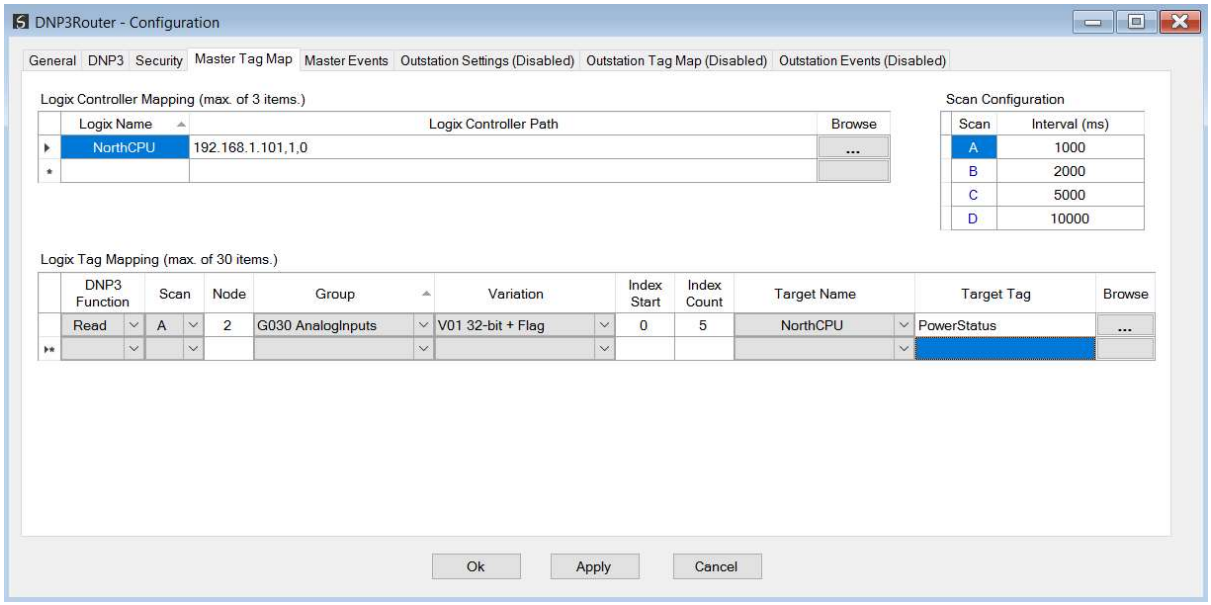


Figure 3.33. – Scheduled Tag Mapping

The Function field specifies whether the transaction will result in a read or write to the Logix controller tag.

NOTE: The DNP3 Router supports four different DNP3 functions in scheduled mode (Read, Select/Operate, Direct-Operate, and Direct-Operate-No-Response). The Read, Select/Operate, Direct-Operate, and Direct-Operate-No-Response functions will all translate into a Logix tag write.

The Scan field specifies at what rate the transaction will be executed. Select a scan class letter that matches the required interval. Care must be taken to select a realistic scan interval, taking into account the configured Baud rate and message size.

The IP address and Node is the remote device's IP address and node number.

NOTE: The IP address is only relevant if the protocol selected is either Ethernet TCP or Ethernet UDP. The Node address is relevant for both the previous mentioned Ethernet protocols as well as serial.

The DNP3 group and variation selected is that of the remote device. The user must ensure that the remote device supports both the group selected as well as the data format (variation). The range of data to be accessed from the remote device must also be specific. This is done by selecting a start index as well as the number of elements (index count).

One of the Target Names configured in the first step can be selected by means of the target Name combo box.

The Target Tag can be either entered manually or selected using the Tag Browser in Slate. The Tag Browser requires the controller to be available on the network.

To browse to the tag, click on the Browse button. The Tag Browser will open and scan all the tags inside that controller. If the controller has been recently scanned in this Slate session, then a cached version of the tags will be displayed. A rescan of the tags can be triggered by selecting the Refresh button in the Tag Browser's toolbar.

Only tags of a relevant type will be enabled, guiding the user to select a suitable tag.

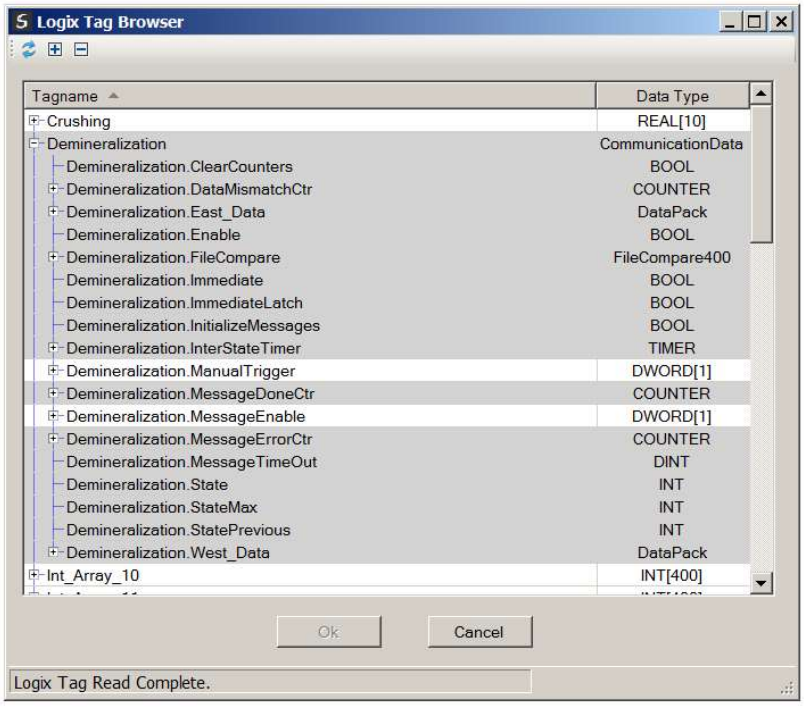


Figure 3.34. – Tag Browser tag selection

NOTE: It is the user's responsibility to ensure that the Logix tag datatype/UDT and size matches that of the DNP3 message requests. Failing to do this can cause unexpected results and communication faults.
A list of recommended data types for each Group – Variant combination is listed in Appendix A.

3.5.3. Unscheduled Mode

There is no additional configuration required when using the Unscheduled Mode. The configuration required for the DNP3 message is contained within the Message Block data, configured in Logix. Refer to the operation section for more information.

NOTE: In this mode the DNP3 Router does support Secure Authentication, but Aggressive mode is **NOT** supported. The DNP3 Master will also change session keys each time the request destination is different from the previous request.

NOTE: In this mode the DNP3 Router does **NOT** support unsolicited responses from DNP3 Outstations.

3.6. DNP3 EVENTS

3.6.1. Reactive Mode (DNP3 Outstation)

When in Reactive Mode the DNP3 Router provides the ability to log various DNP3 elements and commands. The following parameters must be configured to enable DNP3 Events.

Parameter	Description
Enable Events	This parameter will enable or disable the DNP3 Event function for a specific set of DNP3 elements (configured in the same line item)
Event Variation	For each DNP3 Group there are various combinations of DNP3 Event variations that can selected. These event variations will be used to log the default event format for when default event requests are used.
Deadband (DB)	The deadband is used to determine when to log an event for Counters, Analog Inputs, and Analog Outputs Status. If the value changes by more than the deadband an event is logged with the specific DNP3 element's value.

Table 3.7 – Event logging parameters for the DNP3 Router

NOTE: DNP3 elements will always be logged when any status bit changes (e.g. Online, Restart, etc.).

NOTE: When using Binary Groups (e.g. Binary Inputs, Double Binary Inputs, and Binary Output Status elements will be logged whenever there is a change in any value (status or process value).

NOTE: When using DNP3 Commands (e.g. Control Relay Output Block – CROB, or Analog Outputs) events will be logged when commands are received, thus the deadband field is not applicable.

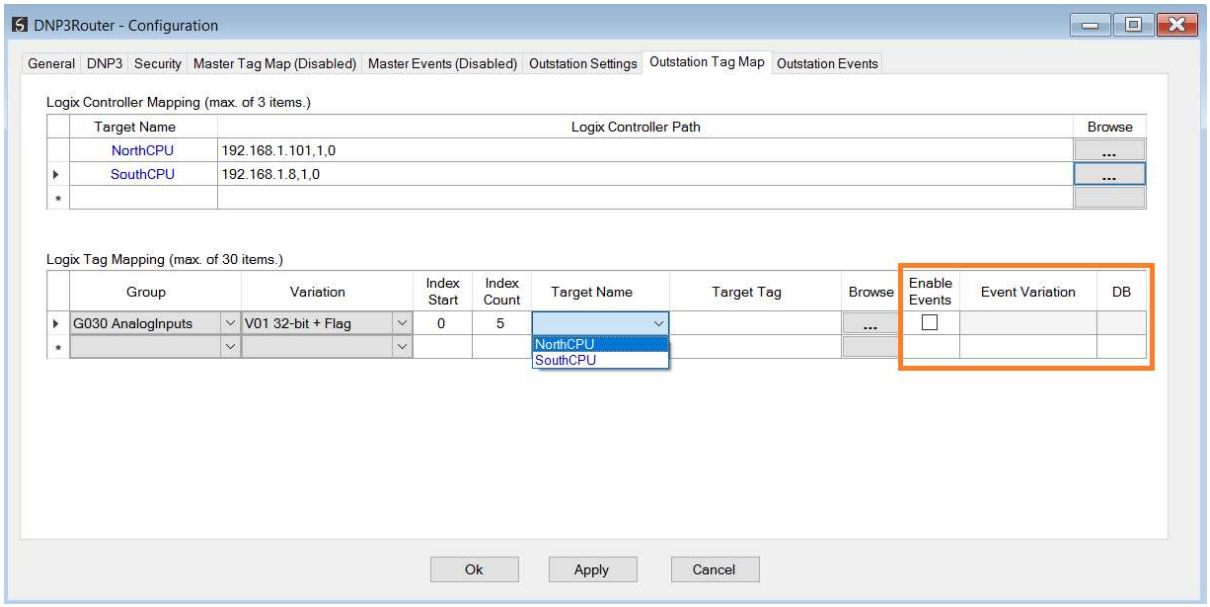


Figure 3.35. – DNP3 Event selection

Each mapped line item will be read every 10ms from the Logix controller. If a mapped line item is sufficiently large then the reading of all the elements in the mapped line item will be spread over multiple Logix controller reads.

In addition to the aforementioned Event trigger mechanism, it is also possible to **trigger events from Logix**. This allows the Logix application code to control when an event should be logged, which could be based on dynamic and individual deadbands, time intervals, other application conditions or any combination thereof.

Logix can trigger an event by changing the state of (the previously unused) Bit7 (***EventTrigger***) of the Status byte, as shown in the example UDT below:

DNP3G30V05	{...}		AparianDNP3AnalogInputRealFlag[100]
DNP3G30V05[0]	{...}		AparianDNP3AnalogInputRealFlag
DNP3G30V05[0].Online	1	Decimal	BOOL
DNP3G30V05[0].Restart	0	Decimal	BOOL
DNP3G30V05[0].CommLost	0	Decimal	BOOL
DNP3G30V05[0].RemoteForced	0	Decimal	BOOL
DNP3G30V05[0].LocalForced	0	Decimal	BOOL
DNP3G30V05[0].OverRange	0	Decimal	BOOL
DNP3G30V05[0].ReferenceError	0	Decimal	BOOL
DNP3G30V05[0].EventTrigger	0	Decimal	BOOL
DNP3G30V05[0].Value	420.0	Float	REAL

Figure 3.36. – DNP3 Logix Controlled Event Trigger Example

NOTE: In the applicable DNP3 objects, Bit 7 is unused. Although used to trigger the logging of an event, this bit is masked off before being transmitted to the DNP3 master and thus complying with the DNP3 specification.

NOTE: The Logix triggered event mechanism requires the ***Enable Events*** parameter to be configured in the Slate Logix Tag Mapping (above).

NOTE: The Outstation Logix example project (***DNP3OutstationExample***) includes Add-On-Instructions and examples where Logix triggers the event logging making use of dynamic deadbands, time intervals and external triggers.

NOTE: When using the Logix controlled event trigger method, it is recommended to set the deadband (DB) in Slate to a large value to avoid duplicate/unexpected events.

A maximum of 100,000 events can be logged per DNP3 Group.

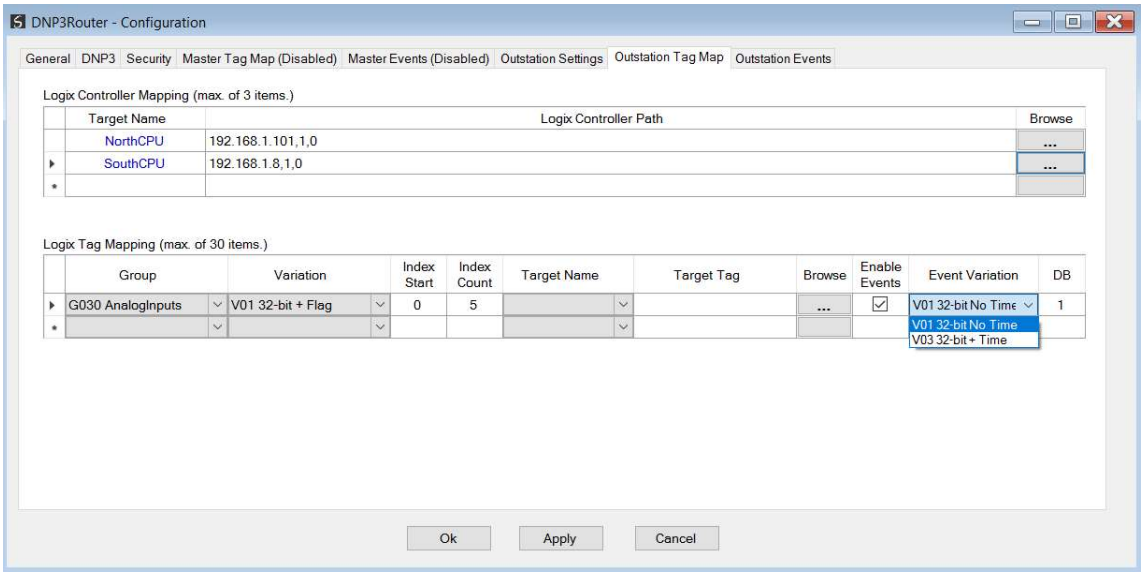


Figure 3.37. – DNP3 Event Variation selection

3.6.2. SCHEDULED MODE (DNP3 MASTER)

The DNP3 Router (when in DNP3 Master mode) can extract or receive DNP3 events from various DNP3 Outstations. This is achieved by enabling the Event Unload Mode in the *Master Events* configuration tab. Once the DNP3 Router has received a DNP3 event it will attempt to update a Logix UDT array (see example Logix code) to allow the Logix application code to use it.

NOTE: Refer to the Logix example code which provides a mechanism to extract the DNP3 Events from the Logix Master Events Tag.

Once there is confirmation from the Logix controller that the event has successfully been written to an index offset of the Logix Master Event Array the DNP3 Router will then send a confirm to the DNP3 Outstation that the event has been received and it can be removed from its internal log.

The configuration below shows the Logix Controller selected (from the list of controllers in the Scheduled Logix Controller Map). Once this is done the user can browse to the required Logix tag (using the Tag browser) to enable the DNP3 Router to unload DNP3 events into the Logix controller.

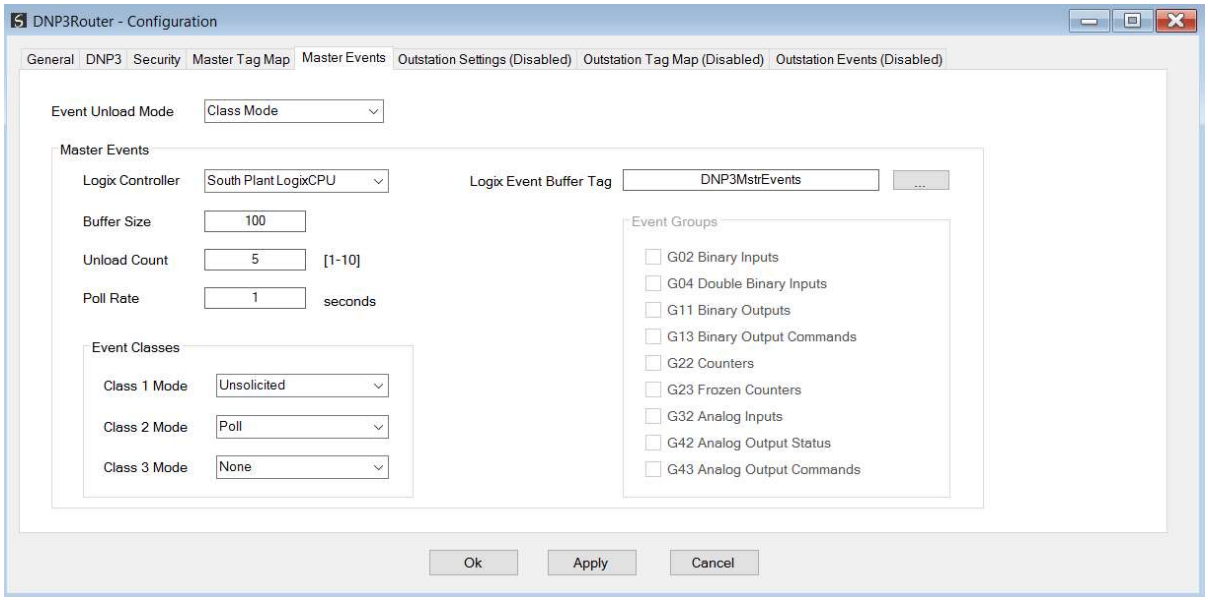


Figure 3.38. – DNP3 Master Event Unloading Configuration

The buffer size in the configuration must match the array size of the Master Event Tag in the Logix controller.

NOTE: This buffer size value must not exceed the Logix controller tag array size. If this is the case the unloading of events to the Logix controller will not operate correctly.

Below is an example of how the DNP3 Router would unload events from the DNP3 Outstations (based on the configuration in the image above). DNP3 events can be unloaded from DNP3 Outstations either by one of the following methods:

- Polling each Event Class (Class1, Class2, Class3).
- Enabling Unsolicited Responses from each DNP3 Outstation.
- Polling individual Groups for each DNP3 Outstation (e.g. Group 32 – Analog Input Events).

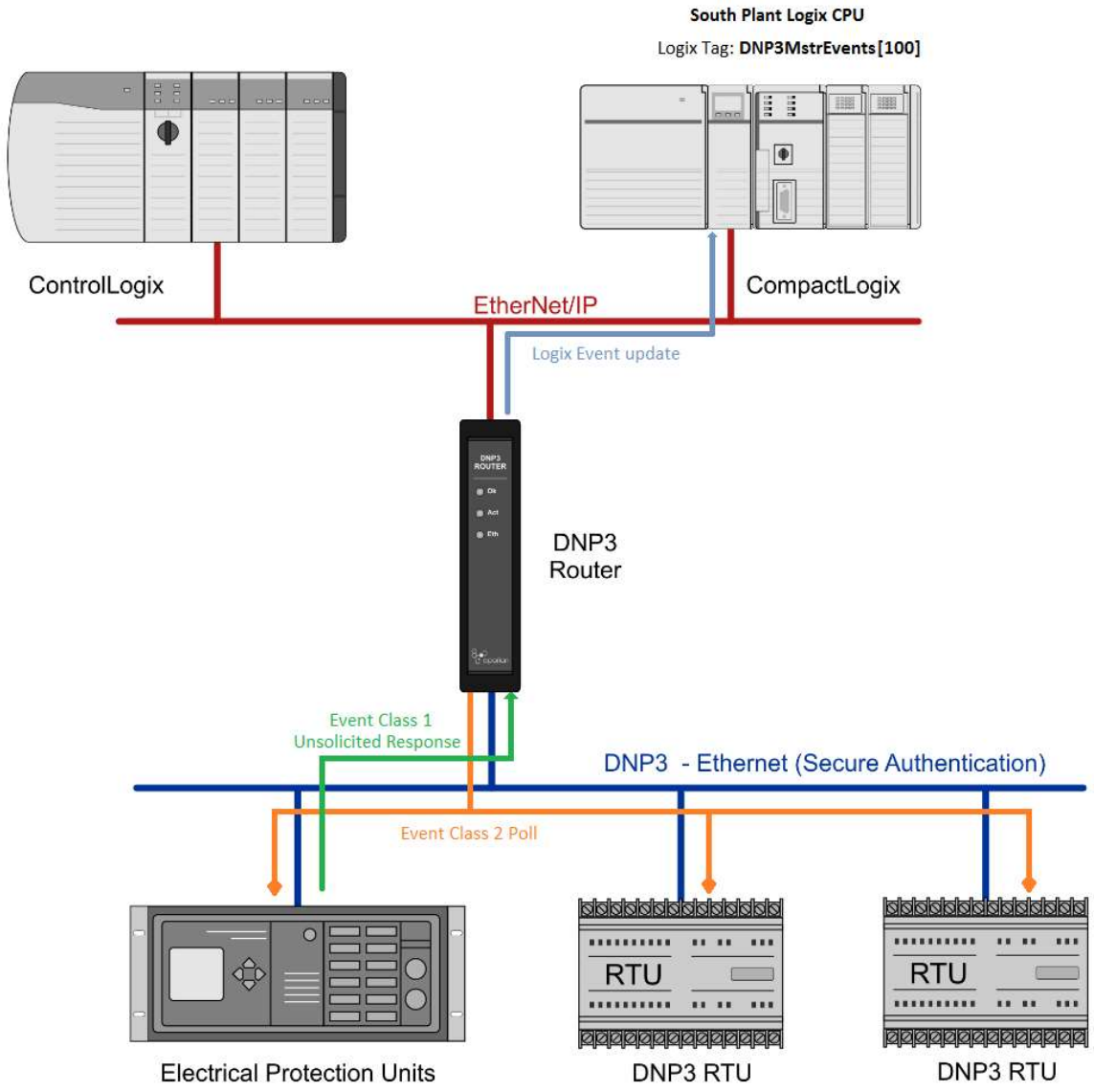


Figure 3.39 – DNP3 Master Event Unloading

The unloading of buffered events into a Logix controller is explained in section 5.

3.7. OUTSTATION REPEATERS

When in Reactive Mode the DNP3 Router provides the ability to repeat certain messages from and to certain DNP3 Outstations. This is particularly useful in radio networks where the DNP3 Master cannot see all the DNP3 Outstations. The DNP3 Router can also be configured to route certain messages to another DNP3 Router (over Ethernet) which will then repeat that message again on its serial network. This will allow the user to have certain messages being routed and repeated to different radio networks (eg. on different frequencies).

The Outstation Repeater configuration consists of the following parameters:

Parameter	Description
Outstation Node	When a message on the network has the following node address in either the source or destination address it will be repeated. Note that the DNP3 Router will keep a lookup table of recent messages to avoid repeating a repeated message.
Forward IP Address	When the user wants to make use of the Routing functionality, this is the IP address of the DNP3 Router to which the messages will be routed.
Delay (ms)	This is the amount of time the DNP3 Router must wait before repeating the message. This can be used to allow multiple repeater paths to the same outstation without causing collisions on the radio network. It can also be used in instances where certain radios/implementations require some “dead” time before another message is sent.

Table 3.8 – Outstation Repeater Settings parameters

The Outstation Repeater configuration is shown in the figure below. The Outstation Repeater configuration window is opened by either double clicking on the module in the tree or right-clicking the module and selecting *Configuration*. Once the window is open the user can select the Outstation Repeater tab in the window.

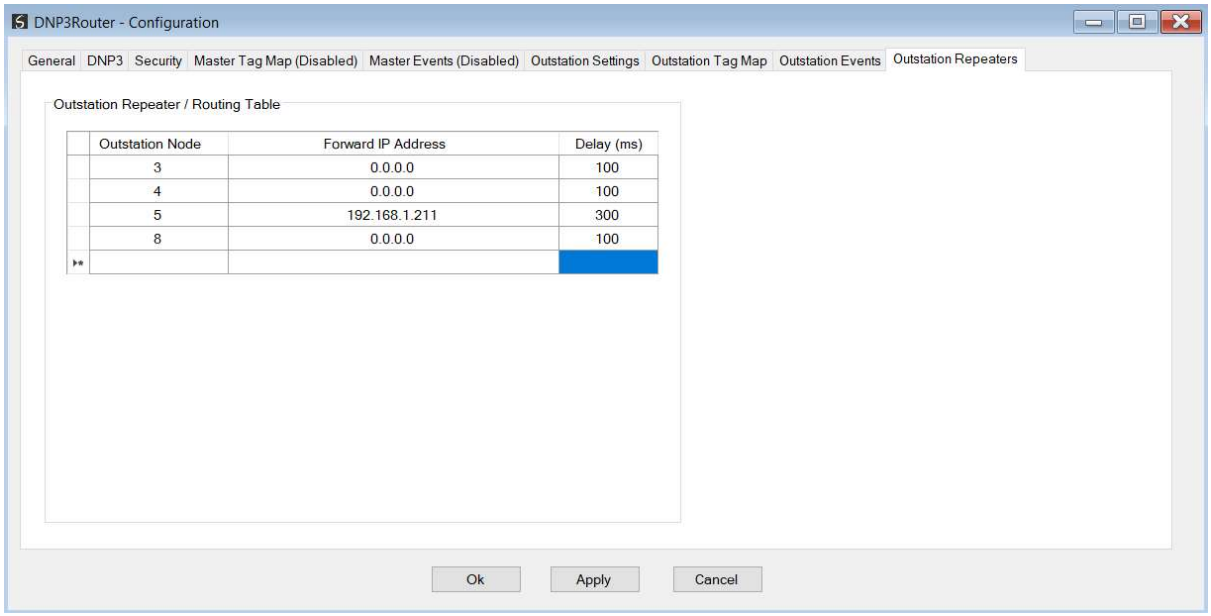


Figure 3.40 – DNP3 Outstation Repeater Configuration

Below are three examples of repeater functionality in the DNP3 Router.

Simple Repeater

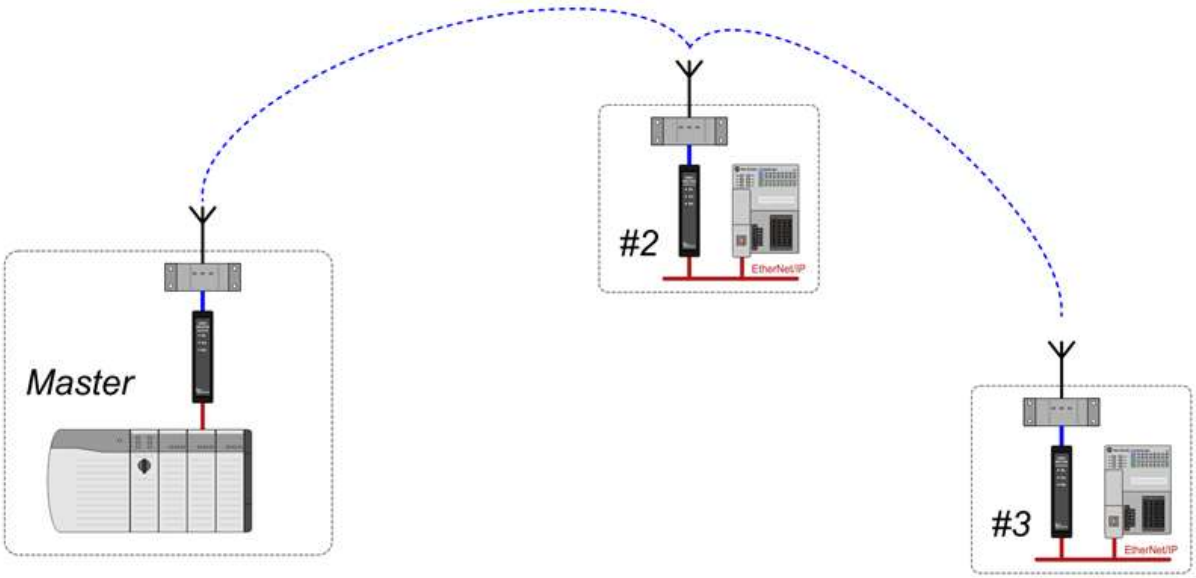


Figure 3.41 – Simple Repeater Example

Redundant Repeater

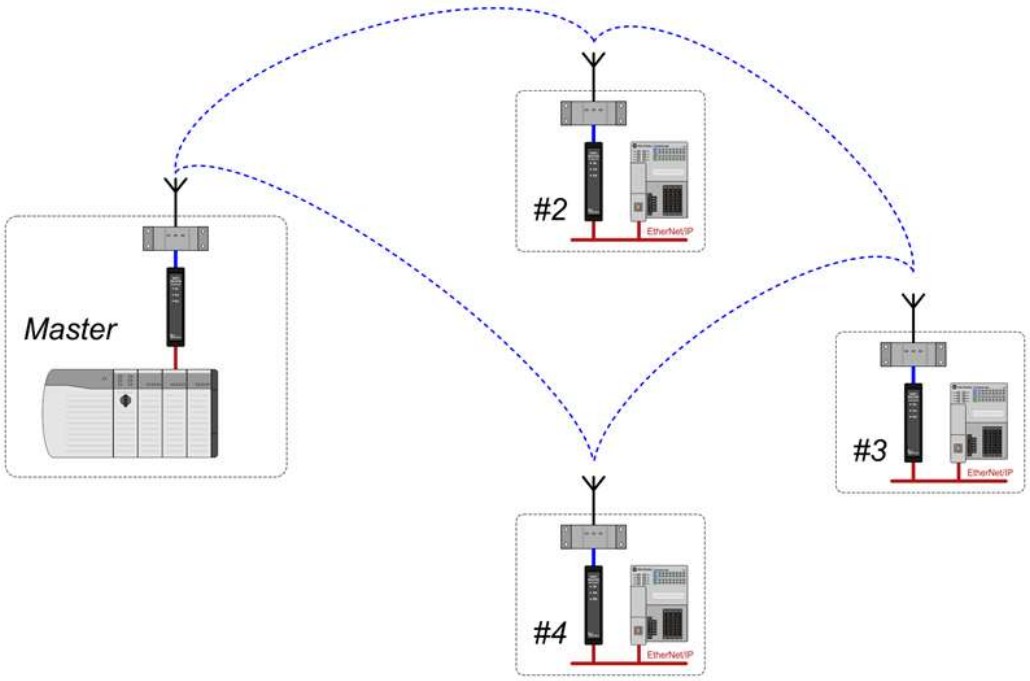


Figure 3.42 – Redundant Repeater Example

Routed Functionality

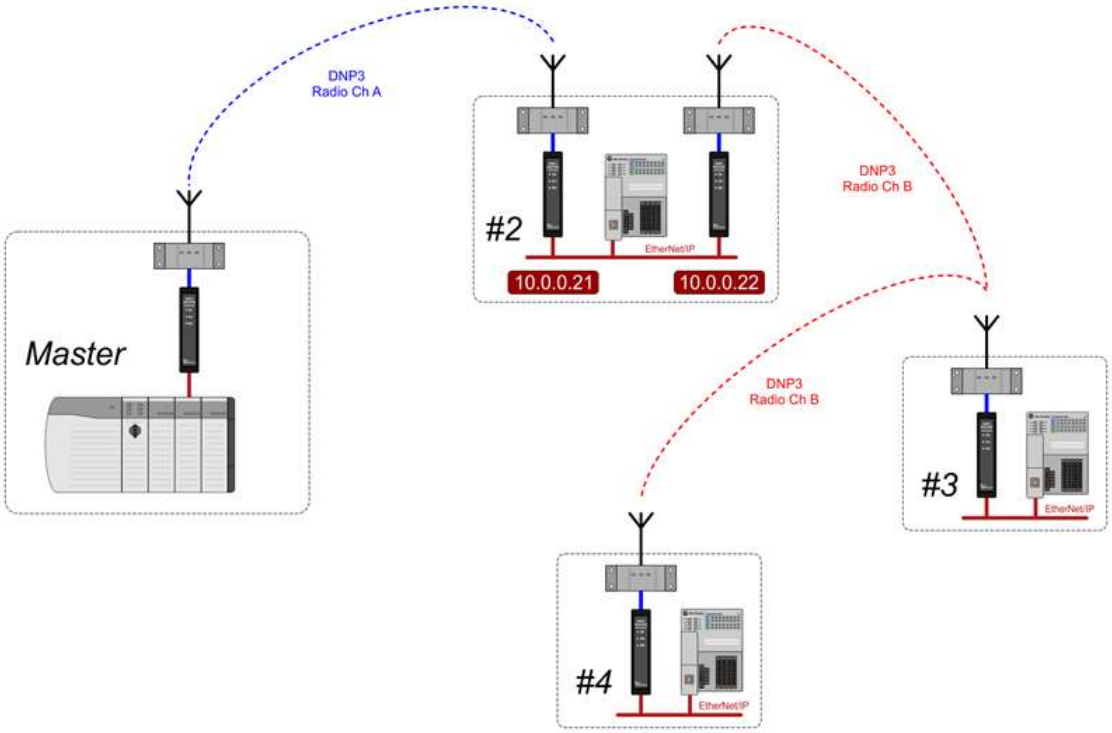


Figure 3.43 – Routed Function Example

3.8. MODULE DOWNLOAD

Once the DNP3 configuration has been completed, it must be downloaded to the module.

Before downloading the Connection Path of the module should be set. This path will automatically default to the IP address of the module, as set in the module configuration. It can however be modified, if the DNP3 Router is not on a local network.

The Connection path can be set by right-clicking on the module and selecting the Connection Path option.

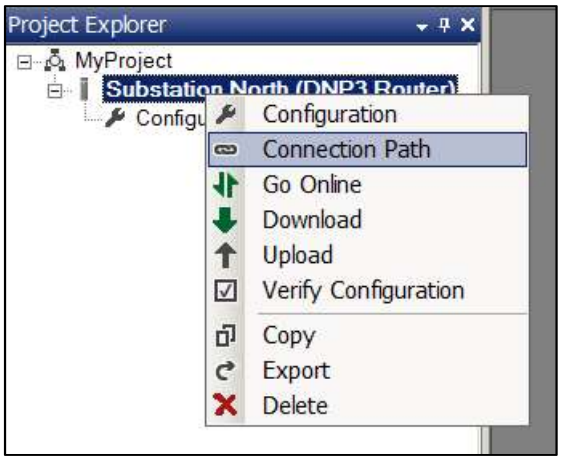


Figure 3.44 - Selecting Connection Path

The new connection path can then be either entered manually or selected by means of the Target Browser.



Figure 3.45. - Connection Path

To initiate the download, right-click on the module and select the Download option.

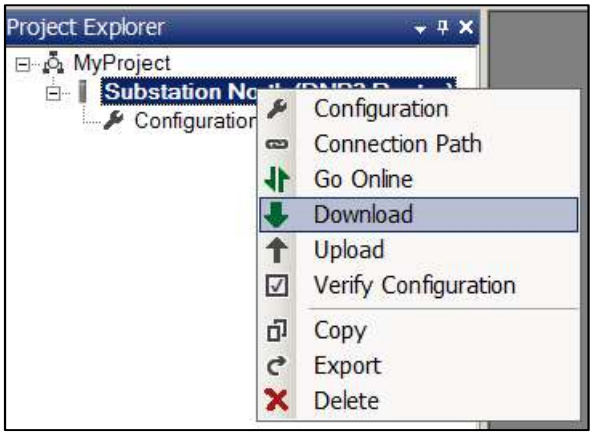


Figure 3.46. - Selecting Download

Once complete, the user will be notified that the download was successful.



Figure 3.47. - Successful download

During the download process the module's time will be compared to that of the PC's time. Should the difference be greater than 30 seconds, the user will be prompted to set the module time to that of the PC time.

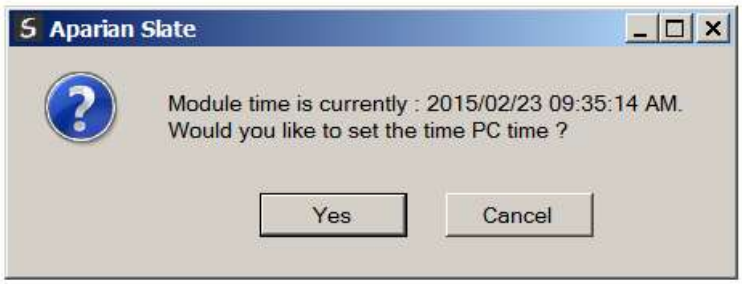


Figure 3.48. – Setting module time

NOTE: When in Reactive (Outstation) mode the time is not synchronized to that of the PC. The DNP3 Master will be responsible for correcting the time on the DNP3 Router (Outstation).

The module time is used only for the event log.Within the Slate environment the module will be in the Online state, indicated by the green circle around the module. The module is now configured and will start operating immediately.

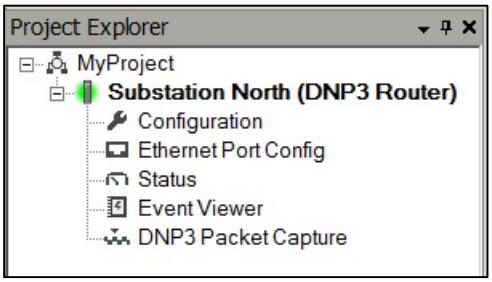


Figure 3.49. - Module online

3.9. RSLOGIX 5000 CONFIGURATION

The DNP3 Router modules can be easily integrated with Allen-Bradley Logix family of controllers.

For Logix versions 20 and beyond, the modules can be added using the EDS Add-On-Profile (AOP), which is described in section 3.8.1.

For older versions (19 and below), the module must be added using a Generic Profile which is described in section 3.8.2.

3.9.1. STUDIO 5000 CONFIGURATION (VERSION 20+)

Integration with the Logix family in Studio5000 makes use of the EDS AOP. Before the module can be added to the tree the module's EDS file must be registered. Using RSLinx, the EDS file can be uploaded from the device after which the EDS Hardware Installation tool will be invoked to complete the registration.

Alternatively, the EDS file can be downloaded from the product web page at http://www.aparian.com/products/dnp3router and registered manually using the EDS Hardware Installation Tool shortcut under the Tools menu in Studio 5000.

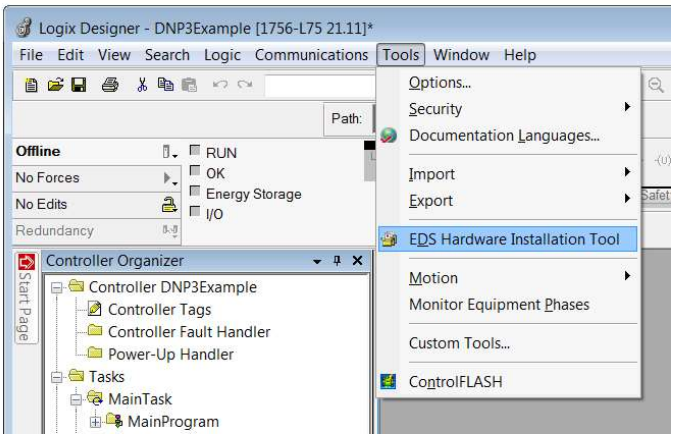


Figure 3.50 - EDS Hardware Installation Utility

After the EDS file has been registered, the module can be added to the Logix IO tree in Studio 5000. Under a suitable Ethernet bridge module in the tree, select the Ethernet network, right-click and select the New Module option.

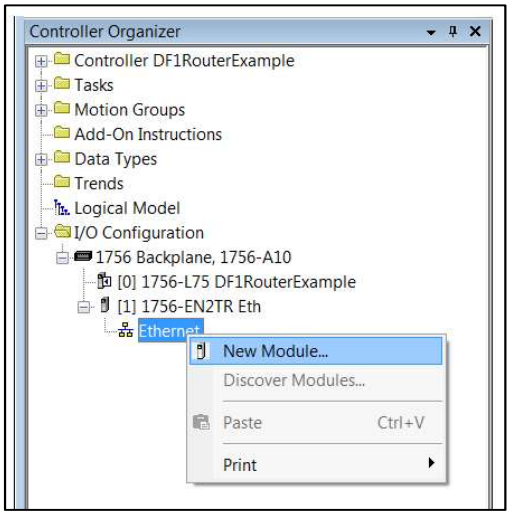


Figure 3.51 – Adding a module

The module selection dialog will open. To find the module more easily, use the Vendor filter to select only the Aparian modules as shown in the figure below.

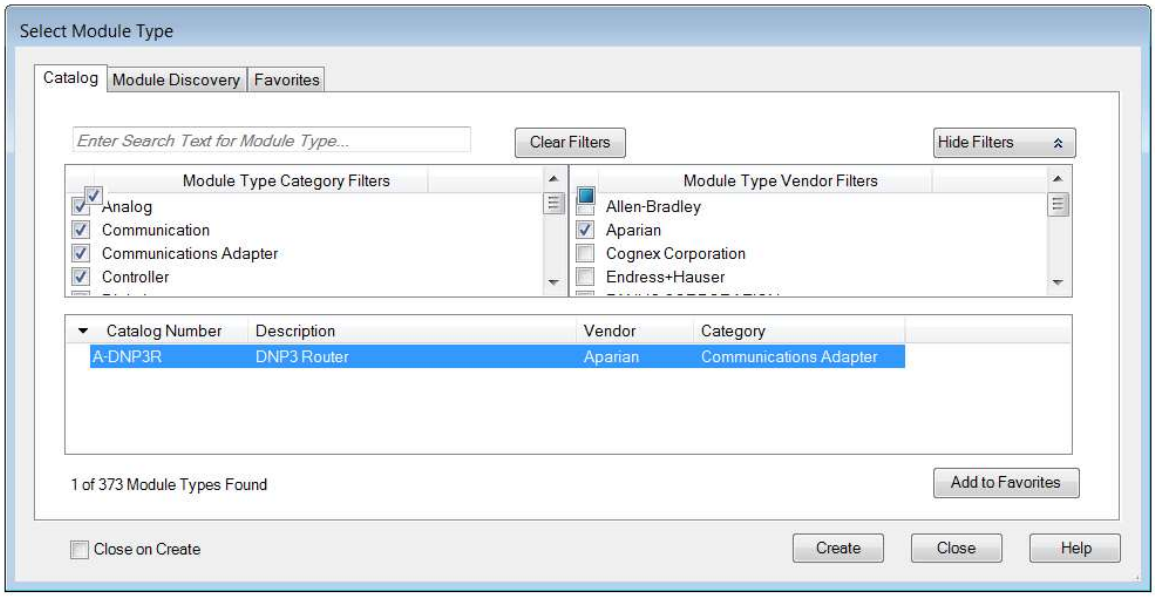


Figure 3.52 – Selecting the module

Locate and select the DNP3 Router module, and select the ***Create*** option. The module configuration dialog will open, where the user must specify the Name and IP address as a minimum to complete the instantiation.

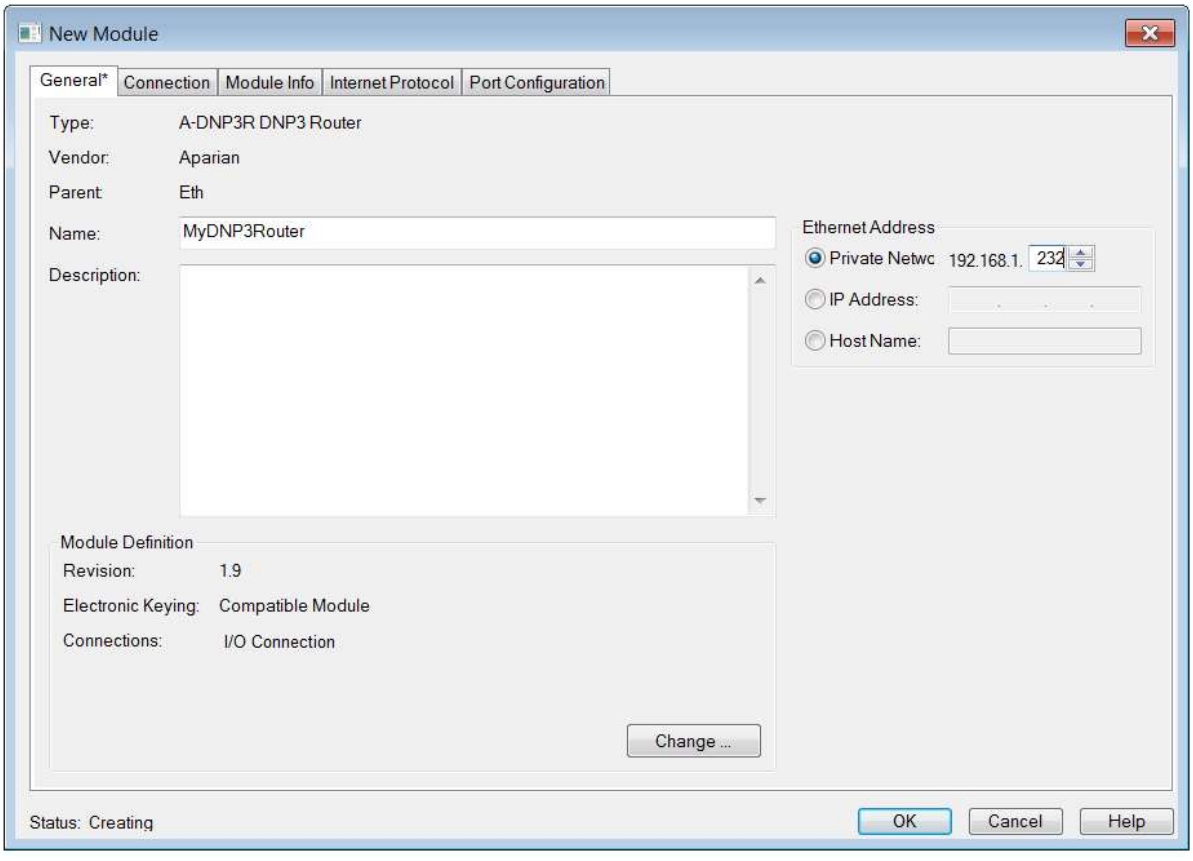


Figure 3.53 – Module instantiation

Once the instantiation is complete the module will appear in the Logix IO tree.

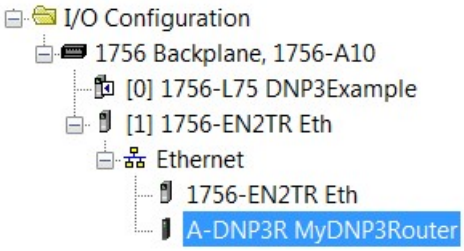


Figure 3.54 – Logix IO tree

The Module Defined Data Types will automatically be created during the instantiation process. These data types provide meaningful structures to the module data. An excerpt of the Input Image is shown in the following figure.

MyDNP3:I	{...}	{...}		_055A:A_DNP3R_CB23...
MyDNP3:I.ConnectionFaulted	0		Decimal	BOOL
MyDNP3:I.InstanceNameLength	0		Decimal	DINT
MyDNP3:I.Status	2#0000_0000_0000_0000_0000_0000_0000_0000		Binary	DINT
MyDNP3:I.ReactiveTagMode	0		Decimal	BOOL
MyDNP3:I.ScheduledTagMode	0		Decimal	BOOL
MyDNP3:I.UnscheduledMode	0		Decimal	BOOL
MyDNP3:I.ConfigurationValid	0		Decimal	BOOL
MyDNP3:I.RoutingInhibited	0		Decimal	BOOL
MyDNP3:I.MasterTagStatus	2#0000_0000_0000_0000_0000_0000_0000_0000		Binary	DINT
MyDNP3:I.ScheduledTagStatus00	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus01	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus02	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus03	0		Decimal	BOOL
• • •				
MyDNP3:I.ScheduledTagStatus27	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus28	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus29	0		Decimal	BOOL
MyDNP3:I.TransactionRate	0		Decimal	DINT
MyDNP3:I.Temperature	0.0		Float	REAL
MyDNP3:I.DNP3RxPacketCount	0		Decimal	DINT
MyDNP3:I.DNP3TxPacketCount	0		Decimal	DINT
MyDNP3:I.DNP3ChecksumErrors	0		Decimal	DINT
MyDNP3:I.DNP3MsgTimeout	0		Decimal	DINT
MyDNP3:I.AuthenticationFailures	0		Decimal	DINT
MyDNP3:I.SessionKeyChanges	0		Decimal	DINT
MyDNP3:I.TagReads	0		Decimal	DINT
MyDNP3:I.TagWrites	0		Decimal	DINT
MyDNP3:I.TagConnectionFailures	0		Decimal	DINT
MyDNP3:I.TagErrors	0		Decimal	DINT
MyDNP3:I.MasterEventBufferIndex	0		Decimal	DINT

Figure 3.55 – Module Defined Data Type

3.9.2. RSLogix 5000 Configuration (Pre-Version 20)

3.9.2.1. ADD MODULE TO I/O CONFIGURATION

The module can operate in both a Logix “owned” and standalone mode. When the module operates in a Logix “owned” mode the DNP3 Router will need to be added to the RSLogix 5000 IO tree. The module will need to be added as a generic Ethernet module. This is done by right clicking on the Ethernet Bridge in the RSLogix 5000 and selecting *New Module* after which the *ETHERNET-MODULE* is selected to be added as shown in the figure below.

NOTE: See the next section for importing the configuration (L5X).

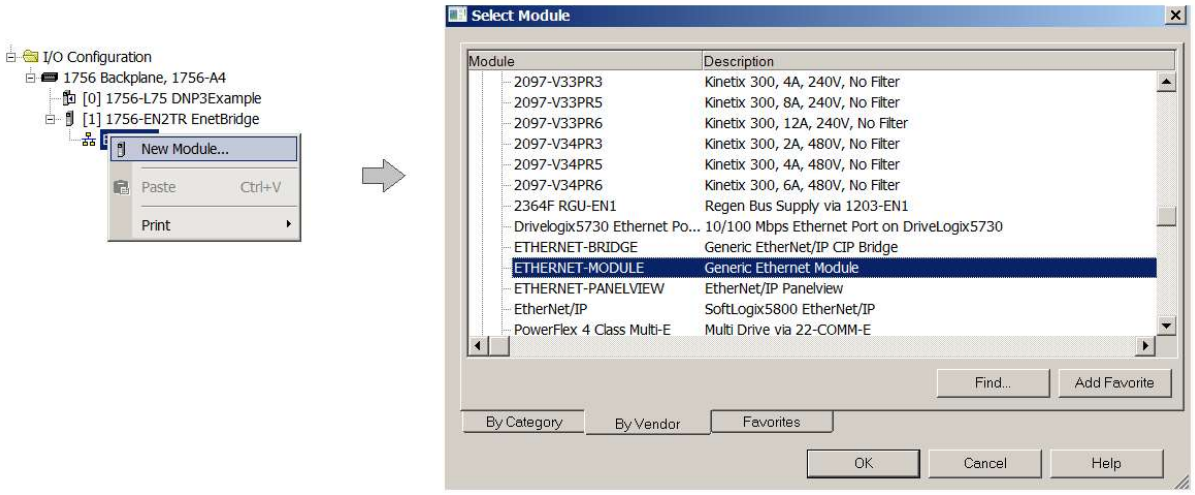


Figure 3.56. - Add a Generic Ethernet Module in RSLogix 5000

The user must enter the IP address of the DNP3 Router that will be used. The assembly instance and size must also be added for the input, output, and configuration in the connection parameters section. Below are the required connection parameters.

Connection Parameter	Assembly Instance	Size
Input	108	37 (32-bit)
Output	101	1 (32-bit)
Configuration	102	0 (8-bit)

Table 3.9 - RSLogix class 1 connection parameters for the DNP3 Router

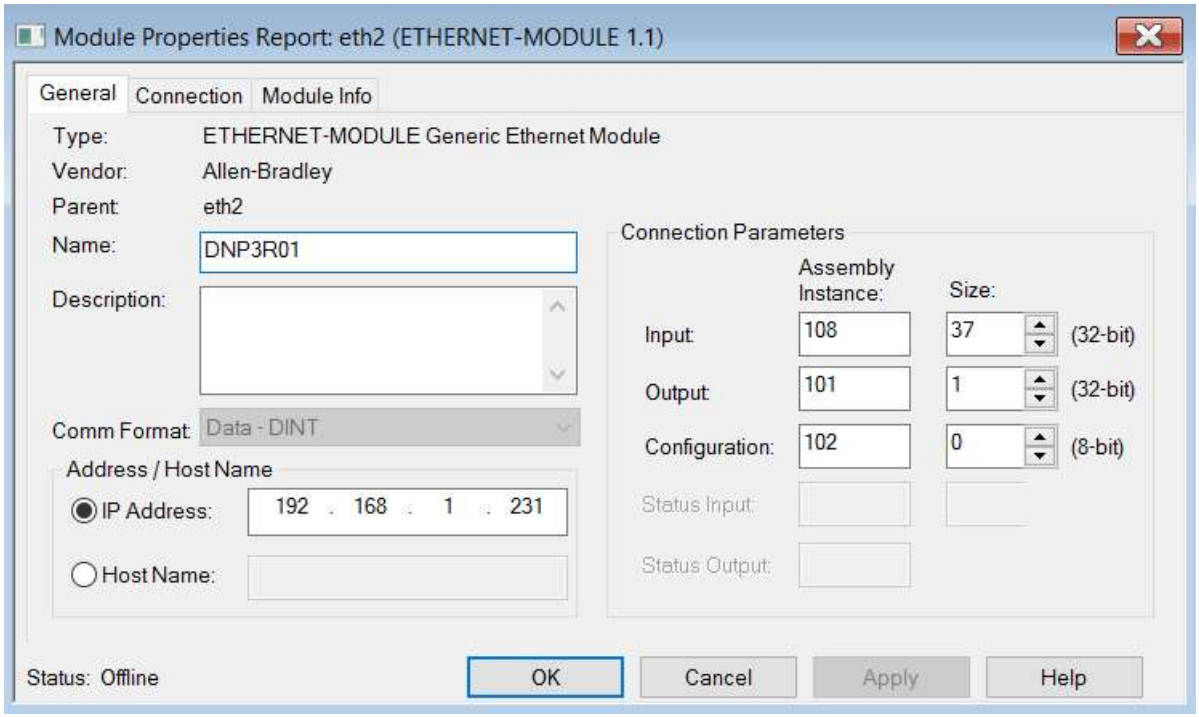


Figure 3.57. - RSLogix General module properties in RSLogix 5000

NOTE: The user will need to enter the exact connection parameters before the module will establish a class 1 connection with the Logix controller.

Next the user needs to add the connection requested packet interval (RPI). This is the rate at which the input and output assemblies are exchanged. The recommended value is 500ms. Refer to the technical specification section in this document for further details on the limits of the RPI.

NOTE: Although the module is capable of running with an RPI of 10ms, it is recommended to set the RPI to 500ms, to avoid unnecessary loading of the module processor.

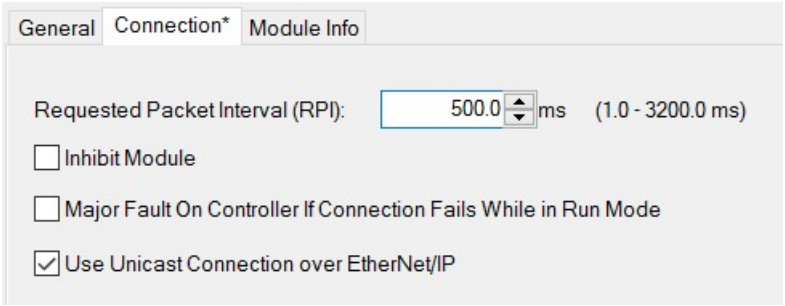


Figure 3.58. - Connection module properties in RSLogix 5000

Once the module has been added to the RSLogix 5000 IO tree the user must assign the User Defined Types (UDTs) to the input and output assemblies. The user can import the required UDTs by right-clicking on *User-Defined* sub-folder in the *Data Types* folder of the IO tree and

selecting *Import Data Type*. The assemblies are then assigned to the UDTs with a ladder copy instruction (COP) as shown in the figure below.

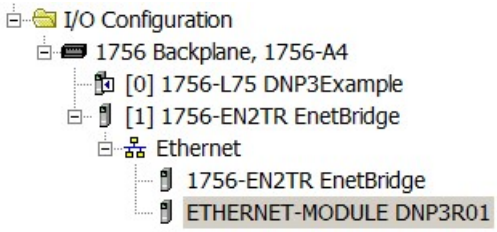


Figure 3.59. – RSLogix 5000 I/O module tree

3.9.2.2. IMPORTING UDTS AND MAPPING ROUTINES

To simplify the mapping of the input image, an RSLogix 5000 Routine Partial Import (L5X) file is provided. This file can be imported by right-clicking on the required Program and selecting the Import Routine option.

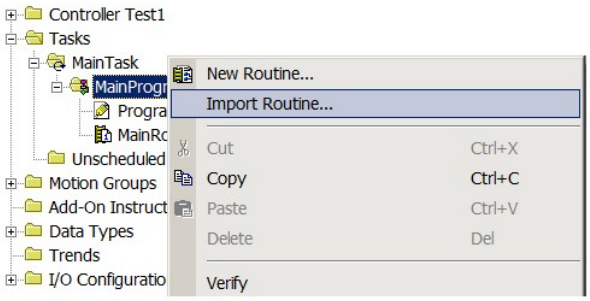


Figure 3.60. – RSLogix 5000 Importing DNP3 Router specific routine and UDTs

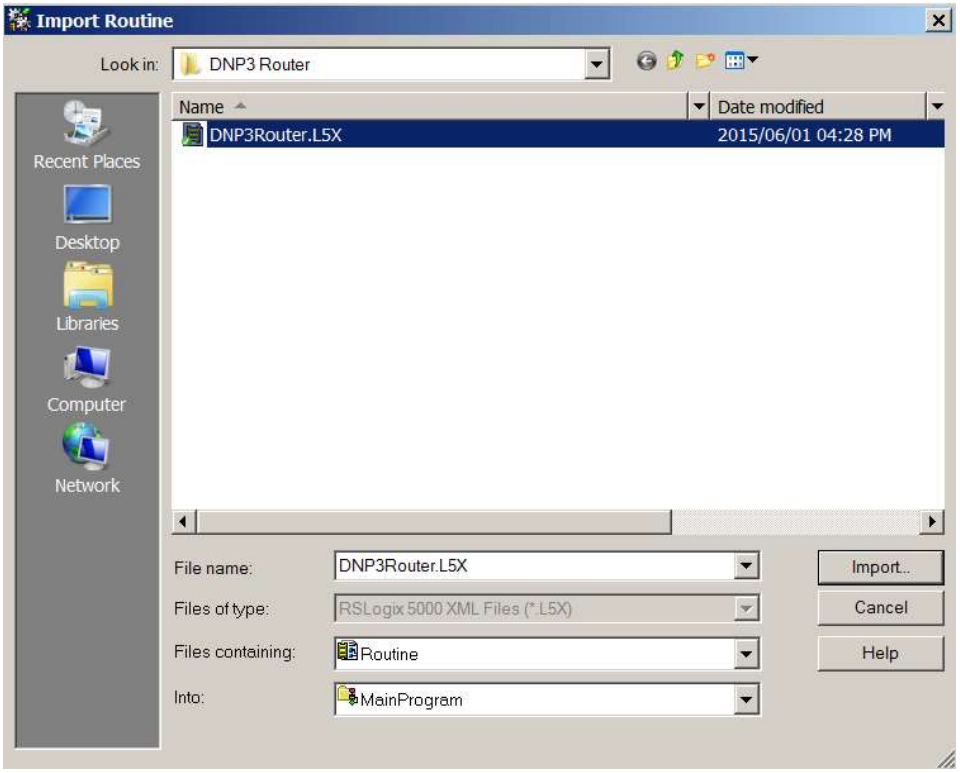


Figure 3.61. - Selecting partial import file

The import will create the following:

- The required UDTs (user defined data types)
- Two controller tags representing the Input and Output assemblies.
- A routine mapping the DNP3Router module to the aforementioned tags.
- An example Unscheduled Message instruction with the associated Tags

The user may need to change the routine to map to the correct DNP3 Router module instance name, and make sure that the mapping routine is called by the Program's Main Routine.

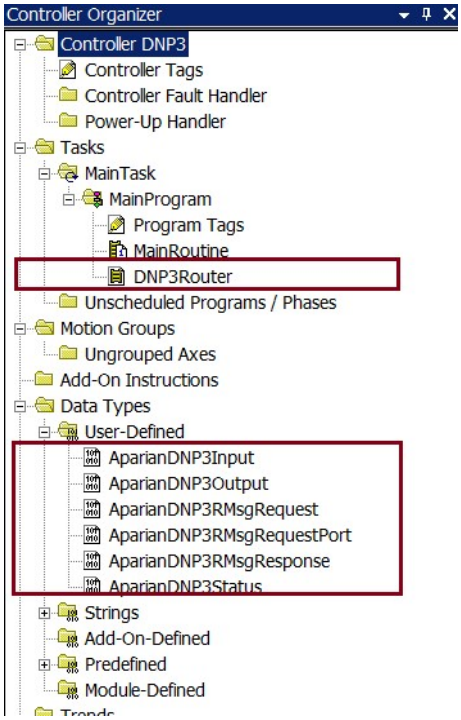


Figure 3.62. - Imported RSLogix 5000 objects

Refer to the additional information section of this document for an example RSLogix 5000 project as well as the required UDTs.

4. LOGIX OPERATION

4.1. MESSAGE ROUTING

When the module has been correctly setup the DNP3 message initiator will send a read/write to a certain DNP3 group and variation which will then be routed to a Logix tag. The messages sent by the initiator must be completed with the correct data for successful operation. There are various indicators to determine if the mapping is routing the DNP3 messages correctly. Refer to the diagnostics section of this document for a more detailed explanation of the various indicators that can be used to diagnose the module.

4.2. RSLOGIX 5000 ASSEMBLIES

When the module operates in a Logix "owned" mode the Logix controller will establish a class 1 cyclic communication connection with the DNP3 Router. An input and output assembly is exchanged at a fix interval. The UDTs provided will convert the input and output arrays into tag based assemblies. Refer to the additional information section in this document for the input and output UDTs.

MyDNP3:I	{...}	{...}		_055A:A_DNP3R_CB23...
MyDNP3:I.ConnectionFaulted	0		Decimal	BOOL
MyDNP3:I.InstanceNameLength	0		Decimal	DINT
MyDNP3:I.Status	2#0000_0000_0000_0000_0000_0000_0000_0000		Binary	DINT
MyDNP3:I.ReactiveTagMode	0		Decimal	BOOL
MyDNP3:I.ScheduledTagMode	0		Decimal	BOOL
MyDNP3:I.UnscheduledMode	0		Decimal	BOOL
MyDNP3:I.ConfigurationValid	0		Decimal	BOOL
MyDNP3:I.RoutingInhibited	0		Decimal	BOOL
MyDNP3:I.MasterTagStatus	2#0000_0000_0000_0000_0000_0000_0000_0000		Binary	DINT
MyDNP3:I.ScheduledTagStatus00	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus01	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus02	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus03	0		Decimal	BOOL
...				
MyDNP3:I.ScheduledTagStatus27	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus28	0		Decimal	BOOL
MyDNP3:I.ScheduledTagStatus29	0		Decimal	BOOL
MyDNP3:I.TransactionRate	0		Decimal	DINT
MyDNP3:I.Temperature	0.0		Float	REAL
MyDNP3:I.DNP3RxPacketCount	0		Decimal	DINT
MyDNP3:I.DNP3TxPacketCount	0		Decimal	DINT
MyDNP3:I.DNP3ChecksumErrors	0		Decimal	DINT
MyDNP3:I.DNP3MsgTimeout	0		Decimal	DINT
MyDNP3:I.AuthenticationFailures	0		Decimal	DINT
MyDNP3:I.SessionKeyChanges	0		Decimal	DINT
MyDNP3:I.TagReads	0		Decimal	DINT
MyDNP3:I.TagWrites	0		Decimal	DINT
MyDNP3:I.TagConnectionFailures	0		Decimal	DINT
MyDNP3:I.TagErrors	0		Decimal	DINT
MyDNP3:I.MasterEventBufferIndex	0		Decimal	DINT

Figure 4.1. - Input assembly UDT structure

4.2.1. INPUT ASSEMBLY

The following parameters are used in the input assembly of the module.

Parameter	Datatype	Description
Instance	STRING	This parameter is the instance name of the module that was configured under the general DNP3 configuration in Slate.
Status.ReactiveTagMode	BOOL	Set if the module is operating in Reactive Tag mode.
Status.ScheduledTagMode	BOOL	Set if the module is operating in Scheduled Tag mode.
Status.UnscheduledMode	BOOL	Set if the module is operating in Unscheduled mode.
Status.ConfigurationValid	BOOL	Set if a valid configuration is executing in the module.
Status.RoutingInhibited	BOOL	Set when the module's routing function has been inhibited. Routing can be inhibited by setting a bit in the output assembly of the module.
Status.DNP3EventLogOk	BOOL	The DNP3 event log was correctly loaded on startup.
Status.DNP3EventLogOverflow	BOOL	At least one of the DNP3 Groups have reached the maximum allowed DNP3 events of 100,000.
MasterTagStatus.ScheduledTagStatus0…29	BOOL[30]	Each bit represents the status of the last scheduled transaction for that specific map item. A true value indicates success.
TransactionRate	DINT	The transaction rate is the number of DNP3 messages per second that the module is currently routing.
DeviceTemperature	REAL	The internal temperature of the module.
DNP3RxPacketCount	DINT	The total number of DNP3 packets received by the module.
DNP3TxPacketCount	DINT	The number of DNP3 packets sent by the module.
DNP3ChecksumErrors	DINT	The number of corrupted DNP3 packets received by the module.
DNP3MsgTimeout	DINT	The number of timed-out DNP3 packets sent by the module. Thus no reply was received.
Authentication Failures	DINT	The amount of authentication failures detected by the module. This could indicate the presence of a security threat in the form of an attacker.
Session Key Changes	DINT	The amount of session key changes done.
TagReads	DINT	The total number of tag reads executed by the module when operating in Tag Map mode.
TagWrites	DINT	The total number of tag writes executed by the module when operating in Tag Map mode.
TagConnectionFailures	DINT	The number of failed class 3 connection attempts when operating in Tag Map mode.

		Tag reading and writing requires the module to first establish a class 3 connection with the Logix Controller.
TagErrors	DINT	The number of failed tag access (read/write) requests when operating in tag Map mode. These may include privileged violations, non-existing tags, etc.
MasterEventBufferIndex	DINT	The Master Event Tag UDT array index number where the next event received from the master will be unloaded.

Table 4.1 - RSLogix 5000 input assembly parameters

4.2.2. OUTPUT ASSEMBLY

The following parameters are used in the output assembly of the module.

Parameter	Datatype	Description
RoutingInhibit	BOOL	This bit inhibits the module routing capabilities. When set, no DNP3 messages will be routed. This may be required in applications running a redundant DNP3 network where one of the DNP3 Routers is to run in a hot-standby mode.

Table 4.2 - RSLogix 5000 output assembly parameters

4.3. UNSCHEDULED MESSAGING

When the DNP3 Router is configured in Unscheduled Mode, it will process DNP3 message requests sent from Logix via a message instruction.



NOTE: The user will need to build the DNP3 objects for the application layer in the request data of the unscheduled message.
See Appendix A for more information on this.

To simplify the configuration of the required message a number of UDTs have been preconfigured and are available on the Aparian DNP3Router webpage (see the further information section).



NOTE: In this mode the DNP3 Router does support Secure Authentication, but Aggressive mode is **NOT** supported. The DNP3 Master will also change session keys each time the request destination is different from the previous request.

NOTE: In this mode the DNP3 Router does **NOT** support unsolicited responses from DNP3 Outstations.

The message instruction should be setup as follows:

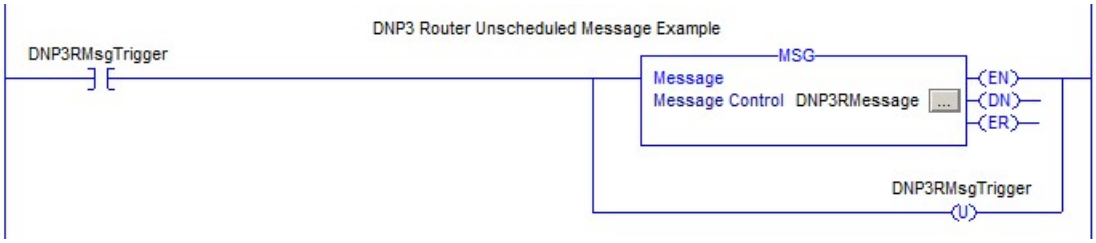


Figure 4.2. - Message Instruction

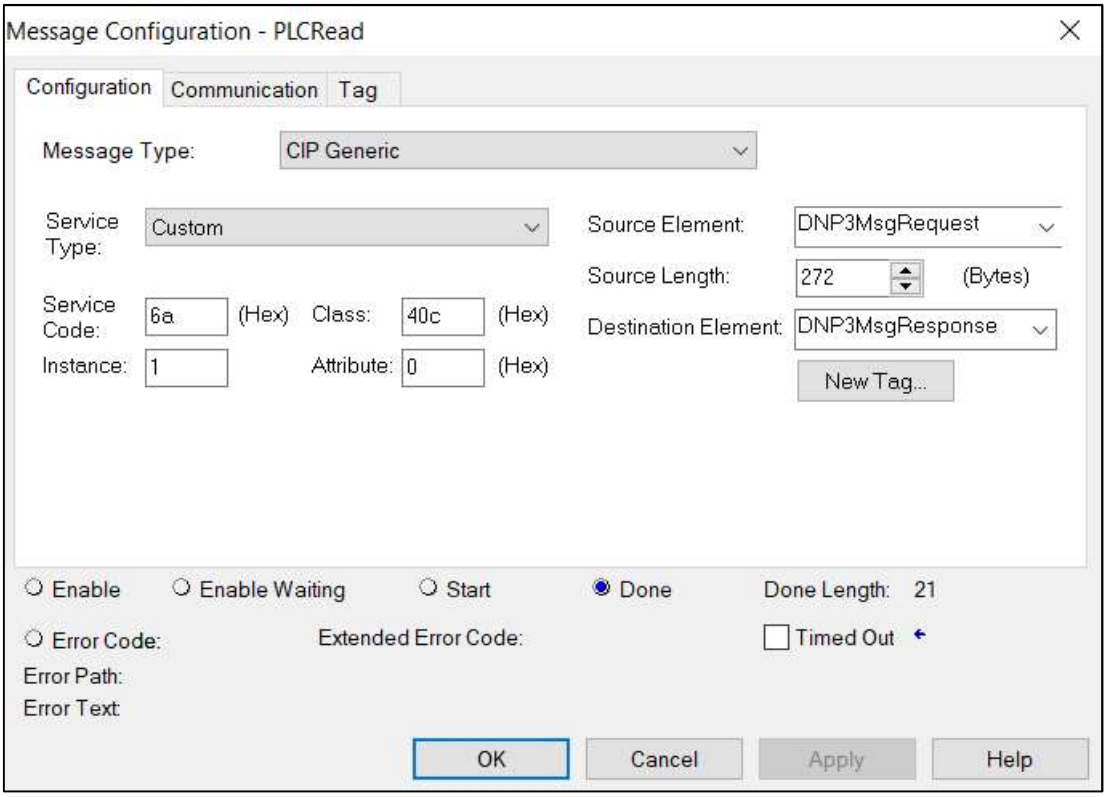


Figure 4.3. - Message Configuration

Parameter	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	6A (Hex) - Unscheduled DNP3 Pass-through
Class	40C (Hex)
Instance	1
Attribute	0

Source Element	The request tag instance. Must follow the structure of the ***AparianDNP3RMsgRequest*** UDT.
Source Length	272
Destination Element	The response tag instance. Must follow the structure of the ***AparianDNP3RMsgResponse*** UDT.

Table 4.3. - Message Configuration Paramaters

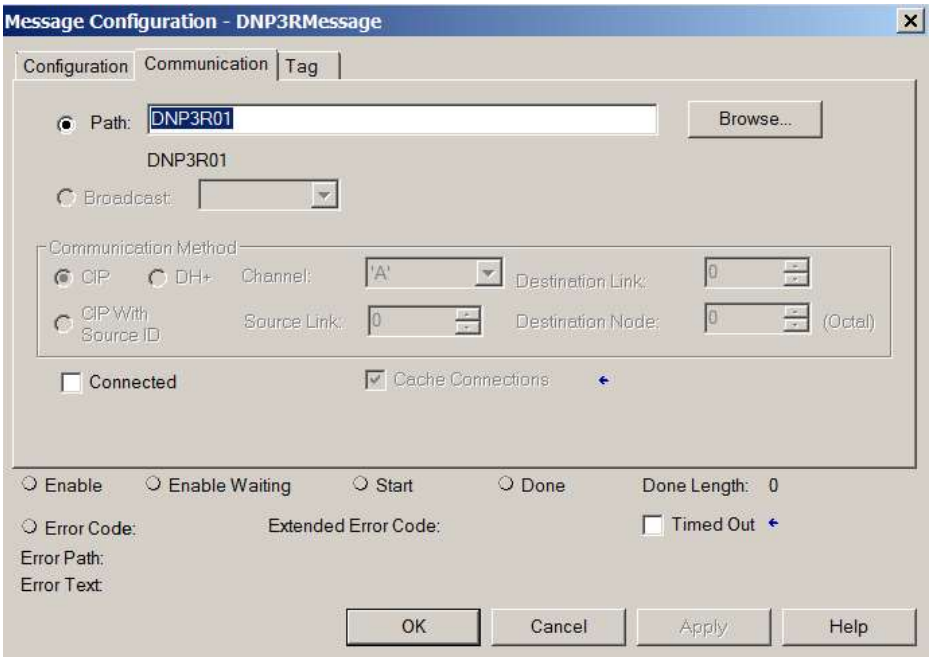


Figure 4.4. - Messsage Configuration - Communication

The Path must be configured to that of the DNP3 Router. If the DNP3 Router has been added in the I/O tree, then the Browse option can be used to select the path.
Alternatively, enter the CIP path in the format :

1,X,2,IP , where
1 represents the backplane port,
X represents the slot of the Ethernet bridge module,
2 represents the Ethernet port of the Ethernet bridge module and
IP represents the IP address of the DNP3 Router.
e.g. **1,1,2,192.168.1.41**

The request tag (e.g. ***DNP3RMsgrequest***) should be configures as follows:

DNP3MsgRequest	{...}	{...}		AparianDNP3RMsgRequest
DNP3MsgRequest.DestinationNode	1		Decimal	INT
DNP3MsgRequest.RequestDataSize	5		Decimal	INT
DNP3MsgRequest.IPAddress	{...}	{...}	Decimal	INT[4]
DNP3MsgRequest.IPAddress[0]	192		Decimal	INT
DNP3MsgRequest.IPAddress[1]	168		Decimal	INT
DNP3MsgRequest.IPAddress[2]	1		Decimal	INT
DNP3MsgRequest.IPAddress[3]	210		Decimal	INT
DNP3MsgRequest.Function	1		Decimal	DINT
DNP3MsgRequest.RequestData	{...}	{...}	Decimal	SINT[255]

Figure 4.5. - Unscheduled Message Request Tag

Parameter	Description
Destination Node	The DNP3 node address of the destination device.
Request Data Size	The size of the request data being sent
IP Address	The IP address of the remote device when an Ethernet port was selected above.
Function	The DNP3 application layer function that will be used. Refer to the DNP3 documentation in the Additional information section.
Request Data	DNP3 Object header and objects. Refer to the DNP3 documentation in the Additional information section.

Table 4.4. - Unscheduled Message Request Parameters

DNP3MsgResponse	{...}	{...}		AparianDNP3RMsgResponse
DNP3MsgResponse.DNP3Indicators	0		Decimal	INT
DNP3MsgResponse.ResponseDataSize	0		Decimal	INT
DNP3MsgResponse.ResponseData	{...}	{...}	Decimal	SINT[255]

Figure 4.6. - Unscheduled Message Response Tag

Parameter	Description
DNP3 Indicators	These 16bits will provide return information of the remote DNP3 device. Refer to the DNP3 documentation in the Additional information section. Bit 0 – Broadcast Bit 1 – Class 1 events Bit 2 – Class 2 events Bit 3 – Class 3 events Bit 4 – Need Time Bit 5 – Local control Bit 6 – Device trouble

	Bit 7 – Device restart Bit 8 – Function code not supported Bit 9 – Object unknown Bit 10 – Parameter error Bit 11 – Event buffer overflow Bit 12 – Already executing Bit 13 – Configuration corrupt Bit 14 – Reserved Bit 15- Reserved
Response Length	Length of the response data received.
Response Data	Response to the DNP3 application layer object request.

Table 4.5. - Unscheduled Message Response Parameters

After the message has been executed successfully (Msg.DN) the Response Data should be copied (using a COP instruction) to the required Data Tag of an appropriate data type.

4.3.1. EXAMPLE

In the following example, the unscheduled message instruction is used to read three Analog Inputs in 32-bit no flag format, from a remote Ethernet DNP3 device located at IP address 192.168.1.65. The Analog Input points required are 0, 1 & 2.

The standard DNP3MessageRequest structure is populated as shown in the figure below.

DNP3MsgRequest	{...}	
DNP3MsgRequest.DestinationNode	2	
DNP3MsgRequest.RequestDataSize	7	
DNP3MsgRequest.IPAddress	{...}	
DNP3MsgRequest.IPAddress[0]	192	IP Address of DNP3 Device
DNP3MsgRequest.IPAddress[1]	168	
DNP3MsgRequest.IPAddress[2]	1	
DNP3MsgRequest.IPAddress[3]	65	
DNP3MsgRequest.Function	1	Function : 1 - Read
DNP3MsgRequest.RequestData	{...}	
DNP3MsgRequest.RequestData[0]	30	Group : 30 - Analog Inputs
DNP3MsgRequest.RequestData[1]	3	Variant : 3 - 32 bit value without flag
DNP3MsgRequest.RequestData[2]	1	Qualifier : 1 - No Prefix, 16-bit Start and Stop Indexes
DNP3MsgRequest.RequestData[3]	0	Start Index : 0
DNP3MsgRequest.RequestData[4]	0	
DNP3MsgRequest.RequestData[5]	2	Stop Index : 2
DNP3MsgRequest.RequestData[6]	0	

Figure 4.7. – DNP3 Message Request Example

The response to the message is shown in the next figure. The data values can them be copied (COP instruction) to the required tag destination. The DNP3 Group, Variant and Qualifier codes are shown in the Appendix.

DNP3MsgResponse	{...}	
DNP3MsgResponse.DNP3Indicators	0	Internal indicators : 0 - No issues
DNP3MsgResponse.ResponseDataSize	19	
DNP3MsgResponse.ResponseData	{...}	
DNP3MsgResponse.ResponseData[0]	30	Group : 30 - Analog Inputs
DNP3MsgResponse.ResponseData[1]	3	Variant : 3 - 32 bit value without flag
DNP3MsgResponse.ResponseData[2]	1	Qualifier : 1 - No Prefix, 16-bit Start and Stop Indexes
DNP3MsgResponse.ResponseData[3]	0	Start Index : 0
DNP3MsgResponse.ResponseData[4]	0	
DNP3MsgResponse.ResponseData[5]	2	Stop Index : 2
DNP3MsgResponse.ResponseData[6]	0	
DNP3MsgResponse.ResponseData[7]	103	Data Point 0 : Value = 103
DNP3MsgResponse.ResponseData[8]	0	
DNP3MsgResponse.ResponseData[9]	0	
DNP3MsgResponse.ResponseData[10]	0	
DNP3MsgResponse.ResponseData[11]	104	Data Point 1 : Value = 104
DNP3MsgResponse.ResponseData[12]	0	
DNP3MsgResponse.ResponseData[13]	0	
DNP3MsgResponse.ResponseData[14]	0	
DNP3MsgResponse.ResponseData[15]	105	Data Point 2 : Value = 105
DNP3MsgResponse.ResponseData[16]	0	
DNP3MsgResponse.ResponseData[17]	0	
DNP3MsgResponse.ResponseData[18]	0	

Figure 4.8. – DNP3 Message Response Example

5. DNP3 OPERATION

5.1. GENERAL

DNP3 supports various formats for each group of data points. The different formats can include additional data to that of the main requested variable needed (e.g. Status, Time, etc.). For this reason, the Logix controllers needs to map the data for these formats to User-Defined Data Types (UDTs). A range of UDTs have been provided to the user allowing for easy and seamless integration with the Logix Controller. Below are some examples of how these UDTs should be used.

When DNP3 group 30 (analog inputs) has been selected there is a range of variations that can be used providing different format and additional information for the user. If variation one (1) was selected Slate would indicate that the data returned will be a 32-bit number with a Flag (or Status bits) as shown below:

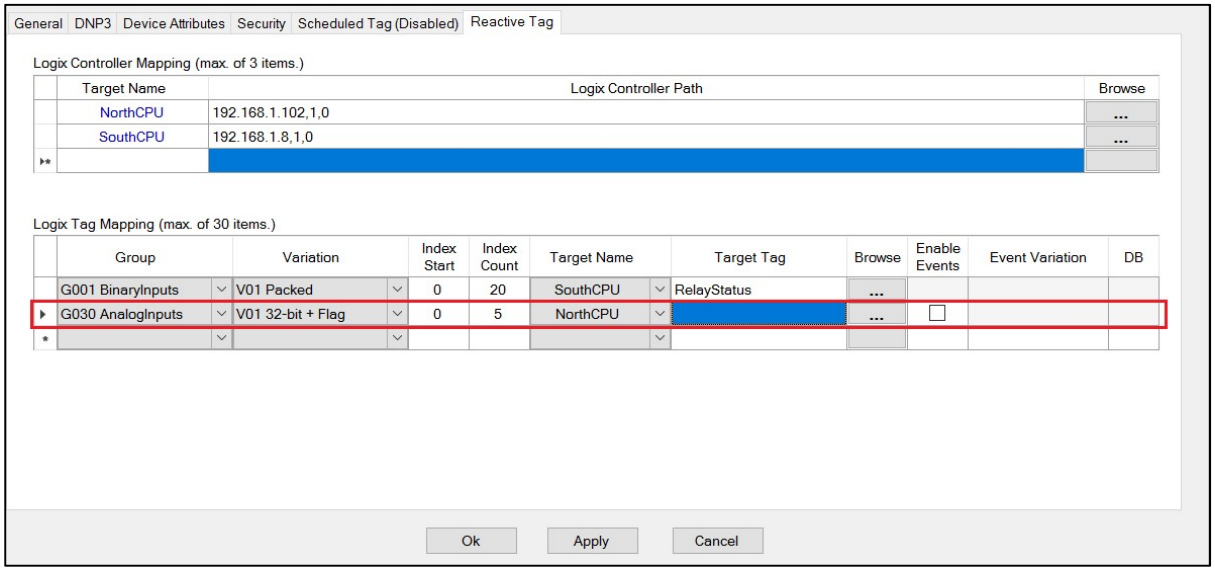


Figure 5.1. – DNP3 Group 30 selected with Variation 1

Next the user must select the correct UDT provided in the example RSLogix 5000 project (see the Additional Information section for further details). In this case the example project has a UDT called *AparianDNP3AnalogInput32Flag* which should be used as this will correctly map the additional information from the DNP3 Object as shown below. The UDT is shown below:

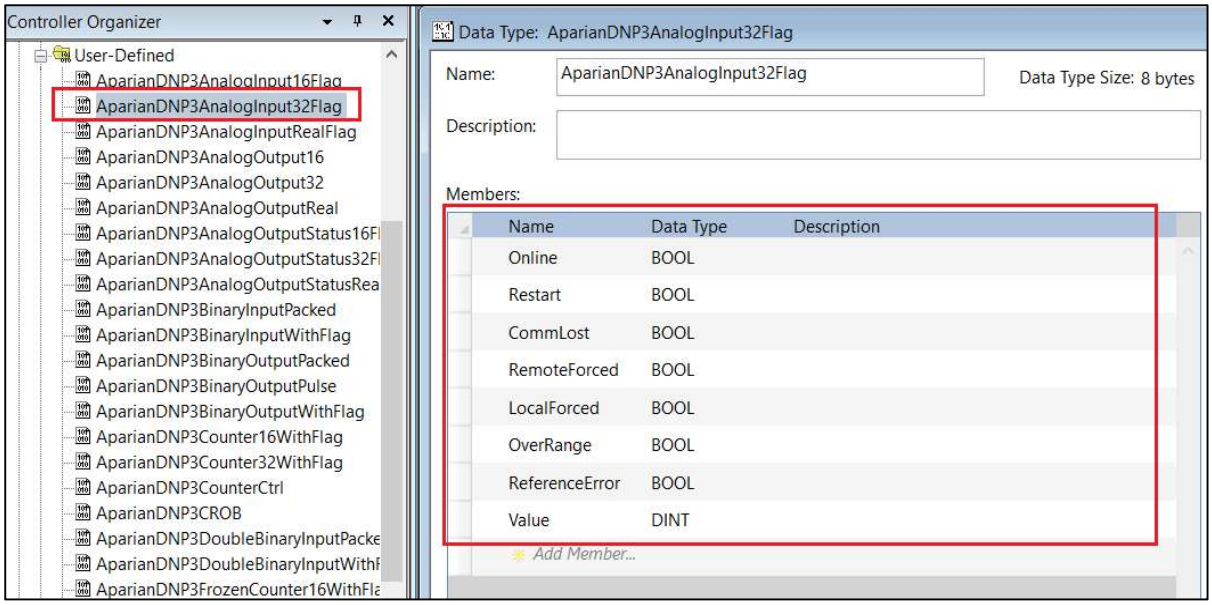


Figure 5.2. – Supported UDT for DNP3 Group 30 with Variation 1

A new tag or array must be created to match the DNP3 Group and Variation.

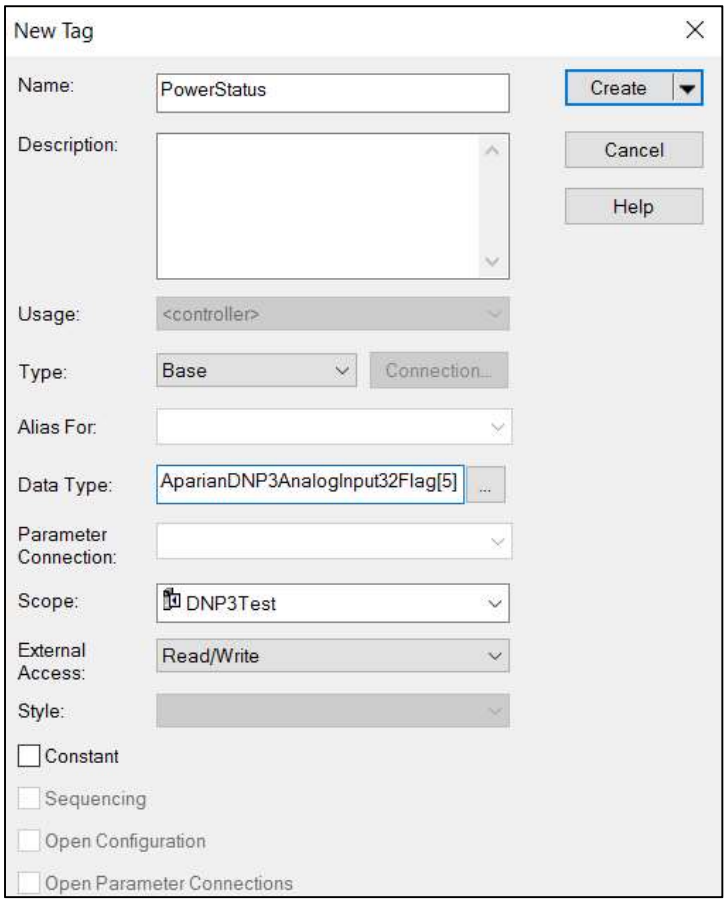


Figure 5.3. – New Tag with Supported UDT for DNP3 Group 30 with Variation 1

In Slate the Target Tag selected must be the Tag or Array with Data Type ***AparianDNP3Analog32Flag*** as shown below.

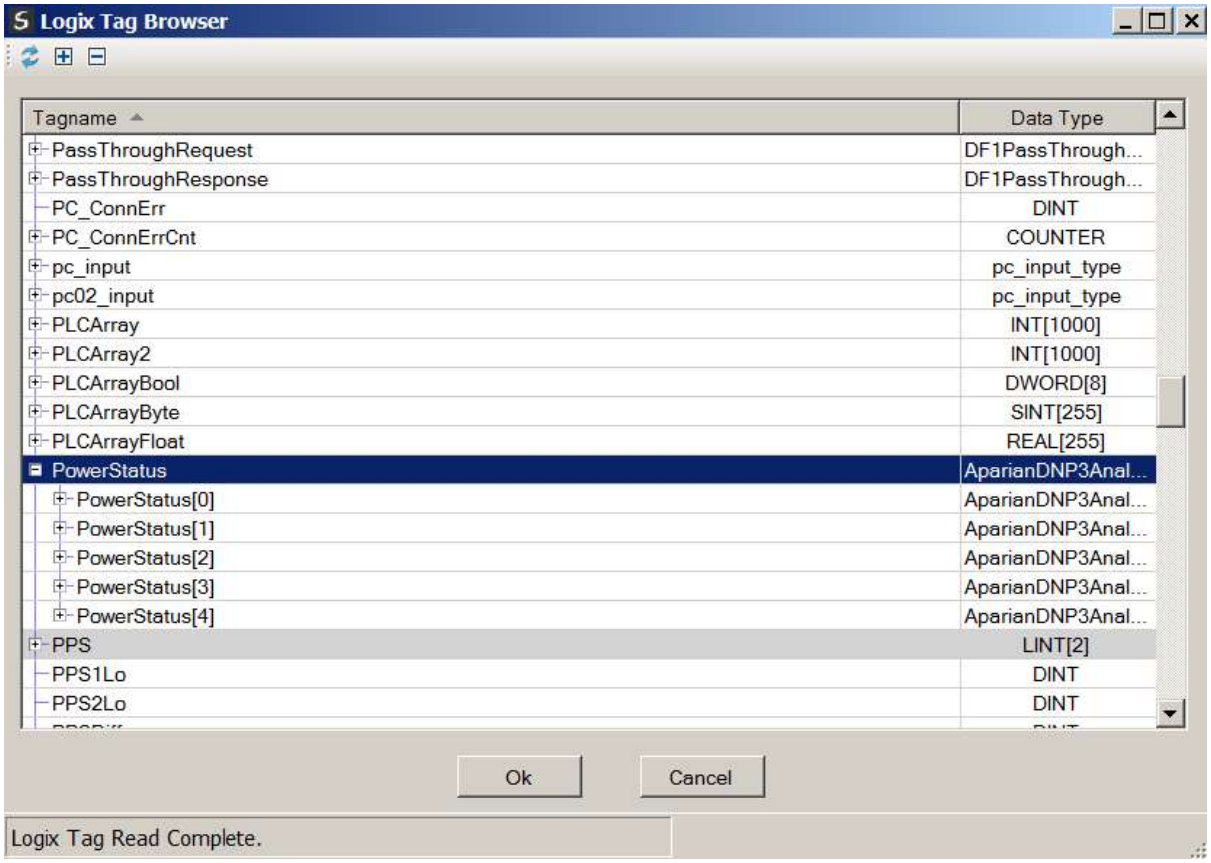


Figure 5.4. – Selecting the correct tag from Slate's Tag Browser.

The same procedure can be followed for numerous other DNP3 Group and Variation combinations.



NOTE: If the user does not use the correct UDT the DNP3 Router will either abandon the routing procedure once it detects the data types are different (the Logix Data Type Mismatch statistic will increase) or incorrect data will be received by the Logix Controller.

5.2. ANALOG/BINARY OUTPUT COMMANDS

The select/operate, direct-operate, and direct-operate with no response DNP3 application functions (which will collectively be referred to as operate commands) are command based functions. Unlike a read function these functions only execute when the DNP3 Master triggers a change (e.g. open a relay or change an analog output). These functions are typically used for Control Relay Output Blocks (CROB) and Analog Output Blocks (AOB). The three functions are described below:

Function	Description
Select/Operate	The select/operate function is a two-step operate where the Master first “Arms” the outputs with the select function before enabling the “Armed” output with the operate function.
Direct-Operate	The Direct-Operate function has a similar outcome to the Select/Operate function but is a one-step function. Thus the outputs are “Armed” and executed in the same function.
Direct-Operate with no response	The Direct-Operate with no response function is similar to the Direct-Operate but does not require an acknowledgement that the operation has been executed.

Table 5.1 – Select/Operate, Direct-operate, and Direct-Operate no reponse functions

The DNP3 Router uses a *RequestPending* bit in the Logix UDTs (refer to the example code for provided UDTs) to inform the user that either an operate request has been received (Reactive Tag Mode) or that an operate request must be executed (Scheduled Tag Mode).



NOTE: When the DNP3 Router is in Scheduled Tag Mode command functions will only be executed once the *RequestPending* bit has been set. Once the command has executed the bit will automatically be cleared. So set *RequestPending* bit only after all other values have been set.

An example of a UDT with the *RequestPending* bit is shown below:

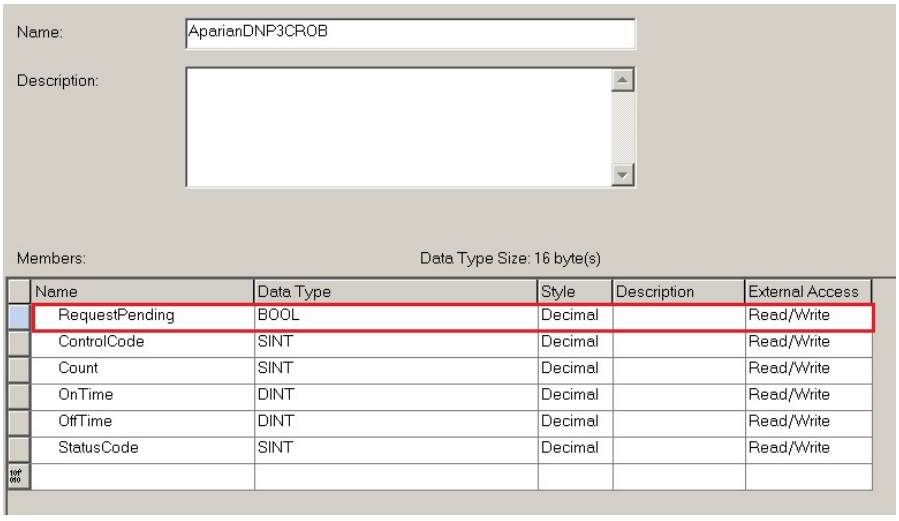


Figure 5.5 – UDT for operate commands

5.2.1. Receiving Output Commands

The Outstation DNP3 Router requires two items to be mapped for each Binary or Analog Output Command. The first being the Command (Group 12 or Group 41) and the second the Output Status (Group 10 or Group 40).

The *RequestPending* bit in the mapped Logix Tag for the control command will be set, indicating that a new operate command was received. The Outstation Controller should copy the values Command UDT to the respective Status UDT (Binary: Group 12 to 10, Analog: Group 41 to 40). Then clear the *RequestPending* bit which signals the master that the operation is complete. The Outstation Example contains AOIs that perform these tasks. Including code to pulse binary outputs. Commands with *StatusCode* other than zero should be ignored.

	Group	Variation	Index Start	Index Count	Target Name	Target Tag
	G012 BinaryOutputCommands	V01 CROB	0	5	Aparian_Demo	DNP3_OC_Binary[0]
	G010 BinaryOutputs	V02 Output Status + Flags	0	5	Aparian_Demo	DNP3_OW_Binary[0]
	G041 AnalogOutputs	V02 16-bit	0	5	Aparian_Demo	DNP3_OC_Analog16[0]
▶	G040 AnalogOutputStatus	V02 16-bit + Flag	0	5	Aparian_Demo	DNP3_OW_AnalogOutput16[0]

Figure 5.6 – Outstation Mapping for Output Commands

Care should be taken to ensure the matching Analog Variations are used with Group 40 and 41.

To ensure the command was executed, the master can either read the Output Status (Groups 10, 40) or configure an event on the Status and Command groups.

5.2.2. Sending Output Commands

When the DNP3 Router is in Scheduled (Master) mode the Logix mapped Tag will be read at the configured scheduled interval, but only once the *RequestPending* bit is set will the operate command be executed and sent to the DNP3 outstation. The automatic clearing of *RequestPending* bit provides Confirmation that the command executed correctly.

	DNP3 Function	Scan	IP Address	Node	Group	Variation	Index Start	Index Count	Target Name	Target Tag
	Sel-Op	B	192....	4	G012 BinaryOutputCom...	V01 CROB	0	5	Apari...	DNP3_MC_Binary[0]
	Read	B	192....	4	G010 BinaryOutputs	V02 Output Statu...	0	5	Apari...	DNP3_MW_Binary[0]
	Sel-Op	B	192....	4	G041 AnalogOutputs	V02 16-bit	0	5	Apari...	DNP3_MC_Analog16[0]
	Read	B	192....	4	G040 AnalogOutputStat...	V02 16-bit + Flag	0	5	Apari...	DNP3_MW_Analog16[0]

Figure 5.7 – Master Mapping for Output Commands

The master can either read the Output Status directly or process the resulting event to obtain the status of the output.

5.2.3. Control Relay Output Block (CROB) Parameters

Below is the UDT for variation 1 (CROB).

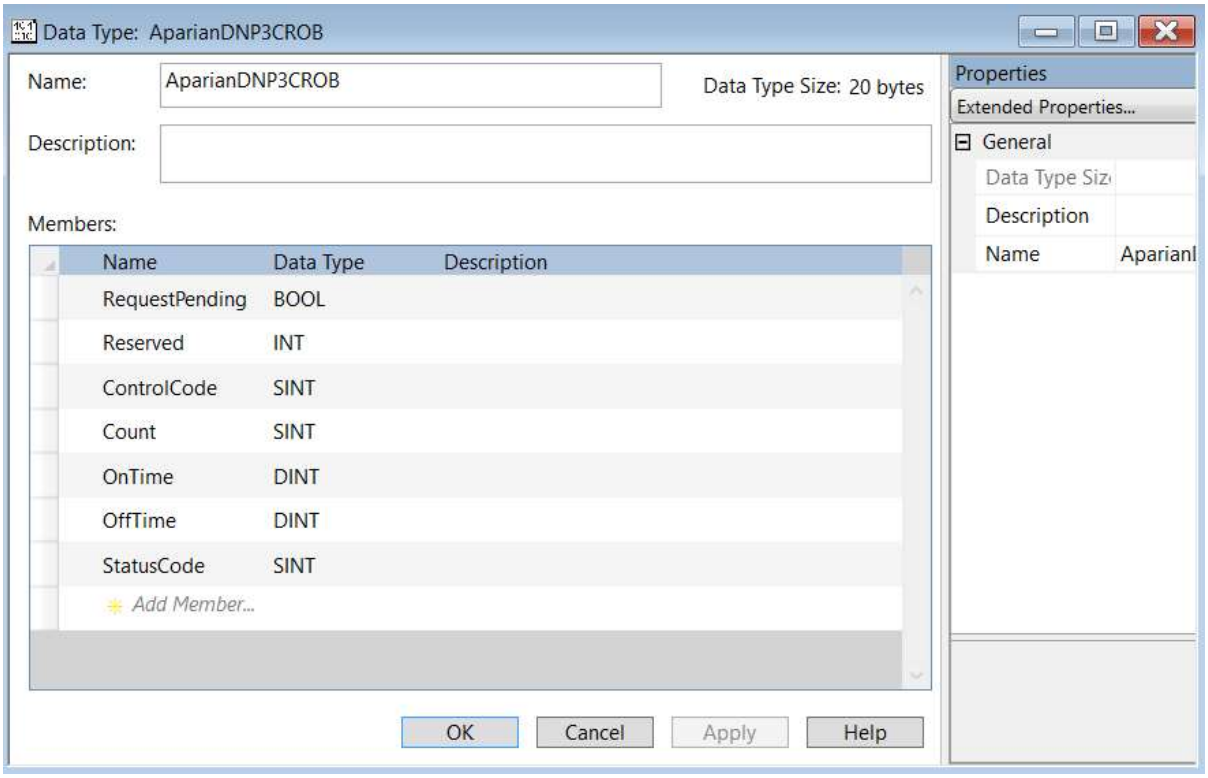


Figure 5.8 - DNP3 CROB Group Variation 1

Below is a table of the control codes that can be received:

Control Code	Description
0	NUL
1	Pulse On
2	Pulse Off
3	Latch On
4	Latch Off

Table 5.2 - DNP3 CROB Control Codes

The Count, OnTime, and OffTime elements are only used when there is a pulse command (1 or 2). The count is the amount of pulses that must be executed whilst the OnTime and OffTime is the relevant duty cycle. Refer to the Logix example code for an implemented example.

5.3. COUNTER FREEZE COMMANDS

When the DNP3 Router operates in Reactive Mode it will respond to Freeze commands from the DNP3 Master. If the DNP3 Master issues a Freeze command the Logix controller will be notified and must execute the requested command. This is done by having a Freeze Counter Control UDT which can be used by the Logix controller to take the needed action.

NOTE: The Control Tag must be named identical to that of the DNP3 Counter Tag used with the addition of "Ctrl" suffix. For example if the DNP3 Counter tag being used is named ***ErrorCounter*** then the Freeze Control Tag must be named ***ErrorCounterCtrl*** for the freeze command to operate correctly. The user must also ensure that the dimensions of the two tag arrays are the same.

The Counter control will use the *AparianDNP3CounterCtrl* UDT as shown below:

⊞ ErrorCounter	{...}	{...}		AparianDNP3Counter32WithFlag[10]
⊞ ErrorCounterCtrl	{...}	{...}		AparianDNP3CounterCtrl[10]

Figure 5.9 – Freeze Command Pair

	Group	Variation	Index Start	Index Count	Target Name	Target Tag
▶	G020 Counters	V01 32-bit + Flag	0	10		ErrorCounter[0]

Figure 5.10 – Outstation Mapping

The Control Tag will either have the Freeze bit or Freeze and Clear bits set to indicate to the Logix controller that the counter values must be copied to the DNP3 Frozen Counter Group tags and if the Counter must be cleared afterwards. Refer to the Logix Example code for an example of how this is done. The time of occurrence is the DNP3 time (Unix time in milliseconds) when the freeze command was received. This must be copied to the DNP3 Frozen Counter Group tag as well.

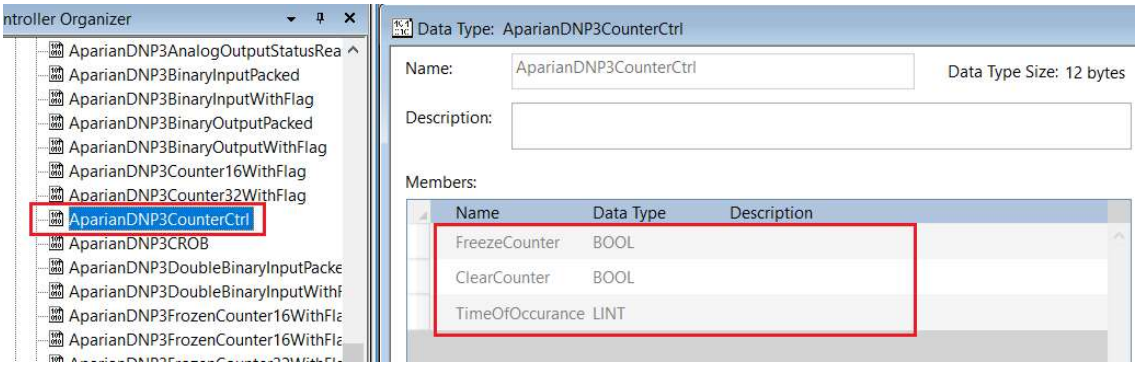


Figure 5.11 – UDT for freeze command

5.4. DNP3 EVENTS – UNSOLICITED RESPONSES

Events are generated in the Outstation and processed by the Master. Events can be grouped during the unloading process by either their assigned class or Data Type Group (e.g. Group 23 – Analog). Unloading can be initiated by the Master via a set interval poll or initiated by the Outstation via an Unsolicited Response message. The DNP3 Master controls each Outstation's ability to send Unsolicited Messages.

Unsolicited Events can be used to reduce network traffic by reducing or turning off polled data exchanges. This method is referred to as Report-By-Exception.

In Scheduled (Master) Mode, DNP3 events are passed directly to an event array in the Logix Controller. In the event that the DNP3 Module, in Master mode, loses connectivity to the Logix controller, received Events will not be marked as received and therefore will be stored in the outstation. Events do not need to be stored in the module in Scheduled Mode.

5.4.1. OUTSTATION EVENT CONFIGURATION

The configuration required from the DNP3 Router's perspective is the following:

5.4.1.1. ENABLING EVENTS

Enable events for each mapped item in the Outstation Mapping. This will enable the DNP3 Router to start reading each Logix item at an interval of 10ms to determine if there has been either a change in the status flags or if the value has changed by more than the deadband.

Logix Tag Mapping (max. of 30 items.)

	Group	Variation	Index Start	Index Count	Target Name	Target Tag	Browse	Enable Events	Event Variation	DB
▸	G030 AnalogIn...	V05 Single...	0	5			...	☑	V07 Single Float + Time	2
*										

Figure 5.12 – Enable Events

5.4.1.2. SELECTING AN EVENT VARIATION

The required event variation must be selected. Note that if “with Time” is selected the logging of an event will be timestamped.

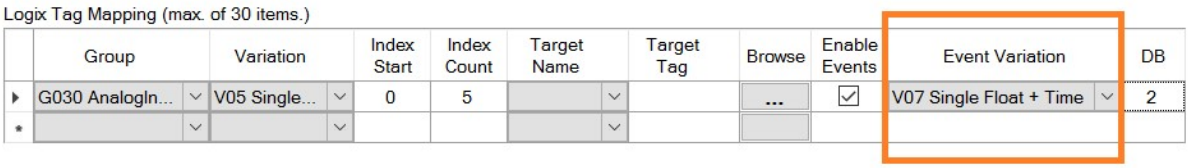


Figure 5.13 – Select variation

5.4.1.3. SELECTING A DEADBAND (DB)

The change deadband must be selected. When the value changes by more than the deadband an event is logged.

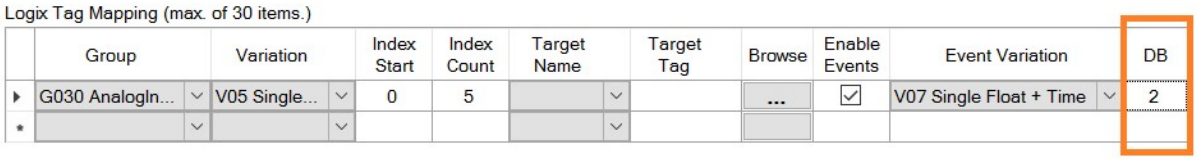


Figure 5.14 – Select Deadband

5.4.1.4. SELECTING THE EVENT CLASS

The Event Class for each group must be selected. This will be used by the Master to enable unsolicited responses.

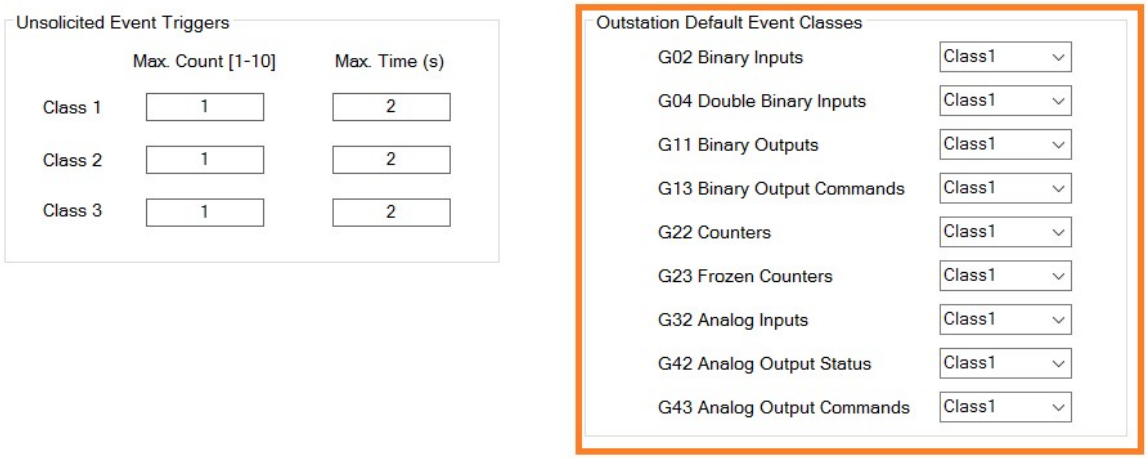


Figure 5.15 – Select Event Class

5.4.1.5. SELECTING THE UNSOLICITED EVENT TRIGGERS

The Event triggers can be used by the DNP3 Router (in Outstation Mode) to limited the amount of individual unsolicited responses sent to the DNP3 Master. To reduce traffic the user can set limits which once reached will only send an unsolicited response.

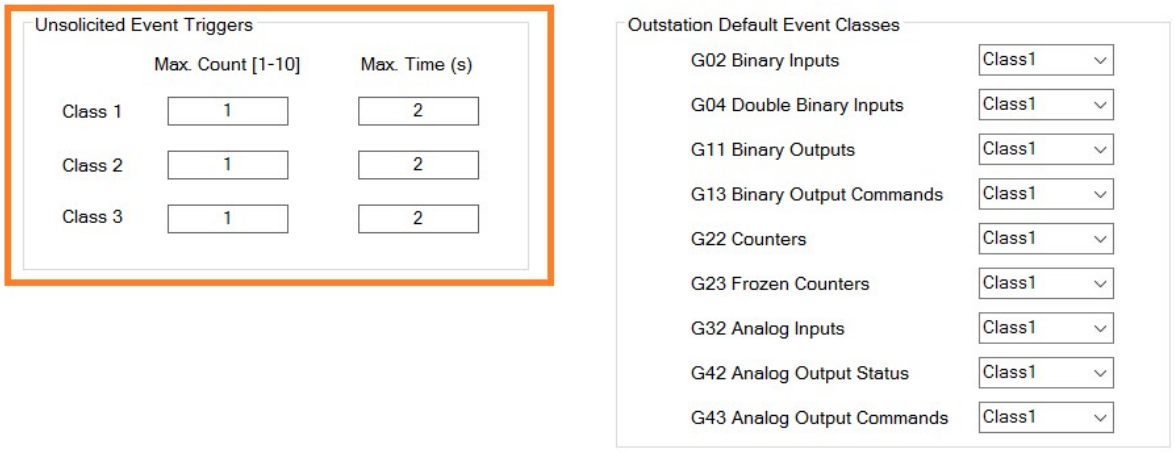


Figure 5.16 – Selecting Event Triggers

5.4.2. MASTER EVENT UNLOADING

The DNP3 Router in Master mode, can extract or receive DNP3 events from various DNP3 Outstations.

The Module does not provide priority to unloading events, it cycles through the classes and empties all the buffers before restarting.

The setup and extracting of DNP3 events from DNP3 outstations is explained in section 3.6.2. This section will focus on the event unloading from the DNP3 Router into a Logix Controller.

The Event unload order is such to unload the oldest event first. Events are unloaded into a Logix UDT array. This is a circular buffer arrangement where the DNP3 Master will start writing at array index 0 and increment the array index each time a new event is written into the Logix Controller Master Event Tag array. Events that are not processed in the Logix Event Buffer Array will be overwritten. This Master Event Index (which shows the index to which the next event will be written) can be found in the Logix Input Assembly as well as the General Status page of the module in Slate.



NOTE: Downloading updated configuration to the DNP3 Module resets the Event Buffer Index to zero.

The structure of the UDT is provided below.

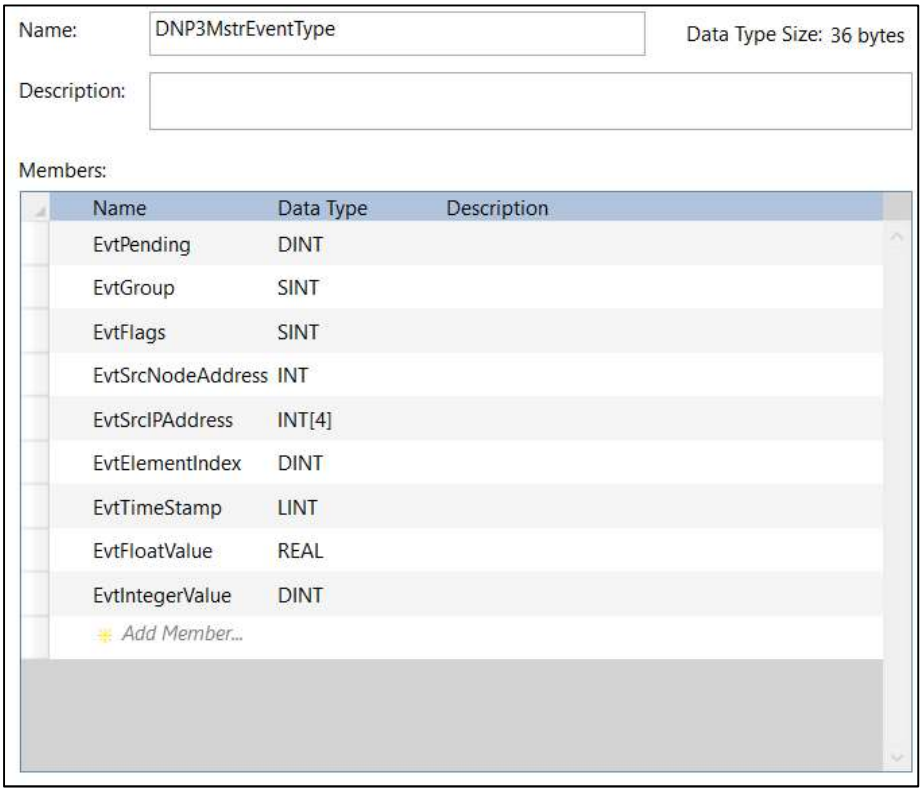


Figure 5.17 – Master Event Logix UDT

Below is an explanation of each element in the structure:

Attribute	Description
EvtPending	This bit is set when the event is written into the controller. The application code can use this bit, and subsequently clear it, when the event has been processed.
EvtGroup	This is the DNP3 group which reported the event (e.g. Group 32 – Analog Input Event)
EvtFlags	Each event group has a set of status flags which indicates the states, quality, etc. of the variable in the event. See the appendix for an explanation of each Group's set of flags.
EvtSrcNodeAddress	The Node Address of the Outstation which reported the event
EvtSrcIPAddress	The IP Address of the Outstation which reported the event (note this is only valid when the DNP3 Router is setup for either TCP or UDP).
EvtElementIndex	This is the element offset which generated the event (Analog Input 5).
EvtTimeStamp	This is the time (in the Outstation) when the event occurred. Note that the appropriate variation must be selected in the DNP3 Outstation to allow for reporting of event time.
EvtFloatValue	When the event value is a 32-bit float the value will appear in this attribute.
EvtIntegerValue	When the event value is a 8-bit, 16-bit, or 32bit integer the value will appear in this attribute.

Table 5.3 – Master Event Logix UDT

Each time a new event is written into the Logix controller, bit 0 of the EvtPending DINT will be set to 1. This is an indication to the Logix application code that an event has not yet been processed. It is recommended to clear this bit once the event has been processed to avoid duplicate processing of events.

NOTE: Refer to the Logix example code which provides a mechanism to extract the DNP3 Events from the Logix Master Events Tag.

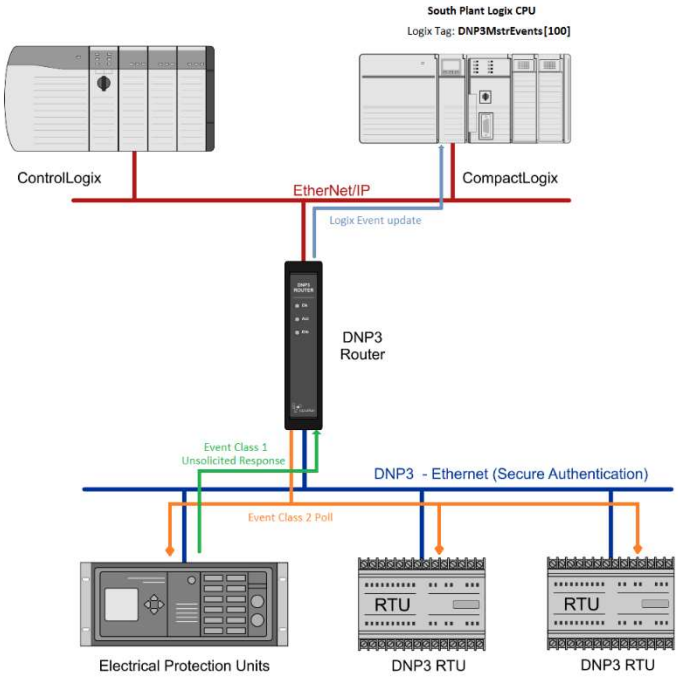


Figure 5.18 – DNP3 Master Event Unloading

Refer to the Logix Master Example code which can be found on the website at the following link http://www.aparian.com/products/dnp3router. The Logix Master Example code provides UDTs and AOIs to process events in the Master Event Buffer and copy the values to the respective static DNP3 objects.

5.5. REPORT-BY-EXCEPTION

Reporting by Exception can considerably reduce network traffic by eliminating or reducing continuous polling.

Reporting by exception can be configured by, enabling Events in each Outstation for all relevant groups. The DNP3 Master needs to have Events enabled in Unsolicited Class mode. At least one Logix Tag Mapping is required to set the Logix Target. This item's scan interval can be set to a large number.

Refer to the Logix Master Example (***DNP3MasterExample***) code which can be found on the website at the following link http://www.aparian.com/products/dnp3router. The Logix Master Example code provides UDTs and AOIs to process events in the Master Event Buffer and copy the values to the respective static DNP3 objects.

5.6. OUTSTATION TIME NEEDED

The DNP3 Router (when in outstation mode) can be forced to set the Time Needed bit in the DNP3 indicators when responding to a request. This will inform the DNP3 Master that it must write the current time to the DNP3 Outstation. When the DNP3 Router powers up the Time Needed bit will by default be set. The Time Needed is force by using a CIP explicit message from Logix.

The message instruction should be setup as follows:

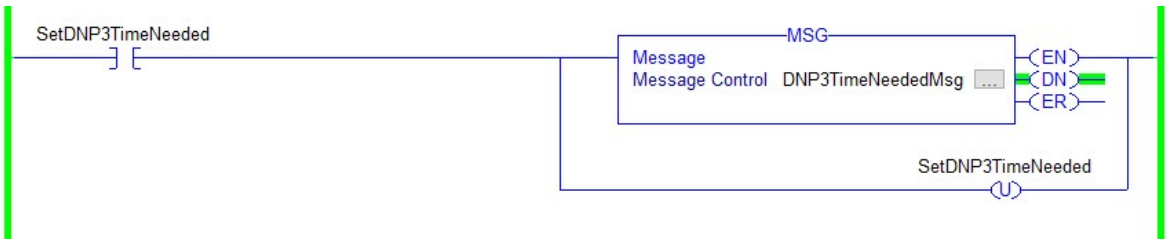


Figure 5.19 - Message Instruction

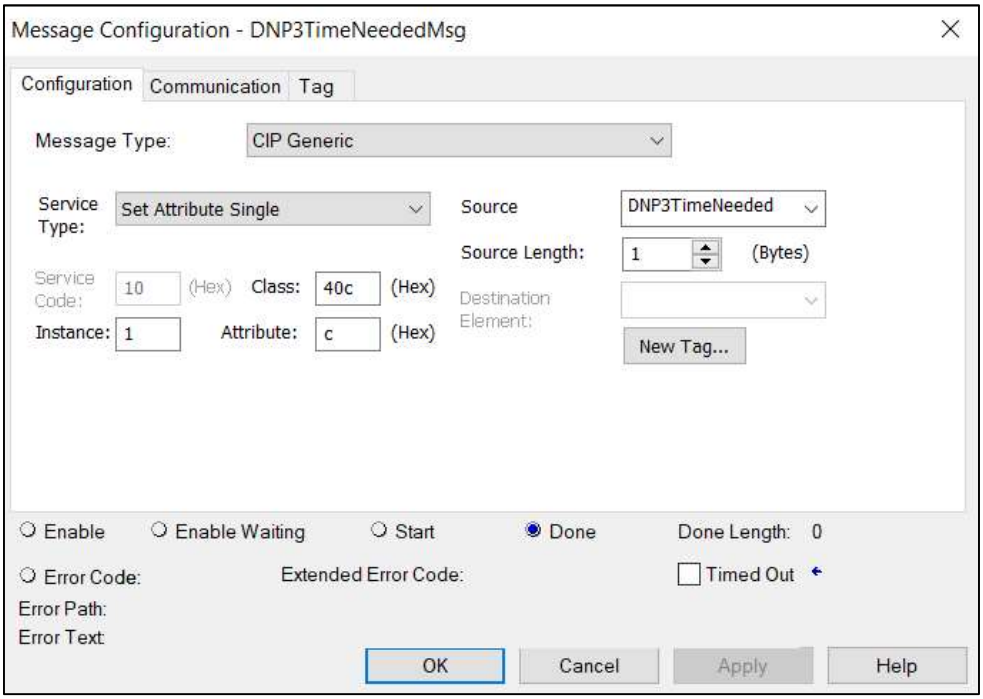


Figure 5.20 - Message Configuration

Parameter	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	10 (Hex) – Set Single Attribute
Class	40C (Hex)
Instance	1
Attribute	C (Hex)
Source Element	SINT
Source Length	1
Destination Element	None

Table 5.4 - Message Configuration Paramaters

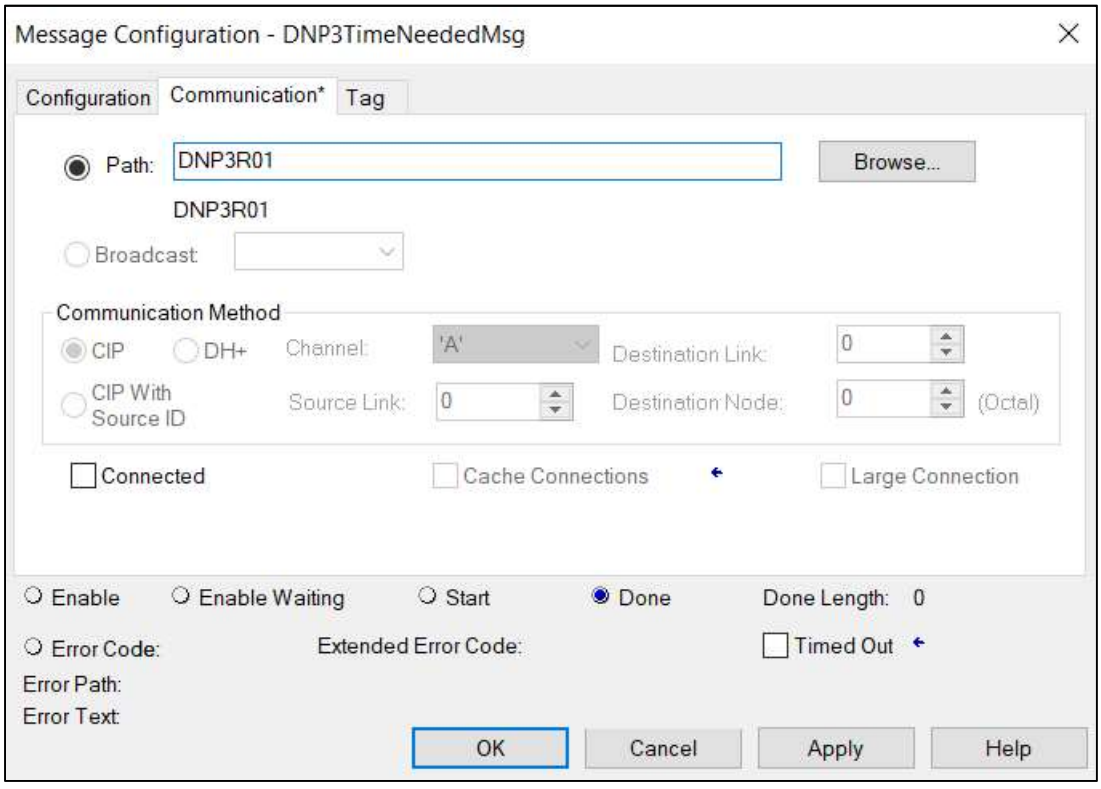


Figure 5.21 - Messsage Configuration - Communication

The Path must be configured to that of the DNP3 Router. If the DNP3 Router has been added in the I/O tree, then the Browse option can be used to select the path.
Alternatively, enter the CIP path in the format :

1,X,2,IP , where
1 represents the backplane port,
X represents the slot of the Ethernet bridge module,
2 represents the Ethernet port of the Ethernet bridge module and

IP represents the IP address of the DNP3 Router.
e.g. **1,1,2,192.168.1.41**

The request tag (e.g. ***DNP3TimeNeeded***) should be configures as follows:



Figure 5.22 - Unscheduled Message Request Tag

Parameter	Description
DNP3TimeNeeded	0 – Force the Time Needed bit in the DNP3 Indicators to **off** 1 – Force the Time Needed bit in the DNP3 Indicators to **on**

Table 5.5 - Unscheduled Message Request Parameters

6. SECURITY

DNP3 offers Secure Authentication for links at risk of being attacked. There are various Key Change methods, Message Authentication Code (MAC) algorithms, and Authentication methods provided in the DNP3 protocol specification.

Various keys are used in DNP3 Secure Authentication. **Session keys** are used most frequently as it is used for Authentication of the requests. These keys are updated by the DNP3 master at a certain interval or every time there has been a message failure. The DNP3 master encrypts these keys before sending them across the wire using the Key Wrap Algorithm selected and the **Update key**. The Update Key can be updated in numerous ways (including sending it across the wire with another set of Keys encrypting that message). The **Transfer Key** is used when the user wants to remotely change the update key of a DNP3 Router outstation. The Transfer Key is used to encrypt the Update Key being sent over the DNP3 network to the remote DNP3 Router Outstation.

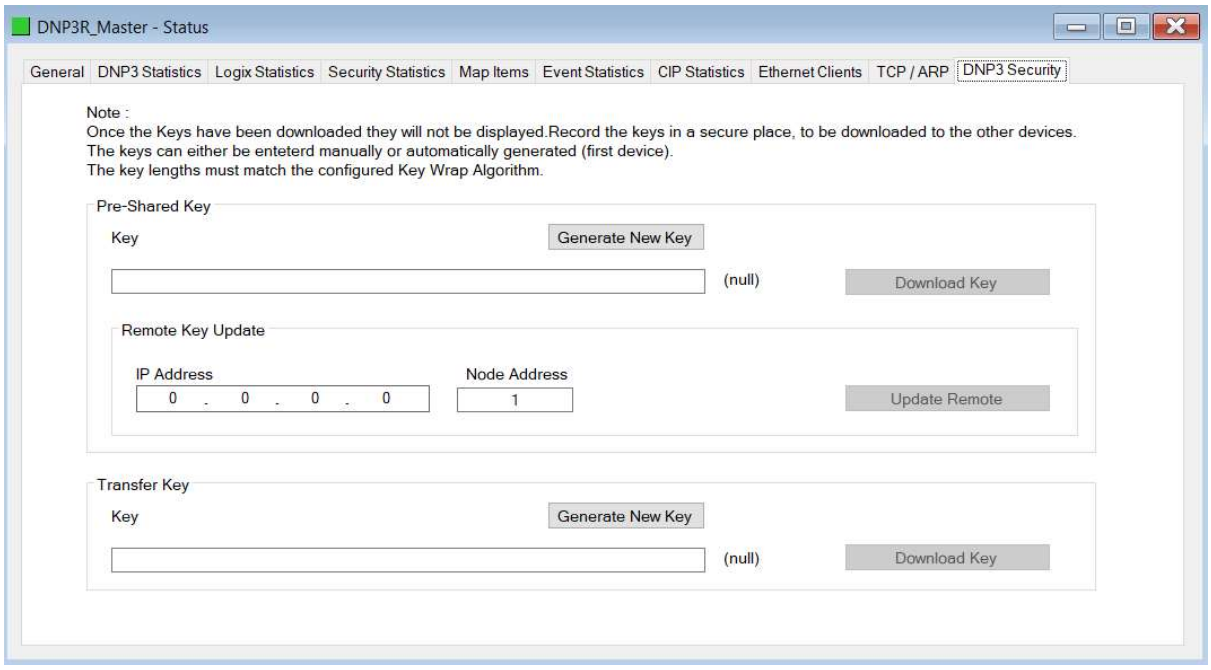


Figure 6.1 - DNP3 Router key update method.

The module supports all DNP3 MAC algorithms and Key Wrap algorithms. The module also supports Aggressive Authentication mode which reduces the amount of traffic on the network (which could be required on busy networks or serial communication).

NOTE: The user needs to ensure that the other DNP3 device with which it is communicating has the same security options configured as the DNP3 Router and that the selected options are supported in the device.

6.1. KEY UPDATES

The DNP3 Router allows the user to change the update key in one of two ways:

6.1.1. LOCAL KEY UPDATE

With this method the user will need to be connected to the actual DNP3 Router and will download the key directly from the user's PC to the module (over Ethernet).

In Slate the user can write the Update Key into the DNP3 Router module using the Key tab in the Online Status window. The key entered must match the Key Wrap Algorithm selected. Thus, if AES-128 Key Wrap was selected the Update Key must be 128-bit (16 bytes) long. If AES-256 Key Wrap was selected, the Update Key must be 256-bit (32 bytes) long. The user can either enter a predetermined hexadecimal code of create a new code in Slate as shown below. This key is encrypted and sent to the DNP3 Router where it is saved into the NV memory of the module.



NOTE: The Key update method in Slate is a **write-only** function. Thus, once the key has been downloaded the user will not be able to view the key again. The user must make provision to document or save the key in a secure manner.



NOTE: The other DNP3 device that is going to be communicated to must have the same Update Key as that of the DNP3 Router. Failing to do this will result in failed data exchange for critical messages.

The user can also change the update key from a Logix controller by using a MSG instruction. Note that unlike the key update from Slate (which is downloaded securely), the update from Logix will not be secure and if the network is exposed an attacker will be able to see the update key.



NOTE: The user will **NOT** be able to change the update key using the unsecure method unless the *Allow Unsecure Key Download* option has been selected in the Security tab of the Configuration form.

Below are the MSG Instruction parameters to be used as well as the structure:

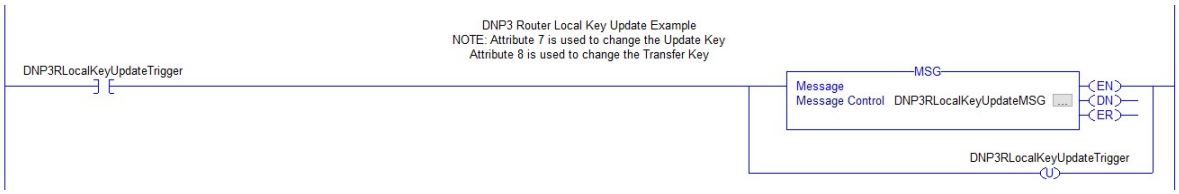


Figure 6.2. - Message Instruction

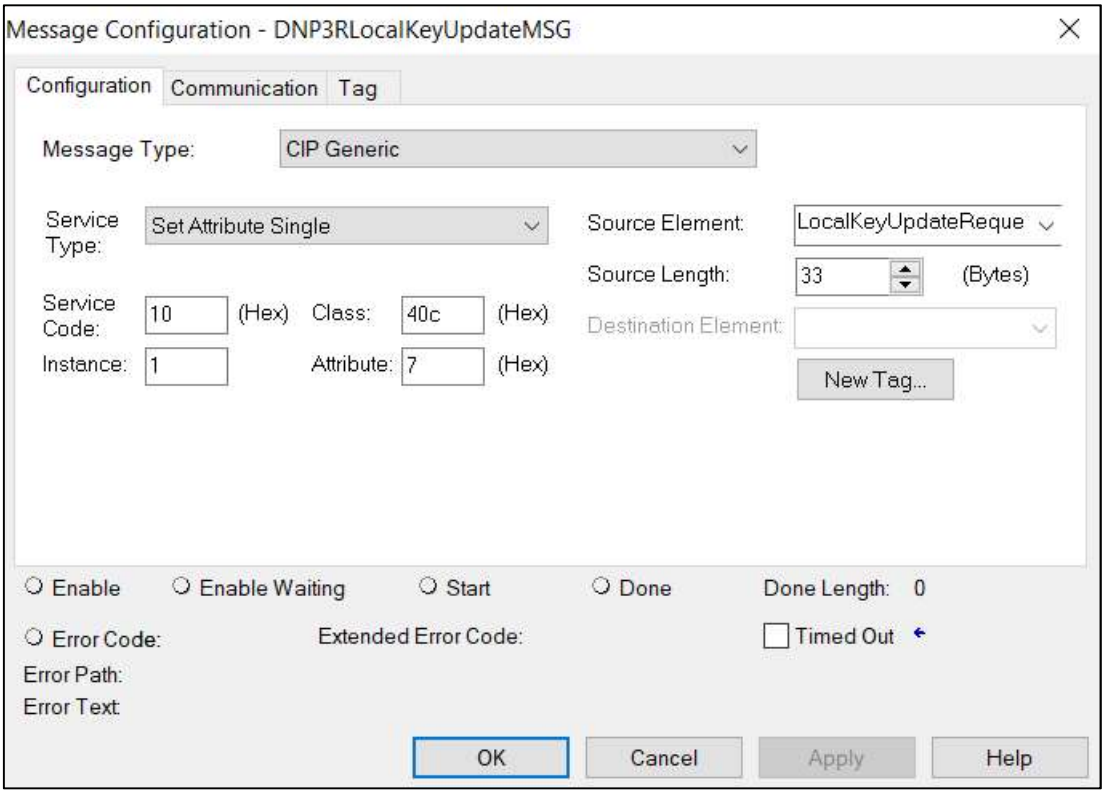


Figure 6.2. - Message Configuration

Parameter	Description
Message Type	CIP Generic
Service Type	Set Attribute Single
Service Code	10 (Hex) – Set Single Attribute
Class	40C (Hex)
Instance	1
Attribute	7 – Update Key 8 – Transfer Key
Source Element	The request tag instance. Must follow the structure of the ***AparianDNP3LocalKeyUpdateRequest*** UDT.
Source Length	33

Destination Element	N/A

Table 6.1. - Message Configuration Paramaters

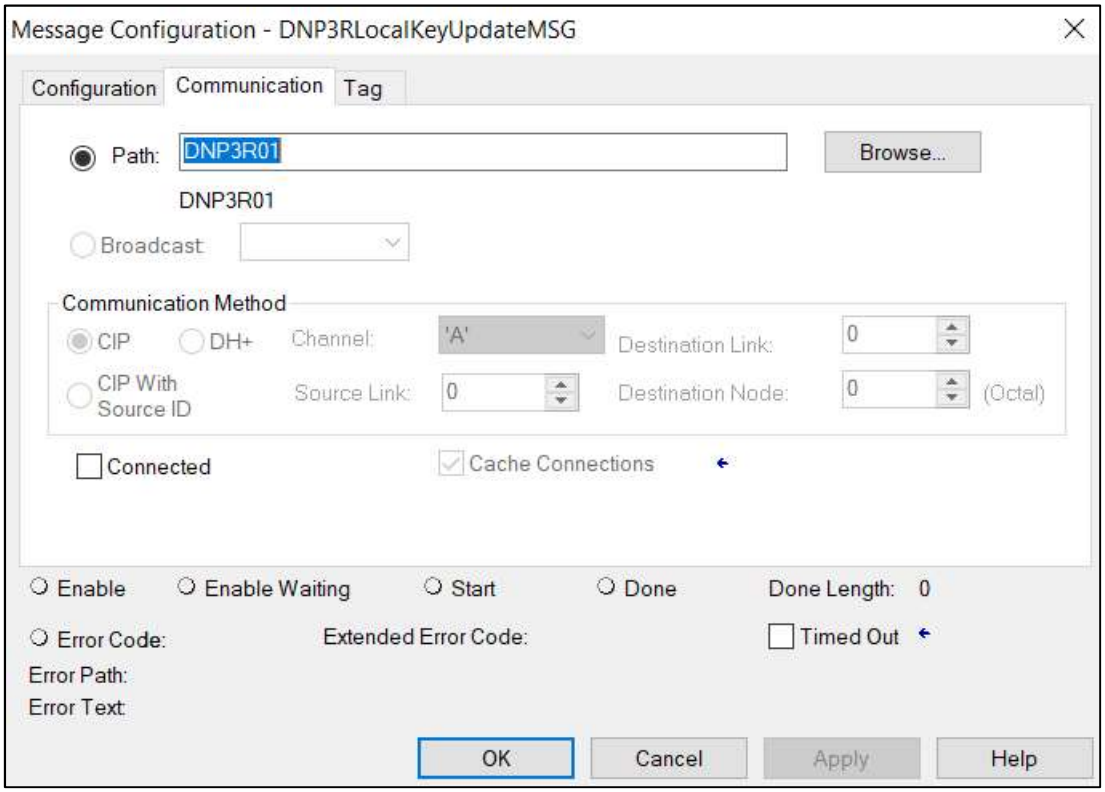


Figure 6.3. - Messsage Configuration - Communication

The Path must be configured to that of the DNP3 Router. If the DNP3 Router has been added in the I/O tree, then the Browse option can be used to select the path.
Alternatively, enter the CIP path in the format :

1,X,2,IP , where
1 represents the backplane port,
X represents the slot of the Ethernet bridge module,
2 represents the Ethernet port of the Ethernet bridge module and
IP represents the IP address of the DNP3 Router.
e.g. **1,1,2,192.168.1.41**

The request tag (e.g. ***AparianDNP3RemoteKeyUpdateRequest***) should be configures as follows:

LocalKeyUpdateRequest	{...}	{...}		AparianDNP3LocalKeyUpdateRequest
LocalKeyUpdateRequest.KeyLength	16		Decimal	SINT
LocalKeyUpdateRequest.KeyData	{...}	{...}	Decimal	SINT[32]

Figure 6.4. – Remote Key Update Message Request Tag

Parameter	Description
Key Length	Size of the key data to follow.
Key Data	The data for the key to be updated.

Table 6.2. - Remote Key Update Message Request Parameters

Similar to the update key, the transfer key can be changed from Slate (securely) or from Logix (not-secured). The only difference is that the user will use attribute 8 to set the Transfer key and attribute 7 (shown previously) for setting the update key.



NOTE: The user will **NOT** be able to change the transfer key using the unsecure method unless the *Allow Unsecure Key Download* option has been selected in the Security tab of the Configuration form.

6.1.2. Remote Key Update

The remote key update method allows the user to remotely change the update key (used to create the session keys for authentication) by encrypting the update key with the transfer key. The user will not be able to update the transfer key remotely (it will need to be downloaded to the module directly from the source).



NOTE: The user will **NOT** be able to remotely change the update key unless the *Key Change Method* option in the Security tab of the Configuration form has been set to *Pre-Shared Key - Allow Remote Update* for both DNP3 Router Master and Outstation.

The DNP3 Router can operate in one of two Master modes when the Update keys are changed remotely.

Operating Mode	Update Key Change Description
Scheduled	Once the transfer key has been downloaded the user can click the **Update Remote** button in the DNP3 Security tab of the online status form in Slate. This will inform the DNP3 Master to automatically change the update keys in each outstation mapped.
Unscheduled	In unscheduled mode the user will need to manually change the key in each outstation. Once the transfer key has been downloaded the user can click the **Update Remote** button in the DNP3 Security tab of the online status form in Slate. The user will need to provide the IP address (if the Ethernet-TCP/UDP protocol has been selected) as well as the Node address of the outstation who's update key must be changed.

Table 6.3. – Operating mode for Key updates



NOTE: The other DNP3 router will not be able to remotely change the update key if the transfer keys of the master and the outstation do not match.

The remote update key method can also be done from Logix controller using the below message instruction. Note that unlike the key update from Slate (which is downloaded securely), the update from Logix will not be secure and if the network is exposed an attacker will be able to see the update key.

Below are the MSG Instruction parameters to be used as well as the structure:

The message instruction should be setup as follows:

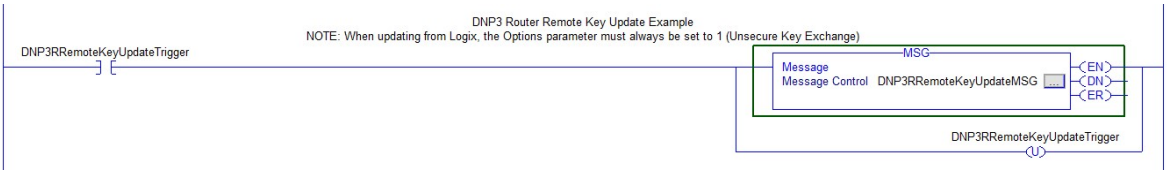


Figure 6.6. - Message Instruction

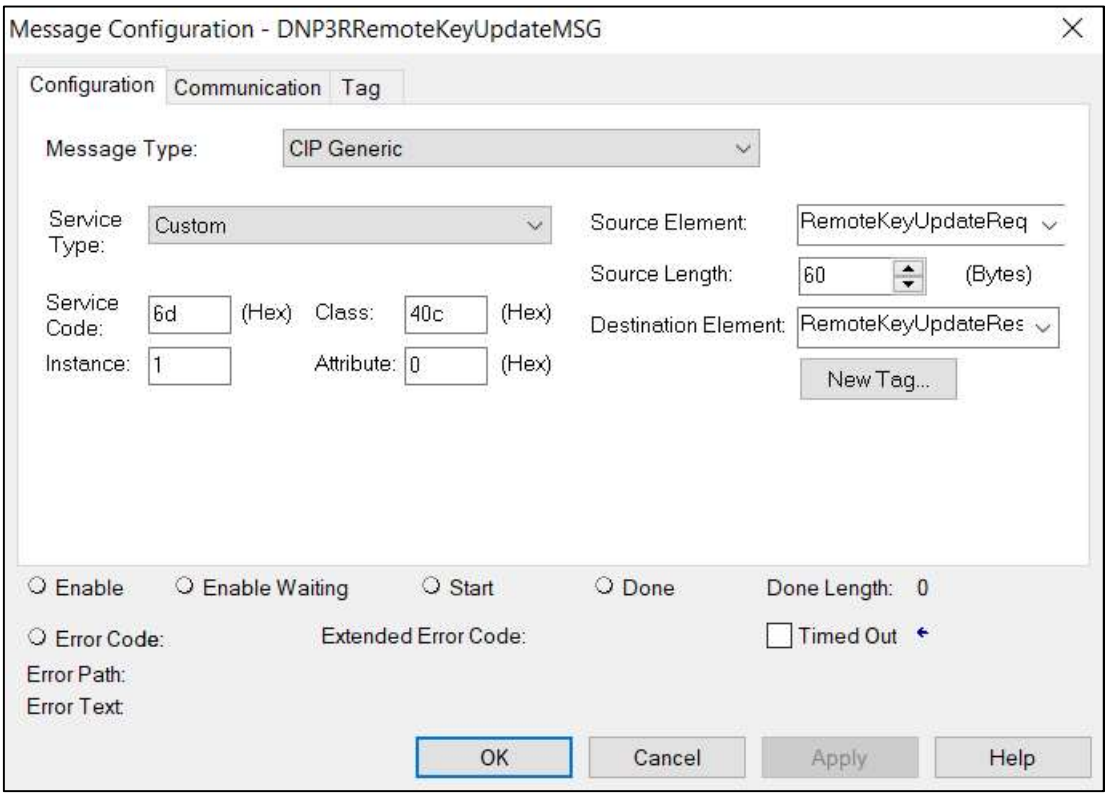


Figure 6.7. - Message Configuration

Parameter	Description
Message Type	CIP Generic
Service Type	Custom
Service Code	6D (Hex) – Remote Key Update
Class	40C (Hex)

Instance	1
Attribute	0
Source Element	The request tag instance. Must follow the structure of the ***AparianDNP3RemoteKeyUpdateRequest*** UDT.
Source Length	60
Destination Element	The response tag instance (DINT).

Table 6.4. - Message Configuration Paramaters

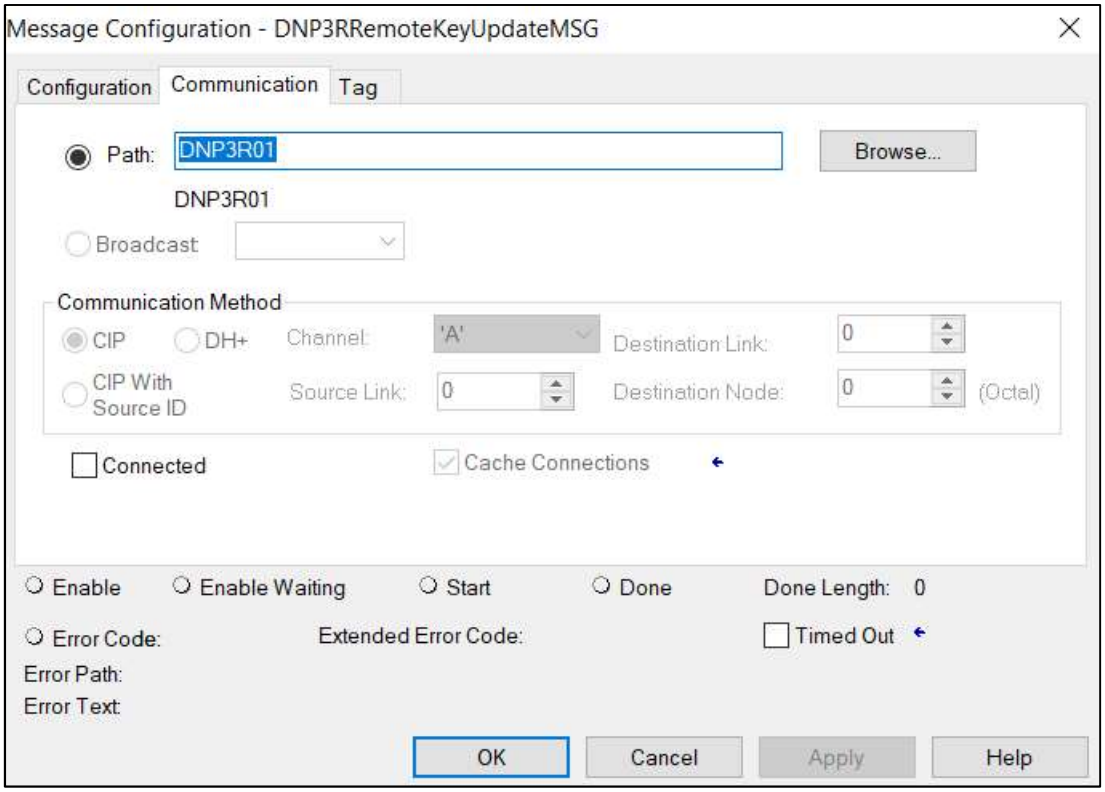


Figure 6.8. - Messsage Configuration - Communication

The Path must be configured to that of the DNP3 Router. If the DNP3 Router has been added in the I/O tree, then the Browse option can be used to select the path.
Alternatively, enter the CIP path in the format :

1,X,2,IP , where
1 represents the backplane port,
X represents the slot of the Ethernet bridge module,
2 represents the Ethernet port of the Ethernet bridge module and
IP represents the IP address of the DNP3 Router.
e.g. **1,1,2,192.168.1.41**

The request tag (e.g. ***AparianDNP3RemoteKeyUpdateRequest***) should be configures as follows:

RemoteKeyUpdateRequest	{...}	{...}		AparianDNP3RemoteKeyUpdateRequest
RemoteKeyUpdateRequest.Command	1		Decimal	SINT
RemoteKeyUpdateRequest.Option	1		Decimal	SINT
RemoteKeyUpdateRequest.DestinationNode	3		Decimal	INT
RemoteKeyUpdateRequest.IPAddress	{...}	{...}	Decimal	INT[4]
RemoteKeyUpdateRequest.IPAddress[0]	192		Decimal	INT
RemoteKeyUpdateRequest.IPAddress[1]	168		Decimal	INT
RemoteKeyUpdateRequest.IPAddress[2]	1		Decimal	INT
RemoteKeyUpdateRequest.IPAddress[3]	222		Decimal	INT
RemoteKeyUpdateRequest.KeyData	{...}	{...}	Decimal	SINT[255]

Figure 6.9. – Remote Key Update Message Request Tag

Parameter	Description
Command	One of two commands can be selected: **0** – Update Scheduled Clients **1** – Update Unscheduled Client
Option	One of two options can be selected: **0** – Secure Key Exchange (not relevant for Logix MSG) **1** – Unsecure Key Exchange
Destination Node	When selecting Update Unscheduled Client Command this parameter will be used to indicate the DNP3 outstation Node number.
IP Address	When selecting Update Unscheduled Client Command this parameter will be used to indicate the DNP3 outstation IP Address (when using TCP/UDP).
Key Data	SINT[0 – 14] – Reserved SINT[15] – Key length SINT[16-47] – Key Data

Table 6.5. - Remote Key Update Message Request Parameters

RemoteKeyUpdateResponse	0		Decimal	DINT

Figure 6.10. - Remote Key Update Message Response Tag

Parameter	Description
DNP3 Indicators	These 16bits will provide return information of the remote DNP3 device. Refer to the DNP3 documentation in the Additional information section. Bit 0 – Broadcast Bit 1 – Class 1 events Bit 2 – Class 2 events Bit 3 – Class 3 events Bit 4 – Need Time

	Bit 5 – Local control Bit 6 – Device trouble Bit 7 – Device restart Bit 8 – Function code not supported Bit 9 – Object unknown Bit 10 – Parameter error Bit 11 – Event buffer overflow Bit 12 – Already executing Bit 13 – Configuration corrupt Bit 14 – Reserved Bit 15- Reserved

Table 6.6. - Remote Key Update Message Response Parameters

7. DIAGNOSTICS

7.1. LEDS

The module provides three LEDs for diagnostics purposes as shown in the front view figure below. A description of each LED is given in the table below.



Figure 7.1 - DNP3 Router front view

LED	Description
Ok	The module's Ok LED will provide information regarding the system-level operation of the module. Thus if the LED is red then the module is not operating correctly. For example if the module application firmware has been corrupted or there is a hardware fault the module will have a red Module LED. If the LED is green then the module has booted and is running correctly.
Act	The activity LED is used for the RS232 serial port. Every time there is a successful DNP3 routing transaction the LED will flash green. The LED will flash red if the routing was unsuccessful (e.g. failed checksum).
Eth	The Ethernet LED will light up when an Ethernet link has been detected (by plugging in a connected Ethernet cable). The LED will flash every time traffic was detected.

Table 7.1 - Module LED operation

7.2. MODULE STATUS MONITORING IN SLATE

The DNP3 Router can provide a range of statistics which can assist with module operation, maintenance, and fault finding. The statistics can be accessed in full by Slate or using the web server in the module.

To view the module's status in the Aparian-Slate environment, the module must be online. If the module is not already Online (following a recent configuration download), then right-click on the module and select the *Go Online* option.

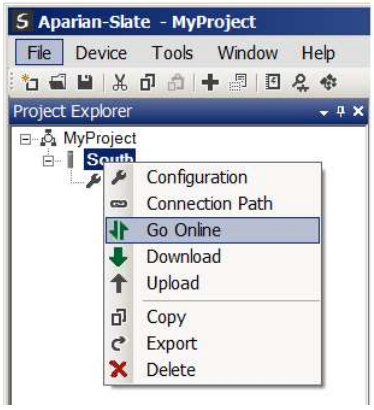


Figure 7.2. - Selecting to Go Online

The Online mode is indicated by the green circle behind the module in the Project Explorer tree.

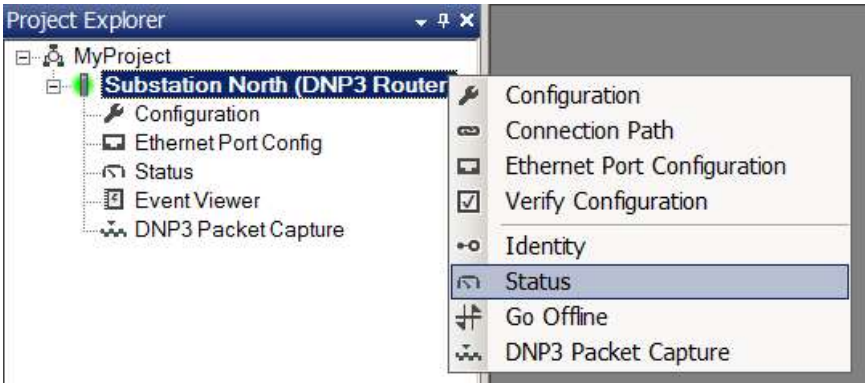


Figure 7.3. - Selecting online Status

The Status monitoring window can be opened by either double-clicking on the *Status* item in the Project Explorer tree, or by right-clicking on the module and selecting *Status*.

The status window contains multiple tabs to display the current status of the module.

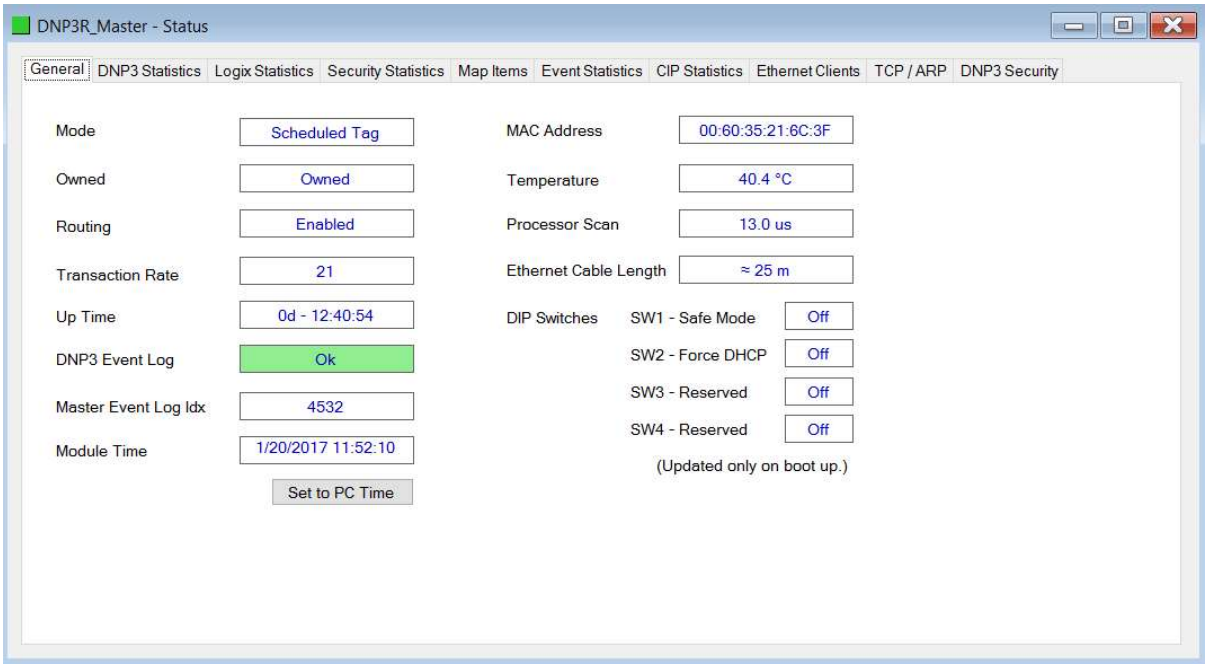


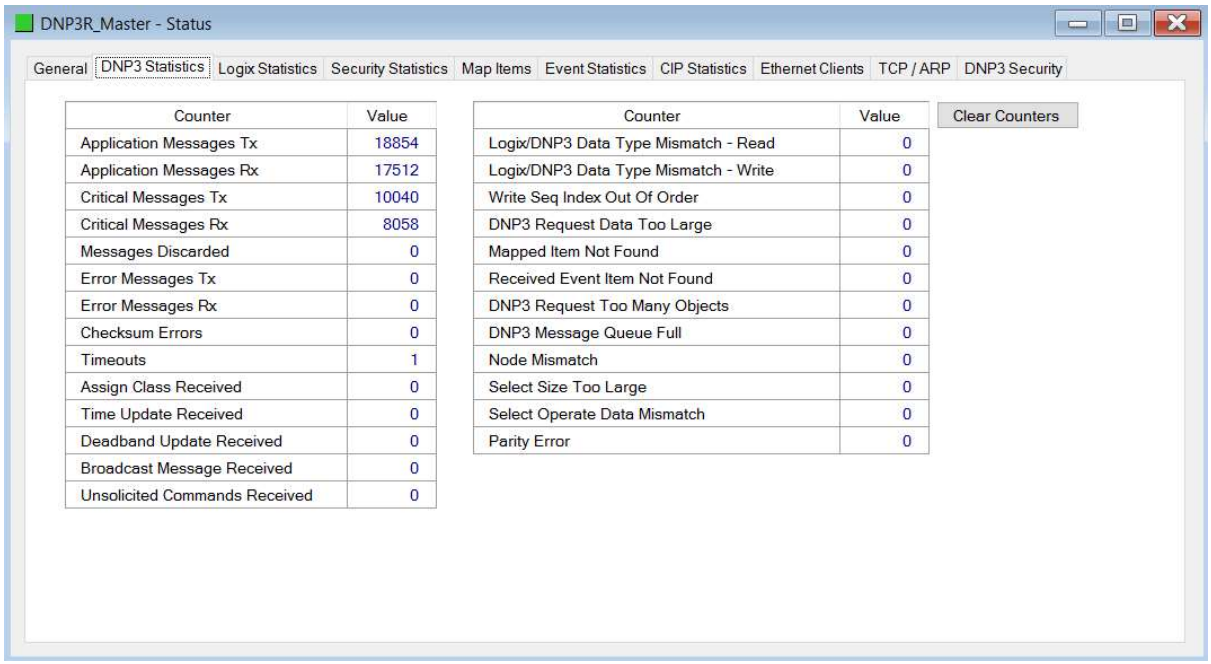
Figure 7.4. - Status monitoring - General

The General tab displays the following general parameters and can also be used to set the module time to the PC time:

Parameter	Description
Mode	Indicates the current operating mode: Transparent, Reactive Tag, Scheduled Tag, or Unscheduled.
Owned	Indicates whether or not the module is currently owned (Class 1) by a Logix controller.
Routing	Indicates whether the routing of module is enabled or inhibited. The routing operation can be inhibited in the output assembly of the module.
Transaction Rate	The transaction rate is the number of DNP3 messages per second that the module is currently routing.
Up Time	Indicates the elapsed time since the module was powered-up.
DNP3 Event Log	This is the current status of the DNP3 Event Log. It will indicate if there was a fault whilst loading the DNP3 Event Log or if there is an overflow on any of the Event Buffers.
Master Event Log Index	The Master Event Tag UDT array index number where the next event received from the master will be unloaded.

Module Time	Indicates the module's internal time. The module time is stored in UTC (Universal Coordinate Time) but displayed on this page according to the local PC Time Zone settings.
MAC Address	Displays the module's unique Ethernet MAC address.
Temperature	The internal temperature of the module.
Processor Scan	The amount of time (microseconds) taken by the module's processor in the last scan.
DIP Switch Position	The status of the DIP switches when the module booted. Note that this status will not change if the DIP switches are altered when the module is running.

Table 7.2 - Parameters displayed in the Status Monitoring – General Tab



Counter	Value
Application Messages Tx	18854
Application Messages Rx	17512
Critical Messages Tx	10040
Critical Messages Rx	8058
Messages Discarded	0
Error Messages Tx	0
Error Messages Rx	0
Checksum Errors	0
Timeouts	1
Assign Class Received	0
Time Update Received	0
Deadband Update Received	0
Broadcast Message Received	0
Unsolicited Commands Received	0

Counter	Value
Logix/DNP3 Data Type Mismatch - Read	0
Logix/DNP3 Data Type Mismatch - Write	0
Write Seq Index Out Of Order	0
DNP3 Request Data Too Large	0
Mapped Item Not Found	0
Received Event Item Not Found	0
DNP3 Request Too Many Objects	0
DNP3 Message Queue Full	0
Node Mismatch	0
Select Size Too Large	0
Select Operate Data Mismatch	0
Parity Error	0

Figure 7.5. - Status monitoring – Transactions

The Transactions tab displays the statistics associated with the following:

- DNP3 messages
- Module error statistics

Statistic	Description
Application Messages Tx	The number of application DNP3 packets sent by the module.
Application Messages Rx	The number of application DNP3 packets received by the module.
Critical Messages Tx	The number of critical DNP3 packets sent by the module when security is enabled.

Critical Messages Rx	The number of critical DNP3 packets received by the module when security is enabled.
Messages Discarded	The number of DNP3 packets discarded by the module.
Error Messages Tx	The number of error DNP3 packets sent by the module.
Error Messages Rx	The number of error DNP3 packets received by the module.
Checksum errors	The number of corrupted DNP3 packets received by the module.
Timeouts	The number of message response timeouts the module has encountered.
Parity errors	The number of bytes with parity errors received by the module.
Assign Class Received	This is currently reserved.
Time Update Received	This number is the amount of times the DNP3 Master has sent a time update command to the DNP3 Outstation.
Deadband Update Received	This is currently reserved.
Broadcast Message Received	This is the number of DNP3 Broadcast messages received.
Unsolicited Command Received	This is the number of DNP3 Unsolicited (enable or disable) commands received.

Table 7.3 – DNP3 statistics

Statistic	**Description**
Logix Data Type Mismatch - Read	The data type in Logix (atomic or UDT) did not match the DNP3 data type during a read operation.
Logix Data Type Mismatch - Write	The data type in Logix (atomic or UDT) did not match the DNP3 data type during a write operation.
Write Seq Index Out Of Order	DNP3 allows the user to write data in a non-sequential manner by using DNP3 object prefixes. For example, a single write operation can be targeted to array offset 2, 3, 4, and 8. This is not allowed in the DNP3 Router due to the nature of the CIP communication protocol. The user will need to write array offset 2, 3, and 4 and then in a separate write function write to offset 8.
DNP3 Request Data Too Large	The request data is too big. The DNP3 Router allows for a maximum of 1000 bytes per transaction.
Mapped Item Not found	The DNP3 request has a range that is outside of the configured DNP3 mapping bounds for the specific group and variation.
Received Event Item Not Found	This is currently reserved.
DNP3 Request Too Many Objects	The DNP3 Router supports a maximum of 10 DNP3 objects in a single DNP3 request. These statistics indicates that more than 10 DNP3 objects were found in a single request.
DNP3 Message Queue Full	The DNP3 Router has received too many simultaneous messages to process.
Node Mismatch	The received message node number did not match the DNP3 Router configured node address.

Select Size Too Large	When the Select/Operate functionality is used the DNP3 Router supports a maximum of 255 bytes per transaction (or one full DNP3 message).
Select Operate Data Mismatch	The Select/Operate functionality requires that the response to the Select function matches the Select request.

Table 7.4 – Module error statistics

The following Logix statistics are only relevant when the module is running in either Reactive Tag or Scheduled Tag mode.

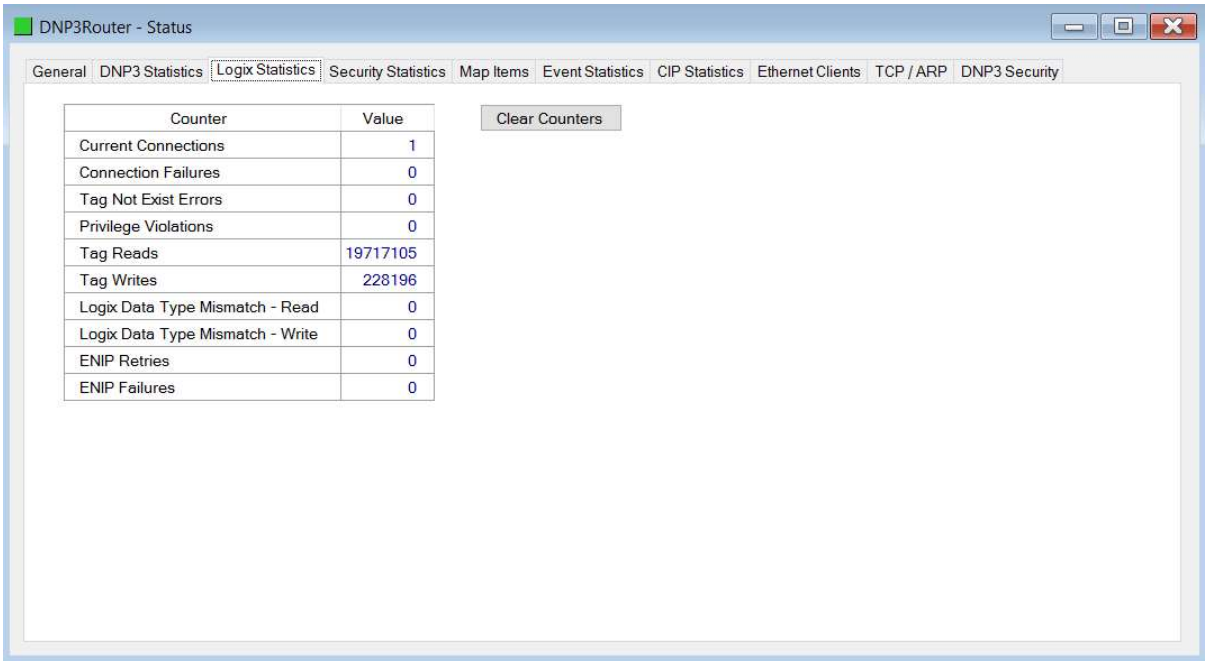


Figure 7.6. - Status monitoring – Logix Statistics

Statistic	Description
Current Connections	The number of current open class 3 connections.
Connection Failures	The number of failed attempts at establishing a class 3 connections with a Logix controller.
Tag Not Exist Errors	The number of tag read and tag write transactions that failed due to the destination tag not existing.
Privilege Violation Errors	The number of tag read and tag write transactions that failed due to a privilege violation error. This may be caused by the External Access property of the Logix tag being set to either None or Read Only.
Tag Reads	The number of tag read transactions executed by the DNP3 Router module.
Tag Writes	The number of tag write transactions executed by the DNP3 Router module.

ENIP Retries	This count increases when no response was received from the Logix Controller by the time the ENIP timeout is reached.
ENIP Failures	This count increases when the ENIP Retry Limit is reached and no response has been received from the Logix Controller.

Table 7.5 - Tag Mapping statistics

The following Security statistics are only relevant when the Security has been enabled in the module configuration.

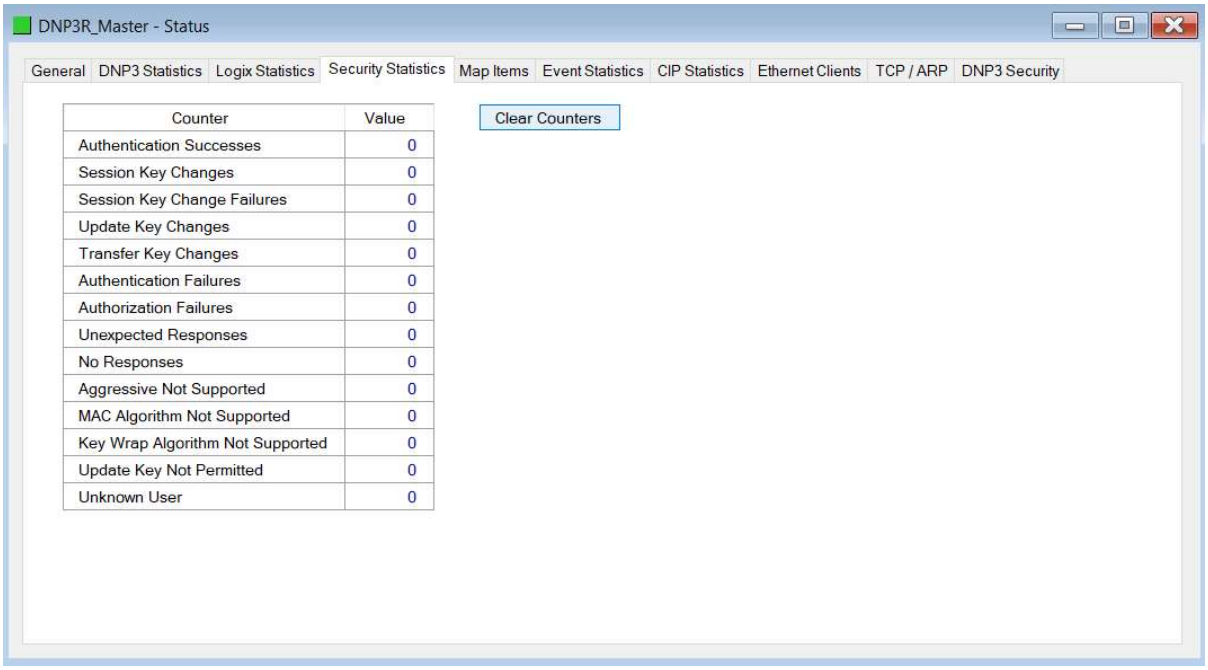


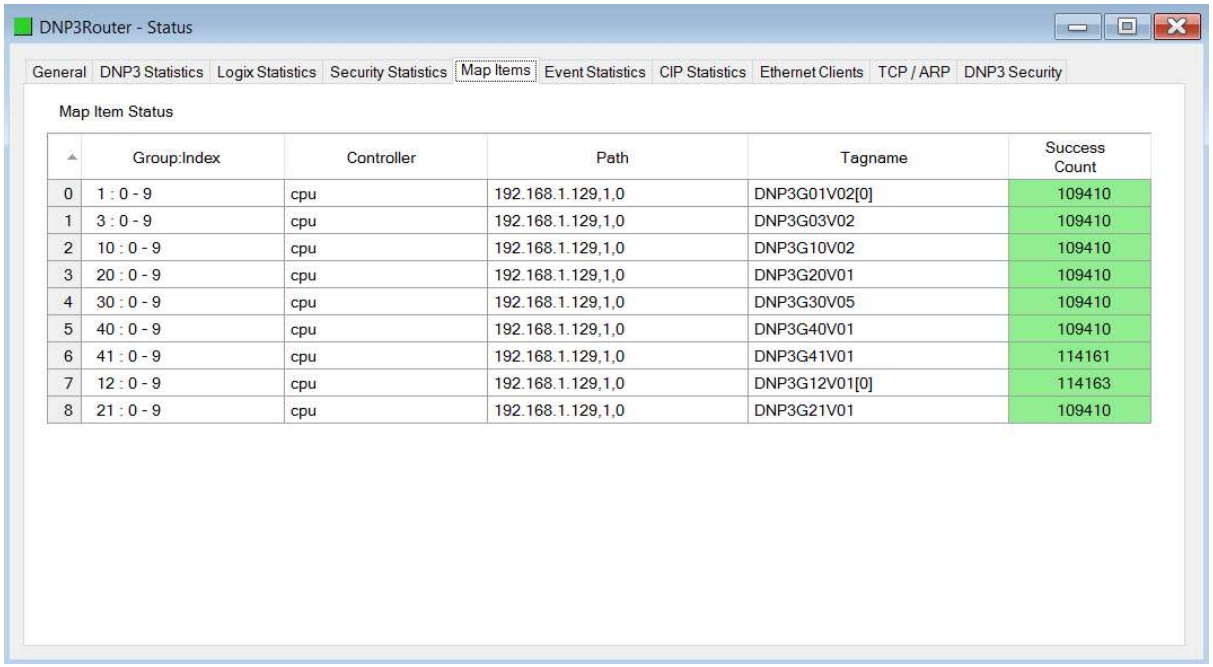
Figure 7.7. - Status monitoring – Security Statistics

Statistic	**Description**
Authentication Successes	Increases every time the device successfully authenticates a message.
Session Key Changes	When the session keys have been successfully updated.
Session Key Change Failures	When the session keys have failed to update.
Update Key Changes	The Update Key has changed.
Transfer Key Changes	The Transfer Key has changed.
Authentication Failures	The other device has provided invalid authentication information such as an incorrect MAC.
Authorization Failures	Increases when a user is not authorized to perform a requested operation.
Unexpected Responses	The other device has responded with a message that was not expected during the authentication process.
No Responses	The other device has not replied during the authentication process.
Aggressive Not Supported	When Aggressive Mode Authentication is not supported this will increase.

MAC Algorithm Not Supported	The MAC algorithm requested is not supported
Key Wrap Algorithm Not Supported	The Key Wrap algorithm requested is not supported.
Update Key Not Permitted	Updating of a key was not permitted.
Unknown User	The user used for authentication was unknown. The default user (1) is the only user supported.

Table 7.6 - Security statistics

The Map Items tab will display the successful packet counts processed by each mapping item. If an item count changes, then the success count field will be displayed with a green background for approximately 3 seconds. This provides quick visual feedback as to which items are currently active. The fields in the map items will adjust to suite the appropriate mode. No items are displayed in Unscheduled mode.



	Group:Index	Controller	Path	Tagname	Success Count
0	1 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G01V02[0]	109410
1	3 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G03V02	109410
2	10 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G10V02	109410
3	20 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G20V01	109410
4	30 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G30V05	109410
5	40 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G40V01	109410
6	41 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G41V01	114161
7	12 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G12V01[0]	114163
8	21 : 0 - 9	cpu	192.168.1.129,1,0	DNP3G21V01	109410

Figure 7.8. - Map Item status

The following Event statistics are only relevant when the module is operating in Reactive mode:

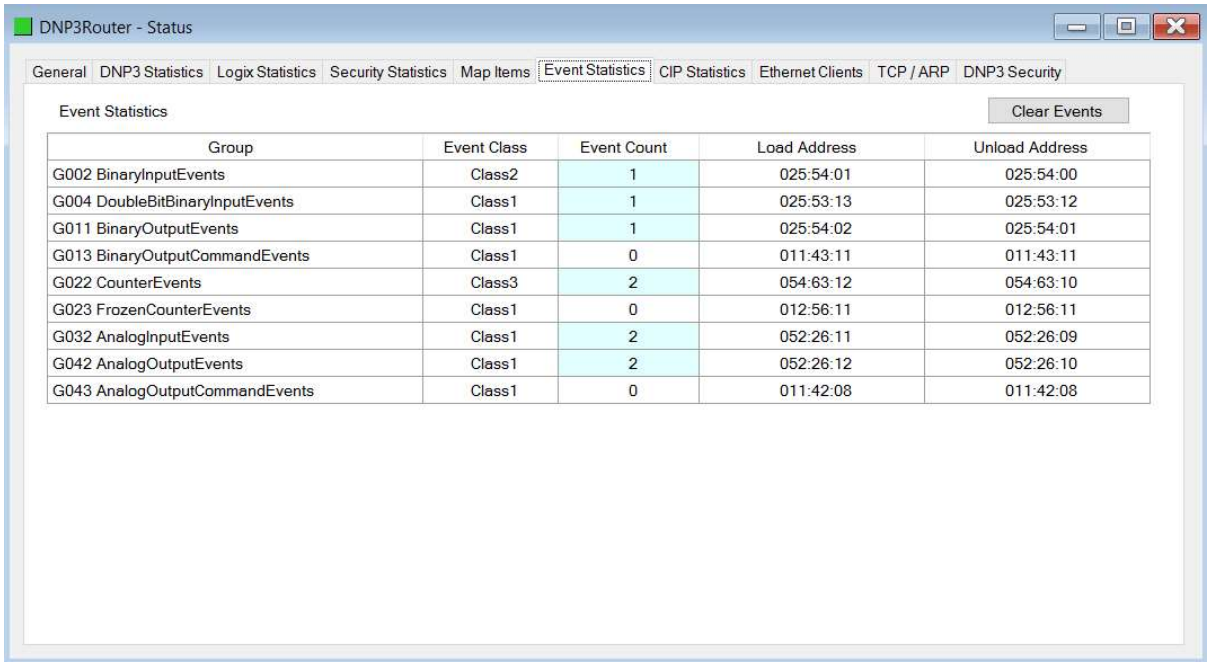


Figure 7.9. - Status monitoring – Event Statistics

Statistic	Description
Group	The specific DNP3 Group used
Event Class	The assigned DNP3 Event Class
Event Count	The number of outstanding events
Load Address	Memory address of event load index
Unload Address	Memory address of event unload index

Table 7.7 - Event statistics

The following Repeater statistics are only relevant when the module is operating in Reactive mode:

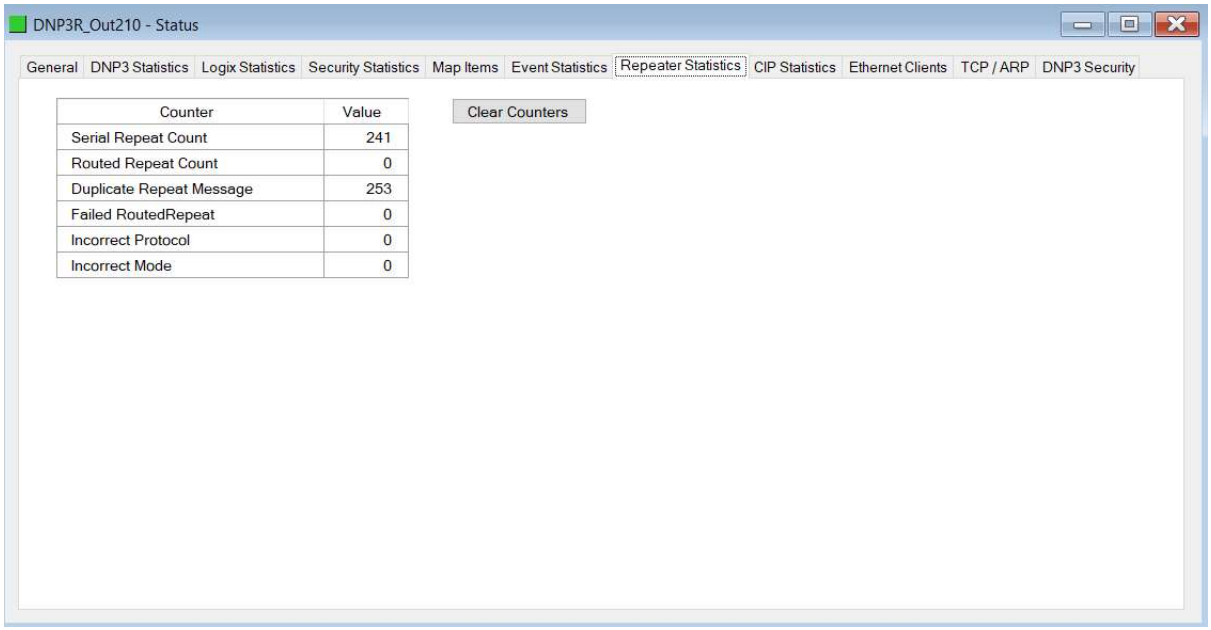


Figure 7.10. - Status monitoring – Repeater Statistics

Statistic	Description
Serial Repeat Count	The number of messages that have been repeated on the serial network.
Routed Repeat Count	The number of messages that have been routed to another DNP3 Router on the Ethernet network.
Duplicate Repeat Message	The number of duplicate repeat messages that have been received. Note that with multi-hop architectures this number will increase during normal operation.
Failed Routed Repeat	The number of times a routed message was sent to a DNP3 Router that returned an error code.
Incorrect Protocol	The number of times a routed message is received by the DNP3 Router which has not been configured for Serial Communication.
Incorrect Mode	The number of times a routed message is received by the DNP3 Router which has is not in Reactive Operating Mode.

Table 7.8 - Repeater statistics

Each DNP3 Router provides a set of Common Industrial Protocol (CIP) communication statistics as shown below:

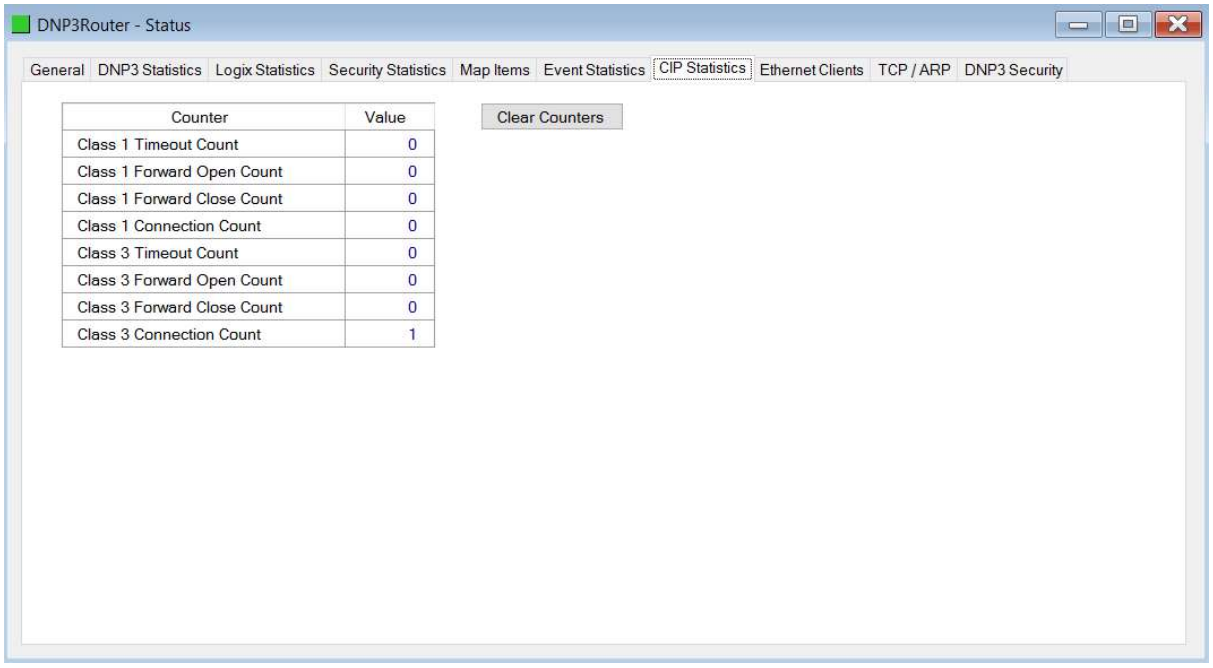


Figure 7.11. - Status monitoring – CIP Statistics

Statistic	Description
Class 1 Timeout Count	Number of times a Class 1 connection has timed out
Class 1 Forward Open Count	Number of Class 1 Connection establish attempts
Class 1 Forward Close Count	Number of Class 1 Connection close attempts
Class 1 Connection Count	Number of Class 1 Connections currently active
Class 3 Timeout Count	Number of times a Class 3 connection has timed out
Class 3 Forward Open Count	Number of Class 3 Connection establish attempts
Class 3 Forward Close Count	Number of Class 3 Connection close attempts
Class 3 Connection Count	Number of Class 3 Connections currently active

Table 7.9. - CIP Statistics

7.3. DNP3 PACKET CAPTURE

The module provides the capability to capture the DNP3 traffic for analysis. The will allow the user and the support team to resolve any possible issue on site.

To invoke the capture of the module, double-click on the DNP3 Packet Capture item in the Project Explorer tree.

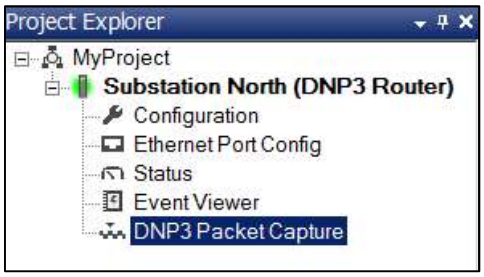


Figure 7.12. - Selecting DNP3 Packet Capture

The DNP3 Packet Capture window will open and automatically start capturing all DNP3 packets.

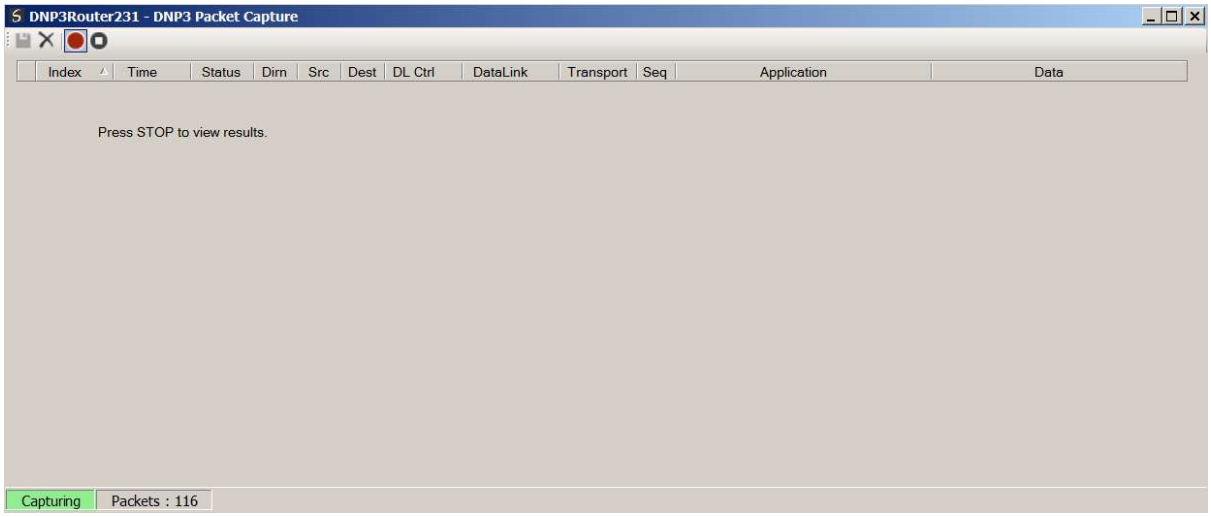


Figure 7.13 – DNP3 packet capture

To display the captured DNP3 packets, the capture process must first be stopped, by pressing the Stop button.

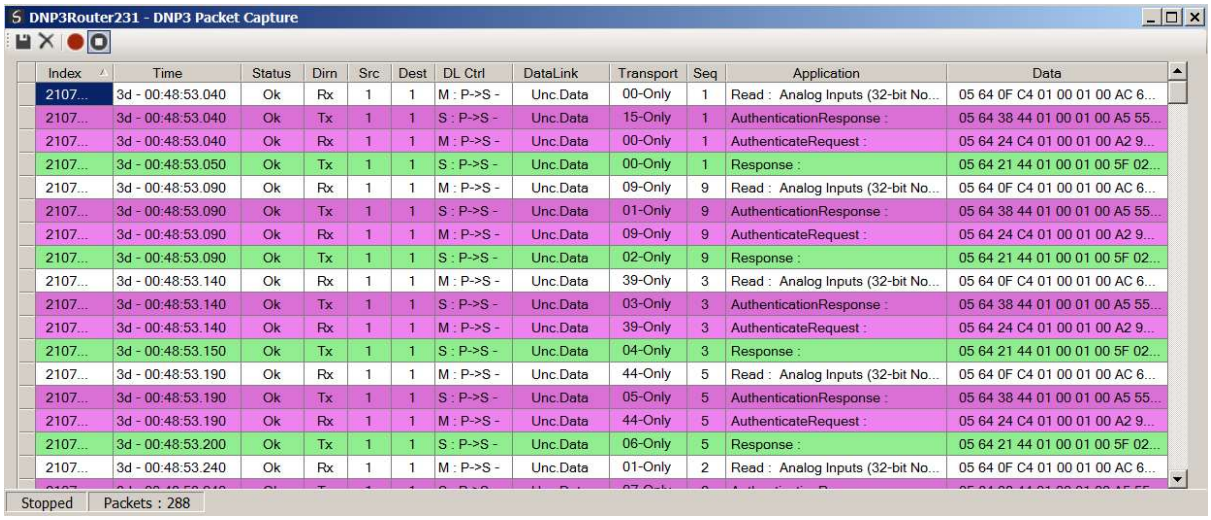


Figure 7.14. – DNP3 Packet Capture complete

The captured DNP3 packets are tabulated as follows:

Statistic	Description
Index	The packet index, incremented for each packet sent or received.
Time	The elapsed time since the module powered up.
Status	The status of the packet. Received packets are checked for valid DNP3 constructs and valid checksums.
Dirn	The direction of the packet, either transmitted (Tx) or received (Rx).
Src	DNP3 node address of the message source.
Dest	DNP3 node address of the message destination.
DL Ctrl	Data Link layer control. Part 1 **: M** – Master / **S** – Slave Part 2 : **P->S** : Primary to Secondary / **S->P** : Secondary to Primary Part 3 : **Frame Count** **-** : FCV = 0 (Frame count ignored) **0** : FCV = 1, FCB = 0 (Frame Count = 0) **1** : FCV = 1, FCB = 1 (Frame Count = 1)
Data Link	Data Link function.
Transport	Transport sequence numbers.
Seq	Application sequence numbers
Application	Application Layer

Table 7.10. – DNP3 Packet Capture fields

The packet capture can be saved to a file for further analysis, by selecting the Save button on the toolbar. Previously saved DNP3 Packet Capture files can be viewed by selecting the DNP3 Packet Capture Viewer option in the tools menu.

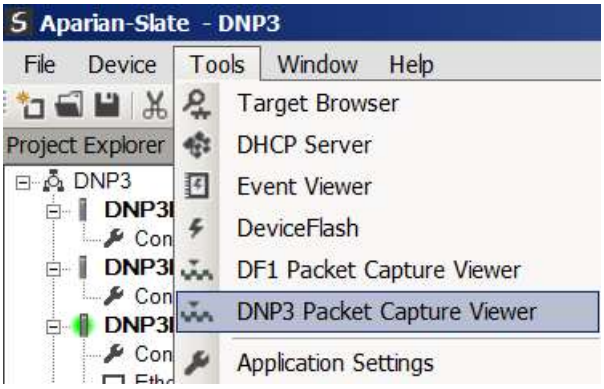


Figure 7.15. - Selecting the DNP3 Packet Capture Viewer

7.4. MODULE EVENT LOG

The DNP3 Router module logs various diagnostic records to an internal event log. These logs are stored in non-volatile memory and can be displayed using Slate or via the web interface. To vie them in Slate, select the Event Viewer option in the Project Explorer tree.

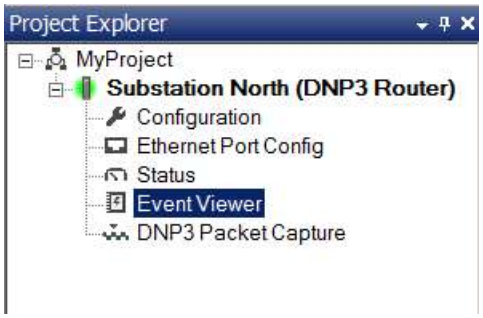
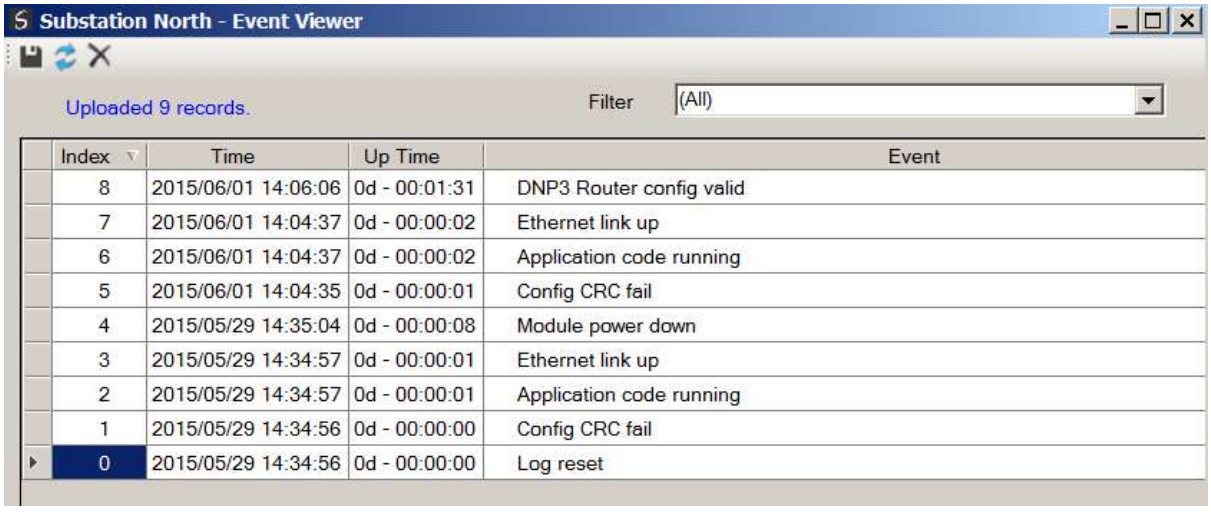


Figure 7.16. - Selecting the module Event Log

The Event Log window will open and automatically read all the events from the module. The log entries are sorted so as to have the latest record at the top. Custom sorting is achieved by double-clicking on the column headings.



Index	Time	Up Time	Event
8	2015/06/01 14:06:06	0d - 00:01:31	DNP3 Router config valid
7	2015/06/01 14:04:37	0d - 00:00:02	Ethernet link up
6	2015/06/01 14:04:37	0d - 00:00:02	Application code running
5	2015/06/01 14:04:35	0d - 00:00:01	Config CRC fail
4	2015/05/29 14:35:04	0d - 00:00:08	Module power down
3	2015/05/29 14:34:57	0d - 00:00:01	Ethernet link up
2	2015/05/29 14:34:57	0d - 00:00:01	Application code running
1	2015/05/29 14:34:56	0d - 00:00:00	Config CRC fail
0	2015/05/29 14:34:56	0d - 00:00:00	Log reset

Figure 7.17. – Module Event Log

The log can also be stored to a file for future analysis, by selecting the Save button in the tool menu.

To view previously saved files, use the Event Log Viewer option under the tools menu.

7.5. WEB SERVER

The DNP3 Router provides a web server allowing a user without Slate or RSLogix 5000 to view various diagnostics of the module. This includes Ethernet parameters, system event log, advanced diagnostics, and application diagnostics (DNP3 diagnostics).

NOTE: The web server is view **only** and thus no parameters or configuration can be altered from the web interface.

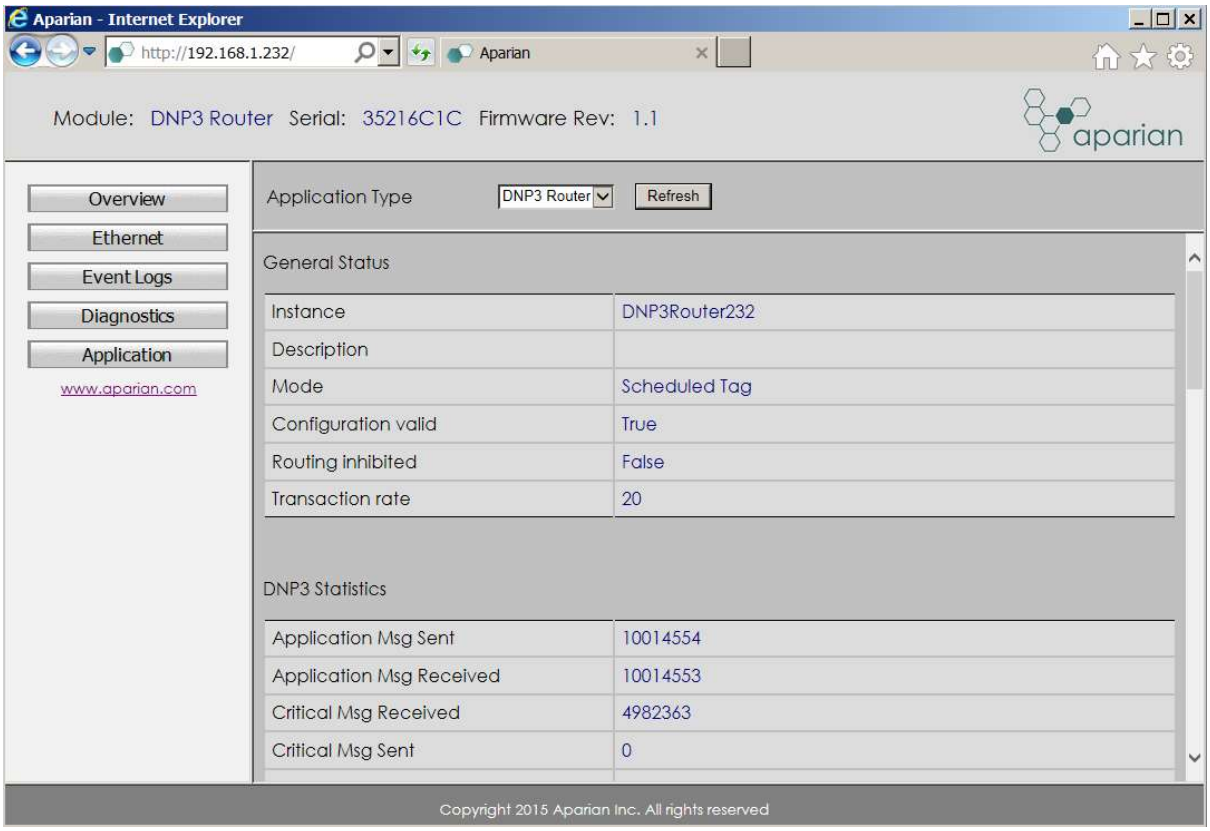


Figure 7.18. - Web interface

8. TECHNICAL SPECIFICATIONS

8.1. DIMENSIONS

Below are the enclosure dimensions as well as the required DIN rail dimensions. All dimensions are in millimetres.

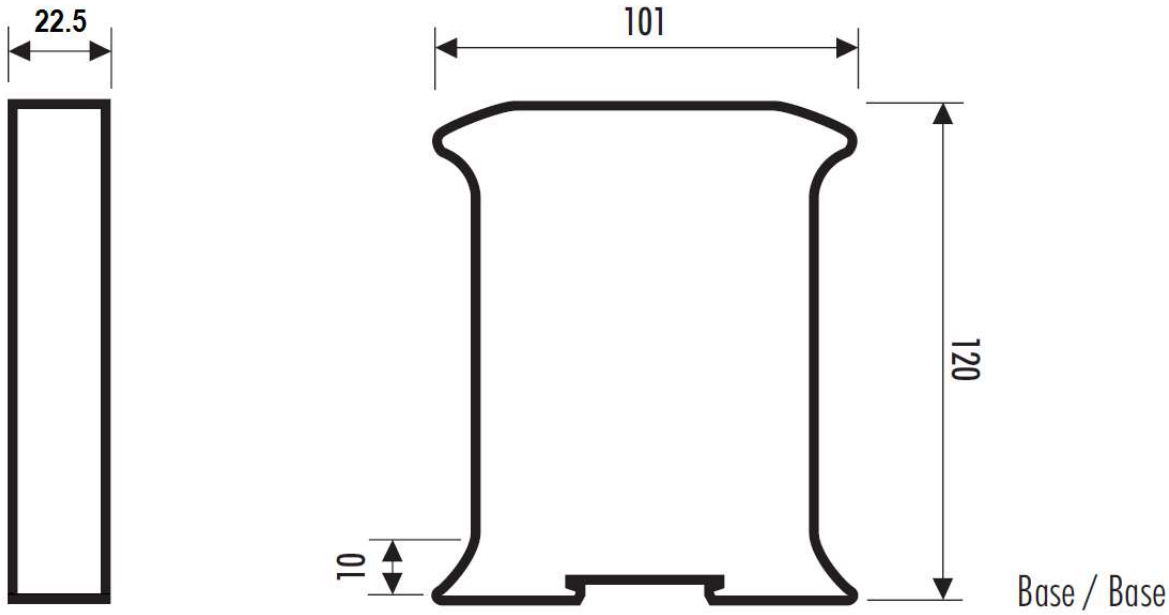


Figure 8.1 – DNP3 Router enclosure dimensions

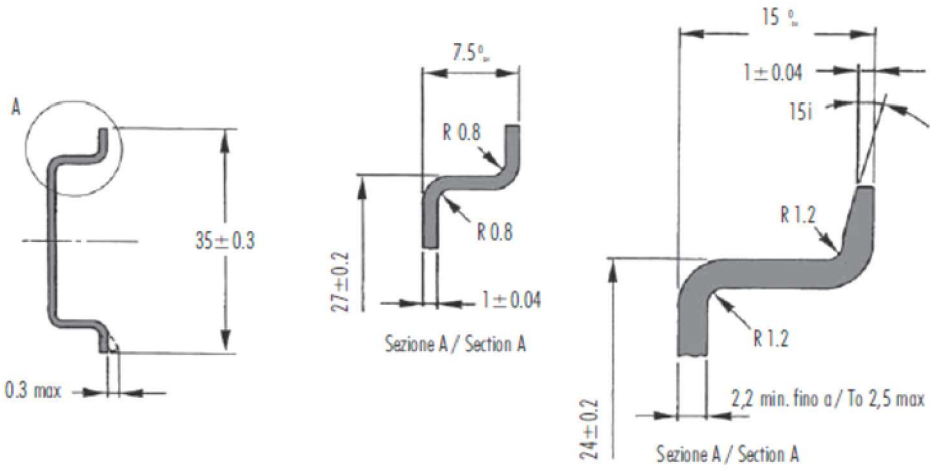


Figure 8.2 - Required DIN dimensions

8.2. ELECTRICAL

Specification	Rating
Power requirements	Input: 10 – 28V DC, (70 mA @ 24 VDC)
Power consumption	1.7 W
Connector	3-way terminal
Conductors	24 – 18 AWG
Enclosure rating	IP20, NEMA/UL Open Type
Temperature	-20 – 70 °C
Earth connection	Yes, terminal based
Emissions	IEC61000-6-4
ESD Immunity	EN 61000-4-2
Radiated RF Immunity	IEC 61000-4-3
EFT/B Immunity	EFT: IEC 61000-4-4
Surge Immunity	Surge: IEC 61000-4-5
Conducted RF Immunity	IEC 61000-4-6

Table 8.1 - Electrical specification

8.3. ETHERNET

Specification	Rating
Connector	RJ45
Conductors	CAT5 STP/UTP
ARP connections	Max 20
TCP connections	Max 20
CIP connections	Max 10
Communication rate	10/100Mbps
Duplex mode	Full/Half
Auto-MDIX support	Yes

Table 8.2 - Ethernet specification

8.4. SERIAL PORT

Specification	Rating
RS232 Connector	4-way terminal
RS232 Conductor	24 – 18 AWG
RS232 Isolation voltage	2.5 kV
BAUD	1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200
Parity	None, Even, Odd
Data bits	8
Stop bits	1

Table 8.3 – Serial Port specification

8.5. DNP3

Specification	Rating
Reactive Tag mode	Max 30 mapping items
Scheduled Tag mode	Max 30 mapping items
Application Functions Supported	Read Write Select/Operate Direct-Operate Direct-Operate-No-Response Confirm (only in Reactive Mode) Immediate Freeze (only in Reactive Mode) Immediate Freeze No Response (only in Reactive Mode) Immediate Freeze and Clear (only in Reactive Mode) Immediate Freeze and Clear No Response (only in Reactive Mode) Cold Restart (only in Reactive Mode) Enable / Disable Unsolicited Messages (only in Reactive Mode) Delay Measure (only in Reactive Mode) Record Current Time (only in Reactive Mode) Unsolicited Response (only in Reactive Mode) Authentication Request Authentication Response
Maximum DNP3 objects per request	30

Maximum DNP3 request size per mapped item in Reactive Tag Mode	1000 bytes
Maximum DNP3 request size per mapped item in Scheduled Tag Mode	230 bytes
Maximum Logix Controller support	3
Unsolicited Response support	Yes
Maximum event buffer per DNP3 group	100,000 (total of 900,000)
Number of Commands per Request	1
Event Read Interval	10ms

Table 8.4 – DNP3 specification

8.6. DNP3 SECURE AUTHENTICATION

Specification	**Rating**
Key Change Method Supported	Pre-shared
MAC Algorithms Supported	HMAC SHA-1 encryption (4 octets – serial) – for legacy support HMAC SHA-1 encryption (8 octets – serial) HMAC SHA-1 encryption (10 octets – networked) HMAC SHA-256 encryption (8 octets – serial) HMAC SHA-256 encryption (16 octets – networked) AES-GMAC (12 octets)
Key Wrap Algorithms Supported	AES-128 Key Wrap AES-256 Key Wrap
Aggressive Mode Supported	Yes

Table 8.5 – DNP3 Secure Authentication specification

8.7. CERTIFICATIONS

Certification	Mark
CE Mark	CE
UL Mark File: E494895	c UL us LISTED CLASS 1, DIV 2, GROUPS A, B, C, D
ODVA Conformance	EtherNet/IP™ * F/W 1.009
RoHS2 Compliant	RoHS2
RCM	

Table 8.6 – Certifications

A. APPENDIX – DNP3 REFERENCE

A.1. DNP3 FUNCTIONS

Code	Function
00	Confirm
01	Read
02	Write
03	Select
04	Operate
05	Direct Operate
06	Direct Operate - No Response
07	Freeze
08	Freeze - No Response
09	Freeze Clear
0a	Freeze Clear - No Response
0b	Freeze At Time
0c	Freeze At Time - No Response
0d	Cold Restart
0e	Warm Restart
0f	Initialize Data
10	Initialize Application
11	Start Application
12	Stop Application
13	Save Configuration
14	Enable Unsolicited
15	Disable Unsolicited
16	Assign Class
17	Delay Measurement
18	Record Current Time
19	Open File
1a	Close File
1b	Delete File
1c	Get File Information
1d	Authenticate File
1e	Abort File
1f	Activate Config
20	Authenticate Request
21	Authenticate Request - No Ack
81	Response
82	Unsolicited Response
83	Authentication Response

Table A.1 – DNP3 Functions

A.2. DNP3 GROUPS

Group	Description
0	Device Attributes
1	Binary Inputs
2	Binary Input Events
3	Double Bit Binary Inputs
4	Double Bit Binary Input Events
10	Binary Outputs (Status)
11	Binary Output Events
12	Binary Output Commands
13	Binary Output Command Events
20	Counters
21	Frozen Counters
22	Counter Events
23	Frozen Counter Events
30	Analog Inputs
31	Frozen Analog Inputs
32	Analog Input Events
33	Frozen Analog Input Events
34	Analog Input Reporting Deadbands
40	Analog Output Status
41	Analog Outputs (Commands)
42	Analog Output Events
43	Analog Output Command Events
50	Time And Date
51	Time And Date Of Occurrence
52	Time Delays
60	Class Objects
70	File Control
80	Internal Indications
81	Device Storage
82	Device Profiles
83	Data Sets
85	Data Set Prototypes
86	Data Set Descriptors
87	Data Sets Present Value
88	Data Set Events
90	Applications
91	Status Of Requested Operations
100	Floating Point
101	BCD Integers
102	Unsigned Integers
110	Octet Strings

111	Octet String Events
112	Virtual Terminal Output Blocks
113	Virtual Terminal Event Data
120	Authentication
121	Security Statistics
122	Security Statistic Events

Table A.2 – DNP3 Groups

A.3. SUPPORTED DNP3 GROUP VARIATIONS

Group	Group Description	Supported Functions	Var. Code	Variation Description	Recommended Data Type	Supports Events
1	Binary Inputs	Read	1	Packed Format	SINT	
			2	With Flags	AparianDNP3BinaryInputWithFlag	●
3	Double Bit Binary Inputs	Read	1	Packed Format	SINT	
			2	With Flags	AparianDNP3DoubleBinaryInputWithFlag	●
10	Binary Outputs	Read	1	Packed Format	SINT	
			2	Output Status With Flags	AparianDNP3BinaryOutputWithFlag	●
12	Binary Output Commands	Operate*	1	Control Relay Output Block	AparianDNP3CROB	●
20	Counters	Read Freeze Clear	1	32-bit With Flag	AparianDNP3Counter32WithFlag	●
			2	16-bit With Flag	AparianDNP3Counter16WithFlag	●
			5	32-bit Without Flag	DINT	
			6	16-bit Without Flag	INT	
21	Frozen Counters	Read	1	32-bit With Flag	AparianDNP3Counter32WithFlag	●
			2	16-bit With Flag	AparianDNP3Counter16WithFlag	●
			5	32-bit With Flag And Time	AparianDNP3Counter32WithFlagTime	●
			6	16-bit With Flag And Time	AparianDNP3Counter16WithFlagTime	●
			9	32-bit Without Flag	DINT	
			10	16-bit Without Flag	INT	
30	Analog Inputs	Read	1	32-bit With Flag	AparianDNP3AnalogInput32Flag	●
			2	16-bit With Flag	AparianDNP3AnalogInput16Flag	●
			3	32-bit Without Flag	DINT	
			4	16-bit Without Flag	INT	
			5	Single Floating Point With Flag	AparianDNP3AnalogInputRealFlag	●
40	Analog Output Status	Read	1	32-bit With Flag	AparianDNP3AnalogOutput32Flag	●
			2	16-bit With Flag	AparianDNP3AnalogOutput16Flag	●
			3	Single Floating Point With Flag	AparianDNP3AnalogOutputRealFlag	●
41	Analog Outputs	Operate*	1	32-bit	AparianDNP3AnalogOutput32	●
			2	16-bit	AparianDNP3AnalogOutput16	●
			3	Single Floating Point	AparianDNP3AnalogOutputReal	●
102	Unsigned Integers	Read Write	1	8-bit	SINT	

Table A.3 - Supported DNP3 Group Variations

*Note: The function Operate refers to all the Operate functions: Select, Operate, Direct Operate and Direct Operate without Acknowledge.

Note: The *Supportes Events* column is only relevant for DNP3 Outstation mode.

A.4. DNP3 QUALIFIER CODE

The qualifier code (byte) is made up of the Object Prefix nibble and the Range Field nibble as described in the table below.

Bit Number -->	7	6	5	4	3	2	1	0
	0	Prefix Code			Range Specifier Code			

Table A.5 – DNP3 Qualifier Code

Prefix Code	Object Prefix
0	Objects packed without a prefix
1	Objects prefixed with 8-bit index
2	Objects prefixed with 16-bit index
3	Objects prefixed with 32-bit index
4	Objects prefixed with 8-bit size
5	Objects prefixed with 16-bit size
6	Objects prefixed with 32-bit size
7	Reserved

Table A.6 – DNP3 Object Prefix Code

Range Code	Range Specifier
0	8-bit Start-Stop index
1	16-bit Start-Stop index
2	32-bit Start-Stop index
3	8-bit Start-Stop virtual address
4	16-bit Start-Stop virtual address
5	32-bit Start-Stop virtual address
6	No range - implies All
7	8-bit Count of objects
8	16-bit Count of objects
9	32-bit Count of objects
A	Reserved
B	8-bit Count of objects, variable format
C	Reserved
D	Reserved
E	Reserved
F	Reserved

Table A.7 – DNP3 Range Field Specifier Code

Qualifier Code	Object Prefix	Range Specifier	Preferred
00	Objects packed without a prefix	8-bit Start-Stop index	●
01	Objects packed without a prefix	16-bit Start-Stop index	●
02	Objects packed without a prefix	32-bit Start-Stop index	
03	Objects packed without a prefix	8-bit Start-Stop virtual address	
04	Objects packed without a prefix	16-bit Start-Stop virtual address	
05	Objects packed without a prefix	32-bit Start-Stop virtual address	
06	Objects packed without a prefix	No range - implies All	●
07	Objects packed without a prefix	8-bit Count of objects	●
08	Objects packed without a prefix	16-bit Count of objects	●
09	Objects packed without a prefix	32-bit Count of objects	
17	Objects prefixed with 8-bit index	8-bit Count of objects	●
18	Objects prefixed with 8-bit index	16-bit Count of objects	
19	Objects prefixed with 8-bit index	32-bit Count of objects	
27	Objects prefixed with 16-bit index	8-bit Count of objects	
28	Objects prefixed with 16-bit index	16-bit Count of objects	●
29	Objects prefixed with 16-bit index	32-bit Count of objects	
37	Objects prefixed with 32-bit index	8-bit Count of objects	
38	Objects prefixed with 32-bit index	16-bit Count of objects	
39	Objects prefixed with 32-bit index	32-bit Count of objects	
4B	Objects prefixed with 8-bit size	8-bit Count of objects, variable format	
5B	Objects prefixed with 16-bit size	8-bit Count of objects, variable format	●
6B	Objects prefixed with 32-bit size	8-bit Count of objects, variable format	

Table A.8 – DNP3 Valid Qualifier Range Codes

A.5. DNP3 EVENT STATUS FLAGS

Group	Flag desciption
2 – Binary Input Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Chatter Filter Bit 6 – Reserved Bit 7 – Input State
4 – Double-bit Binary Input Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Chatter Filter Bit 6 – Input State 0 Bit 7 – Input State 1
11 – Binary Output Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Reserved Bit 6 – Reserved Bit 7 – Output State
13 – Binary Output Command Events	Bit 0 –> 6 • 0 – Success • 1 – Timeout • 2 – No Select • 3 – Format Error • 4 – Not Supported • 5 – Already Active Bit 7 – Commanded State
22 – Counter Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Rollover Bit 6 – Discontinuity Bit 7 – Reserved
23 – Frozen Counter Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Rollover Bit 6 – Discontinuity Bit 7 – Reserved
32 – Analog Input Events	Bit 0 – Online

	Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Over range Bit 6 – Reference Error Bit 7 – Reserved
42 – Analog Output Events	Bit 0 – Online Bit 1 – Restart Bit 2 – Communication Lost Bit 3 – Remote Forced Bit 4 – Local Forced Bit 5 – Over range Bit 6 – Reference Error Bit 7 – Reserved
43 – Analog Output Command Events	Bit 0 –> 6 • 0 – Success • 1 – Timeout • 2 – No Select • 3 – Format Error • 4 – Not Supported • 5 – Already Active Bit 7 – Reserved

Table A.9 – DNP3 Event Group Status Flags

INDEX

A

AES-128, 28, 87, 113
AES-256, 28, 113
Aggressive Mode, 28, 101, 113
assembly instance, 58
Authentication, 64, 86, 101, 115, 117

C

checksum, 95
class 1, 58, 59, 63
CompactLogix, 6, 8
Connection path, 52
Contact Us, 12
ControlLogix, 6, 8, 9
Critical Functions, 28

D

DC power, 13
DHCP, 14, 17, 18, 19
dimensions, 110
DIN rail, 15, 110
DIP, 14
DNP3, 1, 6, 7, 8, 9, 10, 11, 13, 14, 16, 22, 23, 24, 25, 26, 27, 28, 30, 32, 33, 34, 35, 36, 37, 39, 40, 42, 43, 44, 52, 58, 60, 61, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 84, 85, 86, 87, 89, 90, 92, 93, 95, 96, 97, 98, 99, 100, 105, 106, 107, 108, 109, 110, 112, 113, 115, 116, 117, 118, 119, 120, 121
DNP3 general configuration, 24, 30, 32, 33
DNP3 parameters, 23
DNP3 Router, 1, 6, 7, 8, 9, 10, 11, 13, 14, 16, 22, 23, 24, 25, 27, 28, 34, 39, 42, 44, 52, 58, 60, 61, 63, 65, 67, 73, 84, 85, 86, 87, 89, 92, 95, 96, 99, 100, 108, 109, 110

E

Ethernet Bridge, 58
Ethernet connector, 16
Ethernet TCP, 6, 7, 25, 43
Ethernet UDP, 6, 7, 25, 43
Ethernet/IP, 35, 40
EtherNet/IP, 6, 8, 20, 35, 40

F

File Number, 35, 36, 37, 44
firmware upgrade, 23

G

ground (GND), 13

I

input assembly, 64, 98
input voltage, 16

K

Key Change Method, 27, 113
Key Wrap Algorithm, 28, 86, 87, 102

L

LED, 74, 81, 90, 95
Logix controller, 6, 7, 34, 35, 36, 39, 40, 41, 59, 63, 97, 100
Logix platform, 6, 7, 8, 9
Logix tag, 24, 35, 36, 37, 40, 42, 44, 63, 64, 65, 66, 84, 88, 91
Logix Tag Map, 34, 37

M

MAC Algorithm, 27, 102
Mapping Mode, 24
Micro800, 24

O

output assembly, 63, 64, 65, 97

P

Protocol, 17, 25

R

Reactive Tag, 6, 8, 24, 34, 35, 36, 37, 38, 97, 100, 112
receive (RX), 13, 16
requested packet interval (RPI), 59
Rockwell Automation, 21
RS232, 7, 13, 16, 25, 95
RSLinx, 21
RSLogix 5000, 54, 58, 59, 60, 62, 63, 65, 71, 109

S

Safe Mode, 14
Schedule Tag, 34, 40

Scheduled Tag, 6, 9, 24, 39, 40, 42, 97, 100, 112
Secure, 7, 10, 27, 28, 34, 86, 113
Secure Authentication, 7, 10, 27, 28, 34, 86, 113
Security, 27, 28, 29, 86, 101, 102, 117
Serial, 7, 10, 112
Session keys, 86
Slate, 7, 11, 17, 19, 21, 22, 23, 37, 38, 39, 43, 46, 47, 48, 52, 53, 64, 71, 73, 87, 96, 108, 109
statistics, 96, 100, 101, 102, 103, 104
Support email, 12

T

Target Browser, 19, 20, 35, 40, 41, 52
Target Tag, 37, 43, 73
transmit (TX), 13, 16

U

UDTs, 7, 11, 36, 59, 60, 61, 62, 63, 65, 71
Unscheduled, 7, 24, 25, 34, 44, 61, 64, 65, 66, 68, 69, 85, 97, 102
Update Key, 86, 87, 101, 102
User Defined Types (UDTs), 59

W

web server, 96, 109