Quantum with Unity Pro
TCP/IP Configuration
User Manual

04/2015

33002467.08

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result** in minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

PLEASE NOTE

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

About the Book

At a Glance

Document Scope

This documentation describes hardware and software installation procedures for the TCP/IP bus.

Validity Note

This document is valid for Unity Pro 10.0 or later.

The technical characteristics of the devices described in this document also appear online. To access this information online:

Step	Action
1	Go to the Schneider Electric home page *www.schneider-electric.com*.
2	In the **Search** box type the reference of a product or the name of a product range. ● Do not include blank spaces in the reference or product range. ● To get information on grouping similar modules, use asterisks (*).
3	If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you. If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you.
4	If more than one reference appears in the **Products** search results, click on the reference that interests you.
5	Depending on the size of your screen, you may need to scroll down to see the data sheet.
6	To save or print a data sheet as a .pdf file, click **Download XXX product datasheet**.

The characteristics that are presented in this manual should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the manual and online information, use the online information as your reference.

Related Documents

Title of Documentation	Reference Number
Control Panel Technical Guide, How to Protect a Machine from Malfunctions Due to Electromagnetic Disturbance	CPTG003_EN (English), CPTG003_FR (French)

Title of Documentation	Reference Number
Grounding and Electromagnetic Compatibility of PLC Systems, Basic Principles and Measures, User Manual	33002439 (English), 33002440 (French),33002441 (German), 33003702 (Italian),33002442 (Spanish),33003703 (Chinese)
Quantum with Unity Pro Hardware Reference Manual	35010529 (English), 35010530 (French), 35010531 (German), 35010532 (Spanish), 35013975 (Italian), 35012184 (Chinese)
Quantum with Unity Pro, Discrete and Analog I/O, Reference Manual	35010516 (English), 35010517 (French), 35010518 (German), 35013970 (Italian), 35010519 (Spanish), 35012185 (Chinese)
Quantum with Unity Pro, Experts and Communication, Reference Manual	35010574 (English), 35010575 (French), 35010576 (German), 35014012 (Italian), 35010577 (Spanish), 35012187 (Chinese)
Communication Services and Architectures, Reference Manual	35010500 (English), 35010501 (French), 35006176 (German), 35013966(Italian), 35006177 (Spanish), 35012196 (Chinese)
Unity Pro System Bits and Words, Reference Manual	EIO0000002135 (English), EIO0000002136 (French), EIO0000002317 (German), EIO0000002138 (Italian), EIO0000002139 (Spanish), EIO0000002140 (Chinese)

You can download these technical publications and other technical information from our website at www.schneider-electric.com.

Chapter 1
Ethernet - General Information

Ethernet and 802.3

General description

Ethernet was introduced in 1980 as Ethernet 1 and developed by the DEC, Intel and Xerox companies. This Ethernet later formed the basis of the 802.3-LAN from IEEE, that was published as the ISO standard in 1990.

Since 1990, Ethernet products have been produced almost exclusively according to the 802.3 standard.

The topology of an Ethernet corresponds to that of a bus system. However, the physical cabling can be made in point to point form. Hubs/Switches form the logical bus of the Ethernet from a physical point.

Framework formats

An Ethernet LAN and 802.3-LAN have different frame formats. The different formats are shown below.

Ethernet frame format

Preamble	Destination	Source	Protocol	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	n Bytes	4 Bytes

802.3-frames (MAC frame format)

Preamble	SFD	Dest.	Source	Length	Logical Link Control				FCS
					DSAP	SSAP	CTL	DATA and PAD Field	
8 Bytes	1 Bytes	6 Bytes	6 Bytes	2 Bytes	1 Byte	1 Byte	1 (2) Byte	n Bytes	4 Bytes

The following table contains a description of the frame parameters for Ethernet and 802.3.

Parameter	Description
Preamble	Identifies the prefix of an Ethernet / 802.3 frame. Used for synchronizing the destination.
SFD	The SFD field has the bit pattern 10101011 and identifies the start of the frame.
Destination	Target address of the destination
Source	Address of origin of the sender
Length	Gives the number of bytes in the LLC (Logical Link Control) data field (not with Ethernet frames).
Protocol	Specifies the protocol used (not for 802.3 frames).
DSAP	(Destination Service Access Point) Destination address (SAP) for destinations. The DSAP identifies the transfer interface to the next highest protocol (e.g. E0h=IPX).
SSAP	(Source Service Access Point) Destination address (SAP) for sources. The SSAP identifies the transfer interface to the next highest protocol (e.g. E0h=IPX).
CTL	(Control Field) The CTL field is 2 bytes long if the frame contains sequential number. In all other cases it is 1 byte long.
Data	(Also Data and PAD Field) Logging the data to be transferred. Since every Ethernet frame must be a minimum of 64 bytes long, and 18 bytes are used by the MAC Header and Trailer, the minimum length of the data section is 46 bytes. If the useful load of the frame is less than 46 bytes, the frame is padded out to fill the prescribed length (padding).
FCS	(Frame Check Sequence) The checksum is formed in the CRC procedure (CRC=Cyclic Redundancy Check). Frames with invalid checksums are rejected.

LAN Addresses

The Internet Protocol (IP) is the lowest layer in an Internet. The IP is defined in RFC 791. The Transmission Control Protocol (TCP) is set on the IP. The applications refer to this.

With networks that work with the TCP/IP protocol, and also on the internet, every PC can be identified via a numerical address. An IP address (Ipv4 standard) consists of four numbers separated by points, that can each be a value between 0 and 255. A typical IP address is "192.168.000.123". User PCs that access the internet via a Provider also receive an IP address: It is always the same static IP address, or a new dynamic IP address every time a connection is made.

IPv4 and IPv6

The IPv4, developed 20 years ago, uses a 32 bit address system, which theoretically allows up to four billion IP addresses. However in practice, a large part of these adresses cannot be used with group formation and other mechanisms.

The new IPv6 functions with a 128 bit system, an address space, which generally cannot be configured. This significantly increases the number of available IP numbers. Further advantages of the new IP address space include greater security, better support for real-time applications and a higher router capacity. IPv6 should be established by 2005. Backward compatibility with software and network components, which use the IPv4 standard, is to remain guaranteed according to the IETF (Internet Engineering Task Force).

Subnet mask

IP addresses are 32 bit numbers (IPv4) that consists of two components, the power supply and the computer. There are three different types of IP network classes, Class-A, Class-B and Class-C.

The subnet mask determines the size of a network. The combination of the subnet mask and the IP addresses results in the combination composition of the subnets and the number of possible network nodes in the subnet. A part of the IP address is therefore defined as the Subnet. This is defined via the Subnet mask.

Gateway address

The Gateway address determines, where the data packets are to be sent. This can depend on the local network card or a Gateway (Router) in the local subnet.

Cabling

There are different ways to create Ethernet LANs. They differ considerably in the type of cable and method of connection. The following table shows the most common types of cabling.

Type	Description
10BaseT 100BaseT 1000BaseT	Twisted Pair The most heavily used form of Ethernet is the 10xBaseT. 10BaseT was developed in 1986 as shielded cables. A constant development has occurred since then. The standard today is the 100BaseT. The first character in the label stands for the transmission speed in MBits/s. A disadvantage of the 10xBaseT is the low maximum extension of the network. Only a maximum expansion of 205 m between two stations can be achieved. A station can be situated 100 m from the hub. The distance between two hubs can be 5 m.
10BaseF	Fiber Optic Connection of Ethernet components using fiber optic cables. The distance between the fiber optic module and hub can be up to 500 m.

Chapter 2
Start Communication with Unity Pro

Introduction

This chapter tells you how to begin Ethernet network configuration with Unity Pro.

What Is in This Chapter?

This chapter contains the following sections:

Section 2.1
How to Configure the Communication

Overview

This section describes how to configure the communication.

What Is in This Section?

This section contains the following topics:

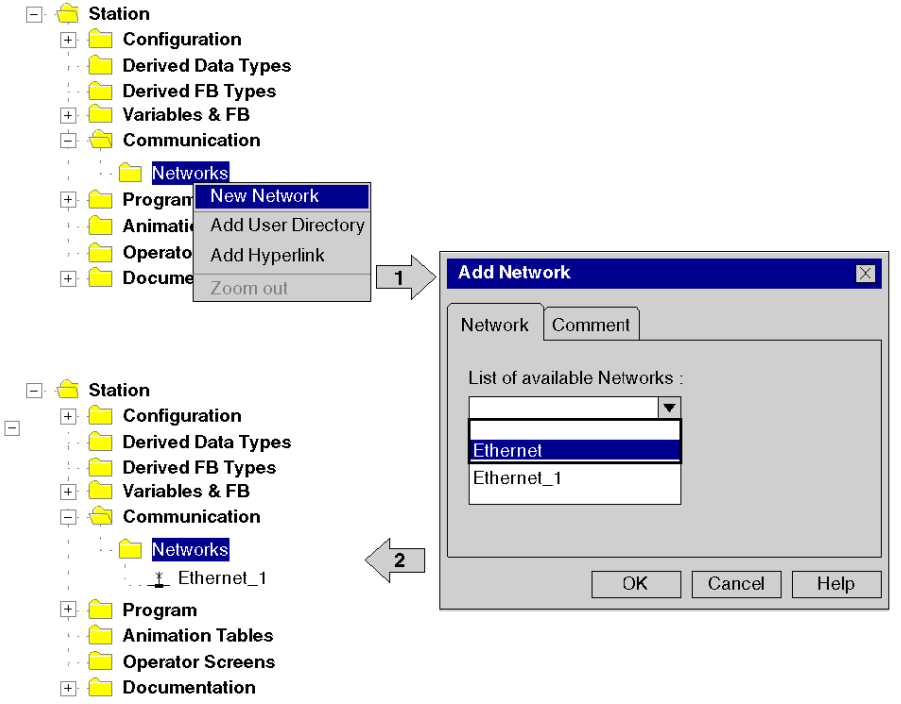
Add a New Network to the Communication Folder

Add a New Network to the Communication Folder

After starting a new application, the **Communication** folder under the **Station** tree branches the **Network** folder and the **Routing** table folder (Premium platforms only). These two folders are empty. Under the **Network** folder, the user can insert the networks by menu. A click on the right mouse-button above **Network** pops up a contextual menu. The user selects the type of network he wants to add. For easier use, a network name will be suggested with the prefix of the network type (**Ethernet_1** or **Modbus+_1**). By choosing a new network the next available number for the network is chosen automatically, for example, **Ethernet_1** then **Ethernet_2** and so on. At any moment, the user may rename any Netlink.

The user can also attach a comment that describes each configured network. The OK button adds the network as subfolder.

The names of network nodes are also called NetLink. These are the names of logical networks.

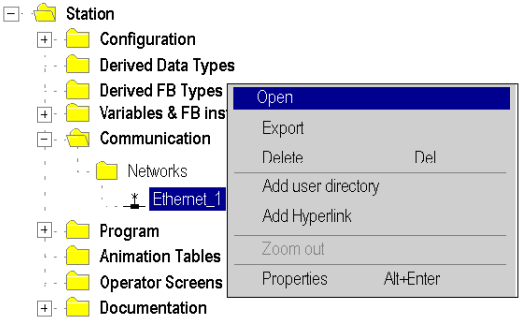


Configure Network

Configure Network

On the network folder, by a double-clicking action or by the Open item on contextual menu, the editor of the corresponding communication screen is opened in order to set the specific network services.

The figure shows the contextual menu to start network properties.

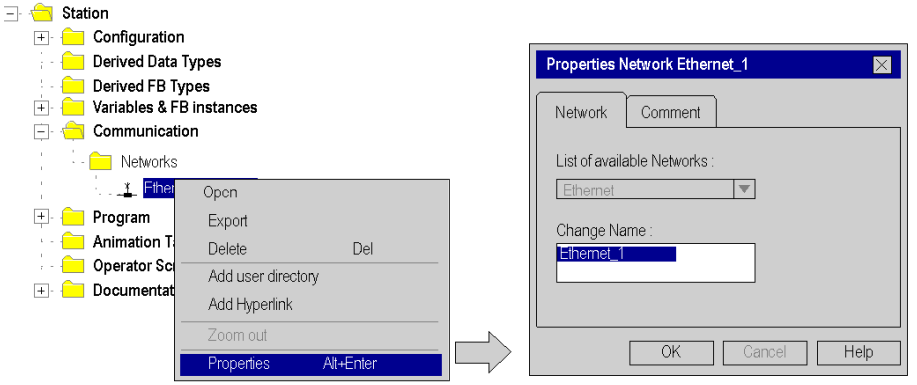


Properties of a Network

Properties of a Network

The contextual menu proposes the user to see again the properties of a configured network. Here, the user can change the NetLink name and the associated comment.

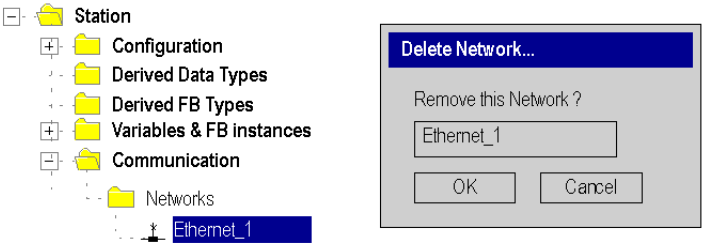
The figure shows the Ethernet property window:



Delete an Existing Network Folder

Delete an Existing Network Folder

With a right-mouse-click above the network folder, a contextual menu appears. Here the user is able to delete the network configuration. In this case, the subfolder of the network will also be removed in application browser.



NOTE: If this removed network was previously attached to a communication module, this module loses its link and it will work with its default parameters.

Section 2.2
Unity Soft Communication Links

Overview

This section presents the principle of communication implementation and describes the relationship between software configuration of networks and the hardware configuration of the network controllers.

What Is in This Section?

This section contains the following topics:

Communication Configuration Principle

Introduction

The configuration of communication links between different devices with Unity Soft includes three different configuration parts.

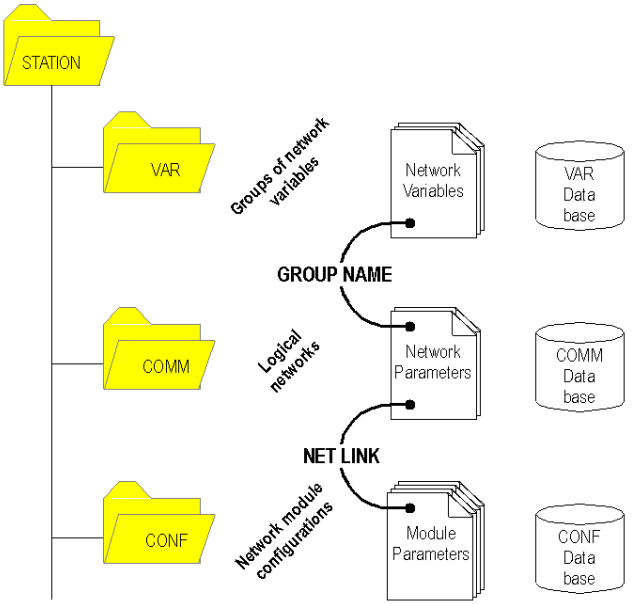
- configuration of the network controller
- configuration of the logical network
- configuration of network variables

Configuration

The communication configuration supports the *free mode* of Unity Soft. That means the user can first configure the module and then the communication or the user can configure the communication and then the module.

This will be provided through a NetLink that must be selected in the module configuration. The network variables including in the VAR folder are linked with a group name that defines an IP domain over Internet network.

The illustration shows the three parts involved in communication configuration:



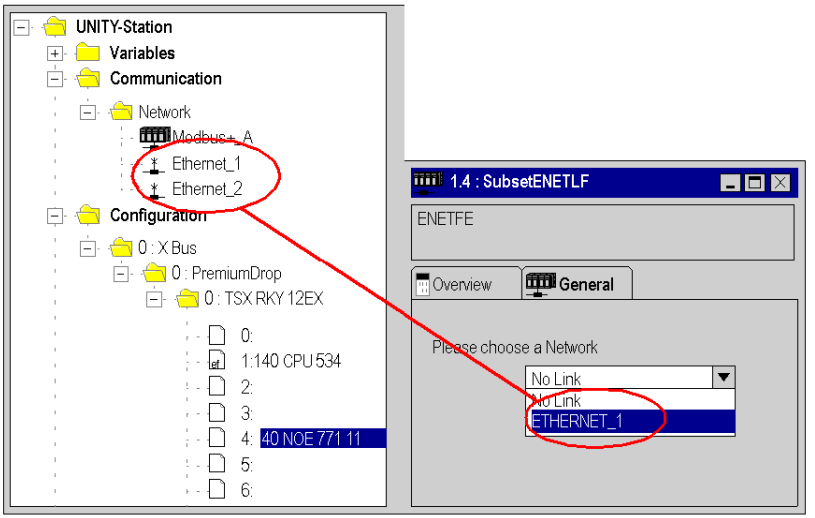
Link between Configuration and Communication

NetLinks

During Unity Pro application design, the NetLinks are created and inserted on sub-folder Communication under Network. These are the names of logical networks.

Under configuration folder, on the communication module node included in the current station, the list of existing NetLinks is proposed to select and attach one network to one module. Only the NetLink that can be managed by this module, are displayed in the list box on module configuration screen. No NetLink can be edited and created here (no edit box), but this list contains at least the No_Link field.

The following figure shows the window for the Ethernet link for the Quantum NOE module.



Attaching a NetLink to a Module

When a network is attached to a module, the icon of the corresponding node is changed and the network editor displays the address of the module in the rack .

The Icon in the Network folder indicates whether the link is attached to a module or not:

	Icon when no communication module is attached to the NetLink
	Icon when a communication module has been attached to the NetLink

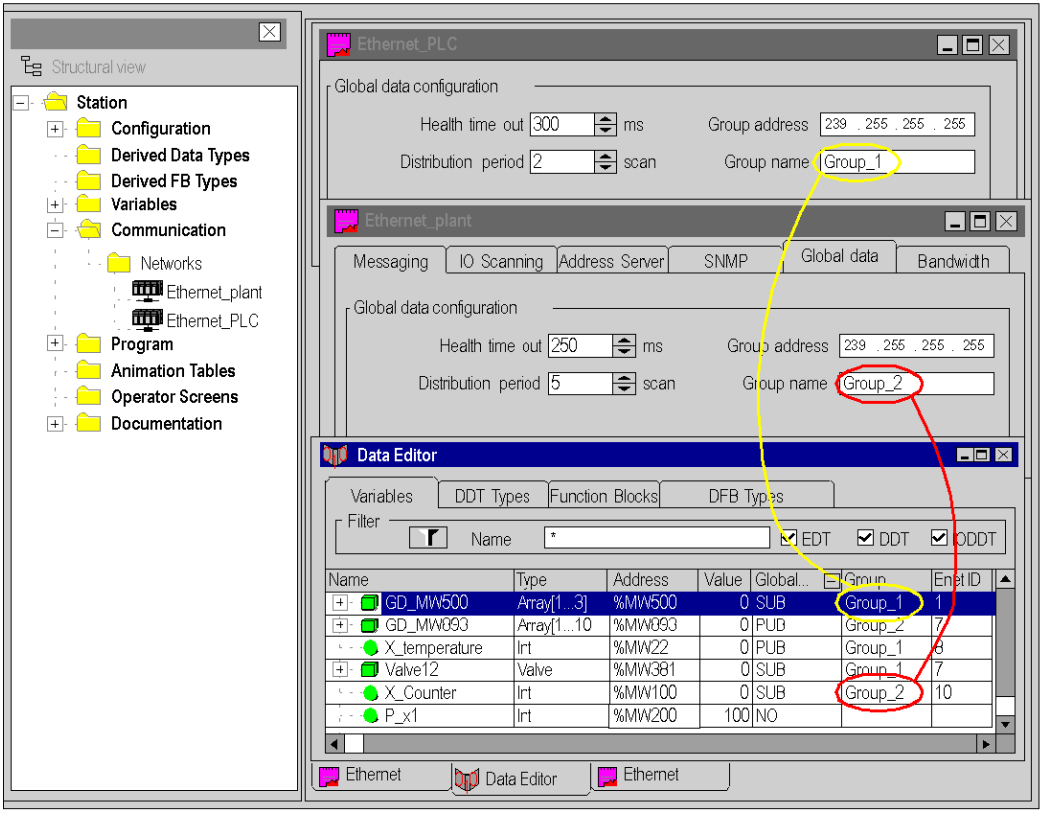
Link between Data and Communication

Network Variables and Groups

The groups of Ethernet network variables are created in the Ethernet network communication folders. An IP domain determines a group. In Unity Pro, one network can support only one group.

In Data Editor, the list of all current groups is provided to select in which group each Ethernet network variables is included. Nevertheless, the group field is also a free entry editing box, in order to give a group name not yet defined in communication folder. The build step checks this link.

The illustration shows corresponding fields in Communication configuration and the Data Editor:



Chapter 3
Software Settings for Ethernet Communication

Introduction

This chapter contains all information required for configuring Ethernet communication software settings.

What Is in This Chapter?

This chapter contains the following sections:

Section 3.1
Selecting the Ethernet Module

Selecting the Quantum NOE Ethernet Module

General Description

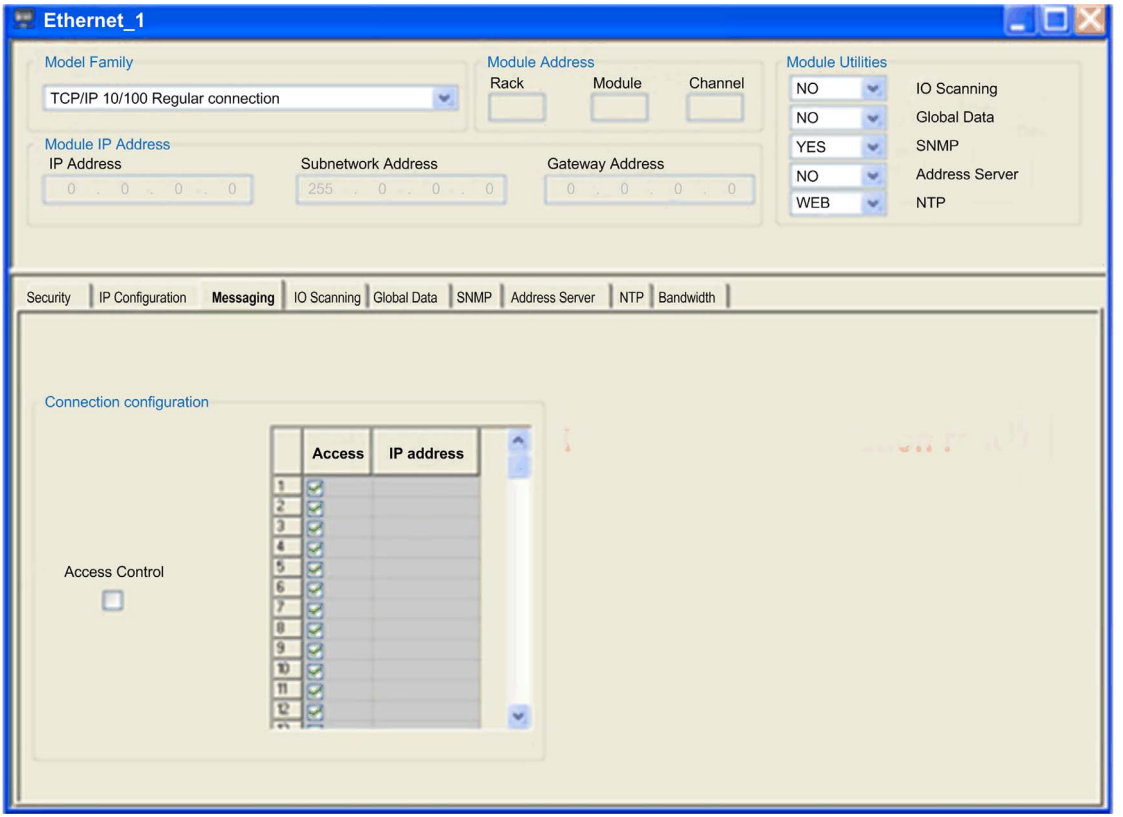
After configuring Ethernet communication *(see page 15)*, the Ethernet module parameters can be configured.

When you select the model family, all the corresponding communication module configuration options are displayed automatically. The module services allow the following settings to be made:

Setting	Description
No	Setting deactivated.
Yes	Setting activated. Parameters are set using the Unity Pro menu window.
Web	Setting activated. Parameters are set using the configured NOE Web pages. Unity Pro menu window deactivated. **Note**: Not available for every model family.

NOTE: The availability of the displayed settings depends on the selected model family and can vary.

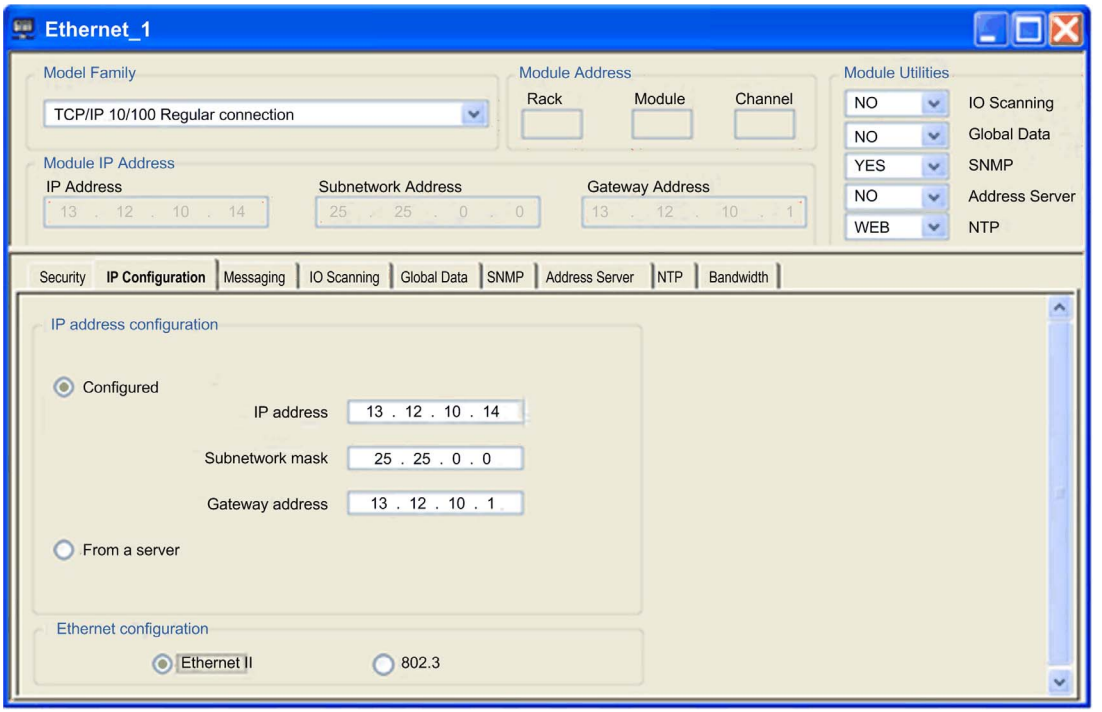
The screen shot shows an example of the menu window of the NOE Ethernet module (TCP/IP 10/100 Regular connection).



Parameter description:

Parameter	Description
Model Family	Quantum NOE Ethernet Module settings
Module Address	Not used
Module Utilities	For module service configuration options, see above
Module IP Address	Overview of the IP address parameter set

After selecting the model family **TCP/IP 10/100 Regular Connection,** the following mask appears. The image also displays the activated module services.



NOTE: The availability of the displayed register depends on the selected model family and can vary.

After selecting the **Yes** option in module services, the tab corresponding to the module is activated.

Section 3.2
IP Configuration

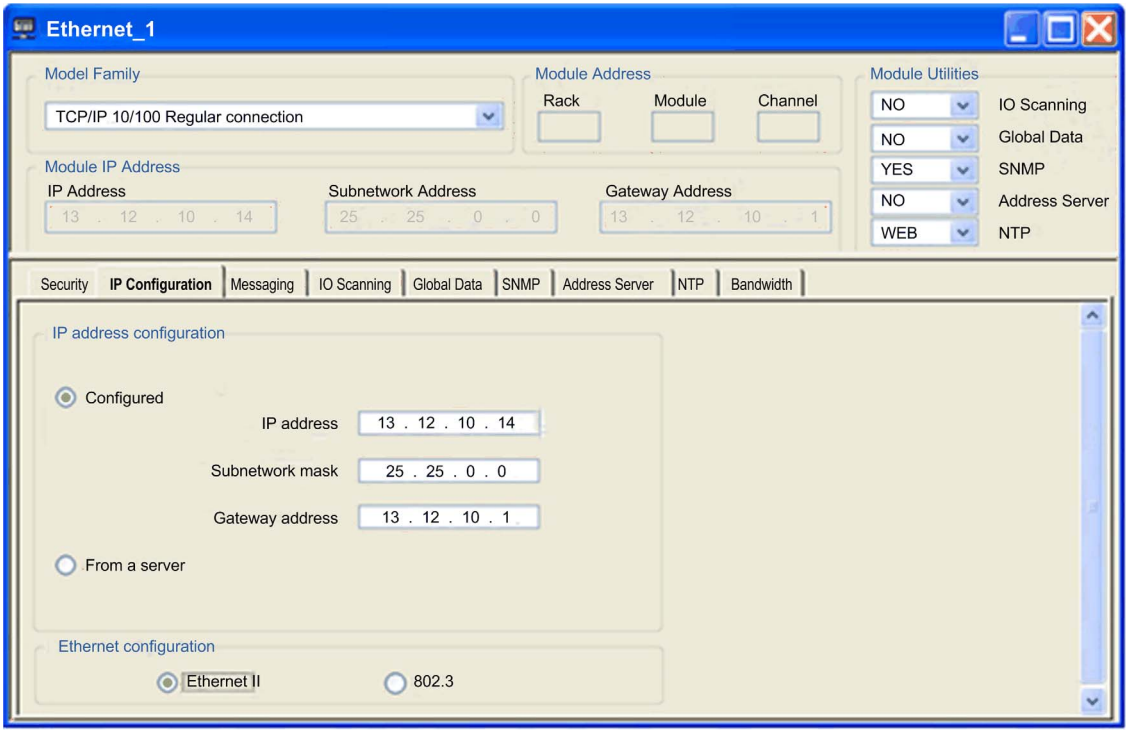
IP Configuration

General Description

The **IP configuration** tab enables you to configure IP address settings for the Quantum Ethernet module. IP address settings become active after:

- the hardware is connected
- the configuration is downloaded to the PLC in the Quantum Ethernet module

The following figure shows the IP configuration for the Quantum Ethernet model family:



Description of the selection properties

Selection	Description
Configured	Activate the IP address, subnet mask, and gateway address. The data is activated after the configuration is downloaded to the PLC.
Client / Server	The Quantum NOE Ethernet module receives its IP address parameter through a BOOTP server on startup.
Ethernet configuration	Select the default protocol as Ethernet or 802.3.

Section 3.3
Messaging

Quantum NOE Ethernet Messaging Configuration

Introduction

Ethernet messaging gives the user the opportunity to send and receive Ethernet messages. Data traffic is handled by the client/server procedure.

Parameter description:

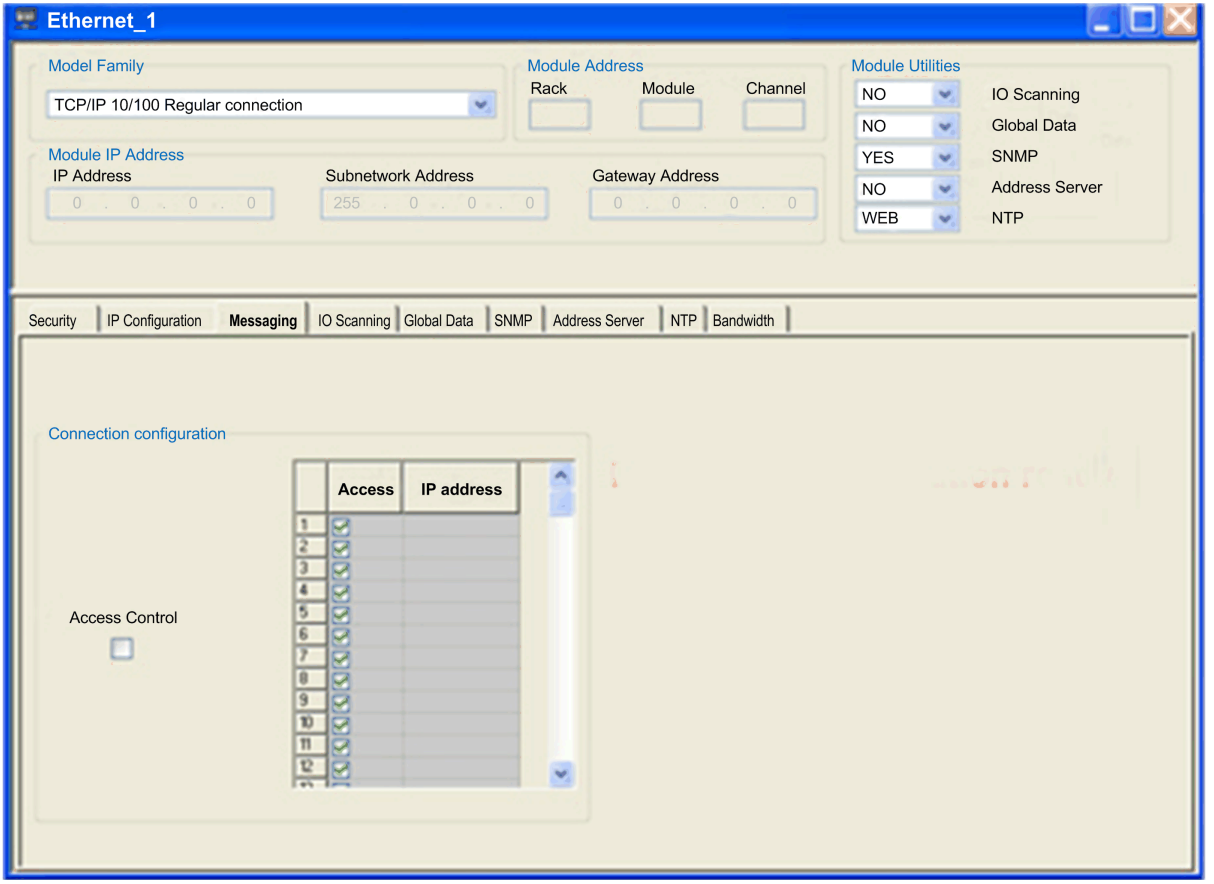
Setting	Description
Connection configuration	Activates general data transfer.
Access	Activates data transfer between specific nodes.
IP Address	Defines the node for the Ethernet Messaging procedure.
Access Control	Activates or deactivates control of remote devices that are attempting to open a TCP connection to the module.

Messaging Tab

The following procedure shows how to access the **Messaging** page:

Step	Action
1	In the Unity Pro project browser, go to the **Structural view**. Expand (**+**) the **Communication** folder until you locate the name of the Ethernet logical network associated with the module.
2	Right click the Ethernet logical network and select **Open**. **Result:** The module configuration screen appears.
3	Select the **Messaging** tab. (See the illustration below.)

The **Messaging** tab is shown below.



Configuration parameters can be accessed in two areas on the Messaging tab screen:

- the **Connection Configuration** area
- the **Access Control** area

Connection Configuration Area

The **Connection Configuration** area is used to:

- activate an access control utility
- list the remote devices that can connect to the module according to a communication protocol

Access Control

The **Access Control** box is used to activate or deactivate control of remote devices that are attempting to open a TCP connection to the module. The functionality depends on whether the box is checked or not:

- **checked:** Access control management is activated and the **Access** column of the table is active (no longer grayed out).
  - The module can only communicate to the addresses entered in the 128 available spaces in the **Slave IP Address** column.
  - With the module in client mode it can only connect to remote devices selected by the **Access** column in the **Connection Configuration** table.
- **unchecked:** Access control management is inoperative and the **Access** column of the table is not active (grayed out).
  - With the module in server mode, remote third-party devices can connect as clients (before communication with the module) without being declared in the table.

NOTE: Access control is only effective on the TCP/IP profile and assists module operations in server and client mode.

Section 3.4
I/O Scanner Configuration

Introduction

This chapter contains a description of the I/O Scanner configuration.

What Is in This Section?

This section contains the following topics:

I/O Scanner Concepts

Overview

The following information describes how to configure the I/O scanner.

Introduction

The NOE 771 0x, -x1 and CPU 651 x0 modules provide an I/O scanner. It will be configured with the Schneider Electric programming packages or directly by using the internal NOE I/O Scanner Web site (NOE 771 0x and -x1 only). In both ways, the user can configure data and transfer it between network nodes without using the MSTR instruction.

I/O Scan List

The I/O Scanner is a feature of the NOE module, which allows repeated reading and/or writing to Input/Output devices.

The I/O scan list is a configuration table that identifies the targets with which repetitive communication is authorized. The list contains enough information to enable each target to construct the MODBUS message addressed to the specified remote device and to designate where on the local controller the input and output data are to be mapped at the end of the scan. While the controller is running, the NOE module transfers data to and from the controller's registers and coils as indicated by the I/O scan list.

The user configures the I/O scan list with the Schneider Electric programming packages. There can be multiple instances of the I/O scan list (Peer Cop restrictions apply). The individual scan lists for each module are identified by the Quantum backplane slot number where the NOE is installed.

I/O Scanner Definitions

NOTE: Health bits run differently.

- I/O Scanner health bits run left to right.
- Global Data health bits run right to left.

The following table lists and defines the terms that are used to describe the I/O Scanner operation.

Term	Definition
Scan List	The list of input and/or output devices that the NOE module is configured to scan.
Specific Input	Input to the controller, on the backplane where the NOE resides.
Specific Output	Output from the controller, on the backplane where the NOE resides.
Peer Cop	Legacy I/O Scanner support to upgrade MODBUS Plus I/O applications to Ethernet.
Ethernet I/O Scanner	Provides high performance cyclic communication service to the controller.

Quantum Status Word Information

For a better diagnostic of the Quantum CPU status, the programmer has the possibility to analyze the Quantum status words.

For detailed information refer to *Unity Pro System Bits and Words, Reference Manual*..

Health Bits

The following bits contain the health status for the Quantum I/O Scanner and/or the Global Data.

- %SW139
  Global Data and I/O Scanning utility load
- %SW160 to %SW167
  Device operating status determined by I/O Scanning
- %SW168 to %SW171
  Operating status of Global Data

For detailed information refer to chapter *Quantum-specific System Words (see Unity Pro, System Bits and Words, Reference Manual)*.

Peer Cop and Enhanced MODBUS/TCP Scanners

The NOE 771 0x and -x1 module's design provides you with the ability to configure its MODBUS I/O Scanner as either a Peer Cop or Enhanced MODBUS scanner. The determination as to which scanner is used depends on the programming package that is installed on your system.

Peer Cop I/O Scanner Features

The following table lists the characteristics of the Peer Cop based MODBUS I/O Scanner.

Parameter	Value
Max. No. of Devices	64
Max. No. of Input Words	500
Max. No. of Output Words	500
Timeout Value	Global Setting (20 ms to 2 s in 20 ms increments
Input TimeOutState	Global Setting (Zero or Hold)
IP Address	Derived from MODBUS address (must be on NOE's subnet)
Remote Register Reference	Not configurable - 400001 is used
Destination ID	Not settable, set to 0
Operation through a MODBUS Plus to Ethernet bridge	Not supported

Enhanced MODBUS I/O Scanner Features

The following table lists the characteristics of the Enhanced MODBUS I/O Scanner.

Parameter	Value
Max. No. of Devices	64 or 128
Max. No. of Input Words	4,000
Max. No. of Input Words	4,000
Timeout Value	Individual Setting (10 ms to 2 s in 10 ms increments
Input TimeOutState	Global Setting (Zero or Hold)
IP Address	IPv4 Address
Destination ID	Not settable, set to 0
Operation through a MODBUS Plus to Ethernet bridge	Not supported
Operation through a MODBUS bridge	Supported

I/O Scanner Support

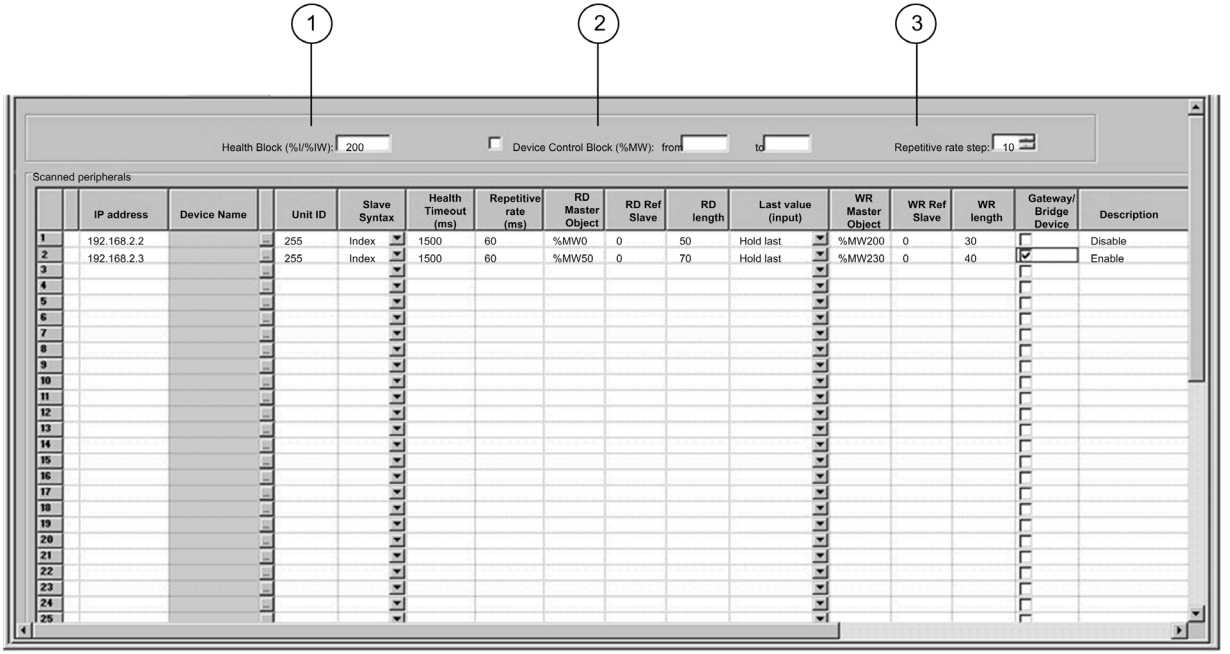
The following table summarizes the permissible mix of I/O scanners and NOE modules per CPU.

Quantum CPU Type	No. of NOEs Supported
140 CPU 311 10	2
140 CPU 434 12A	6
140 CPU 534 14A	6
140 CPU 651 50	6
140 CPU 651 60	6
140 CPU 658 60	6
140 CPU 670 60	3
140 CPU 671 60	6
140 CPU 672 61	6
140 CPU 678 61	6

Configuring the Quantum I/O Scanner

The I/O Scanner Configuration Dialog

When you click the **I/O Scanning** tab in the Ethernet module configuration screen, the **I/O Scanner** screen opens:



NOTE: This screen shows I/O Scanner services for an 140 NOE 771 01 or -11 module. The **I/O Scanner** screen is slightly different for the CPU 651 x0 module, which does not display a **Health Block** field.

Health Block

The **Health Block** field (number 1 in previous figure) lets you define the first word or bit in a health table. That table can be up to 8 words (%IW) or 128 bits (%I) in length. Each bit in the table represents the status of an individual device. The following table shows how the bits are displayed based on the data type you use.

Bit	Data Type	
	%I	%IW
1	%I1	%IW1.15
2	%I 2	%IW1.14
...		
16	%I16	%IW1.0
17	%I17	%IW2.15

By default, the table comprises words starting at %IW1.0. If you want to set the table to bits, you need to specify a %I value in an increment of 16 (%I1, %I16, %I32, etc.).

NOTE: The **Health Block** field is available only for the NOE 771 00, -01, and -11. It is not available for the CPU 651 x0.

NOTE: For Safety Monitor applications, the **Health Block** is mapped on %M/%MW from the UMA zone instead of %I/%IW.

Device Control Block

The **Device Control Block** (number 2 in previous figure) lets you disable any scanned device by setting a bit associated with that device to 1. The I/O scanner closes the connection and sets the Health Bit to 0 (unhealthy state).

To enable the **Device Control Block**, select the check box in the **I/O Scanner configuration** dialog (item 2 in previous figure).

NOTE: To enable the **Device Control Block**, use:
- Unity Pro at V2.0 or later
- an 140 NOE 771 01 or 140 NOE 771 11 at version 3.5 or later
- a 140 CPU 651 x0 at version 2.0 or later

If you attempt to enable the **Device Control Block** with an earlier version of the firmware, the I/O scanning service is disabled.
If the check box is not selected, the I/O scanner service is enabled, and you cannot disable the I/O scanning of individual devices.
Disabling I/O scanning with the **Device Control Block** is equivalent to ending communication between the scanner and the device.

Therefore:

- The fallback positions are applied to the inputs by the scanner.
- Communication with the device stops.
- All entries in the IN and OUT tables still transfer between the CPU and the scanner on each scan.

As a consequence of the last point above, if you modify a %MWi attached to an input, this %MWi is overwritten by the values coming from the I/O scanner in the next scan (with either 0 or the last input value).

It is possible (but meaningless) to access %MW attached to the outputs because they are not transmitted to the device.

Repetitive Rate Step

The **Repetitive Rate Step** (number 3 in previous figure) is set in multiples of 5 ms (the minimum) through 200 ms (the maximum).

The **Repetitive Rate** column is where you enter a rate of time for how often you want the I/O scanner to send a query to the device after the rate has timed out.

NOTE: The repetitive rate of the I/O scanner table is a multiple of the rate displayed in the **Repetitive Rate Step**. The real repetitive rate being executed by the I/O scanner service is shown in the **Repetitive Rate** column.

NOTE: An entry in the **Repetitive Rate** column is rounded up to the next multiple that was entered in the **Repetitive Rate Step** if the entry is not a multiple of the **Repetitive Rate Step**.
For example, if the entry in the **Repetitive Rate Step** is 5 and you enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 10; if you change the **Repetitive Rate Step** to 6 and enter a 7 in the **Repetitive Rate** column, the 7 is rounded up to 12.

I/O Scanner Table Parameters

The I/O Scanner parameters are described in the table below:

Parameter	Description	Example
Entry #	This is the first column; it has no name. Valid range: 1 ... 128 Each entry represents an I/O Scanning exchange on the network.	
IP address	This is the IP address of the scanned Ethernet slave device.	192.168.1.100
Device Name	To configure a device (Advantys island or DTM), click the **...** button to open the **Property** box *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)* to start the device configuration software. For an introduction to this procedure for Advantys, go here *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*. For an introduction to this procedure for DTMs, go to FDT Container *(see Unity Pro, Operating Modes)*. **NOTE:** While the **Property** box is open, **I/O scanning** cannot be edited.	MySTB1 or Master_PRM_DTM_10
Unit ID	This field associates the slave address of the device connected to an Ethernet/Modbus gateway with the IP address of that gateway: ● Value range: 1 to 255 ● Default value: 255 When using a bridge, enter the bridge index (1 to 255) in this field.	255

Slave Syntax	Use this drop-down menu to pick the way **RD Ref Slave** and **WR Ref Slave** values are displayed. There are 4 types of display available:
	● Index: 100
	● Modbus: 400101
	  ● (Modbus register)
	● IEC 0: %MW100
	  ● M340 and Premium PLC slaves
	● IEC 1: %MW101
	  ● Quantum PLC slaves
		Index (default value)

Parameter	Description	Example
Health Timeout (ms)	This field sets the maximum interval between the responses from a remote device. After this time period expires, the received data is invalid. The **Health Timeout** should be longer than the **Repetitive rate** time (ms). For a Quantum NOE Ethernet module, it also should be longer than the CPU scan time. For the **Health Timeout**: ● Range: 0ms to 65535 ms ● Interval: 1ms	1500 ms

Repetitive rate (ms)	The rate at which data is scanned, from 0...65535 in multiples of the **Repetitive Rate Step**:
	● If you are running Unity Pro V3.1 or earlier with the following firmware versions:
	  ● 140 NOE (V4.0 or earlier): 16 ms
	  ● CPU (V2.5 or lower): 10 ms
	● If you are running Unity Pro V4.0 or later with the following firmware versions:
	  ● 140 NOE (V4.3 or later): 5 - 200 ms
	  ● CPU (V2.6 or later): 5 - 200 ms
		60 ms

RD Master Object*	Destination address in the master PLC where, from each device, newly read information is stored	%mw10
RD Slave Ref.**	Source address index in the slave/remote device	The format of this value depends on the **Slave Syntax**: ● Index: 5 ● Modbus: 400006 ● IEC 0: %MW5 ● IEC 1: %MW6
RD length	Number of words to read	10
Last value (Input)	This field configures the behavior of inputs in the event of an access error in relation to the remote device (for example: inoperative network or device power supply, etc.): ● Set to 0: fall back to 0 ● Hold last: maintain last value	Hold last

Parameter	Description	Example
WR Master Object*	Source address of the master PLC whose data is being written into the slave/remote device. Write operations are always performed at the word level.	%mw20
WR Slave Ref.**	The address of the first word written into the slave/remote device.	The format of this value depends on the **Slave Syntax**: ● Index: 1 ● Modbus: 400002 ● IEC 0: %MW1 ● IEC 1: %MW2
WR length	Number of words to be written	10
Gateway/Bridge Device	To allow slower TCP/IP network devices (i.e., gateways and bridges) to be compatible with the I/O Scanner: ● Select the check box to enable this feature. Defines a new bit, and sets it to high (1). ● Deselect the check box to disable this feature (default). Defines a new bit, and sets it to zero (0).	
Description	Additional information	
*Master refers to the client PLC that makes the request. **Slave refers to the server from which data is read or to which data is written.		

NOTE: For more information, refer to the Contextual Menu for Copy/Cut/Paste topic *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

NOTE: For more information, refer to the I/O Scanning with Multiple Lines topic *(see Modicon M340 for Ethernet, Communications Modules and Processors, User Manual)*.

Section 3.5
Global Data Configuration

Introduction

This chapter contains a description about Global Data configuration.

What Is in This Section?

This section contains the following topics:

Planning the Global Data (Publish/Subscribe) System

Overview

Global Data service is a real-time publisher/subscriber mechanism that provides the most efficient data exchange for PLC application coordination.

Devices that support Global Data are arranged in a distribution group for the purpose of application variable exchange and synchronization. Each Global Data device can publish up to one network (application) variable and subscribe to up to 64 network (application) variables.

The Quantum NOE's embedded **Global Data Configuration** Web page provides a configuration screen *(see page 47)* to determine which and how many application variables are exchanged with this service. After configuration, exchanges between all stations belonging to the same distribution group are done automatically.

The Global Data service uses %MW (4x registers) or unlocated variables for Global Data exchanges.

Key Features of Global Data

The main features for Global Data are:

- One publisher and many subscribers
- A device can publish one network variable of up to 512 %MW words (4x registers) or unlocated variables
- A device can subscribe to up to 64 network variables of up to 2048 %MW words (4x registers) or unlocated variables
- A device subscribes to the complete network variable
- One distribution group per network IP address
- Application-defined publication rate
- Up to 64 Global Data Network variables (numbered from 1 to 64) can be part of the data distribution group
- An NOE has only one multicast address. Consequently, it can only publish and subscribe within the group
- A device can participate in several distribution groups by using multiple NOEs in the rack

Global Data has an advantage over client/server services when more than one subscriber is receiving the same data since only one transaction is necessary for all subscribers to receive the data. There are two benefits:

- the reduction of overall network traffic
- tighter synchronization of multiple subscribers

Planning Your System Configuration

The Global Data (publish/subscribe) utility is a powerful function incorporated into the NOE product line. Implementing Global Data requires a configuration that spans many PLCs throughout the system. Therefore, we recommend pre-planning your installation before implementation. Pre-planning saves time and money by:

- reducing errors, which circumvents a debugging effort
- ensuring system consistency

Go to paper before computer.

We offer the following table to assist in system planning. The **Global Data Planning Spreadsheet** below is a graphic representation of a recommended configuration table for system planning. You can create your own table using the format below or you can download a Microsoft *Excel*™ spreadsheet template, which is available on the Schneider public Web site.

Here is the graphic representation of the **Global Data Planning Spreadsheet**:

Parameter Checking	**Variable ID**	**Symbol***	**Length (Registers)**	**Device Number**				**Variable Public. Status**
				1	2	...	3	
	1	*VALVE_STATUS*	*20*	*PUB*	*SUB*		*NONE*	OK
	2	*VALVE_CONTROL*	*10*	*SUB*	*NONE*		*PUB*	OK
	...							
	64	*PUMP_CONTROL*	*50*	*SUB*	*PUB*		*NONE*	OK
			Device Publication Status:	OK	OK		OK	
			Total Publication Size per Node:	20	50		10	
			Total Subscription Size per Node:	60	20		0	
Group IP Address		*239.255.255.0*						
Multicast Filtering Enabled		*OFF*						
Default %MW Address for Health		*%MW100*						
Distribution Period		*10*						
Health Timeout		*1000*						
Data Zone		*%MW200*						
*Entries or changes to the symbol (description) do NOT affect or change a variable or the system. The symbol used in the Quantum product line has no relation to the Concept/Unity product line symbol(s).								

Table of **Global Data Limits**:

Parameter	Limit
Maximum number of publish variables per device	1
Maximum size for the publish variable	512 registers = 512 Words (16 bits) = 1024 bytes
Maximum number of subscription variables per device	64 (63 if this device is publishing)
Maximum size for the subscribe variables per device	2048 registers = 2048 Words (16 bits) = 4096 bytes

NOTE: We recommend that you consider the following when planning.

- Allow for a 10 to 20 % increase in growth of any variable.
- Add variables at the end of the configuration where they do not affect the existing application address. Therefore, you avoid changing the existing addresses in your configuration, which can be a time consuming process.

Table of **Global Data Planning Spreadsheet**

Parameter	Description
Parameter Checking	Reserved
Variable Id	Represents the Data ID on the NOE's **Global Data Configuration** Web page
Symbol	Symbolic name for Global Data exchange.
Length Words (Registers)	Length of Global Data information. Number of %MW words (4x registers) or unlocated variables.
Device Number	Number of devices (up to 64) for the Global Data network.
Variable Public Status	Automatic information of the correct publication status of the Global Data network. Only by using the Microsoft *Excel*™ spreadsheet. Information per symbol.
Device Publication Status	Automatic information of the correct publication status of the Global Data network. Only by using the Microsoft *Excel*™ spreadsheet. Information per device.
Total Publication Size per Node	Publication size for the specific node. The maximum publication size is 512 words (registers) per node
Total Subscription Size per Node	Subscription size for the specific node. The maximum subscription size is 2048 words (registers) per node
Group IP Address Enabled	IP address for multicast networking. Identifies the stations distribution group. The address range is from 224.0.0.0 to 239.255.255.255

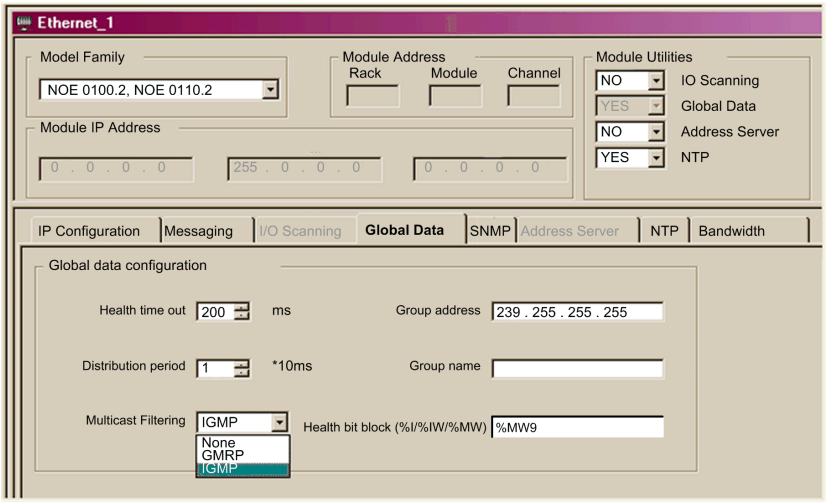
Parameter	Description
Multicast Filtering Enabled	A check box for Ethernet switches that support multicast filtering.
Default Address for Health%MW (4x register)	%MW (4x register) address for the Health bits. This is the memory area where the Health bits are stored. It has the size of 4 words (registers).
Distribution Period	Is the minimum number of controller scan times before an update will occur.
Health Timeout	Is the maximum time between received subscriptions before a subscription is declared unhealthy (faulty). The value is measured in milliseconds and can be set from 50 to 15000 ms in 50 ms increments.
Data Zone	The starting address for the data. This are the registers where the data information are stored.

Quantum NOE Global Data Configuration

Introduction

Global data configuration is carried out in the network configuration as well as the data editor. The variables for the publish/subscribe procedure are configured in the data editor.

The screen shot shows the network configuration global data configuration settings:

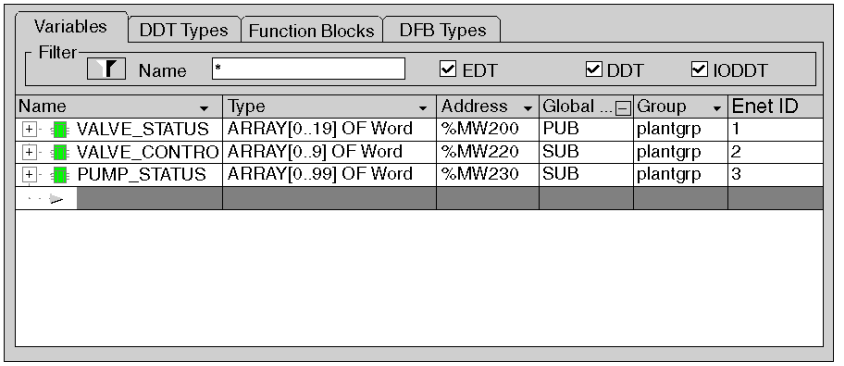


Parameter description:

Parameter	Description
Health time out	After this time period expires, the received data becomes invalid.
Group address	Class D multicast IP address. All nodes in the global data procedure use the same multicast address for distributing or receiving data. The address range is: 224.0.0.0 to 239.255.255.255.
Distribution period	Time after which the data is received or sent. Minimum scan time of the PLC.
Group name	Logical name. Defines the varibale allocation to different communication configurations in the variable editor.
Health bit block	Address for retrieving the status information of the global data procedure.
Multicast filtering	Activates an Ethernet module that supports multicast filtering. From the drop down list, select: ● None: disable both GMRP & IGMP (Data will be sent to all end devices in the network.) ● GMRP Make sure your client, server and switches, and routers support and enable GMRP. ● IGMP V1 Make sure your client, server and switches, and routers support and enable IGMP. **Note:** The following modules support IGMP V1: ● 140 NOE 771 01 V4.4 or later ● 140 NOE 771 11 V4.4 or later ● 140 CPU 651 50/60 V2.7 or later **NOTE:** The **IGMP** and **None** features are only available in Unity 4.1 or later.

NOTE: A Quantum PLC does not update health bits in `STOP` mode.

The screen shot shows an image of the data editor:



Parameter description:

Parameter	Description
Name	Variables symbols
Type	Variable type
Address	Variable address
Global Data	Type of Global Data Variable. Options: No/Publish/Subscribe
Group	Group name for allocating the variables of the existing network description. When creating the different Ethernet networks, a logical connection is arranged here between the network and the variable declaration.
ID	Variable ID

Section 3.6
SNMP Configuration

Introduction

This chapter contains a description about how to configure a Simple Network Management Protocol (SNMP).

NOTE: Simple Network Management Protocol (SNMP) is not supported by the CPU 651 x0 modules.

What Is in This Section?

This section contains the following topics:

SNMP

Introduction

This topic describes the Simple Network Management Protocol (SNMP), which is configured on your NOE or 140 CPU 651 x0. Network management software allows a network manager to:

- monitor and control network components
- isolate problems and identify their causes
- query the status of devices such as a host computer, routers, switches, and bridges
- obtain statistics about the networks to which devices are connected

Manager/Agent Paradigm

Network management software follows the conventional client-server model. To avoid confusion with other network communication protocols that use the client/server terminology, network management software uses the following terms:

- *manager*: the client application that runs on the manager's computer
- *agent*: the application that runs on a network device

The manager uses conventional transport protocols (for example, TCP or UDP) to establish communication with the agent. Managers and agents then exchange requests and responses according to the network management protocol.

Simple Network Management Protocol

Your NOE module is configured with SNMP, which is the standard protocol used to manage a local area network (LAN). SNMP defines exactly how a *manager* communicates with an *agent*.

The SNMP defines the format of the requests that a manager sends to an agent and the format of the replies that the agent returns to the manager.

The MIB

Each SNMP object has to be defined and given a unique name. Both the manager and agent programs must agree on the names and the meanings of the fetch and store operations. The set of all objects SNMP can access is known as a *Management Information Base (MIB*).

Private MIB

Schneider obtained a private MIB, Groupe_Schneider (3833). Under the Groupe Schneider private MIB is a Transparent Factory Ethernet (TFE) private MIB. The Transparent Factory SNMP embedded component controls the Schneider private MIB function.

Choosing an SNMP Manager

If you already have a working SNMP manager, you may continue to use it. Any of the many SNMP version 1-compliant managers on the market will work.

If you do not currently use an SNMP manager in your organization and are evaluating SNMP managers for purchase, then we recommend that you consider HiVision with the ConnexView Add-On developed for use with Schneider Electric PLCs.

Please contact your Schneider Electric sales office for availability and pricing of HiVision and ConnexView.

Using an SNMP Manager

The process for obtaining an SNMP manager:

Step	Action
1	Get Schneider `.mib` file from the NOE Web page. Find the `.mib` file as a packed file under **/wwwroot/SchneiderTFE.zip** on your NOE module.
2	Load `.mib` file to the SNMP manager.
3	When you are done, you will see the Schneider private MIB manager in your manager.

Other SNMP Resources

SNMP and related subjects are well-documented on Web sites and in many books:

- As of this writing, a useful description appears on Microsoft's *Technet* pages. Browse to *http://www.microsoft.com/technet*. Use the **Search** function to find "Network Management for Microsoft Networks Using SNMP."
- Use an Internet search engine to search for an SNMP introduction, tutorial, or other resource.
- The SNMP FAQs from the news group `comp.protocols.snmp` appear on many `.com` and `.org` Web pages. Search for the combination of "`comp.protocols.snmp`" and "`FAQ`."

ASN.1 Naming Scheme

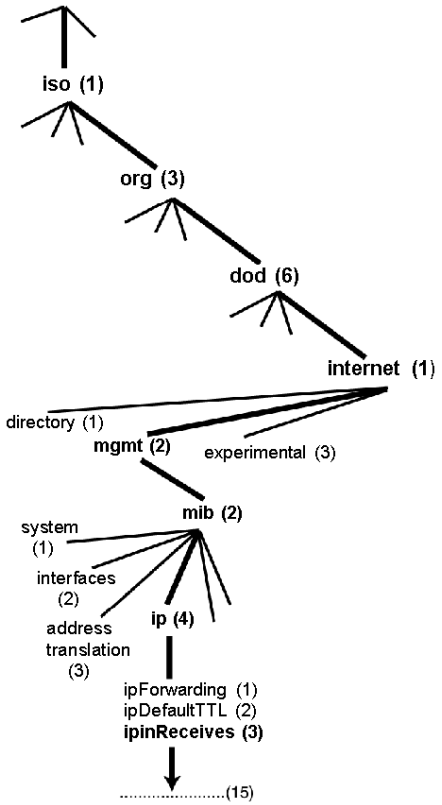
ASN.1 Overview

Abstract Syntax Notation One (ASN.1) is a formal language for abstractly describing messages to be exchanged between distributed computer systems.

An Example

Objects in a MIB are defined with the ASN.1 naming scheme that assigns each object a long prefix that guarantees that the name will be unique. For example, an integer that counts the number of IP datagrams that a device has received is named: *iso.org.dod.internet.mgmt.mib.ip.ipinReceives*.

The following figure depicts the ASN.1 naming scheme example.



This object name is represented in an SNMP message by assigning each part an integer. So, the above message would appear as 1.3.6.1.2.2.4.3.

Each integer has the following meaning:

- 1 = ISO (International Organization for Standardization)
- 3 = identified organization (one of branches under the ISO root)
- 6 = U. S. Department of Defense (DoD) (one of the children under branch1.3)
- 1 = the Internet subtree under 1.3.6
- 2 = the mgm branch — (one of seven) of the Internet subtree. It is managed by the Internet Assigned Numbers Authority, and includes the standard MIBs
- 2 = mib-2(1) group of managed objects
- 4 = ip (the mib-2(1) IP group (one of 11))
- 3 = ipinReceives (the MIB object)

Configuring an NOE with SNMP

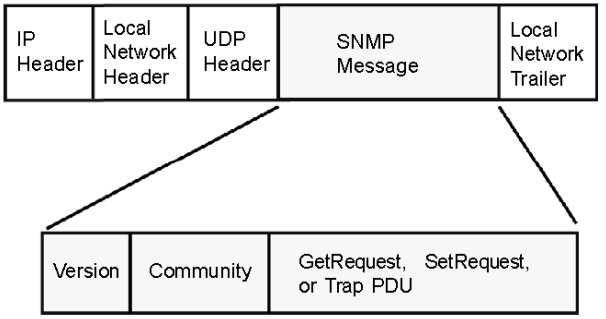
Object Identifier (OID)

In the ASN.1 Naming Scheme example *(see page 53)*, the MIB object identified by the notation 1.3.6.1.2.2.4.3 is referred to as the Object Identifier or OID. All OIDs can be seen as part of a tree structure that begins at the root (ISO) and branches out with each subtree identified by an integer.

SNMP Protocol Data Units

SNMP uses protocol data units (PDUs) to carry the requests and responses, between the manager and the agents, for the information contained in an OID.

As the following figure shows, the SNMP message is the innermost part of a typical network transmission frame.



The PDUs within the SNMP initiate the communication between the manager and the agents.

The SNMP installed on your NOE module uses the following three PDUs:

- GetRequest
- SetRequest
- Trap

GetRequest PDU

The GetRequest (shortened to Get) PDU is used by the SNMP manager to retrieve the value of one or more objects (OIDs) from an agent.

SetRequest PDU

The SetRequest (shortened to Set) PDU is used by the SNMP manager to assign a value to one or more objects (OIDs) residing in an agent.

Trap PDU

The Trap PDU is used by the agent to alert the manager that a predefined event has occurred.

Version & Community Identifiers

The version identifies the version number of the SNMP software being used by the manager and the agent. Your NOE supports Version 1 of the SNMP. The community is an identifier that you assign to your SNMP network. If community names for the manager and the agent do not agree, the agent will send an authentication failure trap message to the manager. If the community names and version number agree, the SNMP PDU will be processed.

What Can Be Configured

Your NOE module can be configured to send an authentication trap to two SNMP managers if it receives a community name in a Get/Set request that does not match the configured name. Also, you can configure the SysContact and SysLocation via the configuration page in the module's embedded web pages. After making changes in the SNMP Configuration Web page and to set those changes, reboot the module using hot swap.

Configuring an NOE with TFE Private MIB

Introduction

A MIB, a Management Information Base, is an element used in network management. Network management services are based on the need to monitor and manage:

- performance
- fault occurrences
- security

Each MIB contains a finite number of objects. Manage your MIB with a management station running an SNMP management application. The management application uses **GETs** and **SETs** to retrieve system information and to set system environment variables.

Schneider Private MIB

Schneider Electric obtained a Private Enterprise Number (PEN) from the Internet Assigned Numbers Authority (IANA). That number represents a subtree in the SNMP MIB, a number that is a unique identifier used for Groupe Schneider.

The object identifier for the root of the Groupe Schneider subtree is **`1.3.6.1.4.1.3833`** and represents a path to the subtree as follows:

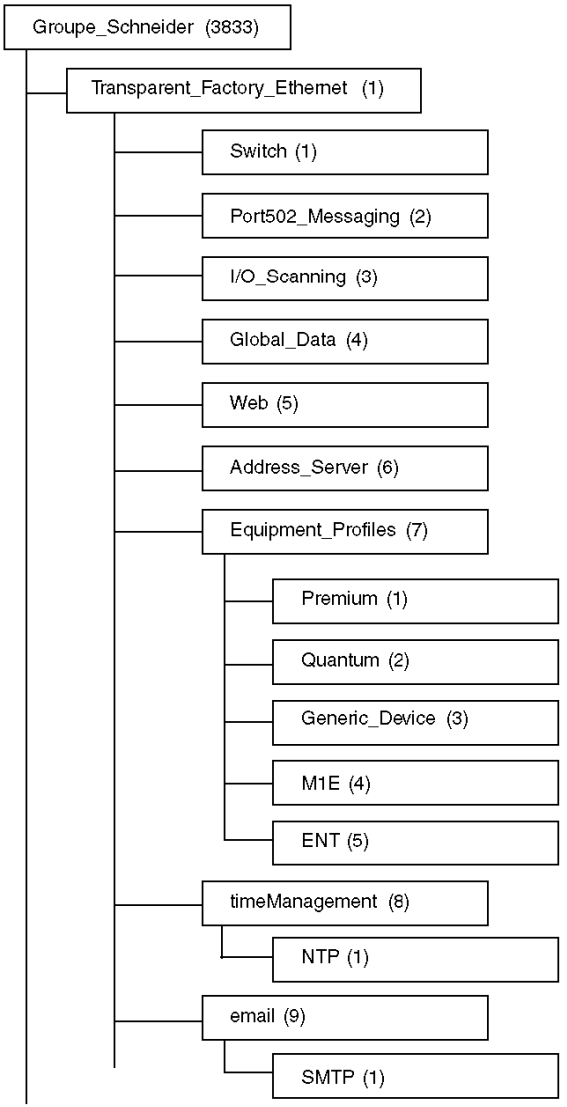
```
iso(1)
        org(3)
                dod(6)
                        internet(1)
                                private(4)
                                        enterprise(1)
                                                GroupeSchneider(3833)
                                                        Transparent_Factory_Ethernet(1)
```

Under the GroupeSchneider private MIB is a Transparent Factory Ethernet (TFE) private MIB, **Transparent_Factory_Ethernet(1)**.

TFE Private MIB

The Transparent Factory SNMP-embedded component controls the Schneider private MIB function. The Schneider private MIB, and associated services, perform Network Management on all system components. The Transparent Factory private MIB provides the data to manage the main Transparent Factory communication services for all the communication components of the Transparent Factory architecture (ETYs, NOEs, third party toolkit, ENTs, M1Es). The Transparent Factory private MIB does not define the specific management applications and policies.

The diagram following illustrates the Schneider Electric (Groupe_Schneider (3833)) private enterprise MIB subtree.



The **Groupe_Schneider (3833)** subtree is the root of Groupe Schneider's private MIB in the Structure of Management Information (SMI) used by SNMP and defined in RFC-1155, which is a specification that defines the structure and identification of management information for TCP/IP-based networks.

Transparent Factory Ethernet Subtree

The **Transparent_Factory_Ethernet (1)** subtree defines groups that support the Transparent Factory Ethernet services and devices.

Service	Subtree Definition
Switch(1)	brand of switches labeled: ConneXium switches private MIB
Port502_Messaging(2)	objects for managing explicit client/server communications supporting applications, such as HMI, SCADA, or programming tools
I/O_Scanning(3)	objects for managing I/O device communications that use the I/O Scanner mechanism with the MB/TCP protocol
Global_Data(4)	objects for managing the application coordination service using a publish/subscribe protocol
Web(5)	objects for managing the activity of the embedded Web servers
Address_Server(6)	objects for managing the activity of the BOOTP and (or) DHCP servers
Equipment_Profiles(7)	objects for each type of device in Transparent Factory Ethernet's product portfolio
timeManagement(8)	objects for managing the UTC time stamp service
email(9)	objects for managing the mail service

Device subtrees, or groups, will be defined for the following devices:

- **Premium(1)**
- **Quantum(2)**
- **Generic_Device(3)**
- **M1E(4)**
- **ENT(5)**

As devices are added to Schneider's catalog, Schneider's private MIB will be extended in the following manner:

- If needed, a Transparent Factory, communication-service object will be added for the new device in the corresponding **Equipment_Profiles(7)** subtree. This subtree can hold as many objects as are required.
- If needed, a new branch will be added at the same level as **Transparent_Factory_Ethernet(1)**. This subtree will be created for product-specific objects (such as the ATV58 object under the **IndustrialControlProducts (3) subtree**).

When a new device is created, a corresponding object description is created in the ASN.1 format. The ASN.1 file(s) are then given to producers of SNMP manager software for inclusion in their products.

Port502 Messaging Subtree

The Port502_Messaging (2) subtree, or group, provides connection management and data flow services. The following list describes the function of each object.

Service	Indicates . . .
port502Status(1)	status of the service (idle, operational)
port502SupportedProtocol(2)	supported protocols (MODBUS, Xway)
port502IpSecurity(3):	status of the Port502 IP Security service (enabled/disabled)
port502MaxConn(4)	maximum number of TCP connections supported by the Port502 entity
port502LocalConn(5)	TCP connection number currently opened by the local Port502 entity
port502RemConn(6)	TCP connection number currently opened by the remote entity to the local Port502 entity
port502IpSecurityTable(7)	a table containing the number of unsuccessful TCP connection open tries from a remote TCP entity
port502ConnTable(8)	a table containing Port502 TCP specific information (MsgIn, MsgOut)
port502MsgIn(9)	total number of Port502 messages received from the network
port502MsgOut(10)	total number of Port502 messages sent from the network
port502MsgOutErr(11)	total number of error messages built by the Port502 messaging entity and sent to the network
port502AddStackStat(12)	the support of additional port502 stack statistics: ● 1 - disabled ● 2 - enabled
port502AddStackStatTable(13)	additional stack statistics for Port502 (optional)

I/O Scanning Subtree

The I/O_Scanning (3) subtree, or group, contains the objects related to I/O scanning device management and associated MODBUS communications on Port502.

Service	Indicates . . .
ioScanStatus(1)	global status of the I/O scanning service: ● 1 - idle ● 2 - operational ● 3 - stopped
ioScanMaxDevice(2)	maximum number of devices supported by the I/O scanning entity
ioScanPolledDevice(3)	number of devices currently polled by the I/O scanning entity
ioScanTransSend(4)	total number of transactions sent by the I/O scanning entity
ioScanGlbHealth(5)	global status of health for the I/O scanning service: ● 2 - OK: Every remote I/O device is responding ● 4- Warning: At least one remote I/O device is not responding
ioScanDeviceTable(6)	a table containing information on each remote devices polled by the I/O scanning entity

Global Data Subtree

The Global_Data (4) subtree, or group, contains the objects related to the Global Data service.

Service	Indicates . . .
glbDataStatus(1)	global status of the Global Data service: ● 1 - idle ● 2 - operational ● 3 - stopped
glbDataMaxPub(2)	maximum number of published variables configured by the Global Data entity
glbDataMaxSub(3)	maximum number of subscribed variables configured by the Global Data entity
glbDataPub(4)	total number of publications sent to the network
glbDataSub(5)	total number of subscriptions received from the network
glbDataPubErr(6)	total number of publication errors detected by the local entity
glbDataSubErr(7)	total number of subscription errors detected by the local entity
glbDataGlbSubHealth(8)	global status of health for the Global Data subscribed variables: ● 2 - OK: The health status of all subscribed variables is OK ● 4 - Warning: At least one subscribed variable has a health fault
glbDataPubTable(9)	a table containing information on each published variable (the number of publications, the source IP address, the number of errors)
glbDataSubTable(10)	a table containing information on each subscribed variable (the number of subscriptions, the source IP address, the number of errors, Health)

Web Subtree

The Web (5) subtree, or group, contains the objects related to the Web server service.

Service	Indicates . . .
webStatus(1)	global status of the Web service: ● 1 - idle ● 2 - operational
webPassword (2)	switch to enable or disable the use of Web passwords: ● 1 - disabled ● 2 - enabled
webSuccessfullAccess (3)	total number of successful accesses to the Web site
webFailedAttempts (4)	total number of unsuccessful accesses to the Web site

Address Server Subtree

The Address_Server (6) subtree, or group, contains the objects related to the Address Server service. The Address Server can be either a BOOTP server or a DHCP server.

Service	Indicates . . .
addressServerStatus(1)	global status of the address server service: ● 1 - idle ● 2 - operational

Equipment Profile Subtree

The Equipment_Profiles (7) subtree contains a set of common objects.

Service	Indicates . . .
profileProductName(1)	the commercial name of the communication product in a string form (for example, 140 NOE 771 11)
profileVersion(2)	the software version of the communication product in a string form (for example, Vx.y or V1.1)
profileCommunicationServices(3)	the communication services supported by the profile (Port502Messaging, I/O scanning Messaging, Global Data, Web, and Address Server)
profileGlobalStatus(4)	the global status of the communication module: ● 1 - NOK ● 2 - OK
profileConfigMode(5)	the IP configuration mode of the communication module: ● 1 - Local: The IP configuration is created locally ● 2 - dhcpServed: The IP configuration is created by a remote DHCP server
profileRoleName(6)	rthe ole name for the IP address management if it exists (empty string if there is none)
profileBandwidthMgt(7)	the status of Bandwidth Management: ● 1 - disabled ● 2 - enabled
profileBandwidthDistTable(8)	the CPU time distribution between Global Data, Port502 Messaging, I/O scanning
profileLedDisplayTable(9)	a table giving the name and the state of each module's LEDs
profileSlot(10)	the position of the communication module inside the rack if there is one. If there is no rack, the profileSlot value will be zero
profileCPUType(11)	the host for which that communication module is a part when a CPU type exists (if there is no host, the string is empty)
profileTrapTableEntriesMax(12)	the maximum numbers of entries in the Trap Table (equal to the number of possible remote managers)

Service	Indicates . . .
profileTrapTable(13)	a table allowing you to enable or disable the private traps for each of the communication services
profileSpecificId(14)	a unique Profile Specific Identification inside the equipmentProfile object of the Schneider Transparent Factory MIB (for example, the PLC Premium family is 100)
profileIpAddress(15)	the IP address of the SNMP agent
profileIpNetMask(16)	the subnet mask associated with the IP address of the SNMP agent (the value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0)
profileIpGateway(17)	the default Gateway IP address of the SNMP agent
profileMacAddress(18)	the Ethernet media-dependent address of the SNMP agent

NTP Subtree

The NTP (1) subtree contains a set of common objects.

Service	Indicates . . .
ntpStatus(1)	the status of NTP service (not server): **1.** 1 = Idle no configuration **2.** 2 = Operational
ntpSrvAddr(2)	the IP address of NTP server in dot notation format
ntpLnkSrvStatus(3)	the status of link between module and NTP server: **1.** 1 = NOK (module can not reach NTP server) **2.** 2 = OK
ntpReqCnt(4)	the number of requests sent to NTP server
ntpRespCnt(5)	the number of responses received from NTP server
ntpErrCnt(6)	the total number of communication errors
ntpDate(7)	date of the day
ntpTime(8)	time of the day
ntpTimeZone(9)	current time zone
ntpDSTStatus(10)	Daylight Savings Time status: **1.** 1 = ON (Daylight Savings Time) **2.** 2 = OFF (Standard Time)
ntpLastErr(11)	Last error code generated by system

SMTP Subtree

The SMTP (1) subtree contains a set of common objects.

Service	Indicates . . .
emailIndex(1)	the index value in the email service table
smtpStatus(2)	the status of SMTP service (not server): ● 1 = Idle (no configuration) ● 2 = operational
smtpSrvAddr(3)	the IP address of SMTP server in dot notation format
smtpMailSentCnt(4)	the total number of emails sent to the network and successfully acknowledged by the server
smtpErrCnt(5)	the total number of email messages that could not be sent to the network or that have been sent but not acknowledged by the server
smtpLastErr(6)	the error code of the last error that occurred while trying to send an email message to the network
smtpLastMailElapsedTime(7)	the number of elapsed seconds since last successful email was sent to the server
smtpLnkSrvStatus(8)	the status of link with SMTP server: **1.** 1 = NOK (not OK), link is down; module failed to contact SMTP server **2.** 2 = OK
smtpSrvChkFailCnt(9)	the number of times the link to SMTP server is detected as ‘down.’

See the Electronic Mail Notification Service subtree table *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

NOTE: A diagram of the Schneider Electric private enterprise MIB subtree appears in Simple Network Management Service (SNMP) *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*.

Private Traps and MIB Files

Traps are used to signal status changes to the manager. Using traps helps to avoid adding traffic.

The status changes signaled by the trap are for the:

- LEDs
- communication ports
- I/O scanning health values
- Global Data health
- NTP service
- SMTP service

The following list describes the characteristics of private traps, which means that they can:

- send messages to the two managers whose IP addresses are configured in the SNMP configuration (either the PL7 or the Web page)
- use the community name given to this configuration
- enable or disable each of the Transparent Factory Ethernet Private MIB groups: Switch (1), Port502_Messaging (2), I/O_Scanning (3), Global_Data (4), Web (5), Address_Server (6), Equipment_Profiles (7), NTP (8), and SMTP (9)

Private traps are described in the MIB ASN.1 description, which is contained in a **`.mib`** text file.

NTP Traps

1. **DST Change Trap:** notifies the manager that the NTP server time has changed either from (a) standard time to daylight saving time or (b) daylight saving time to standard time
2. **NTP Status Change Trap:** sent when the NTP component status changes (ntpStatus(1))
3. **Leap Second Trap:** sent when leap seconds are inserted

SMTP Traps

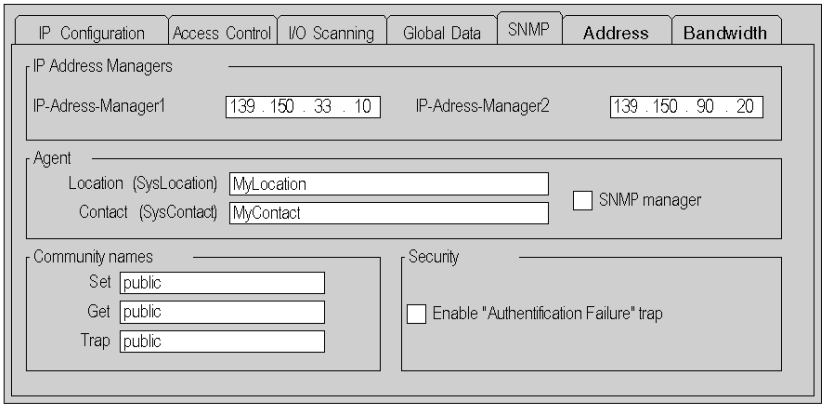
1. **SMTP Status Change Trap:** sent when SMTPStatus changes
2. **SMTP Link to Server Status Change:** sent when tSMTPLnkSrvStatus changes. Trap is sent when service tries to send an email. Every 30 minutes a periodic test checks the connection to the SMTP server.

Quantum NOE SNMP Configuration

Introduction

The SNMP settings described are entered in the following mask.

The screen shot shows an image of the SNMP configuration.



Parameter description

Parameter	Description
IP address manager1	IP Address (Computer) of the SNMP responsibility
IP address manager2	Alternative IP Address (Computer) of the SNMP responsibility, e.g. substitute.
Location (SysLocation)	Information about module location
Contact (SysContact	Information about the system administrator
SNMP manager	Reserved
Setting	Security setting for rights to modify the configuration. (Public/Secret)
Getting	Security setting for rights to view the configuration settings. (Public/Secret)
Trap	Security setting for rights to receive SNMP information. (Public/Secret)
Activate "Authentication error" trapping device	Message for faulty login.

Section 3.7
Address Server Configuration

Introduction

This chapter contains a description about the Quantum NOE Address Server configuration.

What Is in This Section?

This section contains the following topics:

Address Server Configuration/Faulty Device Replacement

Overview

The address server provides two capabilities:

1. **Standard BOOTP server behavior:** Enter the MAC address and IP configuration. The NOE BOOTP server will provide the IP configuration when the device sends a BOOTP request.
2. **Faulty Device Replacement (FDR) behavior:** Enter the role name or the MAC address of the device. The device will send its role name or the MAC address with its DHCP request. With the DHCP response from the NOE, the device will receive its IP Configuration, plus the name and location of a configuration file.
   The next step for an FDR-compliant device is to download its configuration from the NOE.

NOTE: Consult your Schneider Electric sales representative for the current list of FDR-compliant devices.

The address server in the NOE supports both modes at the same time. You select a mode by entering either the MAC address or the role name in the Address Server Node Configuration *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)* page. You may enter only one or the other, but not both.

The Faulty Device Replacement capability allows automatic configuration of FDR-compliant devices.

Identifying a Role Name

Role names play an important role in Faulty Device Replacement. A role name is a logical name that the user assigns to a device, a logical name that has a meaning within the application. Example role names might be:

- **ENT_6**: The sixth Momentum ENT in your application.
- **OUTPUT_VALVE_2**: The second output valve in your application

NOTE: Role names are case-sensitive.

Role Name

The logical role name should be written on devices. The technician can get the new device from stores, enter the corresponding role name into the device, and place the device in the system. The device automatically gets its configuration and starts running with no further input from the technician. This process is designed to get your machine up and running quickly. All the technician has to do for any FDR compliant device is to enter the role name into the new device.

Address Server Limits

This table displays the parameters and limits of the address server:

Parameter	Limit
Maximum number of address server entries	128
Maximum size of the configuration file per device	4K bytes
Total size of Faulty Device Replacement storage	512K bytes
Maximum role name size	16 Characters

NOTE: For the DHCP server to work correctly the following must be observed.

- Address class and subnet class configured for the devices must match.
- Address class of the NOE and of the devices must be the same.

Operating on a Corporate Network

Keep these points in mind when operating on a corporate network:

- Before placing the NOE on a corporate network, Schneider Electric recommends that you discuss the installation with your MIS department. It is likely that your company's corporate network has at least one DHCP server running already. If the NOE's DHCP server is running on the same network, it may disturb the network.
- To avoid any possible problem related to the NOE's DHCP server on the corporate network, you have to ensure that the DHCP server is not running in the NOE by not having address entries in the configuration. If there are no configured devices in the address server Configuration page, then the NOE will not start the DHCP server.

Available FDR Agents

Three FDR agents are available:

- Momentum ENT
- Micro ETZ
- ATV58

The `role-name.prm` configuration files are stored in the NOE in non-volatile memory. Therefore, after a power failure all configurations will be available.

BOOTP and DHCP Compatible Devices

Use either the MAC address or the role name *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)* to assign IP addresses. Therefore, you may use the DHCP server with devices that support BOOTP only, such as Momentum ENT v1.

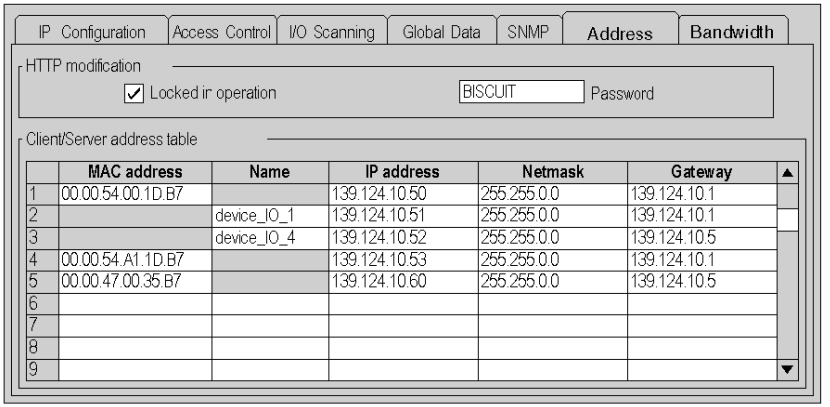
Quantum NOE Address Server Configuration

Introduction

The Quantum NOE 771 module address server function enables the user to enter Ethernet node addresses using BOOTP or DHCP. With BOOTP or DHCP, the IP address is assigned instead of the MAC address or the computer name.

Only Ethernet nodes provided in the list may refer to an IP address.

The screen shot shows the Server Address Configuration screen.



Parameter description

Parameter	Description
Locked in operation	Activates password protection for page security when accessing via the Webserver.
Password	Password for security.
MAC address	MAC address of the IP address destination
Name	Computer name of the IP address destination
IP address	IP address
Subnet mask	Assigned Subnet mask
Gateway	Assigned Gateway address

Section 3.8
Bandwidth Monitor Configuration

Introduction

This chapter contains a description about how to configure the Bandwidth Monitor.

What Is in This Section?

This section contains the following topics:

Bandwidth Monitoring

Overview

Bandwidth Monitoring allows the user to access and monitor the NOE module's CPU allocation for each of the following services:

- Global Data *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*
- I/O scanning *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*
- Modbus messaging *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*

The Bandwidth Monitoring service retrieves workload data and returns one of two pieces of information: whether the module has free resources or whether the module is working at capacity. Knowing the resource allocation helps you:

- assess resource allocation
- determine the number of NOEs needed in a system

NOTE: Users who want to use Bandwidth Monitoring do not need to develop a new set of access functions. The actual NOE CPU load is computed each second.

Bandwidth Monitoring Load Rates

The Bandwidth Monitoring service checks once a second and computes four (4) values in private data. These values are returned as the percentage of the NOE's CPU that is allocated to:

- Global Data *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*
- I/O scanner *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*
- Modbus messaging *(see Modicon Quantum with Unity, Ethernet Network Modules, User Manual)*
- other services and idle

CPU time spent in other services is shown as "Other" or "Free." Bandwidth Monitoring uses the same functions as used by SNMP.

The three service rates, Global Data, I/O Scanner, and Messaging, are computed using the following formula:

```
(Current load * 100) / Maximum Load
```

The table shows the (dynamically computed) **Maximum Load Rate** for the NOE module:

Diagnostic Service	Workload Data Returned	Maximum Load
Global Data	Number of published variables per second	800
I/O Scanner	Number of transactions per second	4200
Messaging	Number of messages treated per second	410

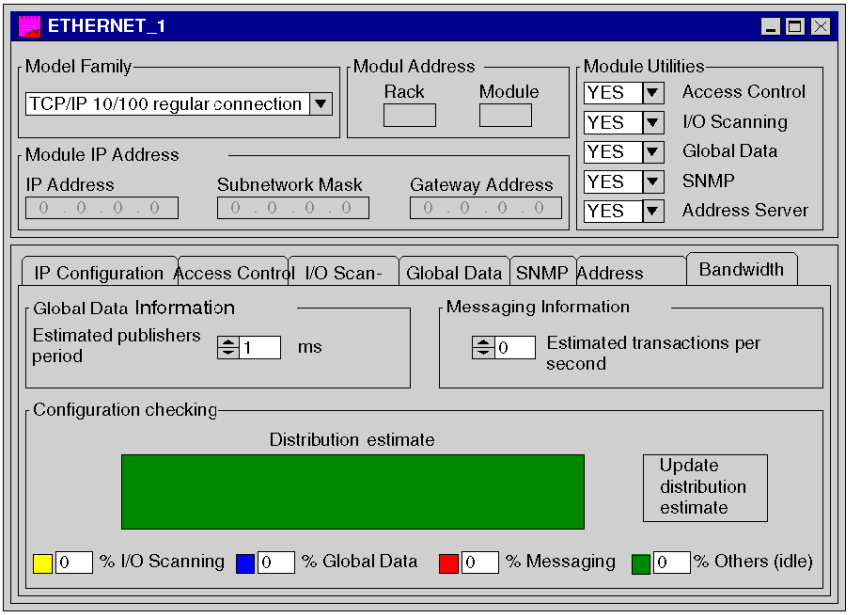
NOTE: The loads depend on controller scan times. Each application has an expected scan time. Therefore, when evaluating loads, ensure that the controller scan time is set to the expected scan time for the modeled application.

Quantum NOE Bandwidth Monitor Configuration

Introduction

Using the program window of the Bandwidth monitor, the user can display the distribution of the network load.

The illustration shows the Bandwidth Monitor dialog box.



Parameter description

Parameter	Description
Time span	Scan time of the network load in milliseconds.
Transactions per second in the message service	Node scan time for the messaging procedure.
% I/O retrieve	Percentage of the network load used for I/O scanner data
% Global data	Percentage of the network load used for retrieving/sending global data
% Messaging	Percentage of the network load used for nodes from the messaging list.
% Other (idle)	Percentage of the network load used for all nodes / network traffic, which would otherwise not be shown.

Index