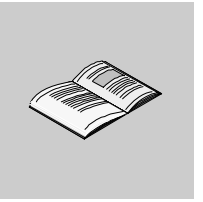
ConneXview
Ethernet Diagnostic Tool
Frequently Asked Questions

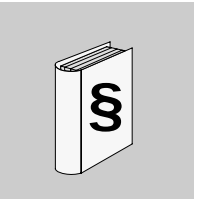
7/2007

31007265.00

Table of Contents



Safety 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 an imminently hazardous situation, which, if not avoided, **will result** in death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation, which, if not avoided, **can result** in death, serious injury, or equipment damage.

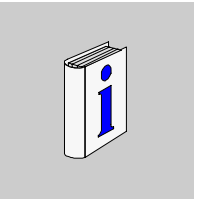
⚠ CAUTION

CAUTION indicates a potentially hazardous situation, which, if not avoided, **can result** in injury or equipment damage.

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.

About the Book



At a Glance

Document Scope

The document answers some frequently asked questions about the ConneXview Ethernet Diagnostic Tool.

Validity Note

The data and illustrations found in this book are not binding. We reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be construed as a commitment by Schneider Electric.

Related Documents

Title of Documentation	Reference Number
ConneXview Reference Guide	31007263
ConneXview Device Type Editor Reference Guide	31007264
ConneXview Ethernet Diagnostic Tool Getting Started	31007893

Product Related Warnings

Schneider Electric assumes no responsibility for any errors that may appear in this document. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of Schneider Electric.

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

When controllers are used for applications with technical safety requirements, please follow the relevant instructions

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 product related warning can result in injury or equipment damage.

User Comments

We welcome your comments about this document. You can reach us by e-mail at techpub@schneider-electric.com

Frequently Asked Questions

1

At a Glance

Overview

Here are some frequently asked questions about the ConneXview Ethernet Diagnostic Tool.

What's in this Chapter?

This chapter contains the following topics:

Can ConneXview Access Remote Networks?

Yes, ConneXview can be used to access remote networks. By default, ConneXview will discover the networks attached to the locally configured interfaces, but you can enter the network IP address of a remote network as long as there is connectivity to that remote network. ConneXview has been tested across routers and virtual private networks (VPNs).

To monitor a remote network, perform the following

Step	Action
1	From the **Tools** menu, select **Discover Network**.
2	From the **Subnets to Discover** dialog box presented, select **Add**.
3	Enter the network IP address or range of the IP addresses to be discovered. **Note** When discovering a remote network, be sure to include the router on the remote network in the IP address range.
4	Delete other networks so that only the remote network is in the Network Discovery Parameters list.
5	Accept by clicking on the **OK** button to begin discovery.

Note: If you configure your discovery to select just a portion of a remote subnet and the router is not within that IP address range, include an additional portion of the subnet that does include the router's IP address. The additional portion can be as small as the single IP address of the router.

Note: Depending on the bandwidth available to reach a remote network such as a wide area network (WAN) or dial-up connection, you may want to adjust the discovery rate to low, particularly if you are sharing this link with other users or services.

Can ConneXview Discover any Ethernet Ring?

Not necessarily.

ConneXview is optimized for the Schneider Electric's Transparent Ready ConneXium ring. This is accomplished using an identity filter for ConneXium switches.

If your OEM supports a private MIB, you may be able to create a custom profile using the Device Type Editor application.

Can ConneXview Perform Discovery using a Wireless Ethernet Adapter?

While monitoring can be performed using a wireless adapter, we recommend that you use a cabled connection for discovery.

It may be possible to perform discovery using a wireless adapter, but it can jeopardize a complete and successful discovery. Discovery makes numerous requests to managed devices. The access point of a wireless connection may not be able to handle this volume of traffic. Among the many factors that need to be considered are:

- proximity of the adapter to your wireless access point
- the number of other devices sharing the access point
- the amount of broadcast activity by other devices
- the latency for discovered devices to respond
- the number of packets lost due to collisions

If incomplete information is received due to congestion or lost packets, the managed device may not be properly discovered. Additionally, ICMP ping requests may be dropped due to wireless congestion or time out resulting in unmanaged devices not being properly recorded.

Monitoring via wireless has greater success than discovery because the table of devices is configured in the database, along with the configurable retry and timeout settings. You can access these in the Network Editor by selecting **Edit** → **Network Settings**

Can Devices on the Serial Side of a Gateway or Bridge Be Discovered?

No, SNMP is not supported for serial communications.

However, a TCP/IP PLC can poll those devices through the gateway and use logic to write a status value within the PLC. ConneXview can then be configured in the Device Type Editor to read that status value from the PLC and report a change in status by applying a monitor to the value.

Can Different Subnets be Included in the Same Monitor Tab?

Yes. More than one subnet can be monitored in the same monitor tab, depending on how you configure the list of subnets in the **Network Discovery** dialog box.

If you have connectivity to multiple subnets and include them in a single network map, you can monitor them simultaneously in a single monitor window (assuming that you have included them in the initial discovery).

If you perform separate discoveries and each subnet is created in a separate Network Editor and saved under a different network name, you need to open different monitor windows for each subnet.

Can Different Thresholds be Set for Different Instances of the Same Device Type in ConneXview?

Yes. Once discovered, the thresholds can be unique to each device on the network including those of the same device type.

Note: If the device is removed from the network and not saved, then is re-discovered in a subsequent discovery, the thresholds are returned to the global values.

Can Serial Modbus Devices Be Discovered?

No. ConneXview is based on SNMP, and SNMP is supported only over Ethernet. Serial devices do not support SNMP and therefore cannot be discovered via ConneXview.

Can the Device Property Editor Be Configured to Alarm Based on the Firmware Revision of a Device?

Yes, for Schneider's Transparent Ready devices. The firmware revision level is found in `profileVersion` in the Equipment Profile of the product's MIB.

If you are using devices that are not Transparent Ready, use the ConneXview Device Type Editor to add the `profileVersion` object to the device type. The SNMP object ID is 1.3.6.1.4.1.3833.1.7.2.0. in the Schneider MIB.

For firmware updates visit one of the following sites:

- *http://www.schneider-electric.com*
- *http://eclipse.modicon.com*

Can Thresholds for Different Alarms Be Configured by Users?

Yes. By opening the Device Property Editor in the Network Editor, you can specify which alarm thresholds apply to a particular device.

Thresholds for existing devices in the Network Editor retain their previous threshold settings. To update an existing device with the new threshold value, do the following:

Step	Action
1	In the Device Property Editor, manually edit the alarm threshold(s) for the specific device.
2	Save your edits.
3	Start monitoring the network or select the **Monitor** tab if the network is already being monitored.
4	If you are prompted to reload the monitored network, answer **Yes**.

The new alarm thresholds are now in effect.

For global changes that affect similar devices, use the Device Type Editor. Open the file containing the profile information. For example, you can select the Unity Quantum processor by opening the file QCOPROHOST.TYP, then edit the thresholds and alarms for all Unity Quantum processors.

Does ConneXview Discover Continuously?

No, ConneXview performs an initial discovery and generates a network map. If you wish to rediscover the network, select **Discover Network** from the **Tools** menu bar.

Does ConneXview Provide Information from any Ethernet Device?

Yes, to a varying extent.

If a device supports SNMP, considered to be a managed device, much information is available. If a device does not support SNMP, very limited information is available. However, ConneXview can scan service ports to obtain information regarding unmanaged devices. The amount of information received by any device depends on:

- the manageability of the device in supporting SNMP
- the proper network parameters configured in the devices
- the proper community names included when performing discovery
- the appropriate MIBs included in the device profile for third-party devices
- any Modbus TCP service that the device may support

How Are Wireless Links Shown in ConneXview?

Wireless links appear just as a hardwired connection. ConneXview determines that a link exists regardless of the medium.

How Do I Determine if Something Has Changed on the Network?

You can use ConneXview to determine if devices:

- have been added
- are no longer available
- have been moved

To see the changes, rediscover the network and click **Apply**. ConneXview indicates changes as follows:

- Any new devices are shown in blue in the network map.
- Devices from the previous discovery not found in the rediscovery are listed in the *Devices Not Found* dialog box. If you decide to keep them, they are shown in red in the network map. Once you select **OK** from the *Devices Not Found* dialogue box and **Save** the network, you will not be notified again, unless you set the *Permanent* flag to **True** in the *Device Property Editor*. Then you will be notified each time after a discovery is performed.
- Devices that have moved are shown in yellow in the network map.

How Do I Know the IP Address of the ConneXview PC?

The ConneXview icon represents the PC running ConneXview.

How Do I Know the Community Name of a Device?

The community name of a device is configured within the device. For Schneider Electric devices, the community name is usually displayed on the Configure SNMP web page when you log in.

Consult your network administrator to add the *read* community name for an Ethernet switch, router, PC, or server into the dialog box for discovery if these names have been set. Otherwise, SNMP requests made by ConneXview are not acknowledged, and the device cannot be properly represented after discovery.

Select **Add** under **SNMP Community Names** to include additional *read* community names.

How Do I Set up SNMP on a PC using Microsoft Windows XP Professional?

SNMP needs to be running on a PC running Microsoft Windows XP Professional so that ConneXview can communicate as a managed device.
SNMP runs as a service on the PC attached to the installed Ethernet adapter. You may need your Windows XP distribution CD. However, you can install support for the service if your IT Administrator has stored the i386 folder on your local hard disk. The i386 folder contains compressed source files for the operating system.
To install SNMP, log in to the PC as an Administrator.

Step	Action
1	Select **Start** → **Settings** → **Control Panel** → **Add/Remove Programs**
2	Select **Add/Remove Windows Components.**
3	Scroll down to **Management and Monitoring Tools** and click on the **Details** button
4	Select **Simple Network Management Protocol**.
5	Accept your changes and provide either the XP CD or browse to the location of the i386 folder to compete the installation.

If your Windows XP Professional PC supports the MIB 2 standard defined in RFC1213, perform the following:

Step	Action
1	Select **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services.**
2	Scroll down to **SNMP Service** and double-click on it.

The property page tabs and selections allow you to manage:

- starting and stopping the SNMP service
- the startup options Automatic, Manual, and Disabled
- the account used to log SNMP on as a service
- recovery options for an SNMP start-up failure
- SNMP agent settings for:
  - contact person
  - location of the device
  - physical (MAC) objects
  - IP objects
  - application objects
  - end-to-end monitored objects
  - data-link objects
- the trap destination, including:
  - the community name for sending the trap
  - the IP address of trap recipients
- Security - community names and permissions
  - Read only (default)
  - Notify
  - Read/Write
  - Read/Create

Note: ConneXview is a read-only diagnostic tool.

How Can I Find Details of Active Modbus Connections on this Device?

Schneider Electric Transparent Ready devices that support the Schneider TFE MIB track local and remote Modbus TCP connections. To determine the number of connections on the device, choose the device in the **Network Monitor**, and view the following objects in the **Device Property Viewer** panel

Object	Definition
port502LocalConn	Displays the number of connections currently opened by the *local* device
port503RemConn	Displays the number of connections currently opened on this device by remote devices.

The actual number of connections is the sum of the two object values above.

To view the current connections on the device, choose the device in the **Network Monitor**, and view the following objects in the **Device Property** panel.

Object	Definition
port502ConnType	Indicates whether the connection has been opened by the *local* device or a *remote* device.
port502ConnLocalPort	Displays the local device's TCP port number for each connection
port 502ConnRemAddress	Displays the IP address of each remote device
port502ConnRemPort	Displays the remote device's TCP port number for each connection

How Many Modbus Messages Are Handled by this Device?

Schneider Electric Transparent Ready devices that support the Schneider TFE [MIB] keep statistics on local and remote Modbus TCP messages. These statistics include the number of Modbus messages sent and received.

To determine the number of messages on a particular connection, choose the device in the **Network Monitor**, and view the following objects in the Device Property panel:

Object	Definition
port502ConnMsgInRate	Displays the number of Modbus messages received on this connection, in messages/s.
port502ConnMsgOutRate	Displays the number of Modbus messages sent from this connection, in messages/s.

How Many Subnets Can Be Monitored at the Same Time?

More than one subnet can be monitored—the number depends on how the networks were discovered and assembled. For example, if you have connectivity to multiple subnets and include them in a single network map, you can monitor them simultaneously in a single Monitor window.

If you perform separate discoveries and each is created in a separate Network Editor and saved under a different network name, you must open different Monitor windows for each subnet.

The limit is bound only by the number of Monitor property page tabs and the capability of the PC on which ConneXview is running.

Note: The best way to monitor multiple subnets in a single window is to include those subnets in your discovery and build a single map in the Network Editor.

How Much Traffic is Generated by ConneXview When it Discovers a Network?

The traffic amount varies based on 3 factors.

1. the total number of possible IP addresses in the discovery range
2. the total number of managed devices versus unmanaged devices
3. the discovery rate configured in the **Discovery** dialog box

For example, if you have a Class B network such as 172.16.1.0 for a network address and a 16-bit subnet mask such as 255.255.0.0, then 16 bits are available for hosts. The number of potential hosts is 65,535 minus 2 (one for the network address shown above and one for the broadcast address 172.16.1.255). ConneXview then pings all 65,533 hosts to see which ones respond. If your subnet mask using the network IP address above is 24 bits (e.g., 255.255.255.0), 8 bits are available for hosts (254 potential hosts).

If a device responds to the discovery ping, ConneXview issues an SNMP Get request to the device on UDP port 161. If the device fails to respond, ConneXview performs retries, increasing the length between each retry.

For an unmanaged device, there is very little traffic generated for each device. Only ICMP ping, and service port scans such as Modbus and HTTP are used if the device does not support SNMP.

If the device is managed and responds to the query, ConneXview makes additional queries for available objects in that device. Depending on the total number of objects available, the traffic rate may be greater.

The discovery rate configured in the **Discovery** dialog box produces varying amounts of traffic. A low discovery rate takes longer but generates less traffic. A high discovery rate produces a faster result and a higher traffic rate.

How Much Traffic Is Generated by ConneXview when It Monitors a Network?

The traffic amount generated by monitoring is configurable by choosing **Edit** → **Network Settings** from the **Network Editor** menu bar.

The total traffic depends on the:

- number of discovered devices
- number of those discovered devices that support SNMP
- priority or frequency of polled SNMP objects
- priority or frequency of Modbus TCP/IP objects
- number of retries configured for SNMP and Modbus TCP/IP
- timeout value between retries—a shorter timeout equals more frequent requests

Choose fewer retries and a longer timeout to generate less traffic during monitoring.

Note: In the Network Settings dialogue box, the field *Estimated Average Network Load KB/Second* indicates the anticipated network load generated by the ConneXview PC or Server.

How Much Traffic Is Generated by this Managed Device?

To show the rate of traffic sent by this device in bytes per second:

Step	Action
1	Within the network Monitor, select the managed device to query on the network map.
2	Select the **Device Properties Monitored** panel.
3	Scroll down to the **IfOutOctetRate** object.

How Much Traffic Is Coming into this Managed Device?

To show the rate of traffic inbound to a device in bytes per second:

Step	Action
1	Within the network Monitor, select the managed device to query on the network map
2	Select the **Device Properties Monitored** panel.
3	Scroll down to the **IfInOctetRate** object.

How Secure Is ConneXview? Can I Write Information to the Devices?

ConneXview is secure because it does not write information to network devices. ConneXview maintains its own database of devices discovered or added and represents them in the topology network map. Data within the devices on network fields can be edited for information purposes, but this data is not written to the devices.

ConneXview reads the information stored in those discovered devices. During discovery and monitoring, ConneXview issues SNMP Get *read* requests but does not issue *write* requests.

Is a Device Type a Specific File Type? Where Is it Located?

Yes. The device type is a file that is a template with a .TYP file extension. These files can be found in the ConneXview Networks folder and edited using the Device Type Editor.

A device type file includes:

- general information
- static SNMP information such as MIBs and graphics
- identity filter for associating the enterprise MIB object ID, any MIB variable, or a Modbus variable
- SNMP objects, which can be edited for thresholds and alarms
- Modbus information for reading registers and setting monitors
- derived information to compare 2 values for alarming
- user-defined groups of properties for streamlined, uncluttered monitoring of changing dynamic property values
- popup information to launch an application by right clicking on the device

ConneXview has device types for managed and unmanaged MBAP and generic devices.

You can also define third-party device types.

Is it Possible to Know the IP Address of a Device that Was Discovered with only a MAC Address?

The answer varies, depending on the device. Some devices such as the Quantum NOE assume an IP address based on the hexadecimal-to-decimal conversion of the 4 least significant bytes of the MAC address. Other devices such as the Premium ETY have the first 2 bytes defined as 85.16, and the last 2 bytes derived from converting 2 least significant bytes of the MAC address.

There are other devices such as label printers or even laser printers using the data link control (DLC) protocol that broadcast over Ethernet and do not require an IP address.

Devices discovered with only a MAC address are usually because the MAC address table in a managed switch indicated a device on the physical switch port.

Is it Possible to Search for Devices?

There is no specific search feature. You can use ConneXview features to sort devices, which will speed the process of locating them. Using either the Network Editor or Network Monitor, open the **Devices On Network** panel to sort devices by name, MAC address, or IP address.

Selecting the device in the **Devices on Network** panel highlights the device on the network map and brings up the details of the device or its link in the **Device Property** panel.

Is it Possible to See Information Exchanged between Two Devices?

With other tools, yes. ConneXview will only show the ModbusTCP port 502 connection status which can be correlated by each device in communication with each other.

ConneXview can tell you the local and remote port 502 connections in the **Device Properties Monitored** panel of the Network Monitor. ConneXview cannot decode the specific information exchanged between the two devices. For this, you need a packet sniffer.

Note: A packet sniffer typically requires a specific network topology. You may need to consult with your IT professional.

A free or OpenSource analyzer is available at ***http://www.ethereal.com***.

Download and install Ethereal and connect a hub to the device you wish to monitor. Ethereal will decode Modbus TCP messages such that you will see each request and response between all devices communicating with the monitored device.

What Are the Device Types included with ConneXview?

Device Type File Names	Description
ATV58Host	Altivar 58 Drive
CEV300Host	CEV30020 Modbus to Ethernet Bridge
CloudHub	Generic or unknown hub
ConneXiumSwitch	499NxS17100/499NxS27100 Switch
ConneXiumSwitchRM	499NxS17100/499NxS27100 Switch Redundancy Manager
ConneXiumSwitchSM	499NxS17100/499NxS27100 Switch Standby Manager
DefaultManagedHost	Generic SNMP Managed host
DefaultManagedMBAPHost	Generic ModbusTCP host
DefaultManagedSwitch	Generic SNMP Managed Switch
DefaultRouter	Generic Router
DefaultUnmanagedHost	Non-SNMP host or device
DefaultUnmanagedMBAPHost	Non-SNMP ModbusTCP host
DefaultUnmanagedSwitch	Generic or unmanaged switch
ENTV1Host	Momentum ENT11000/11002
ENTV2Host	Momentum ENT11001
ETY410Host	Premuim ETY 410x
ETY510Host	Premium ETY 510x
ETYPortHost	Premium embedded ETY port
ETZHost	Premium ETZ Gateway
M1EHost	Momentum M1E Processor
NIMHost	Advantys STB Host
NOEHost	Quantum NOE 771-xx
NWMHost	Quantum FactoryCast HMI
PCoProHost	Premium Unity 5634 CPU
QCoProHost	Quantum Unity 6x1 CPU
TrHost	Generic Transparent Ready host
WMYHost	Premium FactoryCast HMI

You can browse the device type files using the Device Type Editor.

What Are the most Important MIB Objects?

The most important MIB objects are those related to:

- connection status
- errors
- utilization

For Schneider Electric managed devices in Monitor mode, select the device in the Network map and then view the **Device Properties Monitored** panel.

Within the **Device Properties Monitored** panel, scroll down to view Ethernet Errors:

- IfInDiscardRate
- IfOutDiscardRate
- IfInErrorRate
- IfOutErrorRate

This indicates Ethernet or MAC layer errors.

For IP layer 3 network errors, scroll further to view:

- IpInHdrErrorRate
- IpInDiscardRate
- IpOutDiscardRate
- IpDiscardRate

This may indicate a broadcast storm, buffer overrun, or bad device transmitting to the device monitored.

For TCP errors, scroll further to view:

- TcpRetransSegRate
- TcpOutRstRate
- TcpAttemptFails

TCP errors may indicate an out-of-socket condition or a remote device with no sockets available for a TCP connection. Retransmissions indicate that the target or peer device may be unable to service the last TCP segment transmitted.

For general interface errors, scroll further to view:

- Interface Load
- Interface Error Rate
- Interface Bandwidth Utilization

These errors can indicate overload on the interface due to too many messages to service or broadcast traffic, wiring problems, or a faulty switch port.

What Are the Ports and Protocols Supported by Ethernet Devices?

The protocols supported by a device depend upon the services running inside the device. For example, to support an embedded web page like Schneider Electric Transparent Ready devices, a web server process is running on the device to respond to HTTP web page requests.

Some common protocols and port numbers used by Transparent Ready are:

Port	Service	Function
21	FTP	File Transfer Protocol
23	Telnet	Remote Console over TCP/IP
25	SMTP	Simple Mail Transfer Protocol for sending email
67	BootPS	BootP Server for assigning IP parameters
68	BootPC	BootP Client for requesting IP parameters
69	TFTP	Trivial File Transfer for updating profiles
80	HTTP	Web page hosting
161	SNMP	Simple Network Management Protocol
502	Modbus TCP	Modbus communication

What Security Features Are included with ConneXview?

ConneXview version 1.0 does not include embedded security features such as user access profiles with password protection.

To control access to the ConneXview application, consider controlling access to the PC on which it is installed or use Microsoft Windows Access Control Policies and Profiles. Additional information on Access Control Policies and Profiles can be found at *http://www.microsoft.com*. This Windows management feature controls access to applications based upon the user's profile and authentication level.

How Does ConneXview Discover Devices?

ConneXview uses a variety of TCP/IP tools to discover devices. It compares the configured network IP address or range along with the subnet mask either configured on the PC running ConneXview or provided by the user.

Determining Eligible Hosts ConneXview determines the number of eligible hosts. ConneXview performs a ping request to each address in the eligible range.

Determining Managed Devices Of those devices that reply, it further issues an SNMP Get query for ISO information. Should the device respond to the SNMP Get Query, further queries are issued to learn more about the device.

Determining Unmanaged Devices If the device does not respond to an SNMP Get query, it does not support SNMP and is therefore not 'listening' on TCP port 161 (the default SNMP TCP service port),

Determining Modbus Devices ConneXview will then issue Modbus queries to determine if the device in question supports Modbus. If the query is met with a response, ConneXview will determine the device to be a managed or unmanaged MBAP host.

Determining Other Devices You can use the ConneXview companion application, the Device Type Editor, to add MIB, graphics and other device features to the Network Map. Refer to the Device Type Editor Help for details on adding custom managed and unmanaged devices from other OEMs.

What Does it Mean when Devices with only MAC Addresses Are Discovered and Why?

The most common reason why a device appears with only a MAC address is because its IP address is not in the discovery range. However, the device is communicating and its MAC address has been found in an infrastructure device.

Other causes include:

- a discovery performed on a remote subnet when the router for that subnet is not within the discovery range
- ConneXview does not have the community name for this router
- the router does not fully support SNMP—in this case, the devices are displayed twice, once by their IP addresses and once by their MAC addresses

What Happens if a Device Discovered on the Local Subnet Is Configured for Another Network?

If the device is transmitting any packets, it appears only as a MAC address because its IP address is not in the discovery range.

What if the Devices on a Network Uses Different Community Names?

You can add both public and private community names as you wish when performing a discovery or manually adding a device.

When you add a device manually, you can configure ConneXview with the device's community string by selecting the device and editing the **SNMP Community Name** field of the Device Property Editor.

During discovery, ConneXview attempts all available configured community names to achieve the proper response from the device. The default setting includes only one community name, *Public*. Should your device use another community name, select **Add** under the **Community Names** section of the **Discovery** dialog box.

If the community name is not the default (*Public*), and you have not included the new community name as part of discovery, the device will be discovered as an unmanaged device because SNMP requests by ConneXview will be rejected by the device.

What Is a Private MIB? What Is the Information Contained in the Schneider Electric Private MIB?

There are 2 types of MIBs, public and private.

Public MIB information is generic to many or most devices such as number of interfaces, bytes sent and received, interface errors, link status and the like.

Private MIB information describes the unique, non-generic features of a device. The Schneider Electric Private MIB for example includes information such as:

- IO Scanner
- Global Data
- Modbus Messaging

These features are found only in Schneider Electric ModbusTCP devices.

Can ConneXview Print a Network Map on a Plotter?

Yes, provided that the driver that supports large-scale printing has been installed on your PC.

When a network map is open in either monitor mode or edit mode, ConneXview can print:

- the entire network map, or
- only that portion of the network map that is visible in the network map viewer or editor

A network map can printed to:

- a single large-scale sheet in a size that is a selected percentage of the network map's normal size, or
- several smaller-sized pages, with both the height and width of the printout expressed in terms of a selected number of pages

Refer to the ConneXview online help topic for the **Print** command, where you will find step-by-step instructions explaining ConneXview's printing options.

Can ConneXview Print a List of Alarms and Network Events?

Yes. When a network map is open in monitor mode, ConneXview can print filtered and sorted lists of current alarms and event log items.

Printing Current Alarms:

You can elect to print a list of alarms, that includes:

- all alarms, or
- only alarms of a selected severity (critical or attention), or
- only alarms occurring within selected starting and ending dates and times

You can sort the printed list in either ascending or descending order, based on any field included in the current alarms pane.

Printing Network Events:

You can print a list of all or part of the ConneXview event log. You can elect to include all event log items in the list, or you can limit the printed list by applying one or more of the following filters:

- a device filter, that limits the list to events relating to one or more selected network devices
- an event severity filter, that limits the list to one or more selected severity levels (critical, attention, information only)
- a date range filter, that limits the list to selected starting and ending dates and times

You can sort the printed list in either ascending or descending order, based on any field included in the event log.

Refer to the ConneXview online help topic for the Print command, where you will find step-by-step instructions explaining ConneXview's printing options.

Does ConneXview Retain a Record of Alarms and Network Events?

Yes. ConneXview adds an new entry to the event log every time a device property monitor triggers an alarm or an information only event.

ConneXview retains a history of network events up to a user-defined maximum event log size. When the maximum event log size is reached, ConneXview adds a new event to the log and simultaneously removes from the log the oldest recorded event.

To configure the size of the event log:

Step	Action
1	In ConneXview, select **Tools** → **Options**. The User Options dialog opens.
2	In the *Server Options* section, select the **Maximum event log size** (in thousands): ● 1 ● 10 (default) ● 100
3	Click **OK** to closet he User Options dialog and save your edits.

Note: Decreasing the size of the event log applies not only to the current map, but also to all maps later opened in ConneXview. Reducing the size of the event log can cause the loss of saved alarms and other network events for a saved network map when it is next opened.

What Filtering Criteria Does ConneXview Use with the Event Log Filter?

ConneXview applies user-defined filtering criteria to the event log. You can apply one or both of the following filters to event log records:

- a date range filter, that limits the event log display to selected starting and ending dates and times
- a device filter, that limits the event log display to events relating to a single selected network device

To configure the event log filter:

In monitor mode, with the event log pane displayed, click on the **Open filter dialog** button–indicated by an ellipsis (...)–to open the Event Log Filter dialog, where you can configure your event log filter settings.

Refer to the ConneXview *Event Log Filter* help topic for step-by-step instructions on how to enter event log filter settings.

To toggle the filter on and off:

Use the **Enable/Disable filter** button. This button displays either of two icons, depending upon the state of the event log filter, as follows:

- click the  button to turn ON the event log filter
- click the  button to turn OFF the event log filter

Refer to the ConneXview *Event Log* help topic for more information about the event log and its features.

Can ConneXview Send SMS or Text Messaging Notice of Network Alarms?

Yes. ConneXview's event notification service sends email notices of network events to a user-provided SMTP email server. This service can be configured to send SMS (short message service) messages, or text messages, to designated recipients.

To configure ConneXview to send SMS messages, or text messages:

Step	Action	
1	Select **Tools** → **Email configuration...** to open the Email Configuration dialog.	
2	In the Email configuration dialog, configure the following settings:	
	a	Type in an SMTP Server host name or IP address, up to 255 characters.
	b	Type in the SMTP email server's From address, in the format: <local name>@<domain name> where: ● <local name> cannot exceed 64 characters ● <domain name> cannot exceed 255 characters
	c	Use the spin control to set the Send Period–the interval between email transmissions–from 1 to 60 minutes.
3	Click **Add...**. The Add Recipient dialog opens.	
4	In the Recipient section of the Add Recipient dialog:	
	a	Type in the *Name* of the recipient, up to 32 characters. **Note:** this name is added to the Recipient list in the E-mail Configuration window.
	b	In the *E-mail Address* field, type in your cellphone number and the SMSC gateway address of your cellular provider, in the format: <number>@<SMSC gateway address> **Note:** An unofficial list of some common cellphone provider gateways is set forth below. Be sure to confirm any SMSC gateway address with your cellphone provider before implementing and relying upon it.
5	Complete the *Send Criteria* sections of the Add Recipient dialog, where you can filter the sending of event notices by one or more of the following: ● event severity ● network ● devices and device types For information on how to make these filtering choices, refer to the ConneXview Add Recipient online help topic.	
6	After all configuration settings have been made in the Add Recipient dialog, click **OK** to save your changes and close this dialog.	
7	After all configuration settings have been made in the Email Configuration dialog, click **OK** to save your changes and close this dialog.	

Some common cellphone gateway providers and their SMSC gateway addresses are set forth below. Be sure to confirm any SMSC gateway address with your cellphone provider before implementing and relying upon it.

Provider	**SMC Gateway Address**
Alltel	@message.alltel.com
AT&T	@mmode.com
Bell	@txt.bell.ca
Cellular One	@mobile.celloneusa.com
Cingular	@mobile.mycingular.com
Fido	@fido.ca
Nextel	@page.nextel.com
Qwest	@qwestmp.com
Rogers Canada	@pcs.rogers.com
Sprint	@messaging.sprintpcs.com
Suncom	@tms.suncom.com
T-Mobile	@tmomail.net
Verizon	@vtext.net
Virgin Mobile Canada	@vmobile.ca
Virgin Mobile USA	@vmobil.com
Vodacom South Aftica	@voda.co.za

ConneXview does not display the Event Log. How can I open it?

The Event Log is a new ConneXview feature, starting with version 2.0. Network maps created using ConneXview version 1.0 do not initially display an Event Log. However, you can add an Event Log to version 1.0 network maps.

To add an Event Log to network maps created in ConneXview version 1.0:

Step	Action
1	Use ConneXview version 2.0 (or later) to open the version 1.0 network map in edit mode.
2	Save the network map.
3	If the network map is open in monitor mode, close monitor mode.
4	0pen the saved network map in monitor mode. ConnexView adds an Event Log tab to the Current Alarms window.
5	Click on the Event Log tab to display its contents. **Note:** The newly created Event Log contains only items occurring after the creation of the Event Log.

The status bar of ConneXview indicates "Alarm Monitor Disabled". What does this mean and how can I see which monitors are disabled?

Alarm Monitor Disabled indicates that, for a managed device, either:

- the *Monitoring* attribute of a value monitor is **Disabled**, while the *Monitoring* attribute of its parent property is **Enabled**, or
- the device's *Default Gateway Alarming?* static property is **Disabled**

To identify which devices are configured in either of these two ways:

Step	Action
1	Select **Analyze Network** in the Tools menu in either edit or monitor mode. The Network Analysis window opens, displaying a list of network errors.
2	If the list is long enough to require scrolling: a. Click on the *Severity* column header to sort the list, then b. Scroll to items with a *Severity* value of **Information Only** **Note:** Items triggering the *Alarm Monitor Disabled* message have a *Severity* state of **Information Only**.
3	In the *Message* column, look for one of the following: ● *Value Monitor is disabled* or ● *Default Gateway Alarm is disabled* Select a device with one of these messages, then click **Go to** and navigate to the device.
4	(Optional) After navigating to a device in edit mode, you can open the Device Property Editor and: ● Select the device's IP address to display its *Default Gateway Alarming?* static property for editing ● Navigate down the property list and select value monitors to display each monitor's *Monitoring* attribute for editing

Why does ConneXview's email alarm notification service send me email messages long after an alarm occurs?

Your SMTP server is the most likely cause of the delay.

ConneXview sends email notices of network events to your SMTP server whenever an event occurs. However, if your designated SMTP server is not functioning, or is busy, it may not be able to receive the notice sent by ConneXview.

ConneXview continues to send network event notices until receipt of the notice is confirmed by your SMTP server. ConneXview queues the event notices for the recipient and then retries every minute until the e-mail is sent successfully.

Must I perform any special configuration if my ConneXview server or client PC has multiple IP addresses assigned to it?

Overview

If your ConneXview server PC has multiple IP addresses, you must select one of them to be used by its clients when accessing its remote objects. The goal is to select an IP address that all of the server's ConneXview clients can reach via their default gateway.

Similarly, if your ConneXview client PC has multiple IP addresses, you must select a single IP address to receive ConneXview communications. If your ConneXview client PC (with multiple IP addresses) connects to a ConneXview server on the same subnet, no special configuration is required. The client automatically uses the server IP address for this subnet. However, if your ConneXview client PC (with multiple IP addresses) is **not** on the same subnet as the ConneXview server, you must select one of the client's IP addresses to receive event notifications. The goal is to select an IP address that the ConneXview server PC can reach via its default gateway.

Note: For a client or a server with multiple IP addresses, use the rmi.bat utility that ships with ConneXview to select a single IP address for that PC (see *p. 40*).

If all clients are not on the same network subnet, no single server IP address will work for all clients. For each client that cannot reach the selected server IP address–via the client's default gateway–you must add a persistent route to the client's network routing table (see *p. 40*). In this way, the remote client can reach the selected server IP address.

For a client PC (with multiple IP addresses), if none of its IP addresses are reachable by the server PC -- via the server's default gateway -- you must add a persistent route to the server's network routing table (see Adding a Persistent Route to a PC Routing Table). In this way the server can reach the selected client IP address.

Selecting an IP Address

For client or server PCs with multiple IP addresses, you must select a single IP address for ConneXview communications. To do this, use the rmi.bat utility, which is located in the ConneXview folder. In a default installation, the path to this file is:

C:\Program Files\Schneider Electric\ConneXview\rmi.bat

To select a single IP address for a client or server PC with multiple addresses:

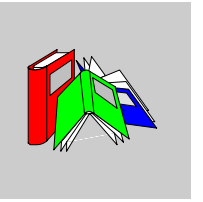
Step	Action
1	Navigate to and double click the file rmi.bat. The ConneXview RMI Settings dialog opens.
2	In the *Address for RMI Servers* list, select an IP address.
3	Click **OK**. **Note:** Changes to the setting for a ConneXview Server do not become effective until the server is re-started (via the ConneXview Server Console.)

Adding a Persistent Route to a PC Routing Table

To add a persistent route to a PC's network routing table:

Step	Action	
1	Open a command prompt.	
	a	Select **Start** → **Run**. The Run dialog opens.
	b	In the Run dialog, in the Open field, type in **cmd**, then click **OK**. A command prompt appears.
2	At the command prompt, use the Windows *route* command to add to the PC's network routing table. For example, the following command adds a persistent route to network 10.10.10.0 via a gateway at 192.168.112.2: C:\>route -p add 10.10.10.0 mask 255.255.255.0 192.168.112.2	
3	After entering the *route* command, click **Enter**. The command executes.	

Glossary



A

acknowledge The act of recognizing the existence of a network alarm. It implies that the person acknowledging the alarm will proceed to diagnose and resolve it.

address server Available in Quantum and Premium communications modules to assign IP address parameters to clients using BootP. Additionally, Quantum NOE 771-01/11 and Premium ETY 4103/5103 modules support Faulty Device Replacement.

alarm An indicator of a network problem. An alarm is triggered when the value of a monitored device property–with its *Severity* attribute set to either **Critical** or **Attention**:

- exceeds a value for a limit monitor, or
- changes more than a pre-set limit for a change monitor, or
- changes to or from one of a group of pre-set values for a state monitor

arithmetic property A derived dynamic property that takes its value from an arithmetic function (add, subtract, multiply or divide) performed against the values of two other dynamic properties.

ARP *Address Resolution Protocol.* The Ethernet protocol used to map an IP address to a MAC address.

attribute One of a collection of field values that together define a property or property monitor.

B

bandwidth The data-carrying capacity of a network connection. ConneXview monitors bandwidth utilization—the percentage of bandwidth that is being used.

bend The point of a curve in a communications link, created in edit mode either by selecting a form of orthogonal layout, or by manually selecting and stretching a communications link.

broadcast A message that is sent out to all devices on the network.

C

change monitor A pre-configured alarm trigger, based on any change in the value of a monitored property.

client/server mode A method of installing and operating ConneXview as a distributed software application, consisting of 2 (or more) separate components including: 1 server component that performs functions and provides information via an NT service, and 1 or more client components–one of which must be installed on the server PC–that act as remote GUIs and subscribe to the ConneXview server's NT service.

color map key A color map key points to a state mapping property and relates the value of that property to a color scheme. Selecting a color map key in monitor mode causes the Network Map Viewer to display each device and communications link in a color reflecting the value of the mapped property.

community name The alpha-numeric character string name used as a security protection mechanism to permit Read/Write access to a group of devices. ConneXview requires only the Read community string. Most vendors give the Read community string a default value of *Public*, but you may alter that string on the device for security.

CRC (*cyclical redundancy check*) A way of checking for errors in a message by doing mathematical calculations on the number of bits in the message, the results of which are sent along with the data to the recipient. The recipient repeats the calculation on the received data. If there are any discrepancies in the two calculations, the recipient requests a retransmission from the originator.

D

data link layer Layer 2 of the seven-layer OSI reference model for communication between computers on networks. This layer defines protocols for data packets and how they are transmitted to and from each network device. It is a medium-independent, link-level communications facility on top of the physical layer, and is divided into two sub-layers—medium-access control (MAC) and logical-link control (LLC).

datagram A discrete package of data - sometimes called a packet - that contains data and a header with address information to route it from a source device to a destination device over a network.

deadband The amount, in measurement units, below (for high settings) or above (for low settings) the threshold value that the monitored property must reach before the alarm or state-mapped message will clear.

default gateway address 1. The gateway in a network that a computer uses to access another network if a gateway is not specified for use.
2. In a network using subnets, the router that forwards traffic to a destination outside of the subnet of the transmitting device.

derived property A dynamic property that takes its value from a function or calculation performed against one or more SNMP, Modbus or other derived properties.

device The hardware located at a network node. An instance of a device type.

device type A category of device, created and editable in the Device Type Editor.

discovery range The devices to be discovered are defined by a range of IP addresses. The range is determined by the subnet address and the subnet mask value which defines a list of all candidate addresses within the subnet. You can manually restrict the range by adjusting the start address and/or the end address in either the **Edit Subnet** or **Add Subnet** dialog box.

dynamic property A device or communications link property whose value is not a constant, but instead can dynamically change during operation.

E

edit mode The state of ConneXview with a network map open and displayed for editing.

Ethernet A family of local area network protocols covered by IEEE 802.3.

F

FDR *faulty device replacement* A process to easily replace a device should it fail and restore the configured parameters of the previous device.

firewall A router or workstation with multiple network interfaces that controls and limits specific protocols, types of traffic within each protocol, types of services and the direction of information flow.

FTP *(file transfer protocol)* The communications protocol that allows file transfer between devices.

G

gateway 1. Typically refers to a router. A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its Internet service provider's network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.
2. A combination of hardware and software that interconnects otherwise incompatible networks or networking devices. Gateways include packet assembler/disassembler (pads) and protocol converters. Gateways operate at layers 5, 6 and 7—the session, presentation and application layers, respectively—of the OSI model.

Global Data Service Global Data Service (GDS) uses *real time publish/subscribe* for a device to publish a variable register table. Other devices within the same subnet then subscribe to the variable table. Global Data uses UDP Multicast to distribute the variable simultaneously to multiple packets with a single UDP packet. Reference the Quantum NOE 771-01/11 or Premium ETY 4103/5103 for additional details on the Global Data Service.

H

header The control information added to the beginning of a transmitted message. It contains essential information such as the packet or block address, source, destination, message number, length and routing instructions.

host An end node attached to a network, for example, a PC, PLC, I/O device or other such device. A host device does not include, and is contrasted with a router or switch.

HTTP *(Hyper Text Transfer Protocol)* The communications protocol that allows web browsing.

I

ICMP *internet control message protocol.* The internet protocol that reports errors and provides information related to datagram processing.

IO Scanning Service An automatic client available on Quantum, Premium and Momentum platforms. IO Scanning allows entry of holding register Reads, Writes and Read/Writes to remote devices at an interval configurable in milliseconds. Setup of IO Scanning is performed in your programming application using a table instead of programming logic functions.

IP *internet protocol.* That part of the TCP/IP protocol family that tracks the internet addresses of devices, routes outgoing messages, and recognizes incoming messages.

IP address A unique 32-bit address assigned to TCP/IP devices on the internet, written as four octets - represented as decimals - separated by periods. An IP address includes a network number, an optional sub-network number, and a device number. The network and sub-network numbers enable the routing of messages; the device number serves as the specific address on a network or sub-network. A subnet mask is a filter that separates the network number from the sub-network number.

J

jabber Network error caused by an interface card placing corrupted data on the network. Also, an error condition caused by an Ethernet node transmitting longer packets than allowed.

L

limit monitor A preconfigured alarm trigger that is actuated when a monitored property's value reaches or exceeds the setpoint value.

link *communications link.* A network connection between two devices.

load property A derived dynamic property that is based upon two interface-related properties - an input measure and an output measure - and expresses their combined value in terms of units/time.

M

MAC address *media access control address.* A 48-bit number unique on a network that is programmed into each network card or device when it is manufactured.

mapping property *state mapping property.* A derived dynamic property that can be linked to a color map key. A state mapping property contains four user-defined value threshold triggers (High-High, High, Low, Low-Low). A color map key points to a state mapping property and relates each threshold trigger to a color.

MBAP *modbus application protocol*. The TCP/IP based standard protocol used to manage master-slave/client-server communications between intelligent devices on an Ethernet network.

MIB *management information base.* A uniformly accepted hierarchical data structure containing objects - sometimes referred to as device properties - that a device in an SNMP network can read and, in some cases, write. The hierarchical data structure contains both public (or standard) branches, and private (or proprietary) branches.

Modbus An application layer messaging protocol. Modbus provides client and server communications between devices connected on different types of buses or networks. Modbus offers many services specified by function codes.

monitor mode The state of ConneXview with a network map open and displayed for real-time network monitoring.

N

network map A diagrammatic representation of a network, in either edit or monitor mode.

node An endpoint of a network section (for example, one leading to a host PC) or an intersecting point of two or more network paths (for example, the location of a hub, switch or router).

NTP *network time protocol* A communication protocol used to exchange and synchronize time over a network.

NWM *network map* A file extension for a network map file, which contains information about all the devices on a network, their interconnections and settings.

O

OID *object identifier.* A dotted decimal numerical sequence that uniquely relates to, and describes, an object in a MIB. Each numerical segment in the sequence describes a unique location in the MIB hierarchy, with each successive numerical segment indicating a sub-branch from higher-level segments.

P

packet A series of bits containing data and control information, formatted for transmission from one node to another. It includes a header with a start frame, the source and destination addresses, control data, the message itself, and a trailer with error control data (called the *frame check sequence*).

packet sniffer A software that intercepts and analyzes traffic on an Ethernet network. It can be used to monitor network usage, detect network intrusion, and gather and report network statistics.

physical layer Layer 1 (the bottom layer) of the OSI reference model is implemented by the physical channel. It governs hardware connections and byte-stream encoding for transmission. It is the only layer that involves a physical transfer of information between network nodes. The physical layer insulates layer 2 (the data link layer) from medium-dependent physical characteristics such as baseband, broadband or fiber optic transmission. Layer 1 defines the protocols that govern transmission media and signals.

ping *packet internet groper.* The combination of an ICMP echo request message and its reply, used in IP networks to determine if a network device can be reached and the time to reach it.

polling Discovery method where a device performing network management requests, of other known intelligent network devices, if the latter have data to transmit. Receipt of this message by a network device authorizes it to send a transmission in response.

publish To make information available and distribute it. The Quantum NOE 771-01/11 and ETY 4103/5103 with the Global Data Service enabled can publish a single multicast network variable containing up to 512 registers to a group of Global Data subscribers, configurable on intervals of CPU Scan.

R

router A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its Internet service provider's network. Routers are located at gateways, the places where two or more networks connect. Routers use headers and forwarding tables to determine the best path for forwarding the packets, and they use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

S

scan A non-intrusive method of identifying active network devices and their open ports.

SMTP *simple mail transfer protocol* The most common communication protocol for sending and receiving email across a network.

SNMP *simple network management protocol.* The UDP/IP standard protocol used to manage devices - including hosts (i.e. client or server PCs), routers, switches and hubs - on an IP network. ConneXview supports SNMP v1.

stand-alone mode A method of installing and operating ConneXview as an integrated software application on a single PC.

standard property An SNMP or Modbus property whose value changes dynamically during the course of operations.

startup mode The state of ConneXview with no network map open.

state monitor A preconfigured alarm trigger that is actuated when a monitored property's value either equals, or does not equal, a member of a set of specified setpoint values.

static property A device or communications link property whose value is set when the device or communications link is created, and does not dynamically change during operation.

subnet *subnetwork*. A collection of devices sharing the same network address. Typically a segment of a larger network.

subnet mask A filter applied to an IP Address to distinguish the network address from the host - or device - address.

subscribe The act of declaring interest in available information by a device. A device can subscribe to up to 2,048 4x registers total from up to 64 Global Data publishers. Note that a subscriber has to subscribe to the entire published network variable, even if only a portion of the register data is required.

T

TCP/IP (*transmission control protocol/Internet protocol*) A set of protocols developed by the U.S. Defense Department's Advanced Research Projects Agency (ARPA) during the early 1970s. Its intent was to develop ways to connect different kinds of networks and computers. TCP/IP does not have the functionality that OSI provides.
TCP/IP is a transport and Internet working protocol—i.e., the de-facto networking standard. It is commonly used over X.25 and Ethernet wiring and is viewed as one of the few protocols available that is able to offer a true migration path towards OSI. TCP/IP is able to operate in most environments. TCP/IP operates at Layers Three and Four of the OSI model (Network and Transport respectively).
TCP and IP are the standard network protocols in UNIX environments. They are almost always implemented and used together.

TFTP *(trivial file transfer protocol)* A very simple form of the File Transfer Protocol, implemented on top of UDP and which provides no security features.

U

UDP *user datagram protocol.* A connectionless mode protocol in which messages are delivered in a datagram to a destination device. The UDP protocol is typically bundled with the Internet Protocol (UDP/IP).

X

XWAY Premium addressing in {Network, Station} format for using Modbus or UNI-TE protocol messaging.