SNMP Driver Help

Table of Contents

SNMP Driver Help

Help version 1.035

CONTENTS

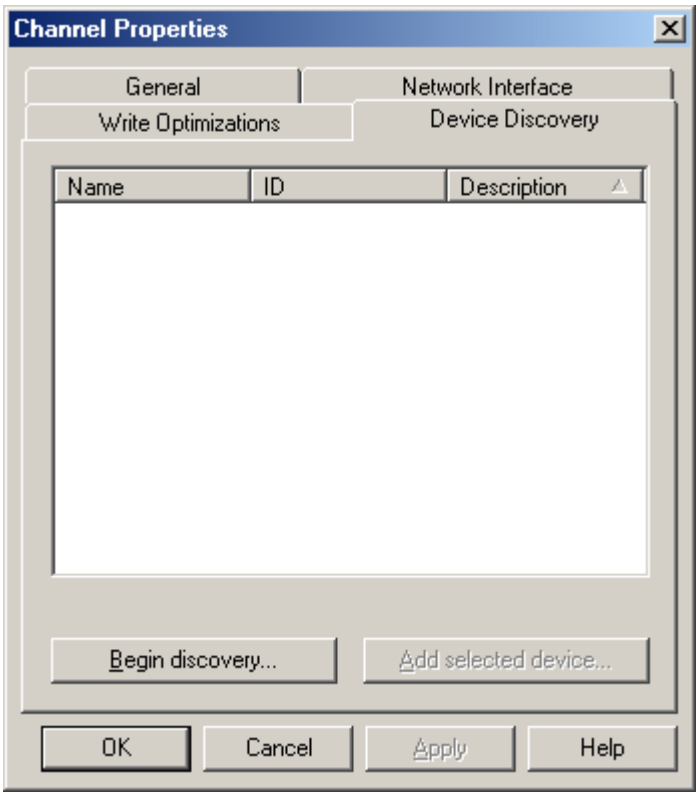
Overview

The SNMP Driver provides an easy and reliable way to connect managed and unmanaged Ethernet network devices to OPC Client applications, including HMI, SCADA, Historian, MES, ERP and countless custom applications. It is intended to work with all devices supporting the SNMP protocol (versions 1 and 2c).

Channel Setup

Device Discovery

This channel-level dialog is used to specify parameters for locating devices on the network. Once devices are found, they may be added to the channel. The maximum number of devices that can be discovered at once is 65535.

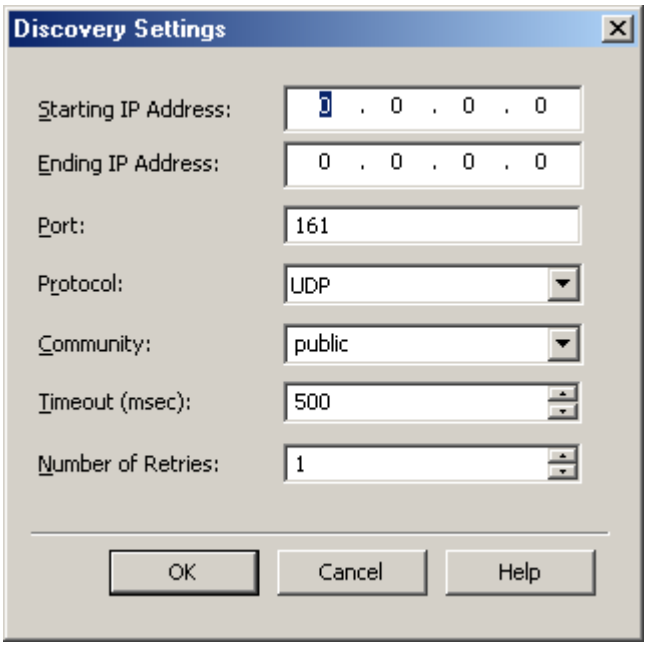


Descriptions of the parameters are as follows:

- **Name:** This parameter specifies the name of the discovered device.
- **ID:** This parameter specifies the IP address of the discovered device.
- **Description:** This parameter specifies the description of the discovered device.
- **Begin discovery...:** This button launches the Discovery Settings dialog. For more information, refer to **Discovery Settings**.
- **Add selected device...:** This button launches the General tab in the driver's Device Properties.

Discovery Settings

This dialog is used to specify the discovery parameters.



Descriptions of the parameters are as follows:

- **Starting IP Address:** This parameter specifies the starting IP address. The default setting is 0.0.0.0.
- **Ending IP Address:** This parameter specifies the ending IP address. The default setting is 0.0.0.0.
- **Port:** This parameter specifies the port number, which may range from 1 to 65535. The default setting is 161.
- **Protocol:** This parameter specifies the protocol, which may be UDP or TCP. The default setting is UDP.
- **Community:** This parameter specifies the community name, which can be defined by the user and depends entirely on the configuration of the remote device. Common options include Public or Private. The default setting is public.
- **Timeout (msec):** This parameter specifies the time that the driver will wait for a connection to be made with a device, as well as the time that the driver will wait on a response from the device before giving up and going on to the next request. The default setting is 500 msec.
- **Number of Retries:** This parameter specifies the number of times the driver will retry a message before giving up and going on to the next message. The default setting is 1.

See Also: **Communication Parameters**

Device Setup

Supported Devices

The SNMP Driver is designed to work with any SNMP Agent (typically in a device) that supports the Simple Network Management Protocol (SNMP) versions 1 and 2c. The driver works with a broad range of SNMP managed devices, such as the following:

Alarm Management RTUs
Device Servers
Environment Monitoring Equipment for Server Rooms
Managed Industrial Ethernet Switches
Net-SNMP Software Version: 5.4.1
Printers
Routers
Uninterruptible Power Supplies (UPS)
Unix-based Servers
Windows-based PCs and Servers

Maximum Number of Channels and Devices

The maximum number of channels is 100. The maximum number of devices supported per channel are 100.

See Also: **Communications Parameters** and **Auto-Demotion and SNMP**.

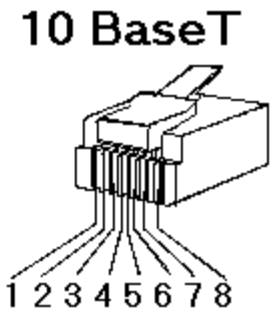
Cable Diagrams

Patch Cable (Straight Through)

TD + 1	OR/WHT	OR/WHT	1	TD +
TD - 2	OR	OR	2	TD -
RD + 3	GRN/WHT	GRN/WHT	3	RD +
4	BLU	BLU	4	
5	BLU/WHT	BLU/WHT	5	
RD - 6	GRN	GRN	6	RD -
7	BRN/WHT	BRN/WHT	7	
8	BRN	BRN	8	
RJ45			RJ45	

Crossover Cable

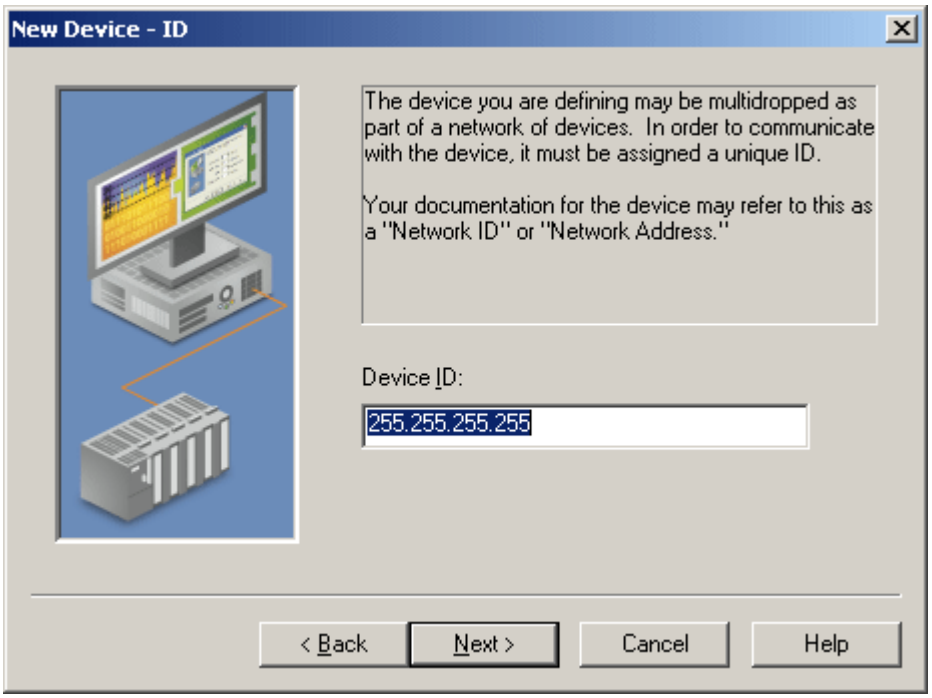
TD + 1	OR/WHT	GRN/WHT	1	TD +
TD - 2	OR	GRN	2	TD -
RD + 3	GRN/WHT	OR/WHT	3	RD +
4	BLU	BLU	4	
5	BLU/WHT	BLU/WHT	5	
RD - 6	GRN	OR	6	RD -
7	BRN/WHT	BRN/WHT	7	
8	BRN	BRN	8	
RJ45			RJ45	



Device ID Selection

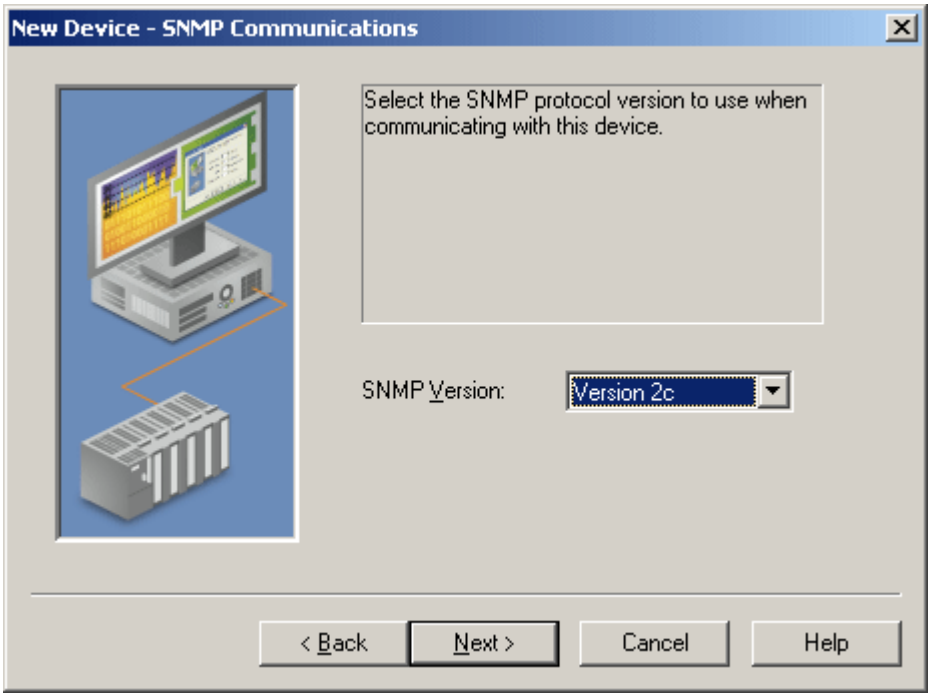
Device ID

This parameter specifies an IP address or resolvable domain name that will be used for the Device ID. Names will be resolved when the SNMP Driver first connects to the device. If the name resolution fails, the SNMP session will fail to initialize.



Communication Parameters

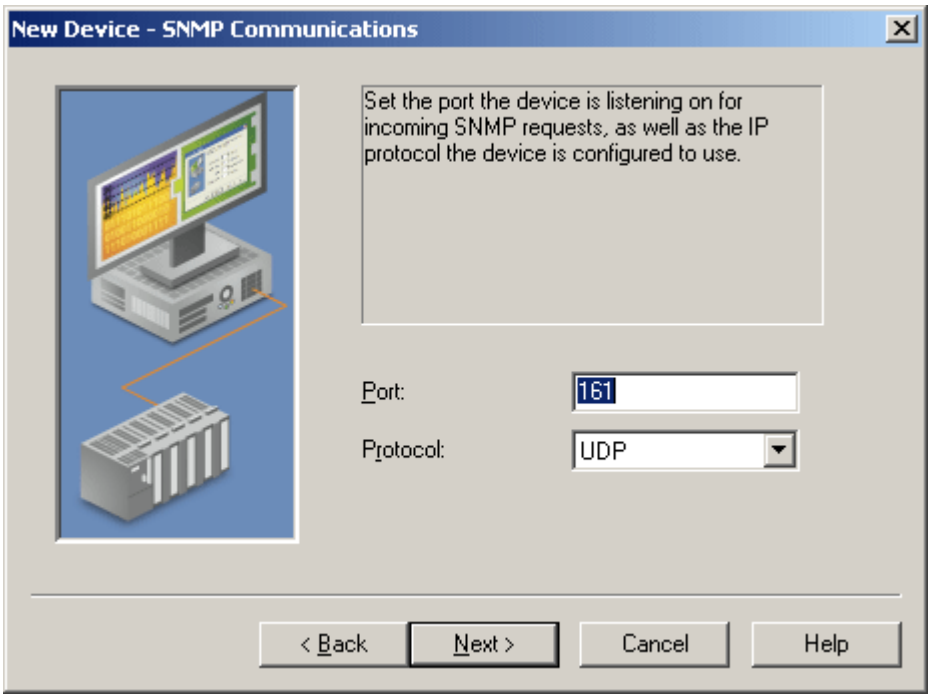
SNMP Protocol Version



This parameter specifies the version used by the remote device. Versions 1 and 2c are available.

Port and IP Protocol

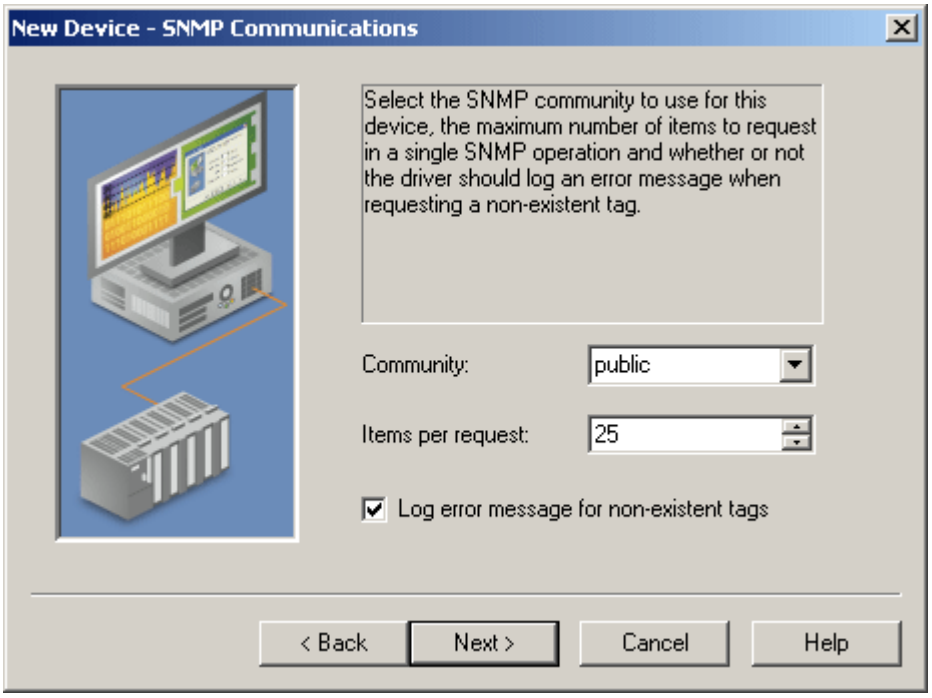
These parameters are used when communicating to the remote device.



Descriptions of the parameters are as follows:

- **Port:** Ports may range from 1 to 65535. The default port is 161.
- **Protocol:** UDP and TCP protocols are available. The default protocol is UDP.

SNMP Community



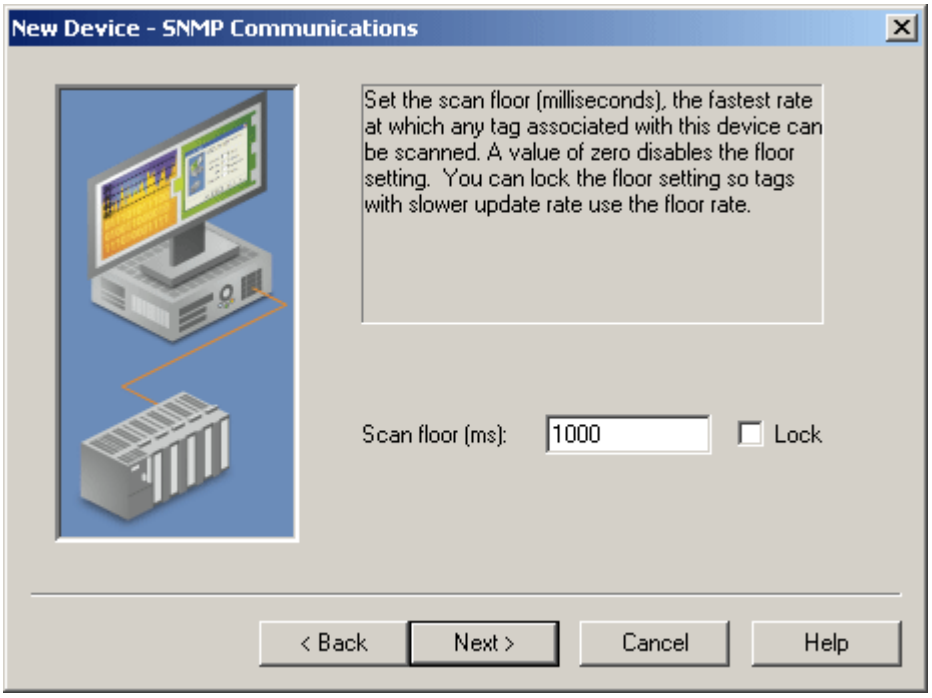
Descriptions of the parameters are as follows:

- **Community:** This parameter is used when accessing the remote SNMP device. The community name can be defined by the user and depends entirely on the configuration of the remote device. Common options include **Public** and **Private**. Typically, the public community is for reading data, whereas the private community is for

writing data to an Agent. For information on determining the correct community name, refer to the device's help documentation. This field is limited by the driver to 256 characters.

- **Items per request:** This parameter controls how many SNMP data items will be bundled together in each read request. For Agents or devices supporting SNMP v1, this may need to be set to a value as low as 1. SNMP version 2c devices can typically handle the maximum items per request. The valid range is from 1 to 25. The default setting is 25.
- **Log error message for non-existent tags:** An SNMP Agent or device is dynamic and may change during operation. When checked, this parameter has the OPC server display an error notice when a specified OID address does not exist on the target device. When unchecked, the messages will be suppressed.

SNMP Scan Floor



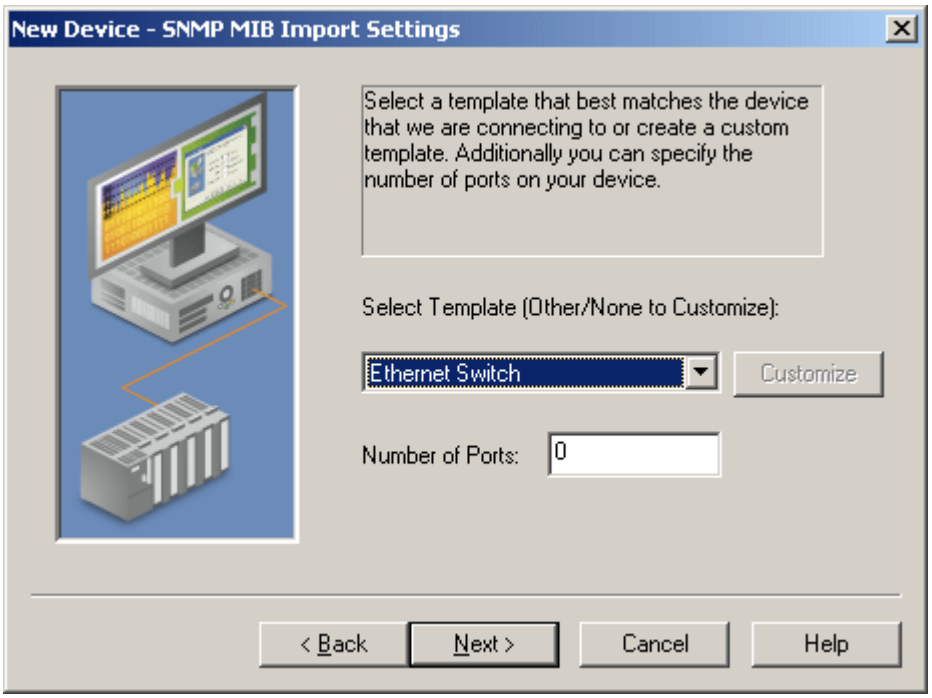
Descriptions of the parameters are as follows:

- **Scan Floor (ms):** This parameter prevents users from inadvertently overloading Agent and devices with read requests. Since SNMP devices are normally scanned at slower rates than other controls equipment, scanning an SNMP device too quickly may result in degraded device performance. This parameter specifies the minimum rate at which to scan SNMP devices. The valid range is 0 to 2147483646. The default setting is 1000 milliseconds.

  Note: When set to a non-zero value, the SNMP Driver will not scan the remote device more often than what is specified. The OPC client can still poll the server, however, in order to obtain the last read value at a faster OPC Group Update Rate. When set to zero, this feature will be disabled.

- **Lock:** When checked, this option will lock the Scan Rate for this device at the given value. When locked, the driver will always poll at the Scan Rate setting (regardless of OPC client update rates that are below or above this rate).

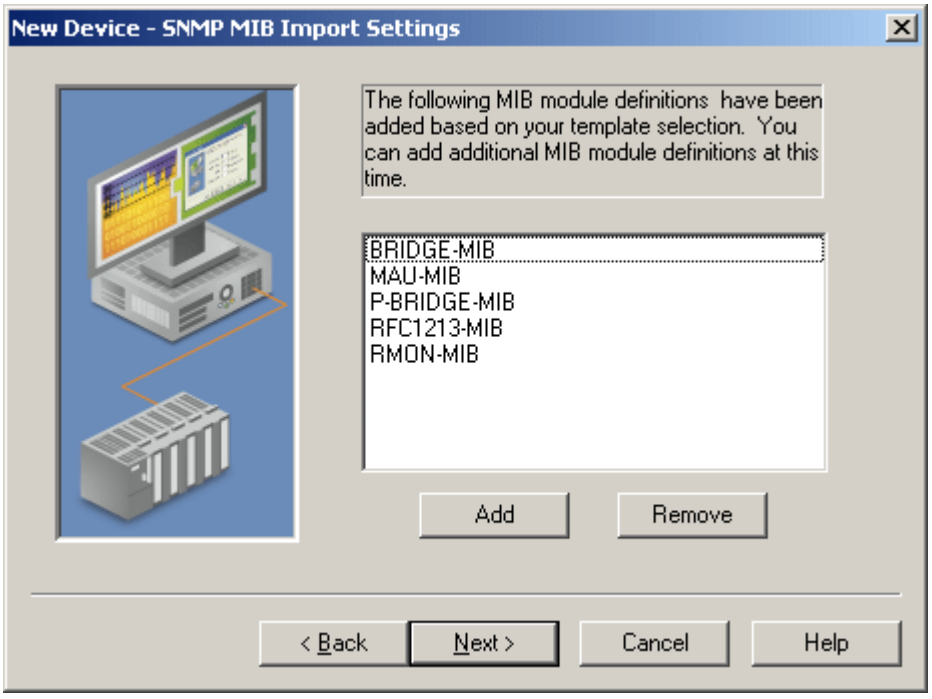
MIB Import Settings



Descriptions of the parameters are as follows:

- **Select Template (Other/None to Customize):** This parameter specifies the template that will guide the automatic creation of tags for the new device. Templates include **Ethernet Switch**, **Single-phase UPS**, **Three-phase UPS**, **Other Device** and **None**. Other Device will create a generic set of tags for a multi-port SNMP-enabled device. None has no associated preset tag set.
- **Number of Ports:** All templates (except for UPS) must enter the number of Ethernet ports on the device. Tags will be generated for each port present. The valid range is 0 to 2147483647.

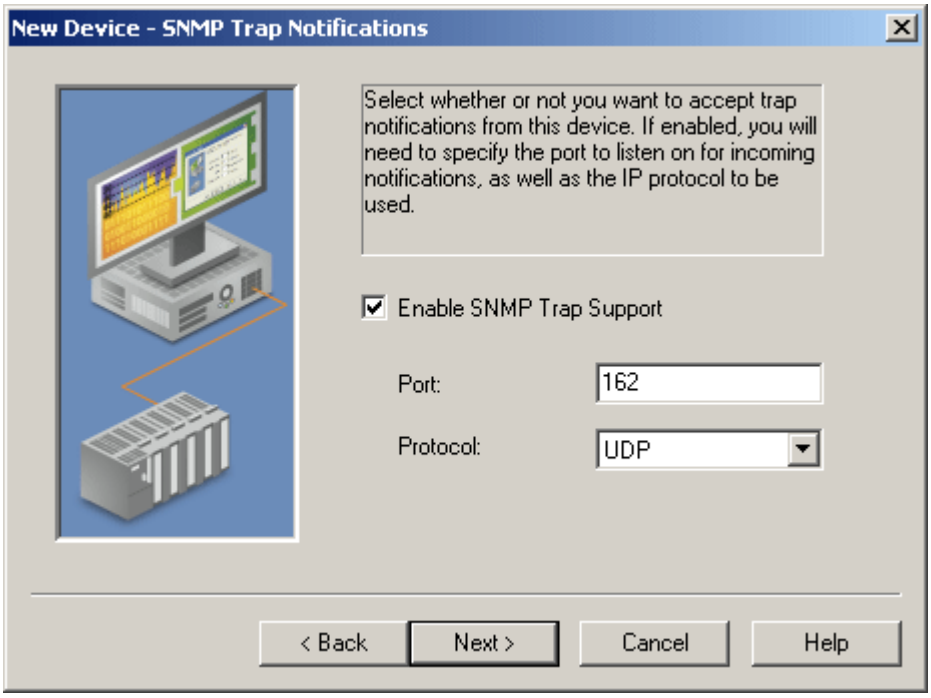
Additional MIB Modules



This dialog displays the MIB modules associated with the chosen template. Other MIB modules can be added at this point. For more information, refer to **About MIB Modules**.

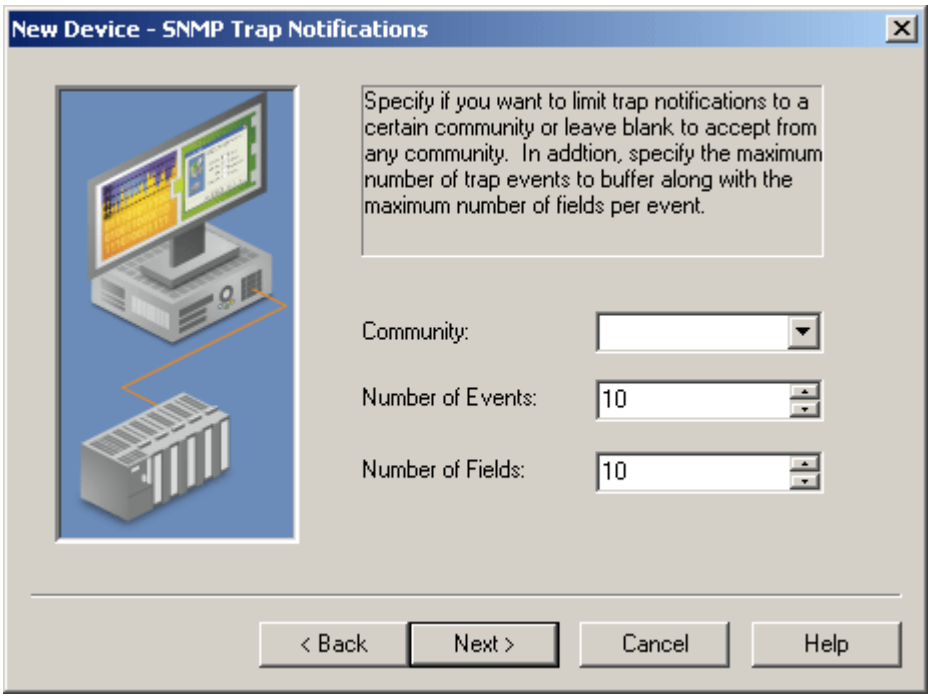
SNMP Trap Notification

SNMP managed devices can often be configured to send unsolicited messages (known as traps or notifications) to host systems or managers.



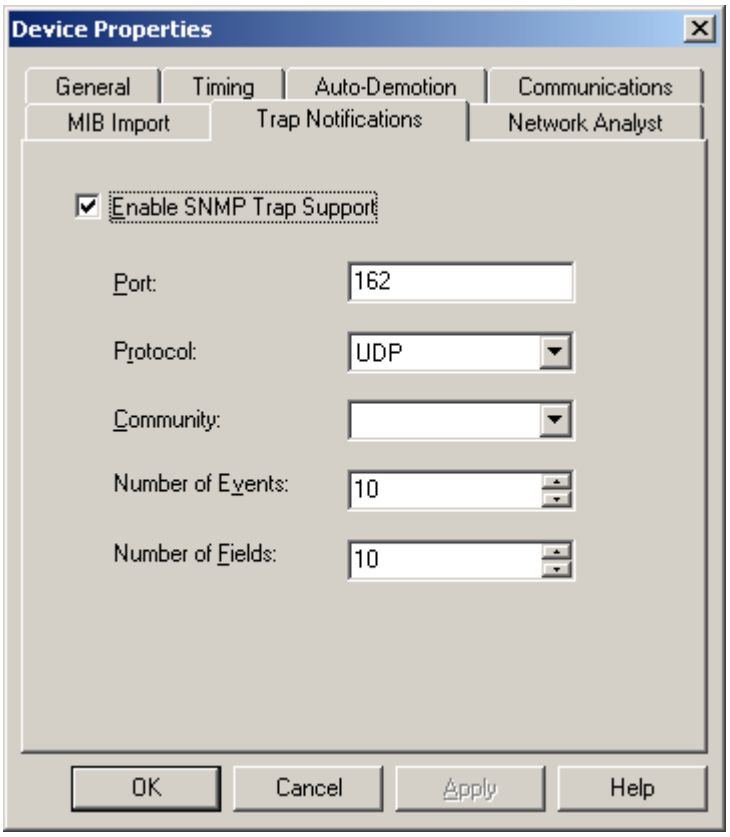
Descriptions of the parameters are as follows:

- **Enable SNMP Trap Support:** When checked, the SNMP managed devices will send traps to the host system and managers. It is enabled by default.
- **Port:** This parameter specifies the port on which the device will listen for notifications. The valid range is 1 to 65535. The default setting is 162, which is the most commonly used port for sending and receiving traps.
- **Protocol:** The protocol may be UDP or TCP. The default setting is UDP.

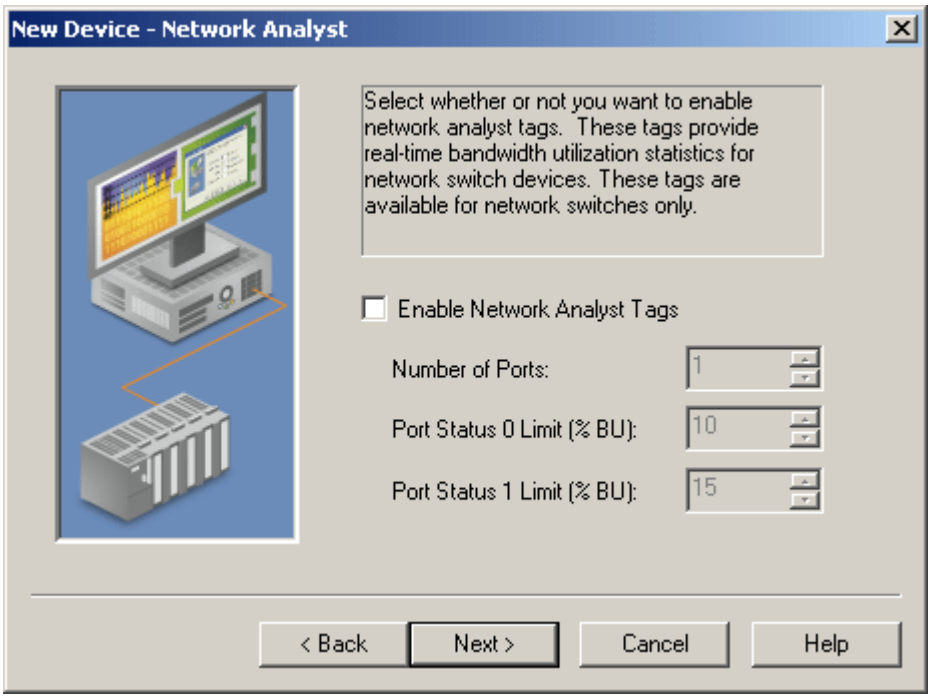


Descriptions of the parameters are as follows:

- **Community:** This is an optional setting. If a community name is entered, the SNMP Driver will only accept trap messages addressed to that community. In addition, traps will only be accepted from the IP address configured in the OPC server device. Leaving this field blank will allow trap messages to be received that are addressed to any community (or none at all). The community is limited to 256 characters.
- **Number of Events:** Trap messages are provided to client applications via an event queue in the driver. The queue is a FIFO stack that displays several trap messages that were received last. This parameter specifies the amount of trap messages to retain in the queue. The driver allows between 1 and 100 events to be collected. The default setting is 10.
- **Number of Fields:** Each trap message may carry additional variables, which are then parsed into a number of individual tag fields. The default setting is 10. It is recommended that users choose the maximum number in order to allow extra fields for the server-generated timestamp and a generic trap description (which is only for SNMP version 1). The driver allows between 1 and 20 fields. For more information on trap message addressing, refer to **Trap Events Queue** and **Trap Tags**.

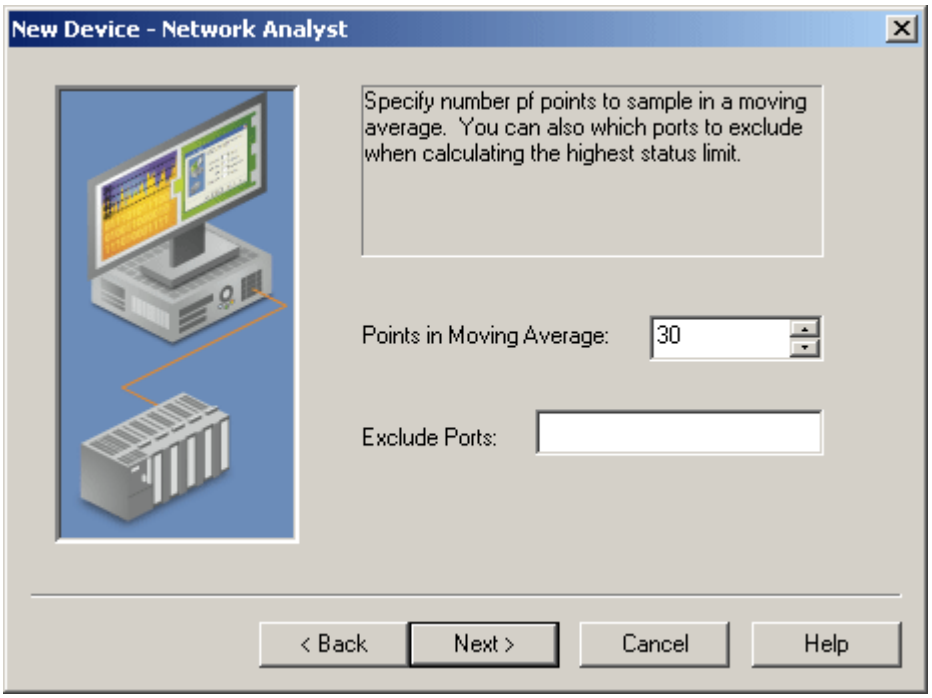


Network Analyst Tags



Descriptions of the parameters are as follows:

- **Enable Network Analyst Tags:** When enabled, network analyst tags are made available with the **Ethernet Switch** and **Other Device** profiles. For more information, refer to **About Network Analyst Tags**.
- **Number of Ports:** This parameter specifies the number of ports for the switch device. This is separate from the port number setting in Profile Selection. The valid range is 1 to 99.
- **Port status 0 limit** and **Port status 1 limit:** These parameters specify the threshold settings for each switch port's buStat tags. The buStat tags are a three-state indicator of the rough class of utilization for incoming bandwidth. When the buPctIn for a port rises above the **Port status 0 limit**, that buStat tag will change from 0 to 1. Similarly, when the buPctIn rises above the **Port status 1 limit**, the buStat tag will change from 1 to 2. The valid range is 0 to 100. The Port status 0 limit should not be greater than Port status 1 limit.



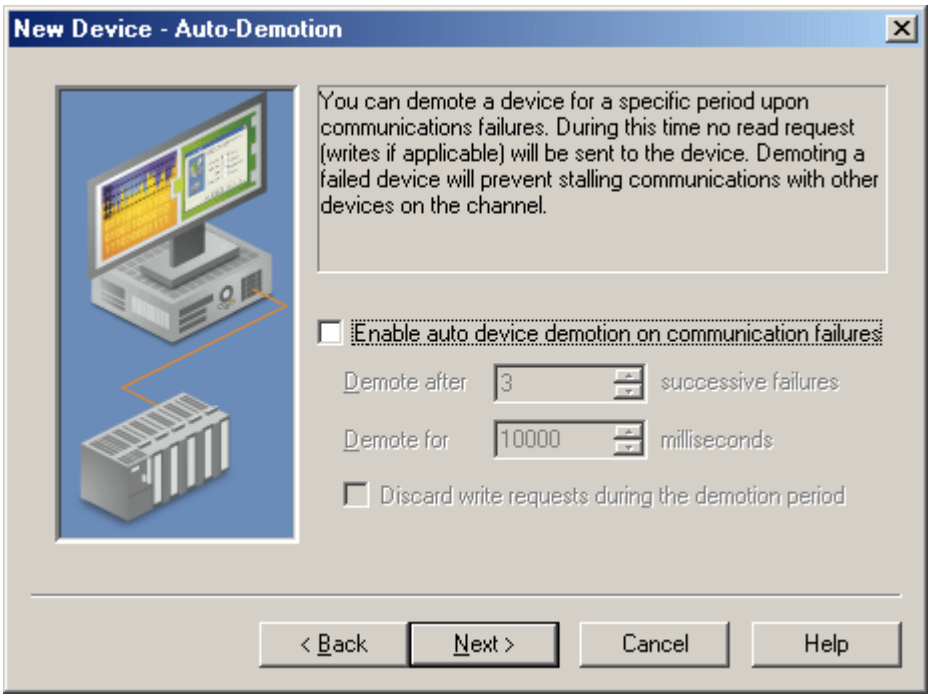
Descriptions of the parameters are as follows:

- **Points in Moving Average:** This parameter specifies how many sample values will be used when calculating the buPctIn and buPctOut values. The data points' average is taken in order to smooth the Ethernet traffic's inherently erratic behavior. The number of points in the moving average can be from 1 to 200.
- **Exclude Ports:** This parameter allows the switchBUStat tag to ignore some ports when calculating the highest buStat value. This is a list (1, 3, 6, 8) that can also contain ranges (1, 3-7, 9-11).

See Also: **About Network Analyst Tags**

Auto-Demotion and SNMP

Because of the way the SNMP Driver processes OPC tags, a non-responsive device with many tags may impede communications with other devices on the same channel. This is due to the timeout period being used on each successive query to the non-responsive device. Auto-Demotion is recommended for each device when communication may be unreliable.



Data Types Description

The SNMP Driver supports the following data types.

Data Type	Description
Boolean	Single bit
DWord	Unsigned 32 bit value bit 0 is the low bit bit 31 is the high bit
DWord Example	The driver interprets two consecutive registers as a single precision value.
Long	Signed 32 bit value bit 0 is the low bit bit 30 is the high bit bit 31 is the sign bit
Long Example	The driver interprets two consecutive registers as a single precision value.
String	ASCII text string
Float	32 bit floating point value bit 0 is the low bit bit 31 is the high bit
Float Example	The driver interprets two consecutive registers as a single precision value.
Double	64 bit floating point value bit 0 is the low bit bit 63 is the high bit
Double Example	The driver interprets four consecutive registers as a double precision value.

Each tag used in the driver has a fixed data type when there is MIB information for the address. Therefore, it is recommended that the driver be allowed to use the default data type for the point.

In a few cases, SNMP-centric data types do not exist in standard OPC. These items should be mapped or correlated to a valid OPC data type in order to be read. Extensive testing has been performed to assure that SNMP-centric data types can be served to and written from correctly with OPC client applications.

SNMP Centric	OPC Data Type
Integer32	Long
UInteger32	DWord
Counter64	NS*
Octet String	String
Bits	NS**
Object Identifier	String
Sequence	NS***
IPAddress	DWord
Counter32	DWord
Guage32	DWord
Timeticks	DWord
Opaque	NS****
Trap/Notification	String

*This is a 64 bit integer.
**Bit string.
***A sequence is a list of data. Complex data is currently not supported in OPC.
****Opaque data is a memory BLOB.

Note: There is no corresponding data type in OPC to handle these data types.

Address Descriptions

Addresses in the SNMP Driver are specified by the Object Identifier (OID) followed by an instance number. The OID can be defined in one of several forms and as follows:

Object Identifier	Description
SNMPv2-MIB::sysDescr.0	(Module::Object notation)
.1.3.6.1.2.1.1.1.0	(Numeric notation)
.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0	(Verbose notation)

Note: For more information about address structure, refer to **About SNMP Addresses**.

Table Offsets

To address an SNMP Table, specify the OID of the table head followed by the table offset (in brackets).

IF-MIB::tcpConnState[1]

Note: All SNMP table offsets begin at 1. Tags addressed to table offsets beyond the end of the table will be reported with bad quality until the table grows to that offset or beyond.

Historical Data

Each SNMP address has one or more historical data options available. Historical values are generated by the SNMP Driver , not the remote Agent or device.

See Also:
Previous Value
Delta Time
Moving Average

Scan Rate Floor

The scan rate can be set in milliseconds for each SNMP device. The _ScanRateFloor tag will display the setting's current value. When it is set greater than zero, the SNMP Driver will not allow tags to be scanned faster than specified. The device can also be set to lock the scan rate at this value, prohibiting any change by the OPC client. The _ScanRateFloorLock tag will show the lock option's status. The tags are Read Only.

Note: Setting the feature to zero will disable it.

Unsolicited Data

SNMP-enabled devices may be configured to send unsolicited messages, called traps (or notifications). For more information, refer to **Trap Events Queue** and **Trap Tags**.

About SNMP Addresses

The Simple Network Management Protocol accesses information in a **Management Information Base (MIB)**. The MIB is a tree structure whose origin is at the top, which is a node labeled ".1" or ".iso." Although many discussions of SNMP refer to MIBs as a plural, there is only one. The plural references actually refer to MIB modules (which describe portions of the MIB tree).

The SNMP address is known as an **Object Identifier (OID)** and consists of a series of elements that describes its location in the MIB tree. The elements are separated by a character referred to as dots ('.'). Most addresses of interest will begin with *.iso.org.dod.internet.mgmt* (or .1.3.6.1.2). From that point, the address extends into particular modules that describe related sets of information. For example, consider the IF-MIB module: it contains a variety of objects' definitions that access data about the network interfaces of the remote device. These include port status, traffic counters and so forth.

The *Module::Object* syntax of SNMP addresses means that "IF-MIB::" can be written instead of ".iso.org.dod.internet.mgmt.mib-2.interfaces" (or the less understandable ".1.3.6.1.2.1.2.2"). Thus, the address "IF-MIB::ifOutOctets.1" refers to the number of octets (bytes) sent out of interface 1 on the target device. That form is easier to write than ".iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.1" or ".1.3.6.1.2.1.2.2.1.16.1". The SNMP Driver will accept all three of these address notations.

Enterprise or Private MIB Modules

Much of the SNMP address space is defined by Internet RFC standards. Individuals are not permitted to change or extend these module definitions. For that purpose, the SNMP standard provides an extension area of the address space under ".iso.org.dod.internet.private.enterprises." The value following this base is known as a **Private Enterprise Number (PEN)** and every address below that point is defined by the PEN owner. Manufacturers that need to provide unique information not otherwise described in standard MIB modules will need to define them in their own Enterprise space and typically supply a MIB module definition with their equipment. The SNMP Driver uses these supplied MIB definitions to correctly access the unique information in remote device.

Instances

The OID "IF-MIB::ifOutOctets.1" above provides an example of SNMP instances. A managed switch will have a set of "IF-MIB::ifOutOctets" OIDs, one for each network interface. They will use a trailing digit (or digits) to index into the set of instances. Instances may be numbered beginning at 1 for groups that map to physical attributes, such as "IF-MIB::ifOutOctets.1," "IF-MIB::ifOutOctets.2," "IF-MIB::ifOutOctets.3" and so forth. The number of instances for a given OID is typically fixed. Other OIDs may have multiple instances, such as "SNMPv2-MIB::sysLocation." Although the first instance will be "SNMPv2-MIB::sysLocation.0," an agent may optionally provide "SNMPv2-MIB::sysLocation.1" and so on.

Note: Instances should not be confused with tables.

Tables

The SNMP address space is dynamic. The SNMP Agent on the remote device may add and remove OIDs as necessary. The most frequent occurrence of this is in SNMP Tables. An SNMP Table is a grouping of logically related data into conceptual rows. The reason that the rows are "conceptual" is that SNMP protocol does not have a facility to retrieve a full row at a time. Table access is accomplished by enumerating a table's columns. The SNMP Driver uses an array-like notation for table access, as in "RFC1213-MIB::tcpConnState[1]." That OID is part of the "tcpConnTable." Tables differ from instances in the following two ways:

1. Tables may grow or shrink during operation. An SNMP Driver tag that references a table column element will lose data quality if the table shrinks to less than the referenced element (offset).

2. The OIDs representing table column elements are not necessarily consecutive. The OIDs for individual column elements may not be predictable, and may change from moment to moment in the Agent or device.

Device Implementation RFC-Standard Modules

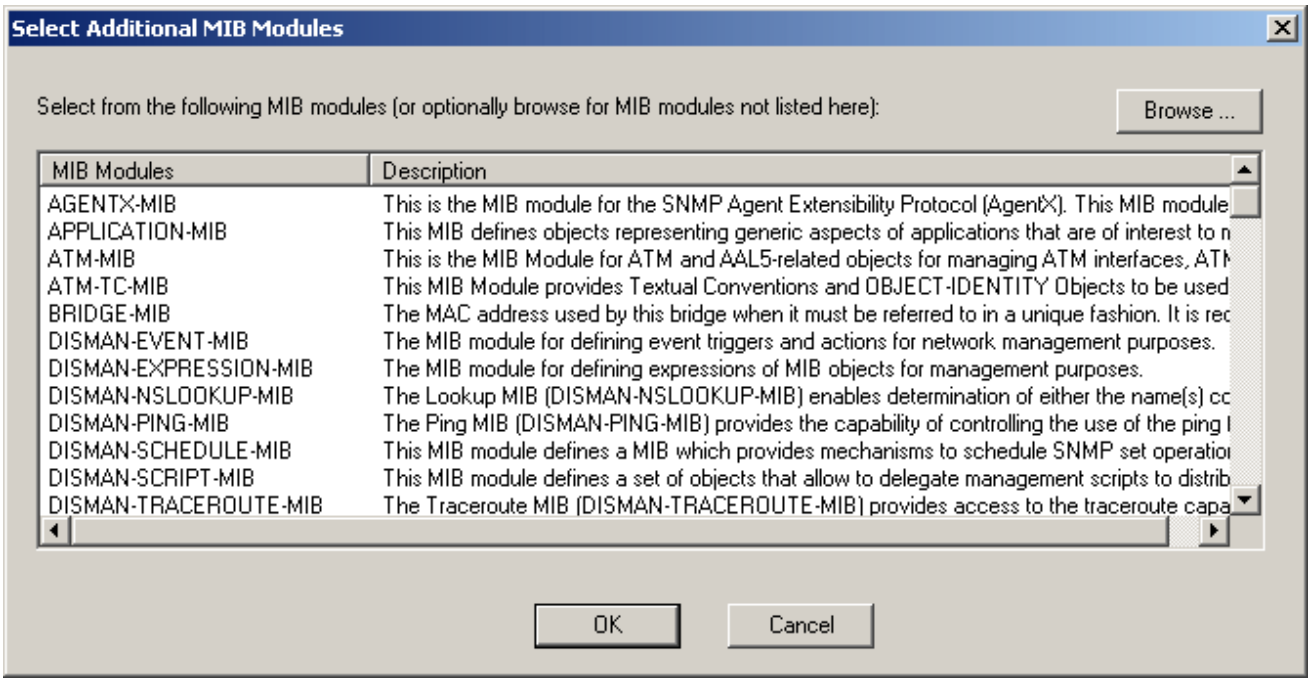
SNMP has defined a large and rich set of data that may or may not be implemented in SNMP-enabled devices. Although many device manufacturers implement the complete MIB module definition, others do not. If the SNMP Driver is able to poll some but not all of the OIDs defined in the server project, users should start by verifying what OIDs are fully supported in the remote device.

Community Credentials

There is also the question of the credentials used to connect to the SNMP device (the community name), and whether those credentials have permission to access certain data. The final authority for the presence and accessibility of an OID lies with the remote device. For more information, refer to the device's help documentation.

About MIB Modules

Much of the SNMP address space is defined by Internet RFC Standards. These standards break up the address space into modules, many of which are drawn from the RFC standards. Selecting a device template also selects a number of MIB modules to be referenced. Additional MIB modules may be associated with a device to support specialized capabilities. The SNMP Driver ships with a number of MIB modules pre-installed. To access these MIB definitions, click **Add** on the **SNMP MIB Import Settings** wizard page. Then, click **OK**.



Adding New MIB Modules

New MIB definitions, such as MIB modules supplied by a manufacturer, may be installed by clicking **Browse...** to import. Navigate to the MIB definition file and then click **Open**. The MIB definition will be checked for correctness and its description will be displayed if present. To accept the file for import, click **OK**. The module will be added to the current project and tags will be created for the objects that are defined.

Note 1: If the selected MIB module is already present in the repository, the relative dates of the two versions will be displayed. The user will be given the option to replace the module.

Note 2: If a MIB module contains errors, it cannot be imported. The import process automatically considers all MIB definition files in the same folder with the import candidate, and will bring in additional files if needed. Be sure that all MIB files associated with the device are present in the folder.

Note 3: Adding or importing a MIB module does not guarantee that new tags will be created. Some MIB modules (including those supplied by manufacturers) do not define any accessible objects.

About Network Analyst Tags

Ethernet switches carry traffic around networks. The SNMP Driver features a set of Network Analyst tag in order to easily keep track of a switch's capacity and utilization. These tags track the percentage of bandwidth in use on each switch's ports at any given time.

The buPctIn and buPctOut tags show the usage of each port in percent, averaged over a number of sample periods. The OPC client's scan rate is the sample period. For best results, the scan rate should be at least 1000 milliseconds. Longer periods are acceptable, whereas shorter periods may cause network congestion (because a number of SNMP data points must be read on each sample). The readings are averaged in order to smooth out the Ethernet traffic's inherently erratic behavior and make the values more useful for alarming.

The buStat tags utilize the threshold settings **Port status 0 limit** and **Port status 1 limit** in order to present a simple three-state "health" indicator. When a given port's buPctIn tag rises above the 0 limit, the buStat changes from 0 to 1. Likewise, when buStat rises above the 1 limit, buStat changes to 2. This provides a simple "traffic light" style, indicating the available capacity.

The switchBUStat tag assumes the highest value of the buStat tags, giving a single indication of the device's available capacity. The switchBUStat tag's behavior may be altered through the use of a list of ports to exclude. For example, a switch may have two ports that always run at or near capacity. By excluding these two ports, switchBUStat can indicate when the rest of the switch's capacity is nearing exhaustion without the known high-capacity activity causing false alerts.

Note: When enabled, the SNMP Driver will automatically create Network Analyst tags for a switch device.

Trap Tags

Trap tags are a notification mechanism for incoming trap messages, which may be generic or Enterprise-specific.

Version 1 Trap Tags

The syntax for a generic SNMP Version 1 trap tag is as follows:

TRAP_V1:.1.3.6.1.2.1.11:Gx

All V1 generic traps use this same OID. The ':Gx' field specifies the generic trap to which it is subscribed. Valid values for x are as follows:

coldStart: 0
warmStart: 1
linkDown: 2
linkUp: 3
authenticationFailure: 4
egpNeighborLoss: 5

For Enterprise-specific traps, the Enterprise OID is used in place of the generic OID in addition to a ':G6' field. Trap type 6 also requires a specific trap type, using the notation ':Sx' where x is the specific trap number. For example, an Enterprise-specific address may appear as follows:

TRAP_V1:.1.3.6.1.2.1.17:G6:S2

Note: For information on which Enterprise-specific traps may be sent, refer to the device manufacturer's help documentation.

To reset Boolean tags that transition to 1 on trap reception, users can write 0. To reset the notification tag for OPC clients who receive OnDataChange events for subsequent trap messages, users can write a 0 or a FALSE value.

Additionally, linkUp, linkDown and Enterprise traps may use the ':Px' field to specify which port will be monitored on the switch device. Enterprise traps must provide an "ifIndex" varbind for this to be useful. An incoming trap will populate both the port specific tag and the base tag. For example, a tag that monitors for linkDown on port 3 is as follows:

TRAP_V1:.1.3.6.1.2.1.11:G2:P3

Version 2 Trap Tags

The syntax for a generic SNMP Version 2C trap uses a set of OIDs in place of the ':Gx' field.

coldStart: .1.3.6.1.6.3.1.1.5.1
warmStart: .1.3.6.1.6.3.1.1.5.2
linkDown: .1.3.6.1.6.3.1.1.5.3
linkUp: .1.3.6.1.6.3.1.1.5.4
authenticationFailure: .1.3.6.1.6.3.1.1.5.5

Note: egpNeighborLoss generic traps are not implemented in SNMP Version 2C.

For example, a tag to monitor for linkDown on port 3 is as follows:

TRAP_V2C:.1.3.6.1.6.3.1.1.5.3:P3

Version 2C Enterprise-specific traps use the OID that the remote device places in the snmpTrapOID.0 varbind field. No specific trap field is used. Version 2C doesn't use the specific trap property. For information on which Enterprise-specific traps may be sent, refer to the device manufacturer's documentation.

Additional Functionality

All trap tags may use a table-like syntax for accessing additional trap information. The virtual table fields are as follows:

[1] Local time stamp, generated on trap arrival (string).
[2] Enterprise OID (string, empty for Version 2c).
[3] Generic trap type (int, 0 for Version 2c).
[4] Specific trap type (int, 0 unless Version 1 and the generic type is 6).
[5] SysUpTime (in timeticks. 0 for Version 2c, and not a time stamp).
[6] Number of varbind items.
[7] First varbind OID (as string).
[8] First varbind value (as string).
[9]..[n] Successive varbinds.

All the virtual table tags are Read Only. Automatic Tag Generation provides a number of virtual table tags by default.

Note 1: Virtual table entry [5], sysUpTime, refers to the tap event's time-of-occurrence. This is expressed as the number of timeticks beginning when the remote SNMP agent started. It does not represent any specific wall/clock time.

Note 2: Although the older trap syntax (which is the OID to be monitored followed by a (T) modifier) is deprecated, it is still supported. The older syntax does not support the virtual table information.

Historical Data Attributes

Addresses may be accompanied by one of three modifiers in order to access historical attributes. Historical values are generated by the SNMP Driver (not the remote Agent or device) when valid historical modifiers append to an OID. For more information, select a link from the list below.

Previous Value (PV)
Delta Time (DT)
Moving Average (MA5)

Previous Value

The Previous Value historical attribute returns the value of the SNMP address from the previous read cycle. This is not the previous differing value. If the address data has not changed, the previous value will be the same as the current value.

(Module::Object notation)
RFC1213-MIB::ifOutOctets.1(PV)

(Numeric notation)
.1.3.6.1.2.1.2.2.1.16.1(PV)

(Verbose notation)

.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.1(PV)

Delta Time

The Delta Time historical attribute returns the time difference between the current and previous read cycle, and is expressed in whole seconds for compatibility with legacy projects. Delta values of less than 1 second will report as 0.

(Module::Object notation)
RFC1213-MIB::ifOutOctets.1(DT)

(Numeric notation)
.1.3.6.1.2.1.2.2.1.16.1(DT)

(Verbose notation)
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.1(DT)

Moving Average

The Moving Average historical attribute returns the average of the last n readings, as specified in the address modifier. The modifier form is Max, where x is the number of points to use in calculating the moving average. Values for x may be anything larger than 1. If the x value is left out, the moving average calculation defaults to 5 points.

(Module::Object notation)
RFC1213-MIB::ifOutOctets.1(MA5)

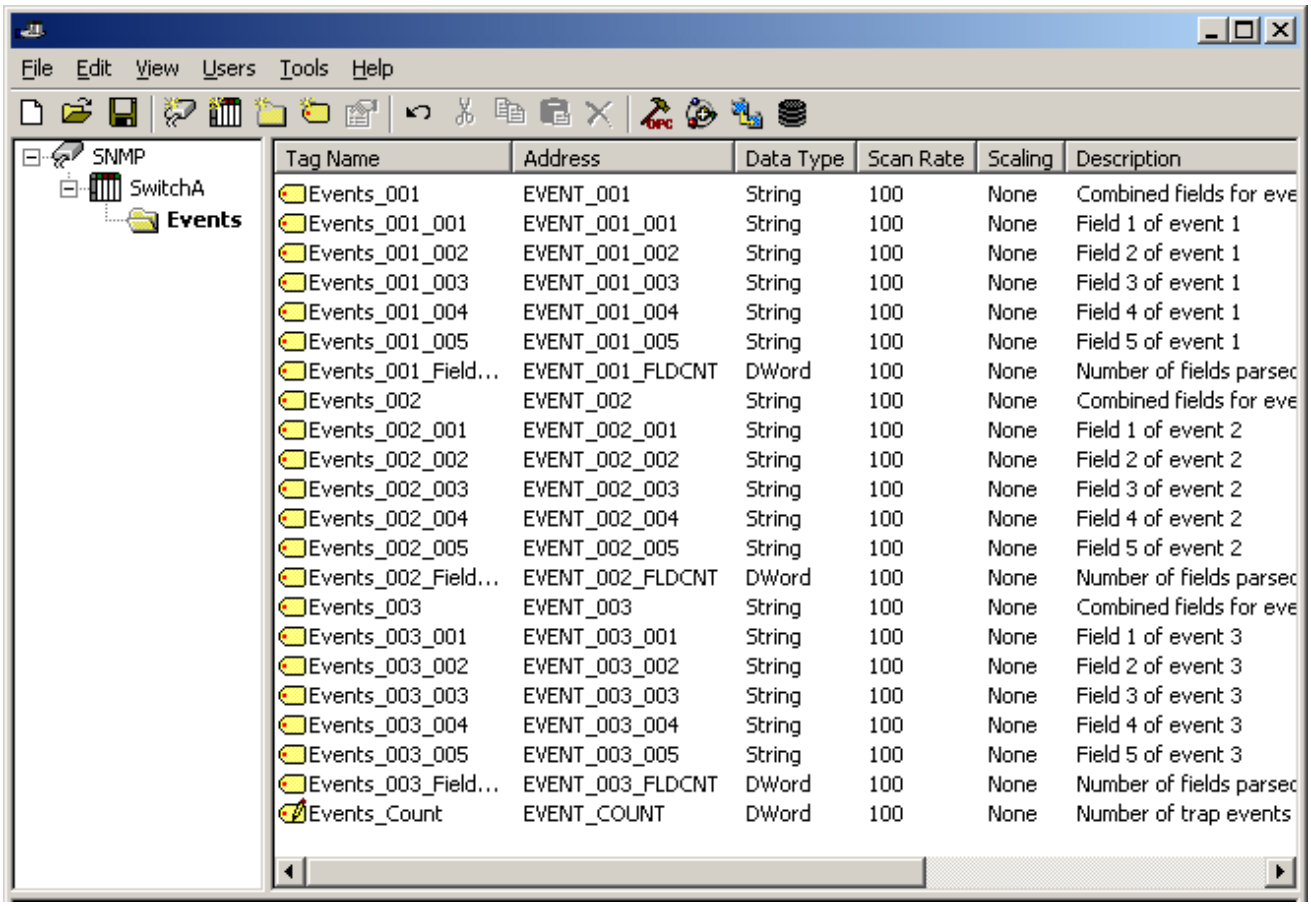
(Numeric notation)
.1.3.6.1.2.1.2.2.1.16.1(MA5)

(Verbose notation)
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOutOctets.1(MA5)

Trap Events Queue

SNMP remote devices may be configured to send unsolicited messages back to the SNMP Driver . To configure traps, users must login to the device to check the SNMP settings and then enable the traps. This includes defining Host IP(s) to receive the trap notifications. Since configuration changes usually require warm or cold restart of the device, users should check related network dependencies before performing a restart. Description of the messages are as follows:

- **Receiving Trap Messages:** These messages are configured during SNMP Driver setup. They may also be referred to as Notification messages. For more information, refer to **Communications Parameters**.
- **Incoming Trap Messages:** These messages are placed into an Events queue. The most recent message is placed at position 1.



Tag Name	Address	Data Type	Scan Rate	Scaling	Description
Events_001	EVENT_001	String	100	None	Combined fields for eve
Events_001_001	EVENT_001_001	String	100	None	Field 1 of event 1
Events_001_002	EVENT_001_002	String	100	None	Field 2 of event 1
Events_001_003	EVENT_001_003	String	100	None	Field 3 of event 1
Events_001_004	EVENT_001_004	String	100	None	Field 4 of event 1
Events_001_005	EVENT_001_005	String	100	None	Field 5 of event 1
Events_001_Field...	EVENT_001_FLDCNT	DWord	100	None	Number of fields parsed
Events_002	EVENT_002	String	100	None	Combined fields for eve
Events_002_001	EVENT_002_001	String	100	None	Field 1 of event 2
Events_002_002	EVENT_002_002	String	100	None	Field 2 of event 2
Events_002_003	EVENT_002_003	String	100	None	Field 3 of event 2
Events_002_004	EVENT_002_004	String	100	None	Field 4 of event 2
Events_002_005	EVENT_002_005	String	100	None	Field 5 of event 2
Events_002_Field...	EVENT_002_FLDCNT	DWord	100	None	Number of fields parsed
Events_003	EVENT_003	String	100	None	Combined fields for eve
Events_003_001	EVENT_003_001	String	100	None	Field 1 of event 3
Events_003_002	EVENT_003_002	String	100	None	Field 2 of event 3
Events_003_003	EVENT_003_003	String	100	None	Field 3 of event 3
Events_003_004	EVENT_003_004	String	100	None	Field 4 of event 3
Events_003_005	EVENT_003_005	String	100	None	Field 5 of event 3
Events_003_Field...	EVENT_003_FLDCNT	DWord	100	None	Number of fields parsed
Events_Count	EVENT_COUNT	DWord	100	None	Number of trap events

Trap messages may carry several variables or components of information. These variables are placed into the Event field tags. When a new trap is received, the entire message is placed into address EVENTS_001 as a semicolon-delimited string. Each component is broken into EVENTS_001_001, EVENTS_001_002, EVENTS_001_003 and so forth. The EVENTS_001_FLDCNT address contains the number of fields found in the trap message.

Note: The address EVENTS_COUNT increments with each incoming trap message. To reset the counter, users can write a new value. To reset the EVENTS_COUNT address from client applications, users can write a zero.

Auto Created Trap Tags

If traps are enabled, a set of trap tags will be created for the trap OIDs present in the device profile. For the Ethernet Switch and Other Device profiles, these will be coldStart, warmStart, linkUp and linkDown. A base tag is created for each of these, along with 20 table entries representing the first 20 rows of the virtual trap message table. For more information on table entries, refer to **Trap Tags**.

Note: Trap OIDs defined in any included MIB modules will also have a similar set of trap tags created.

Error Descriptions

The following error/warning messages may be generated. Click on the link for a description of the message.

Address Validation

Address '<address>' is out of range for the specified device or register
Data Type '<type>' is not valid for device address '<address>'
Device address '<address>' contains a syntax error
Device address '<address>' is read only

The remote device reports that the requested name <OID> does not exist on <Device Name>

Run-Time Error Messages

'<channel name>.<device name>': unable to open a SNMP session to host '<host>' on port <port>, using protocol <protocol>

'<channel name>.<device name>': Unable to establish a trap listener on port <port>, using protocol <protocol>. No trap events will be received

Access to address'<address>' on '<channel name>.<device name>' is not permitted

Address '<address>' on '<channel name>.<device name>' is not writable

Address '<address>' on '<channel name>.<device name>' is unavailable

Device <device name> does not support the necessary information required to perform network analysis. Network Analyst tags will be disabled for this device

Device <Device Name> does not support the number of ports currently configured in this application. Network Analyst tags will be disabled for this device

Device Discovery has exceeded <max devices> maximum allowed devices

High capacity counters for network analysis are not available for device <Device Name>. Attempting to use low capacity counters

The remote device reports that the requested name '<name>' does not exist on '<channel name>.<device name>'

The response message for the current transaction on '<channel name>.<device name>' would have been too large, and has been discarded by the remote device

Unable to bind trap socket on binding address '<address>', port '<port>' and protocol '<protocol>' for device '<device>'

Unable to bind trap socket on binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Unable to create communications thread on trap socket for binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Unable to create listener on trap socket for binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Unable to create trap socket on binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Unable to resolve host address <IP Address> on device <Device Name> for trap processing

Unable to send transaction: <reason>

SNMP Agent Error Messages

Data for address '<address>' on '<channel name>.<device name>' has an inconsistent value

Data for address '<address>' on '<channel name>.<device name>' has the wrong encoding

Data for address '<address>' on '<channel name>.<device name>' has the wrong length

Data for address '<address>' on '<channel name>.<device name>' has the wrong value

XML Error Messages

Invalid XML document [Reason: The excluded port list is invalid for device <device name>]

Invalid XML document [Reason: Port status 0 limit must be less than port status 1 limit for device <device name>]

Communications Error Messages

Unable to bind to adapter: '<Adapter Address>'. Connect failed. Winsock Err # n

Winsock initialization failed (OS Error = n)

Winsock shut down failed (OS Error = n)

Winsock V1.1 or higher must be installed to use the SNMP device driver

Authentication Error Messages

The authentication passphrase fields do not match. Please retype the passphrase identically in both fields

The privacy passphrase fields do not match. Please retype the passphrase identically in both fields

MIB Parser Error Messages

Address Validation

The following error/warning messages may be generated. Click on the link for a description of the message.

Address Validation

Address '<address>' is out of range for the specified device or register

Error Type:
Warning

Possible Cause:
A tag address that has been specified dynamically references a location that is beyond the range of supported locations for the device.

Solution:
Verify the address is correct; if it is not, re-enter it in the client application.

Data Type '<type>' is not valid for device address '<address>'

Error Type:
Warning

Possible Cause:
A tag address that has been specified statically has been assigned an invalid data type.

Solution:
Modify the requested data type in the client application.

Device address '<address>' contains a syntax error

Error Type:
Warning

Possible Cause:
An invalid tag address has been specified in a dynamic request.

Solution:
Re-enter the address in the client application.

Device address '<address>' is read only

Error Type:
Warning

Possible Cause:

A tag address that has been specified statically has a requested access mode that is not compatible with what the device supports for that address.

Solution:
Change the access mode in the client application.

The remote device reports that the requested name <OID> does not exist on <device name>

Error Type:
Warning

Possible Cause:
An object in the project is not available in the physical device. It has been deactivated.

Solution:
1. Remove the object from the project.
2. It is possible that the process the object is referring to is disabled in the physical device. Make sure it is enabled. The error should not occur in the next request.

Run-Time Error Messages

The following error/warning messages may be generated. Click on the link for a description of the message.

Run-Time Error Messages

'<channel name>.<device name>': unable to open a SNMP session to host '<host>' on port <port>, using protocol <protocol>

Error Type:
Warning

Possible Cause:
1. The Device ID contains a bad IP address or hostname.
2. The port specified is incorrect for the remote device.
3. The protocol specified is incorrect for the remote device.

Solution:
Check the Device Properties and ensure that the Device ID and Port and Protocol are correct.

See Also:
Device ID
Communication Parameters

'<channel name>.<device name>': Unable to establish a trap listener on port <port>, using protocol <protocol>. No trap events will be received

Error Type:
Warning

Possible Cause:
The specified port is unavailable for listening.

Solution:
1. Check for other applications listening for IP traffic on the chosen port.
2. Ensure that the Windows SNMP Trap Service is not running on the OPC server host machine.

Access to address '<address>' on '<channel name>.<device name>' is not permitted

Error Type:
Warning

Possible Cause:
The remote SNMP does not permit access to the requested SNMP OID.

Solution:
Verify that the community name is correct and permits access to the address.

See Also:
About SNMP Addresses
Communication Parameters

Address '<address>' on '<channel name>.<device name>' is not writable

Error Type:
Warning

Possible Cause:
The configured community name does not have write privileges for this address.

Solution:
Verify that the community name is correct and permits write access to the address.

See Also:
About SNMP Addresses
Communication Parameters

Address '<address>' on '<channel name>.<device name>' is unavailable

Error Type:
Warning

Possible Cause:
A tag address that has been specified dynamically references a location that is beyond the range of supported locations for the device.

Solution:
Verify the address is correct; if it is not, re-enter it in the client application.

Device <Device Name> does not support the necessary information required to perform network analysis. Network Analyst tags will be disabled for this device

Error Type:
Warning

Possible Cause:
Although Network Analyst functions were selected, the device does not support the OIDs required by this function.

Solution:
Disable the device's Network Analyst functions.

Device <Device Name> does not support the number of ports currently configured in this application. Network Analyst tags will be disabled for this device

Error Type:
Warning

Possible Cause:
The number of ports specified in the Network Analyst settings exceeds the number of ports available in the device.

Solution:
Verify the number of ports in the device. Then, edit the Network Analyst tab in Device Properties in order to regenerate the project tags with the correct number of ports specified.

Device Discovery has exceeded <max devices> maximum allowed devices

Error Type:
Warning

Possible Cause:
The Device Discovery has exceeded the maximum number of allowed devices.

Solution:
Limit the discovery range and then try again.

High capacity counters for network analysis are not available for device <device name>. Attempting to use low capacity counters

Error Type:

Warning

Possible Cause:
The device does not support the 64 bit counters that the project is created with. The server is attempting to use low capacity 32 bit counters instead.

Solution:
1. Verify that the supplied MIB is correct.
2. Edit the MIB to reflect the correct counter type and then import again.

The remote device reports that the requested name '<name>' does not exist on '<channel name>.<device name>'

Error Type:
Warning

Possible Cause:
The remote SNMP Agent has not implemented the requested SNMP OID.

Solution:
Remove the tag referring to the address.

See Also:
About SNMP Addresses

The response message for the current transaction on '<channel name>.<device name>' would have been too large, and has been discarded by the remote device

Error Type:
Warning

Possible Cause:
The remote SNMP Agent was unable to fit the requested data into a single SNMP reply.

Solution:
Reduce the number of items per request. For older SNMP V1 Agents, this may need to be as low as 1.

See Also:
Communication Parameters

Unable to bind trap socket on binding address '<address>', port '<port>' and protocol '<protocol>' for device '<device>'

Error Type:
Fatal

Possible Cause:
More than one channel has been assigned the same IP address, with SNMP Trap Support enabled.

Solution:
1. The trap socket is only allowed to bind to one IP address: ensure that that IP address is the one assigned to the PC.
2. Ensure that SNMP Trap Support is not enabled on more than one channel using the same address.

Unable to bind trap socket on binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Error Type:
Warning

Possible Cause:
Unable to bind the trap socket to the specified network card.

Solution:
Some other application has already bound a socket to the binding address/port pair.

Unable to create communications thread on trap socket for binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Error Type:
Warning

Possible Cause:
A thread that handles unsolicited communications for the specified socket/port and protocol could not be created.

Solution:
1. Check the operating system's event log for resource errors.
2. Check the number of process threads being used by the OPC server. Some older operating systems will limit the number of process threads to 1024 per process. For newer operating systems, this is limited by available memory.

Unable to create listener on trap socket for binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Error Type:
Warning

Possible Cause:
An incoming connection request (TCP/IP only) could not be listened for.

Solution:
1. Verify that there is not a resource conflict.
2. Verify that the remote device is able to establish a connection to the trap socket.

Unable to create trap socket on binding address <IP Address>, port <Port Number> and protocol <Protocol> for device <Device Name>

Error Type:
Warning

Possible Cause:
The server was unable to create the specified trap socket on the bound network card.

Solution:
1. Check for other applications listening for IP traffic on the chosen port and IP address.
2. Ensure that the Windows SNMP Trap Service is not running on the OPC server host machine.

Unable to resolve host address <IP Address> on device <Device Name> for trap processing

Error Type:
Warning

Possible Cause:
The server's Hostname Resolver is unable to resolve the hostname string for the device to an IP address.

Solution:
1. Verify the spelling of the hostname.
2. If the connection was working before, verify the Cache Lifetime settings in the Server Runtime Hostname Resolution settings.

Unable to send transaction: <reason>

The following error/warning messages concern transaction transmission to the remote device.

Reason	Possible Cause	Solution
Generic error	The protocol subsystem has reported a non-specific error.	N/A
Invalid local port	The local port may be restricted or in use.	Select an available port.
Unknown host	The remote hostname did not resolve.	Check the Device ID.
Unknown session	The SNMP session terminated unexpectedly.	Disconnect and reconnect the client to refresh the session.
Too long	The SNMP message was too long.	Reduce the number of items per request.
No socket	The local port may be restricted or in use.	Select an available port.
Failure in send to	Unable to send the transaction.	Check the Device ID and port.
Bad community specified	Bad community specified.	Check the community name.
Authentication failure	Incorrect password, community or key.	Check the community name.
MIB not initialized	MIB module file is not installed.	Check that the MIB module file is installed.

SNMP Agent Error Messages

The following errors reflect problems with the data received from the remote SNMP Agent. They are advisory and no local action is indicated.

SNMP Agent Error Messages

Data for address '<address>' on '<channel name>.<device name>' has an inconsistent value

Error Type:
Advisory

Possible Cause:
Problem with the data received from the remote SNMP Agent. Data for address has an inconsistent value.

Solution:
Check configuration of the remote SNMP Agent.

Data for address '<address>'on '<channel name>. <device name>' has the wrong encoding

Error Type:
Advisory

Possible Cause:
Problem with the data received from the remote SNMP Agent. Data for address has the wrong encoding.

Solution:
Check configuration of the remote SNMP Agent.

Data for address '<address>'on '<channel name>.<device name>' has the wrong length

Error Type:
Advisory

Possible Cause:
Problem with the data received from the remote SNMP Agent. Data for address has the wrong length.

Solution:
Check configuration of the remote SNMP Agent.

Data for address '<address>'on '<channel name>. <device name>' has the wrong value

Error Type:
Advisory

Possible Cause:
Problem with the data received from the remote SNMP Agent. Data for address has the wrong value.

Solution:
Check configuration of the remote SNMP Agent.

XML Error Messages

The following error/warning messages may be generated. Click on the link for a description of the message.

XML Error Messages

Invalid XML document [Reason: The excluded port list is invalid for device <device name>]

Invalid XML document [Reason: Port status 0 limit must be less than port status 1 limit for device <device name>]

Invalid XML document [Reason: The excluded port list is invalid for device <device name>]

Error Type:
Fatal

Possible Cause:
The XML project file was edited such that the ExcludePorts element for the device is invalid.

Solution:
Search the XML project file for the ExcludePorts element of the device and make sure that the string value complies with the following guidelines:

1. Port numbers are in ascending order.
2. Port numbers are separated by a comma. For example, 1,3,10.
3. A hyphen may be used for consecutive ports in order to indicate a range. For example, 2, 5-7, 15-18.
4. Port numbers are in the range 1-'Number of Ports' setting.

See Also:
Network Analyst Tags

Invalid XML document [Reason: Port status 0 limit must be less than port status 1 limit for device <device name>]

Error Type:
Fatal

Possible Cause:
The XML project file was edited such that the PortStatusLimit0 element for the device has an integer value that is greater than or equal to the integer value of the corresponding PortStatusLimit1 element.

Solution:
Search the XML project file for the PortStatusLimit0 element of the device and make sure that the integer value is less than the integer value of the corresponding PortStatusLimit1 element.

See Also:
Network Analyst Tags

Communications Error Messages

The following error/warning messages may be generated. Click on the link for a description of the message.

Communications Error Messages
Unable to bind to adapter: '<Adapter Address>'. Connect failed. Winsock Err # n
Winsock initialization failed (OS Error = n)
Winsock shut down failed (OS Error = n)
Winsock V1.1 or higher must be installed to use the SNMP device driver

Unable to bind to adapter: '<Adapter Address>'. Connect failed. Winsock Err # n

Error Type:
Fatal

Possible Cause:
The driver was unable to bind to the specified network adapter, which is necessary for communications with the device. This may have occurred because of the following:

1. The adapter is disabled or no longer exists
2. There was a network system failure (such as Winsock or network adapter failure).
3. There are no more available ports.

Solution:
1. Check the Network Adapter list in the communications server application for network adapters available on the system. If '<adapter>' is not in this list, steps should be taken to make it available to the system. This includes verifying that the network connection is enabled and connected in the PC's Network Connections.
2. Determine how many channels are using the same '<adapter>' in the communications server application. Reduce this number so that only one channel is referencing '<adapter>'. If the error still occurs, check to see if other applications are using that adapter and then shut down those applications.

Winsock initialization failed (OS Error = n)

Error Type:
Fatal

OS Error	Indication	Possible Solution
10091	Indicates that the underlying network subsystem is not ready for network communication.	Wait a few seconds and restart the driver.

10067	Limit on the number of tasks supported by the Windows Sockets implementation has been reached.	Close one or more applications that may be using Winsock and restart the driver.

Winsock shut down failed (OS Error = n)

Error Type:
Fatal

Possible Cause:
The network was unable to disable or shut down a network connection.

Solution:
NA.

Winsock V1.1 or higher must be installed to use the SNMP device driver

Error Type:
Fatal

Possible Cause:
The version number of the Winsock DLL found on the system is less than 1.1.

Solution:
Upgrade Winsock to version 1.1 or higher.

Authentication Error Messages

The following error/warning messages may be generated. Click on the link for a description of the message.

Authentication Error Messages
The authentication passphrase fields do not match. Please retype the passphrase identically in both fields
The privacy passphrase fields do not match. Please retype the passphrase identically in both fields

The authentication passphrase fields do not match. Please retype the passphrase identically in both fields

Error Type:
Information

Possible Cause:
The authentication passphrase entered in the server does not match the passphrase entered into the remote device.

Solution:
Enter the correct passphrase.

The privacy passphrase fields do not match. Please retype the passphrase identically in both fields

Error Type:
Information

Possible Cause:
The privacy passphrase entered in the server does not match the passphrase entered into the remote device.

Solution:
Enter the correct passphrase.

MIB Parser Error Messages

The following error/warning messages may be generated. Click on the link for a description of the message.

MIB Parser Error Messages

The following MIB modules could not be successfully parsed and will not be added: \r\n\r\n <MIB Module>

Error Type:
Information

Possible Cause:
The driver was unable to resolve dependency and data type issues, and thus was unable to parse the specified MIB module.

Solution:
Correct the errors and then import again.

Unable to initialize required dependencies for MIB parsing (general exception)

Error Type:
Error

Possible Cause:
The driver was not able to initialize or load required dependent MIB files.

Solution:
These files could be locked by another process. Retry initialization.

Unable to initialize required dependencies for MIB parsing (missing imports)

Error Type:
Error

Possible Cause:
The MIB file references MIBs for importing that are not present.

Solution:
Find and import the referenced MIBs.

Unable to uninitialize required dependencies for MIB parsing (general exception)

Error Type:
Error

Possible Cause:
A required MIB file was unable to be unloaded.

Solution:
Verify that the MIB file is no longer in use and then attempt to close it again.

Index

- < -

- A -

- C -

- D -

- E -

- H -

- I -

- M -

- N -

- O -

- P -

- R -

- S -

- T -

- U -

- W -

- X -