Network Ping ICMP Connector

Network PING test

- Name: **Ping**
- Version: 1.2.0.0
- Protocol: ICMP
- Interface: TCP/IP
- Runtime: .NET 2.0 (Multiplatform)
- Configuration:
    - Devices / Protocols

Configure the Ping Driver
Supported Operands:
Channels Configuration
Nodes Configuration
Points Configuration
Troubleshoot
Driver Revision History

Overview

This document guides you through the process of setting up the Ping driver to execute pings at a specified frequency, such as every 10 or 30 seconds. It walks you through the steps of creating a new channel with the "Ping - IT Infrastructure" protocol, setting up a new node in this channel, creating a new AccessType, and applying this AccessType to your desired points. By following this process, you can have the Ping driver run automatically at your chosen frequency, with the results conveniently displayed in the TraceWindow. This setup can be particularly useful for regular network health checks and performance monitoring.

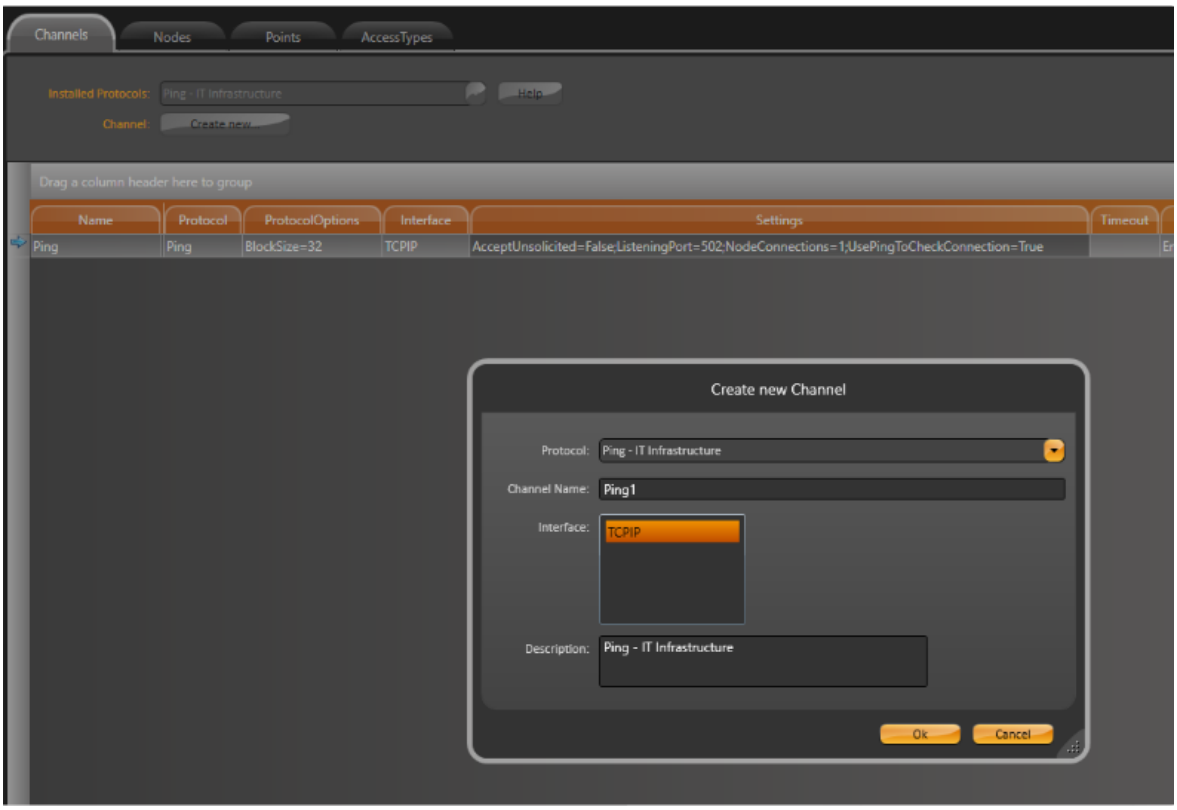
Ping driver is responsible for checking whether an IP address is responding or not by sending a package and receiving it back.

Communication Driver Information	
Driver name	Ping
Assembly Name	T.ProtocolDriver.Ping
Assembly Version	1.2.0.0
Available for Linux	False
Devices supported	N/A (Not Applicable)
Manufacturer	N/A (Not Applicable)
Protocol	Proprietary over TCP/IP
PC Requirements	Ethernet port

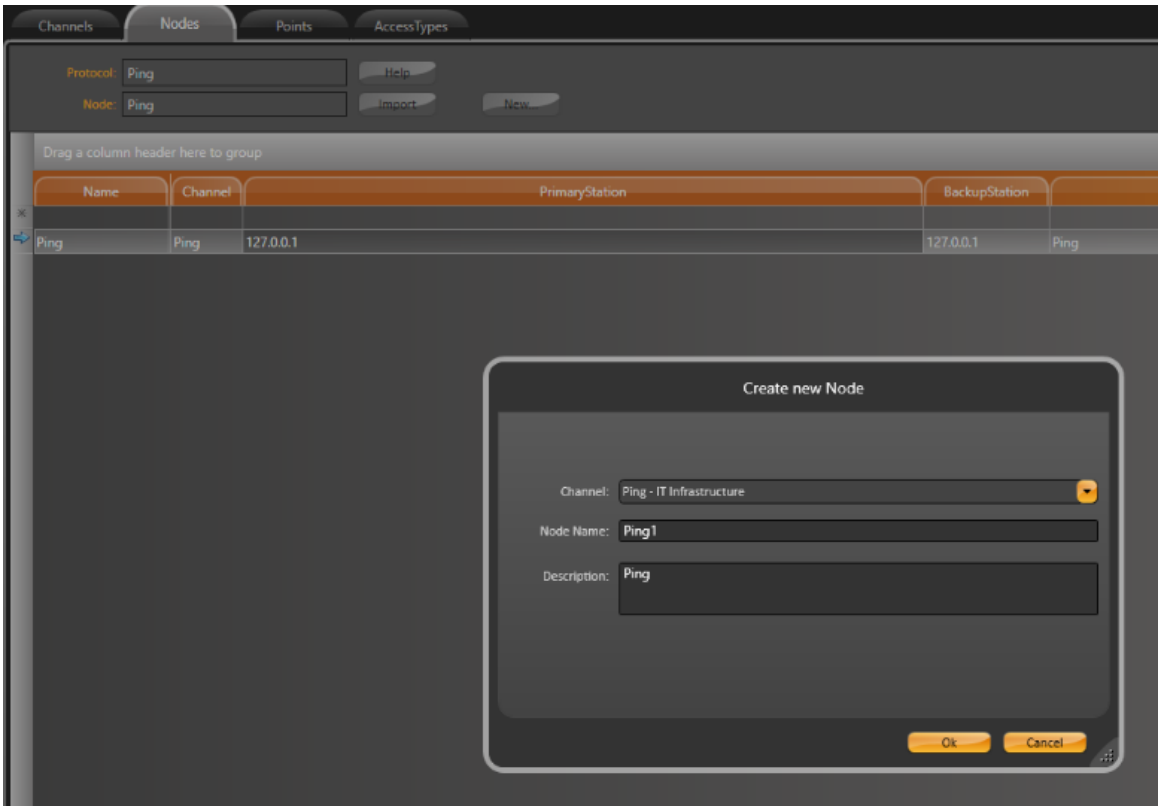
Configure the Ping Driver

To set up the Ping driver to run at a specified frequency such as every 10 seconds or every 30 seconds, please follow these steps:

- On **Devices / Channels**, create a new Channel using the “**Ping for IT Infrastructure**” protocol:



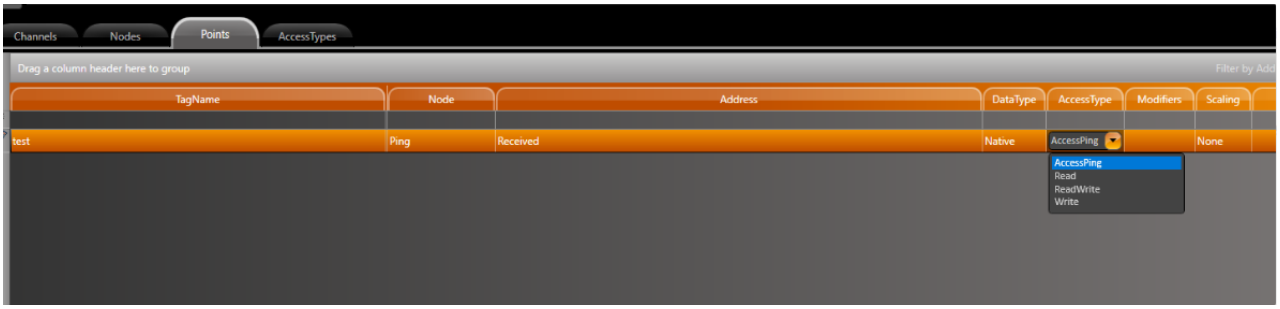
- On **Devices / Nodes**, create a new Node and set the Ping channel you created:



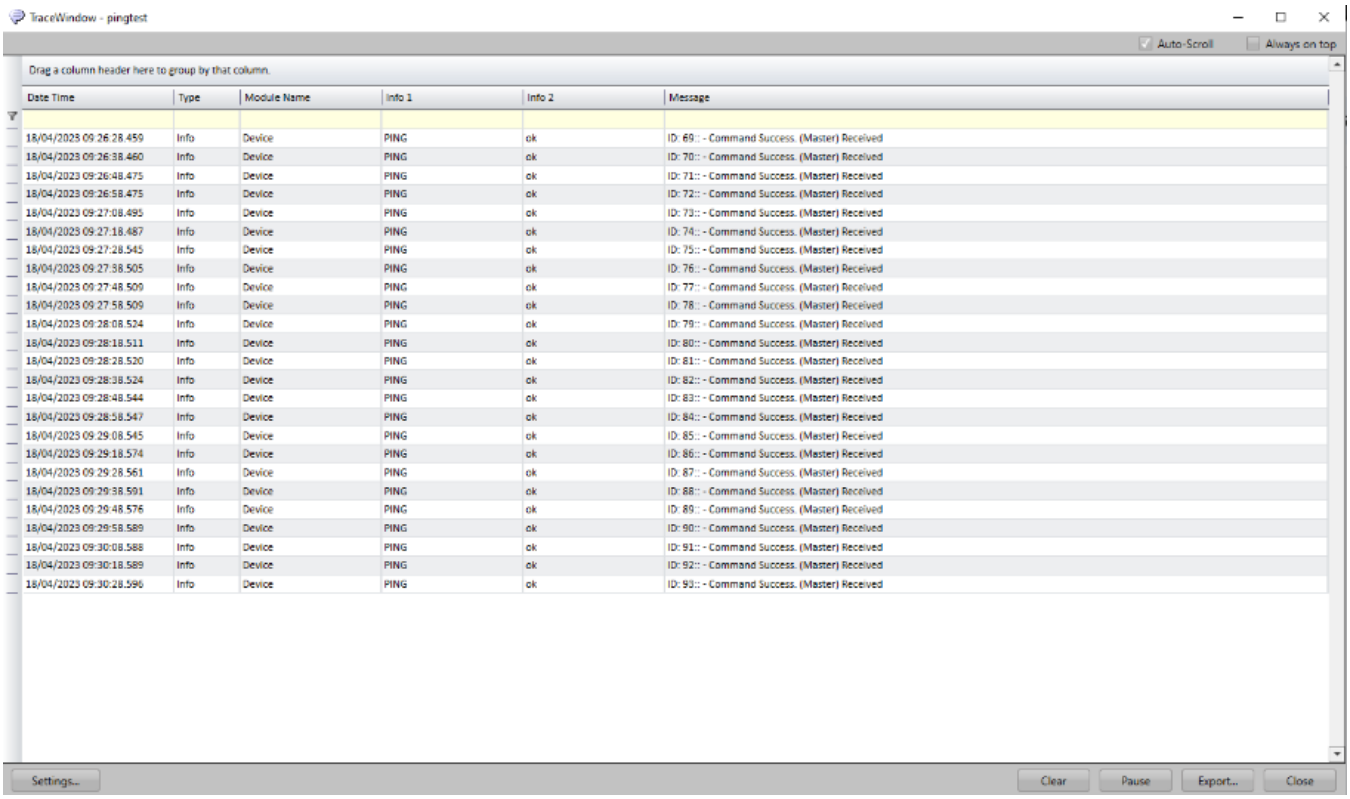
- On **Devices / AccessTypes**, create a new AccessType and fill in the 'PollingRate' field with the desired frequency.



- Go to **Devices / Points** and create or edit points with the AccessType you just created.



Once you've completed these steps, the ping results will be displayed in the TraceWindow at the specified frequency. See below an example configured to ping every 10 seconds:



Supported Operands:

Operand	Read	Write	Data Type	Address size
AverageTime	**Yes**	-	Real	8 bytes
Lost	**Yes**	-	Integer	4 bytes
Received	**Yes**	-	Integer	4 bytes
MinimumTime	**Yes**	-	Long	8 bytes
MaximumTime	**Yes**	-	Long	8 bytes

Channels Configuration

Protocol Options

- **Maximum size of blocks:** Defines package size that will be sent.

Settings

- **Number of Retries:** Defines how many times the package will be sent. When it is zero, the driver uses 4 retries as default.

TimeOut

- **TimeOut RxStart:** Defines how long the driver will wait for a response in milliseconds.

Nodes Configuration

Station Configuration

TCP/IP:

Station syntax: ***<IP address>***

Where :

- ***<IP address>***: IP address in the network that will be checked for the Ping driver.

E.g.: ***192.168.1.1***

Points Configuration

The syntax for the Ping address points is: <*Property*>.

Where <*Property*> can be:

Property	Description
AverageTime	Average response time (ms) of last execution
Lost	Number of lost packages in last execution
Received	Number of received packages in last execution
MinimumTime	Minimum response time of last execution
MaximumTime	Maximum response time of last execution

Troubleshoot

Possible error codes	
Error Code	**Description**
-1	The ICMP echo request failed due to an unknown reason.
1102	The ICMP echo request failed because the network that contains the destination computer is not reachable.
1103	The ICMP echo request failed because the destination computer is not reachable.
1104	The ICMP echo request failed because the destination computer that is specified in an ICMP echo message is not reachable, because it does not support the packet's protocol.
1105	The ICMP echo request failed because the port on the destination computer is not available.
1106	The ICMP echo request failed due to insufficient network resources.
1107	The ICMP echo request failed because it contains an invalid option.
1108	The ICMP echo request failed due to a hardware error.
1109	The ICMP echo request failed because the packet containing the request is larger than the maximum transmission unit (MTU) of a node (router or gateway) located between the source and destination. The MTU defines the maximum size of a transmittable packet.
11010	The ICMP echo Reply was not received within the allotted time. The default time allowed for replies is 1 second. You can change this value using the channel configuration.
11012	The ICMP echo request failed because there is no valid route between the source and destination computers.
11013	The ICMP echo request failed because its Time to Live (TTL) value reached zero, causing the forwarding node (router or gateway) to discard the packet.
11014	The ICMP echo request failed because the packet was divided into fragments for transmission and all fragments were not received within the time allotted for reassembly. RFC 2460 (available at www.ietf.org) specifies 60 seconds as the time limit within which all packet fragments must be received.
11015	The ICMP echo request failed because a node (router or gateway) encountered problems while processing the packet header. This is the status if, for example, the header contains invalid field data or an unrecognized option.
11016	The ICMP echo request failed because the packet was discarded. This occurs when the source computer's output queue has insufficient storage space, or when packets arrive at the destination too quickly to be processed.

11018	The ICMP echo request failed because the destination IP address cannot receive ICMP echo requests or should never appear in the destination address field of any IP datagram. For example, specifying the IP address "000.0.0.0" in node configuration returns this error.
11040	The ICMP echo request failed because the destination computer that is specified in an ICMP echo message is not reachable; the exact cause of the problem is unknown.
11041	The ICMP echo request failed because its Time to Live (TTL) value reached zero, causing the forwarding node (router or gateway) to discard the packet
11042	The ICMP echo request failed because the header is invalid.
11043	The ICMP echo request failed because the Next Header field does not contain a recognized value. The Next Header field indicates the extension header type (if present) or the protocol above the IP layer, for example, TCP or UDP.
11044	The ICMP echo request failed due to an ICMP protocol error.
11045	The ICMP echo request failed because the source address and destination address that are specified in an ICMP echo message are not in the same scope. This is usually caused by a router forwarding a packet using an interface that is outside the scope of the source address. Address scopes (link-local, site-local, and global scope) determine where on the network an address is valid.

Driver Revision History

Ping Revision History	
Version	**Notes**
1.2.0.0	Initial release on new documentation standards.

In this section...