

Ping – IT Infrastructure

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

Summary Information

Communication Driver Name: Ping

Current Version: 1.0.0.0

Implementation DLL: T.ProtocolDriver.Ping.dll

Interface: TCP/IP

Max number of nodes: User defined

PC Hardware requirements: Standard PC Ethernet interface board

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

Channel Configuration

Protocol Options

Maximum size of blocks: Defines the size of the package that will be sent

Settings

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

TimeOut

TimeOut RxStart: Defines how long the driver will wait for a response (in milliseconds)

Node Configuration

Station Configuration

TCP/IP:

- Station syntax: <IP address>
- Where:
 - **<IP address>** = The IP address that will be checked by the Ping driver

Ex: 192.168.1.1

Point Configuration

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

Where:

- **AverageTime** = Average response time (ms) of the last execution
- **Lost** = Number of lost packages in the last execution
- **Received** = Number of received packages in the last execution
- **MinimumTime** = Minimum response time of the last execution
- **MaximumTime** = Maximum response time of the last execution

Troubleshoot

The status of the driver's execution can be observed through the diagnostic tools, which are:

- Trace window
- Property Watch
- Module Information

The above tools indicate if the operations have succeeded or have failed. A status of 0 (zero) means communication is successful. The possible error codes are in the table below:

Error Code	Description
-1	The ICMP echo request failed for 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 because of insufficient network resources
1107	The ICMP echo request failed because it contains an invalid option
1108	The ICMP echo request failed because of 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 the 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 the destination computer
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 of the 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 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 because of an ICMP protocol error
11045	The ICMP echo request failed because the source address and the destination address that are specified in an ICMP echo message are not in the same scope. This is typically 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