IP WATCHDOG IEEE 802.3 ,RJ45

Power outlet with automatic or manual control

(c) 2007 Mikrovlny s.r.o.

Description

IP WATCHDOG is designed for automatic watching and restart devices connected to power outlet. Output outlet can be manually switched to ON/OFF.

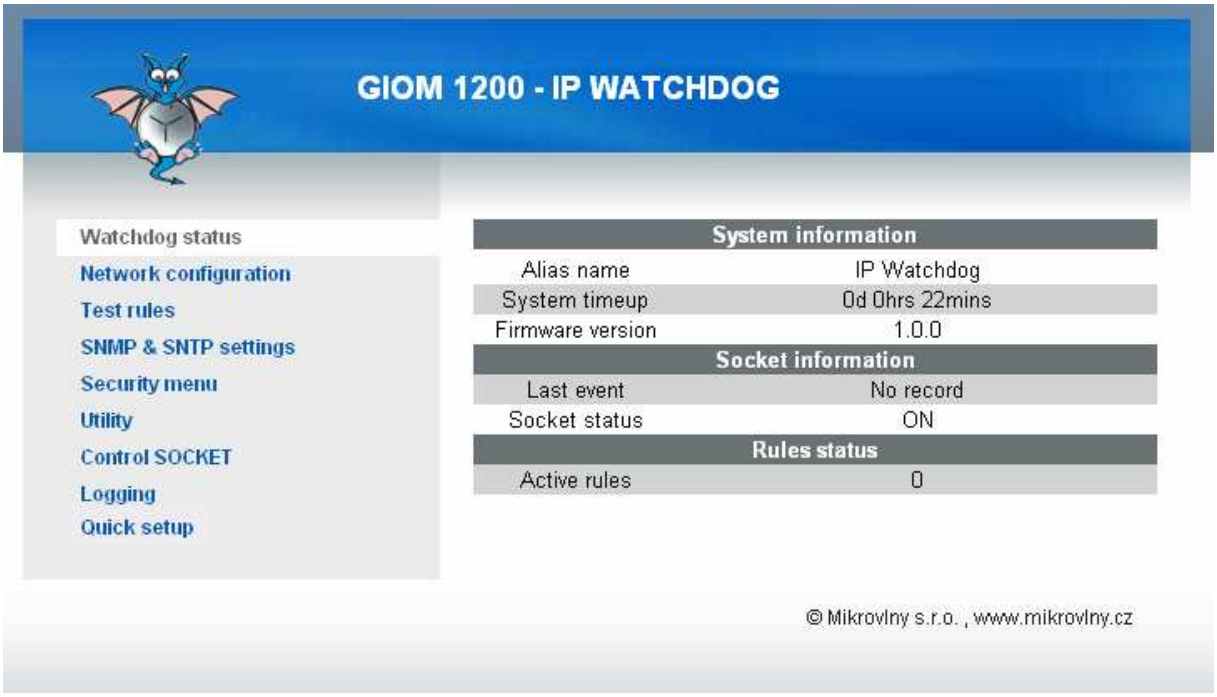
IP Watchdog is equipped by one Ethernet interface for settings by HTTP protocol.

Output outlet is 230V with max. power load 16A.

Configuration

- Connect IP Watchdog to 230VAC
- Connect PC Ethernet to IP Watchdog's RJ45 connector.
- Set PC network interface to IP address to 192.168.0.11, mask 255.255.255.0
- Default IP address for IP Watchdog is 192.168.0.100
- Enter 192.168.0.100 IP address to your Web browser

IP Watchdog's settings table appears like on figure bellow.



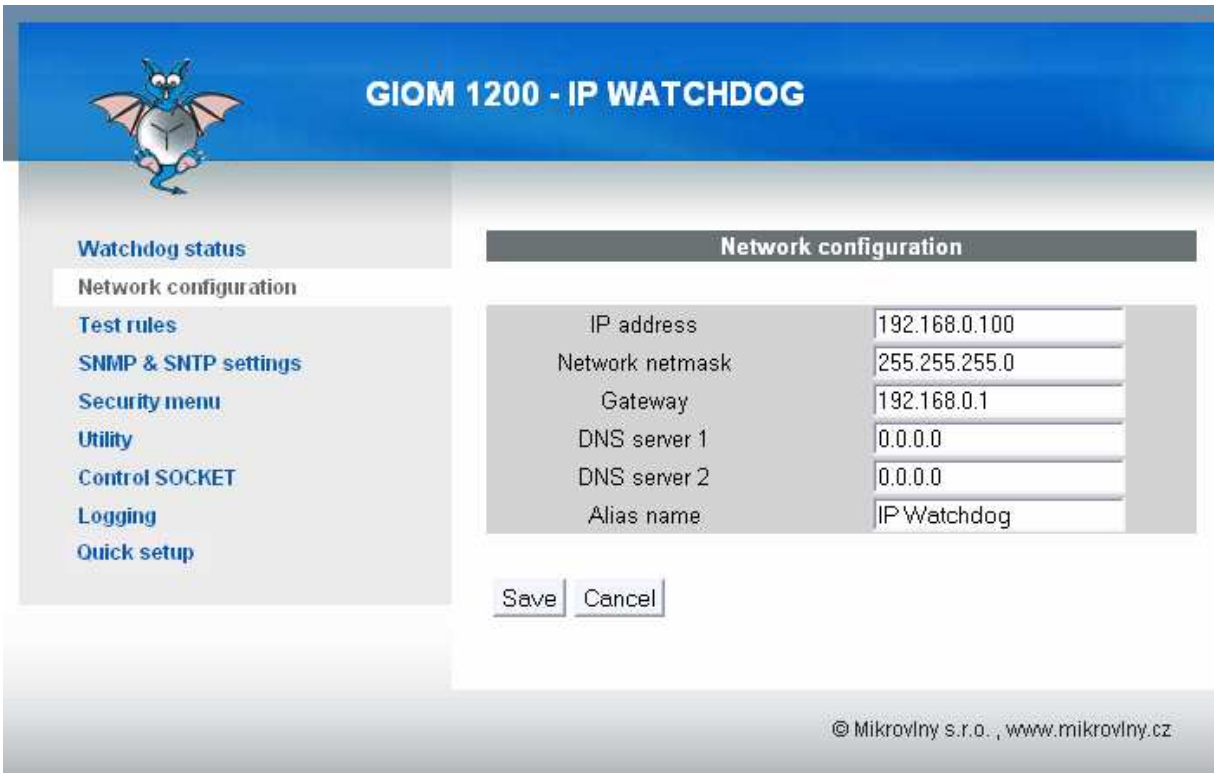
System information – current system status
Alias name - Network alias.
System time up – time from last restart
Firmware version - current firmware version.

Socket information – power outlet status
Last event - date/time of last output change.
Socket status – ON/OFF

Rules status – Testing rules. For automatic testing you need configure this rules, see chapter Test Rules

Right column contain all configure menus:

MENU - Network configuration



Contain information about remote control, there is **IP address, Mask and Gateway** from which can be IP Watchdog configured.

DNS server 1 and 2 is used only for translation domain names for Test rules section. At least one server must be working if you want to use domain names in Test Rules section.

Alias name - network name, you can use any name with maximum length 15 characters.

MENU – Test rules

In this menu you can set rules for automatic testing connected devices by theirs IP address or domain name. Up to 5 devices can be tested, 3 by IP address (**configure rule 1 to 3**) and 2 by domain name (**configure rule 4,5**).

Interval for send test packet - time interval for packet sending, range 2 – 20 minutes.
Interval for next test - time interval for next test starting, only if event was issued in last test. After this interval is next test started – range 2 – 30 minutes.
Inaccessibility maximum reboot - Count of connected device's restarts in case permanent nonavailability of device – range 1-10 restart tries.

Reboot SOCKET hold time - time period when the output outlet is in "reset" state (ON or OFF due settings) 1 – 60 sec.
Number of packets for evaluate - count of testing packets for losses - range 10 – 100 packets.
Rules evaluation - AND –outlet is OFF/ON/Reset if the losses exceed in all rules, **OR –** outlet is reset if at least one rule is fulfilled.
Send SNMP TRAP before socket action - Before ON/OFF/Reset is SNMP TRAP packet sent on entered IP address (SNMP MENU).
SNMP cancel SOCKET ACTION - Waiting SNMP for command to cancel current action.
SNMP timeout for CANCEL - If there is no cancel command in selected time, RESET is not executed. Range 1 to 60 (-1 -> wait for next test)

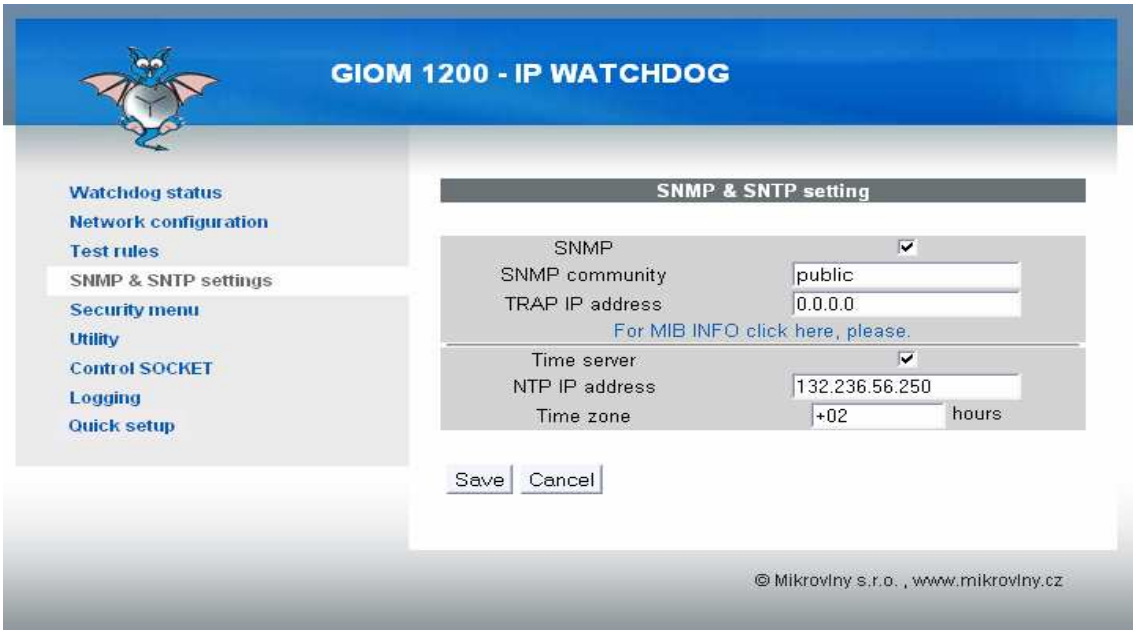
Submenu Configure rule 1,2,3 - Test packet settings

Rule 1 enable - First rule enabled.
Destination IP address - Tested IP address.
Ping data – test packet length - range 32 to 1460 Bytes.
Packet loss - max. losses in %.

Submenu Configure rule 4,5 - Test packet settings

Rule 4 enable **-** Fourth rule enabled/disabled.
Domain name **-** domain name for tested device, at least one DNS server must be working. See **Network configuration** menu.
Ping data – test packet length, range 32 to 1460 Bytes.
Packet loss **-** max. losses in %.

MENU – SNMP and SNTP setting



SNMP - Enable SNMP protocol
SNMP community - password for SNMP protocol
TRAP IP address - Destination IP address for SNMP TRAP packet about success rules evaluation.

Time server - Enable NTP server for time settings
NTP IP address - IP address of NTP server
Time zone - can entered in positive or negative hour shift. This time is issued in log entries.

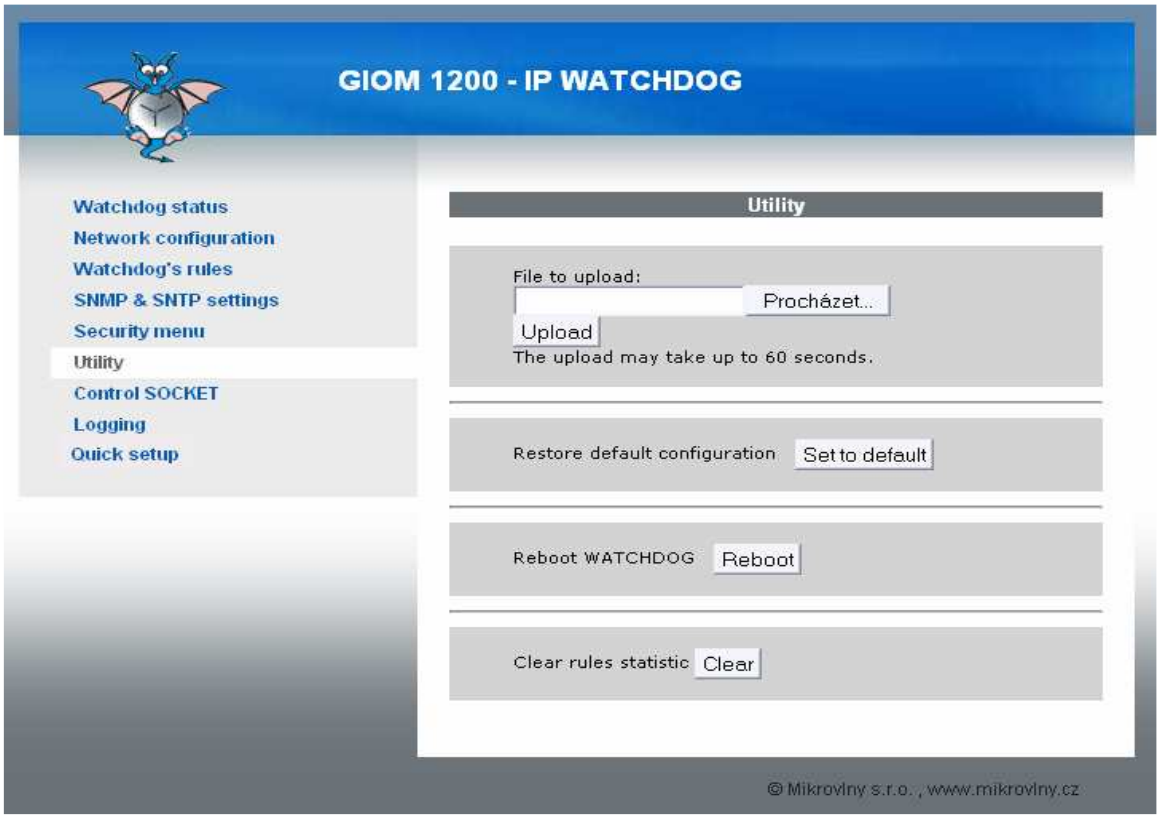
If you click to ***MIB info*** link, you get information about MIB for SNMP configuration.

SECURITY MENU

Note: In default configuration is password and user name blank. If you enter new password, IP Watchdog ask you to verify old password, please enter blank name and password.

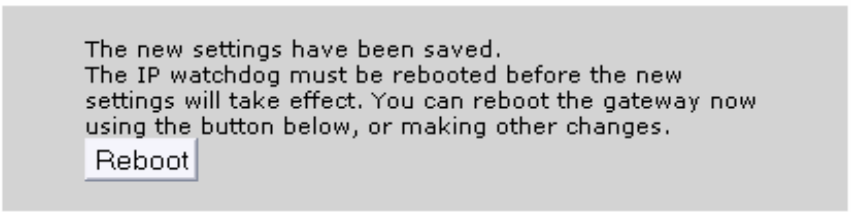
HTTP port - Port for configuration, default 80

MENU - Utility



Firmware upload
Select new firmware file by click to **procházet** button and press **Upload** button. After success firmware update is shown this message:

If you click to **Set to default** button, IP WATCHDOG rewrites all values by factory settings.

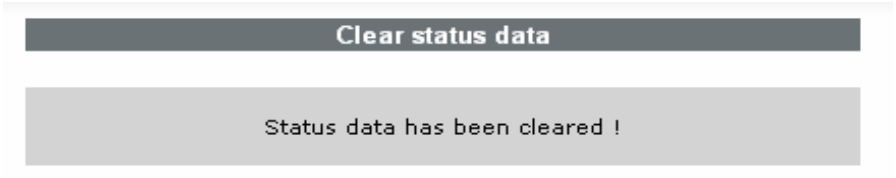


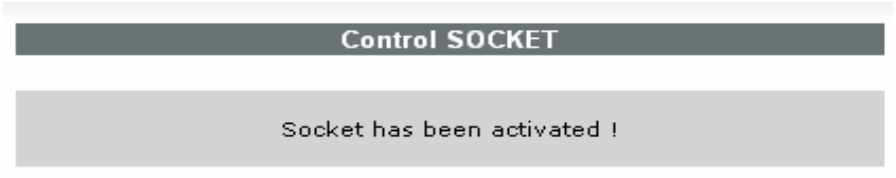
Clear rules statistic - all packet counters are reset in **Watchdog status** – if the rules are defined.

VOLBA - CONTROL SOCKET

Clear EVENTS DATA - Erase events log**.**
RESET socket - Reset connected device (turn OFF and ON output outlet) in dependency of **Test rules.**
TURN ON socket – Permanently turn ON output socket.
TURN OFF socket - Permanently turn OFF output socket.
TURN ON socket for time- Temporary turn ON socket for X minutes.
TURN OFF socket for time- Temporary turn OFF socket for X minutes.

After success you can see this message:





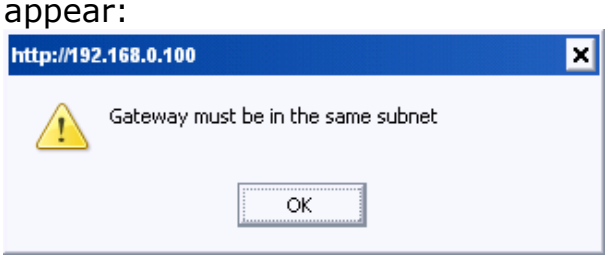
MENU - LOGGING

All actions which has influence to output outlet are logged. If the NTP server is properly configured, time is attached to log. Actions executed from **Control SOCKET** are logged too. Device can store up to 20 actions, last one is erased after limit exceed.

MENU - Quick setup

This configuration menu is intended for fast and easy settings. It is minimal configuration for automatic watching. In **Test rule** choice can be selected IP addresses or domain names.

If you enter wrong Gateway address and press save button, message box appear:



Other dependencies are checked by the same way.

For manual outlet control use menu **Control SOCKET.**

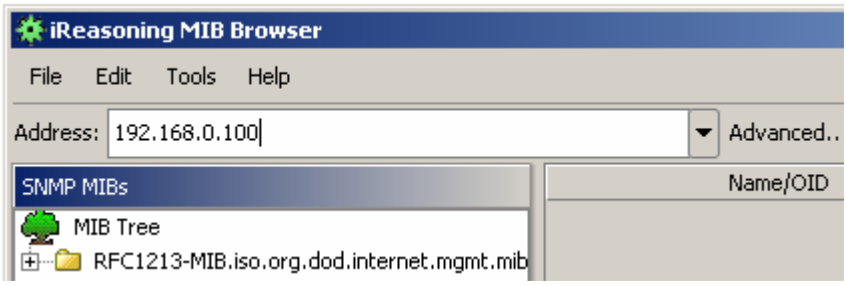
Control by SNMP protocol

Main advantage is that SNMP protocol is supported by many operating systems and small data amount need to execute SNMP command. SNMP protocol is enabled in default settings. On figures us IP Watchdog with 2 x RJ45, but other models can be configured by the same way.

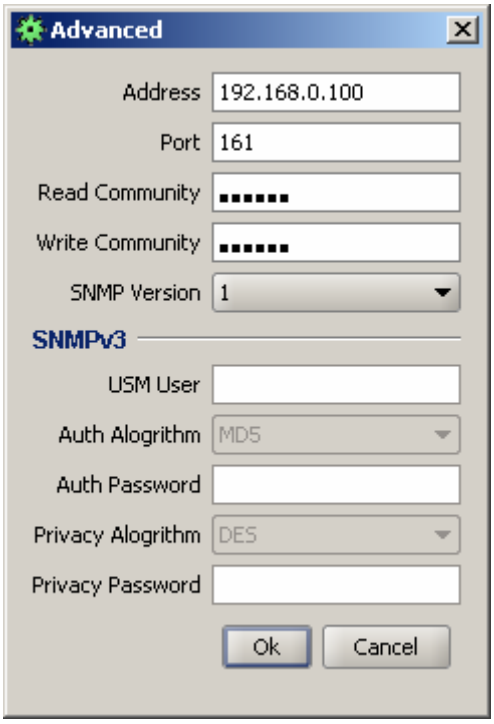
Using under MS Windows

You have to install SNMP browser - PRTG or MIB browser by IREASONING. Both programs are free and you can download them from our homepage - www.mikrovlny.cz in software section.

After success install execute the SNMP browser

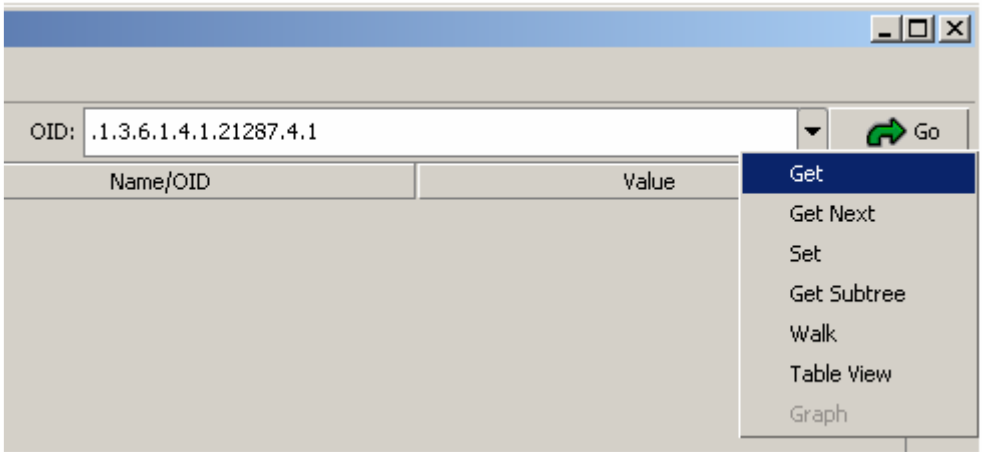


In the **address** field enter IP address of IP Watchdog and press **Advanced**



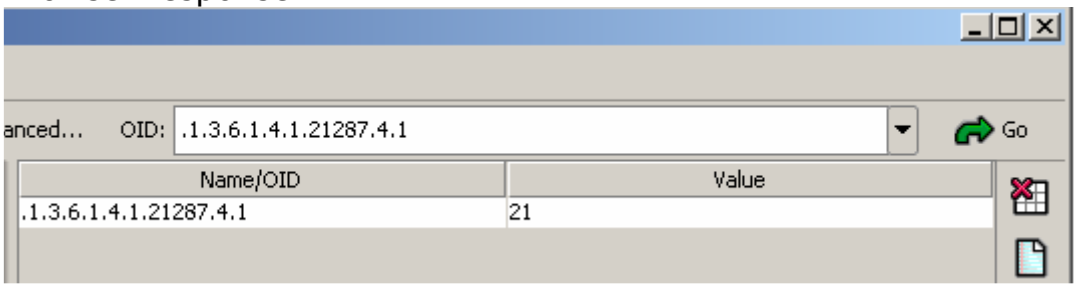
Enter values like on above figure. Read and Write Community password is public, which is default in IP Watchdog's SMNP configuration.

GET command example:



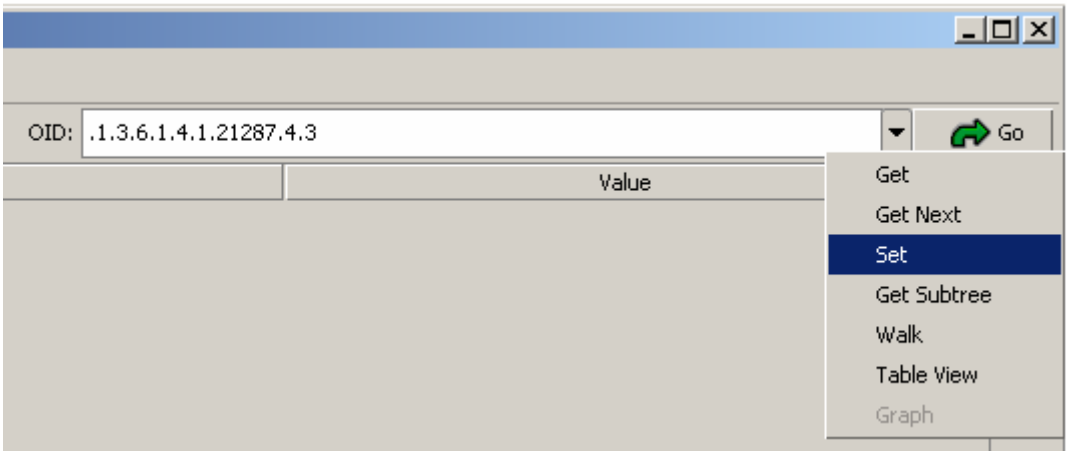
Into OID window enter OID (Object Identifiers) tree. Each OID for selected commands you can get from MIB INFO link from **SNMP & SNTP** menu.

Browser response:



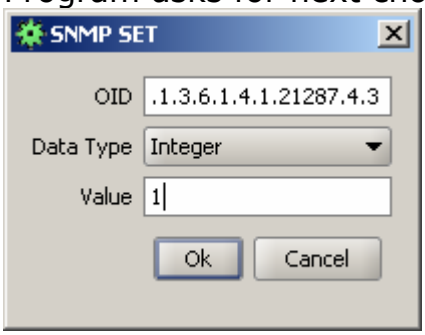
Value **Events** is 21, it means that there was 21 restarts (manual restarts are included too).

Example for write/SET command:

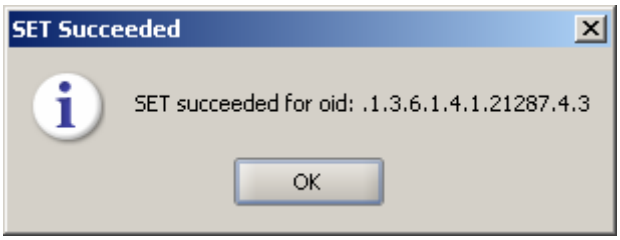


Enter tree for outlet control and choose **Set** option.

Program asks for next choice:



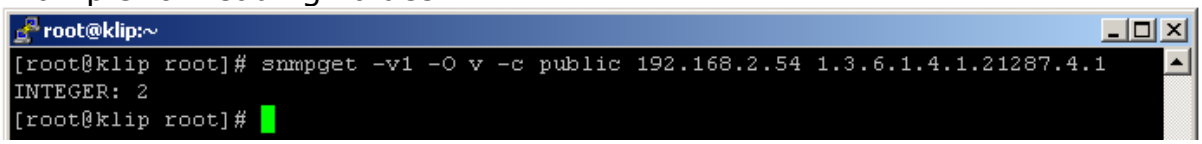
You choose variable type, in IP Watchdog the type is always integer. After OK click, outlet is switched and watched device is restarted for period which is entered in **Time intervals -** default is 3 seconds. If succeed, message on bellow figure appears else timeout.



Using under Linux or Unix-like OS

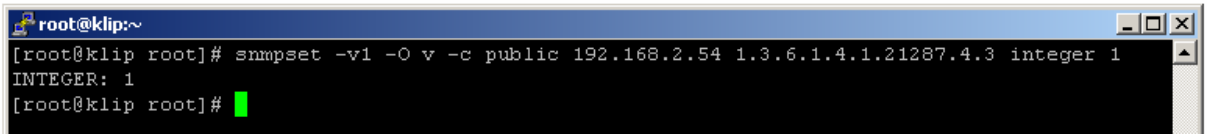
In Linux system is SNMP protocol installed by default. You can use **snmpget and snmpset** commands**.**

Example for reading values:



Return **Events** - 2 or timeout.

Write example:



We restarted watched device. In error case is timeout returned.

LED indicators

On IP Watchdog's front panel are 3 indicators.

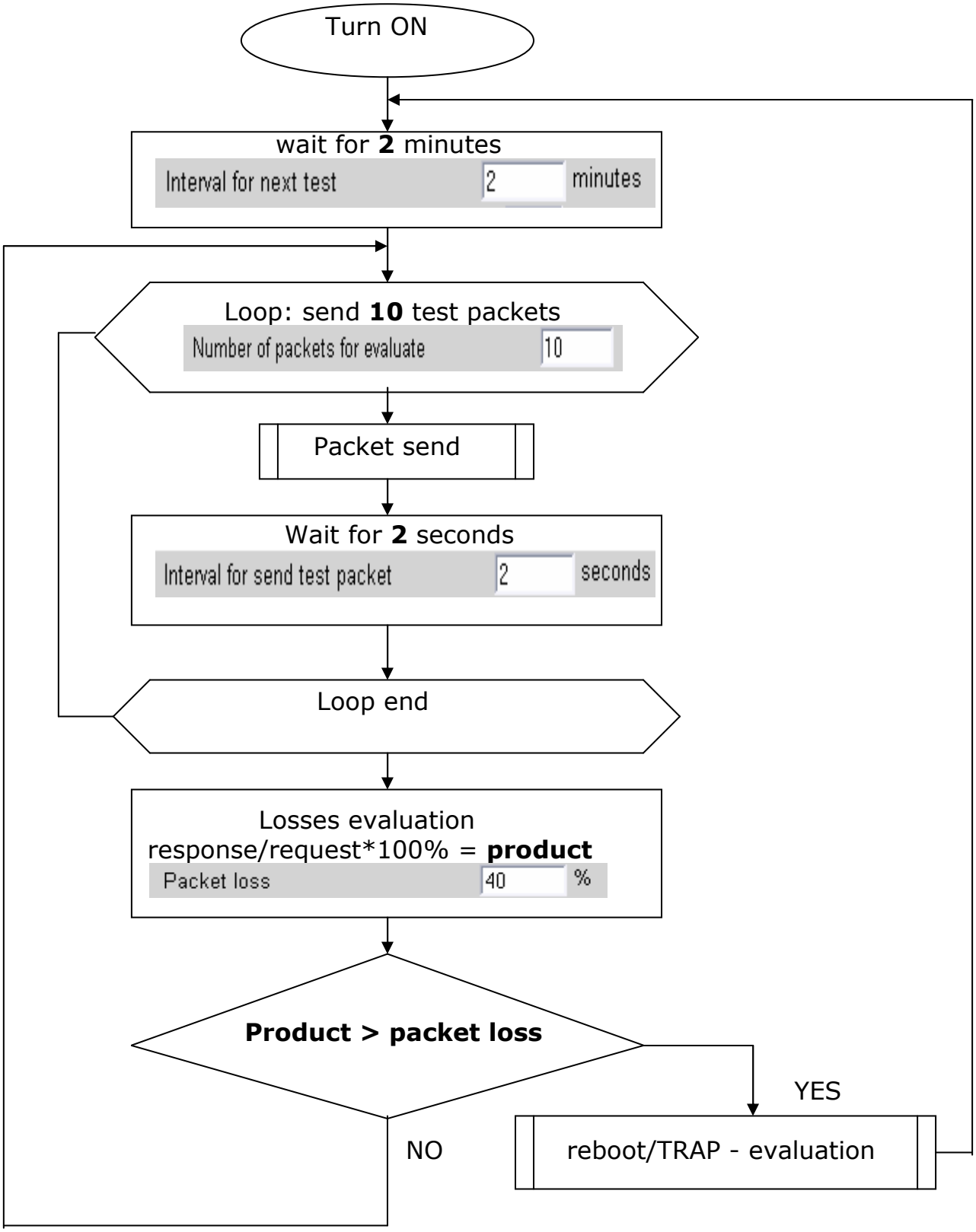
1xRED - signalized power supply – flash each half sec in proper function
1xGREEN - continuous light indicated network connection (LINK) RJ45, flashing indicate RX-TX data flow.
1xYELLOW - Light=outlet is ON, DARK=OFF

Manual reset and factory settings.

Press default button on IP Watchdog's side. After pressing indicators start flashing for 10 seconds. If you press this button by 2 times in indicators flashing time, IP Watchdog read factory settings.

Main loop of IP Watchdog device test
All values can be found in TEST RULES menu

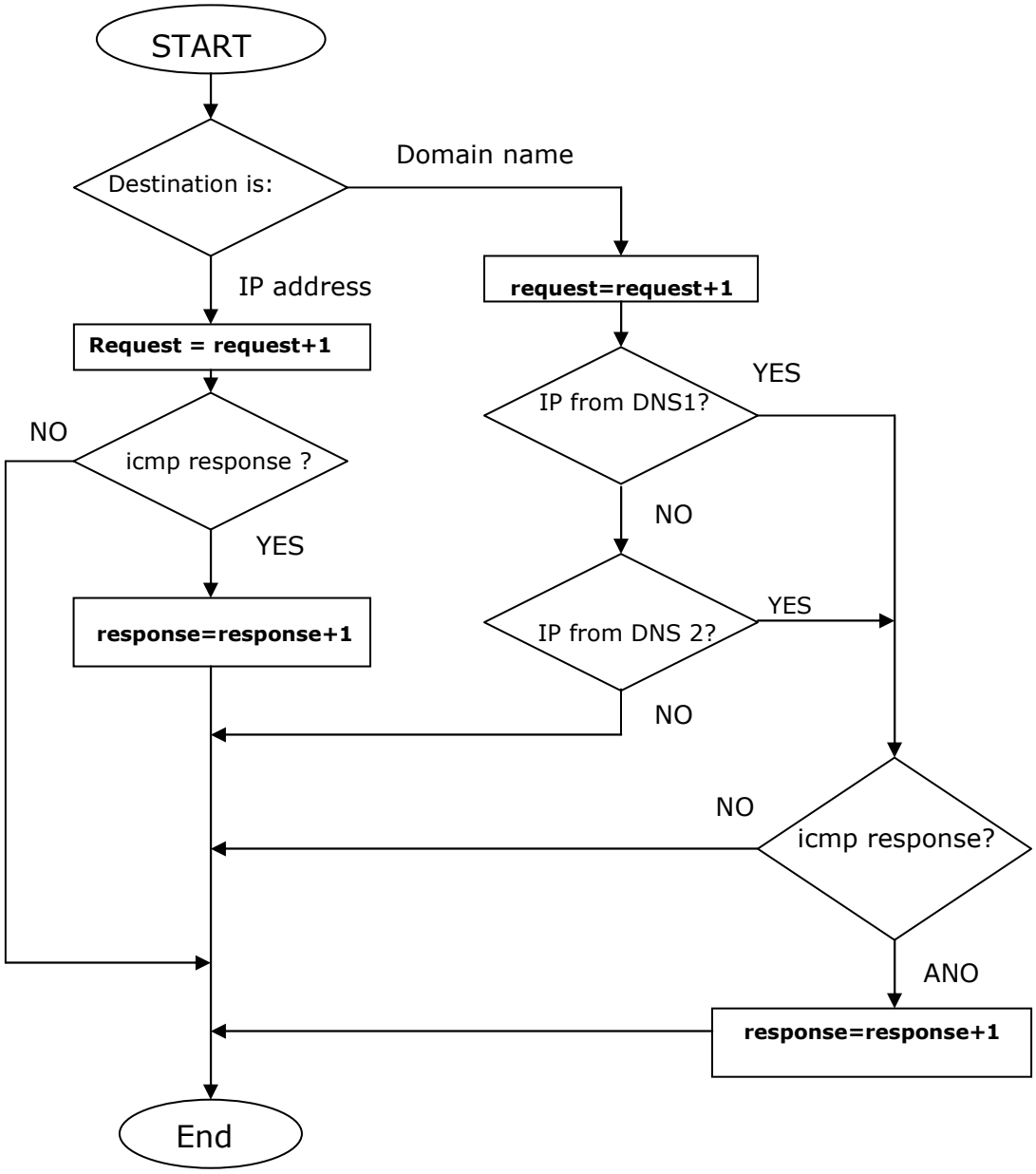
Variable **request** are test packets sent to tested device.
Variable **responses** are answers received from tested device.



Subroutine : **PACKET SEND**

This program sends DNS or ICMP packets with defined length.

Ping data (bytes)	32



Subroutine: **reboot/TRAP evaluation**

Subroutine depend on evaluation of packet loss send SNMP TRAP packet and wait for cancel or restart connected device to output outlet.