

**Configuration Manual**

Teleport-01 Teleport-02

Integration unit /

dry contacts transfer

Manual Version 6

Firmware Version 1.6

© Fort-Telecom, Perm 2019

Table of contents

[Designations 3](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250074)

Safety instructions……………………………………………………………………………………………………….4

1. [Designation 5](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250073)

1.1 Application options………………………………………………………………………………………………..5

1. [Technical characteristics 10](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250072)
2. [Description 13](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250071)
3. [Mounting and connection 15](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250070)
4. [Configuration 19](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250069)
   1. [Management interfaces 19](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250068)
   2. [What you need to know before connection 19](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250067)
   3. [Management via web interface 20](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250066)
      1. [First connection, quick start 20](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250065)
      2. [Network settings 26](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250064)
      3. [Configuring user accounts 27](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250063)
      4. [Device description 28](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250062)
      5. [Telnet configuration 28](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250061)
      6. [SNTP configuration 30](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250060)
      7. [Web interface language setting 31](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250059)
      8. [Transfer mode configuration 32](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250058)
      9. [Configuring RS-485 port 34](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250056)
      10. [Configuring digital inputs 36](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250054)
      11. [Configuring digital outputs 37](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250053)
      12. [Configuring Modbus 39](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250052)
      13. I/O network controller mode configuration……………………………………………………………39
      14. [Configuring the event list 41](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250051)
      15. [Configuring Syslog 42](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250050)
          1. [Syslog message list 45](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250049)
      16. [Configuring SMTP 46](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250048)
          1. [Example of configuration with a dedicated mail server on the local network 47](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250047)

[5.3.16.2. Example of configuration with an external mail server 52](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250046)

* + 1. [Configuring SNMP 54](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250045)
       1. [Configuring SNMP v1 54](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250044)
       2. [Configuring SNMP v3 55](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250043)
    2. [Remote Ping function 56](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250042)
    3. [Statistics 5](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250041)7
       1. [Summary information 57](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250040)

[5.3.19.2 ARP table 58](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250039)

* + - 1. [DNS table 58](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250038)
      2. System log…………………………………………………………………………………………59

5.3.20 [Firmware update 59](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250036)

5.3.21 [Saving and restoring settings 61](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250035)

[5.3.21.1 Saving settings to a file 61](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250034)

[5.3.21.2. Restoring settings from a file 62](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250033)

[5.3.21.3 Editing configuration file 62](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250032)

* + 1. Resetting to factory settings [66](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250031)

5.3.23 [Reboot 66](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250030)

* 1. [Management via Telnet 67](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250029)
     1. [Configuration example 69](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250028)
     2. [Description of Telnet commands 70](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250027)
     3. [config group 71](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250026)
        1. [network settings (config ipif) 71](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250025)
        2. [Configuring SNMP 72](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250024)
        3. [Configuring Syslog](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250023) 73
        4. [Configuring SNTP 73](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250022)
        5. [Configuring TFTP 73](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250021)
        6. [Configuring events](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250020) 74
        7. [Configuring user accounts 74](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250019)
        8. Configuring device description…………………………………………………………………….75
        9. [Configuring inputs 75](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250018)
        10. [Configuring outputs 76](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250017)
        11. [Configuring RS485 77](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250016)
        12. [Configuring Modbus 78](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250015)
        13. [Setting the list of remote devices 79](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250014)
     4. [Show group 80](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250013)
        1. [Viewing summary information 81](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250012)
        2. Viewing [Teleport integration unit settings 82](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250011)
     5. Firmware update using [TFTP](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250010) 86
     6. [Saving and loading configuration and log via TFTP 88](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250009)
        1. [Saving configuration 88](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250008)
        2. [Restoring configuration 88](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250007)
        3. [Saving system log 89](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250006)
     7. [Saving settings 89](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250005)
     8. [Reboot 89](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250004)
     9. Exiting the management mode [89](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250003)
     10. [Diagnostic functions 90](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250002)
         1. [Ping utility 90](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250001)

1. Troubleshooting………………………………………………………………………………………………………91
2. Warranty………………………………………………………………………………………………………………92
3. [Technical support 93](file:///C:\Users\BRAUN\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\ODORKYIM\Teleport%2012%20v1%20руководство%20по%20настройке(en).docx#_TOC_250000)

Designations

The following designations are used in this manual:

|  |  |
| --- | --- |
| **Designation** | **Meaning** |
|  | WARNING sign |
| *Basic Settings → Network Settings* | When describing configuration process via the web interface, italics are used to show the path to the web page |
| **DEFAULT** | Bold type is used to highlight important parameters, values, button names, etc. |
| #IPADDRESS=[192.168.0.1] | Courier New font is used to highlight parameters in the settings file |
| <VALUE> | Angle brackets are replaced with the variable value in the console command |
| ***config syslog state <STATE>*** | The console command is in bold and italics |
| *config syslog state enable* | The output of control commands is italicized |

Safety instructions

This safety manual describes regulations of TFortis equipment operations.

To reduce the risk of physical harm, electric shock and burns to people, as well as damage to equipment, the following precautions must be observed:

• Follow the labeling instructions carefully.

• Do not service the device without documentation for it.

• Only a trained service technician can service the internal components of the device.

• If any of the following cases occurs, you must unplug the device, replace a failed module or contact service department:

- Power cable, extension cord or plug damage.

- A foreign object got inside the device.

- The device has been exposed to water.

- Damaged or dropped device.

- The device does not work correctly when operating manuals are strictly followed.

• Keep the device away from radiators and heat sources, and avoid blocking ventilation openings designed for cooling.

• Do not spill food or liquids on system components and never operate the device in a humid environment. If the system has been exposed to moisture, it is necessary to contact the specialists of the service department.

• Do not place objects in the openings of the system. This may result in a fire or electric shock due to the short circuit of the internal components of the system.

• Use this device only with certified equipment.

• Before removing the enclosure of the device or touching its internal components, you must turn off the power and allow the device enough cooling time.

• Do not use the device with power sources which specifications are different from those indicated on the label with electrical parameters.

• Ensure that the power specifications of the connected devices are in accordance with the local regulations.

• Use only suitable power cables. Power cable must comply with the voltage and current characteristics required for this device.

• The voltage and current characteristics of the cable must be greater than the power indicated on the device.

• To avoid electric shock use properly grounded electrical outlets and cables when operating the device.

• Follow the specifications for the extension cable and power bus. Make sure that the total rated current of all devices connected to the extension cable or power bus does not exceed the limit of 80% of the rated current of the extension cable or power bus.

• Use a voltage limiter, line driver or uninterruptible power supply (UPS) to protect the system from sudden short-term power surges.

1. Designation

TFortis integration units are designed to connect TFortis PSW switches to security systems. Integration units have discrete inputs and relay outputs, RS-485 and Ethernet ports.

Teleport integration units perform the following functions:

* Transfer RS-485 over Ethernet
* RS-485 to Ethernet conversion
* Broadcast dry contacts over Ethernet
* Transmitting of alarm events from PSW switches
* Remote control of automation
  1. **Application options**

1. **Transfer RS-485 over Ethernet**
   1. **Integration of video surveillance and perimeter security systems**

Two devices: Teleport-1 and Teleport-2 allow you to organize “Virtual channel” RS-485 over Ethernet. At the same time, the ready-made transport infrastructure is used and there are no restrictions on the length of the RS-485 line. Thus, in the presence of an existing video surveillance system, you can very easily deploy perimeter security system. The Teleport-2 unit, in addition to the RS-485 port, allows you to supply power to the detectors, while at the same time it is powered by the same cable that connects to the switch (PoE) .

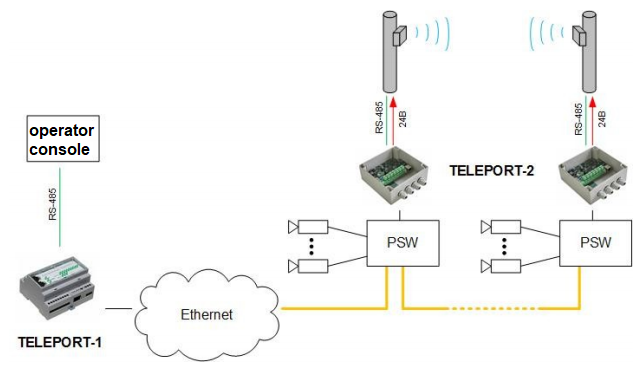


Fig 1.1 Application for perimeter security systems

**1.2 Remote control of devices with RS-485 interface**

Similar to the application with perimeter security systems, you can use the RS-485 broadcast over Ethernet to control actuators, for example, a servo drive for some PTZ cameras that are located at a considerable distance from the server.

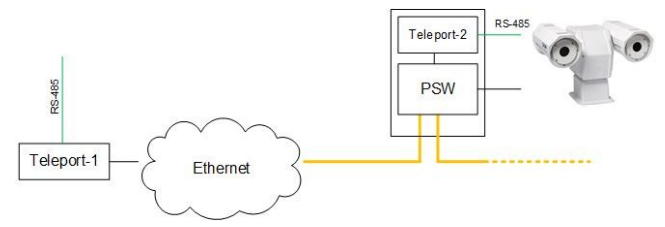


Fig. 1.2 Application for control of devices with RS-485 interface

**1.3 Electricity monitoring**

For remote reading of indications of energy consumption at the facility, you can use meters with RS-485 interface.

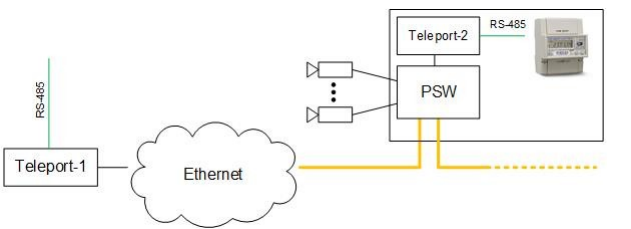


Fig. 1.3 Application in the monitoring of electricity meters

**1.4 Converting RS-485 to Ethernet**

There is another option to connect detectors working via RS-485 to the server. In the Teleport integration units, an Ethernet frame is formed that contains data from the RS-485 port. Reverse decompression can be performed on another integration unit, or in upper layer application. (as shown in Fig. 1.4)

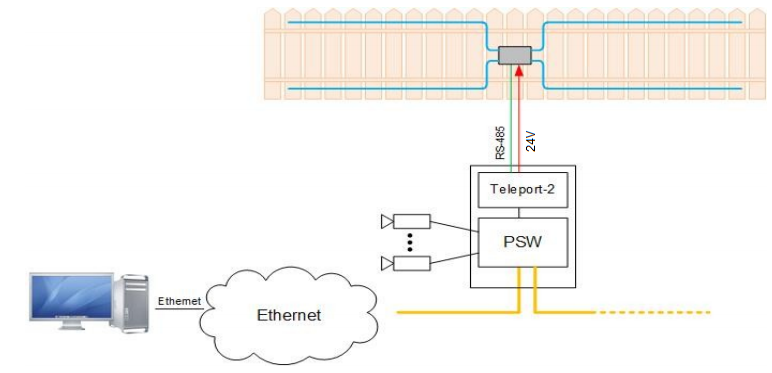
****

Fig. 1.4 Converting RS-485 to Ethernet

In addition, the TFortis Administrator program is developed, which runs on a server and translates data into a virtual COM port. The connection of the program for detectors monitoring is made to this port.

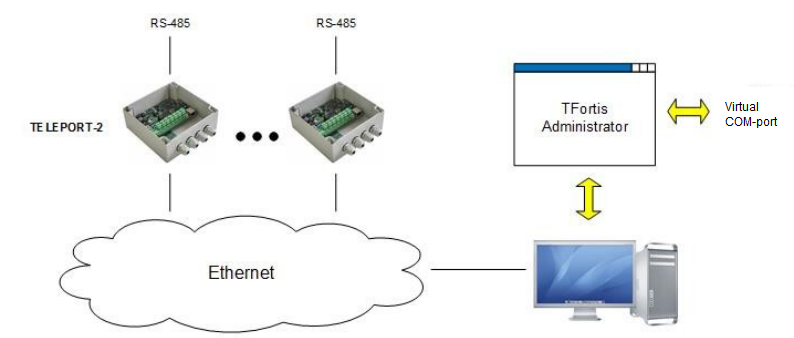


Fig. 1.5 Converting RS-485 to Ethernet

1. **Transfer of Dry contacts**
   1. **Control of unauthorized access to cabinets**

TFortis PSW switches have discrete inputs to which you can connect any sensors such as "dry contact", for example, reed switches, limit switches, to organize control of opening the cabinets. The signal of opening is transmitted by the switch to the integration unit. Thus, when the input is triggered on the switch, the corresponding output on the Integration Unit is triggered.

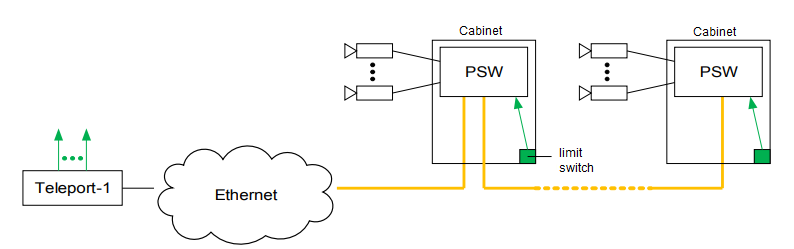
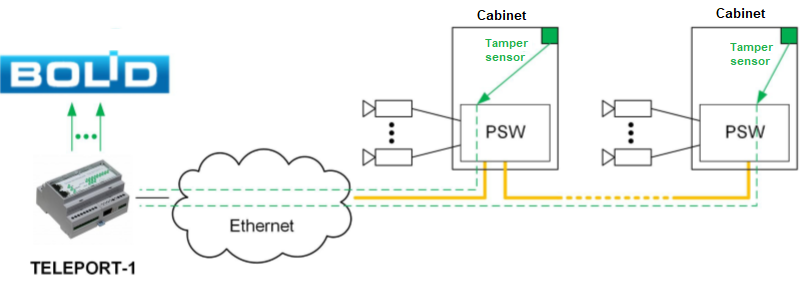


Fig. 1.6 Cabinets opening control

**

*Figure 1.7 Transmission of alarm signals from TFortis PSW switches to Orion integrated security system*

**2.2 Remote control automation**

Transfer the input of one device to the output of another can also be used for remote control of actuators.

However, it should be kept in mind that the built-in output relays are low-power. To switch a powerful load, you need to use additional switching devices (contactors).

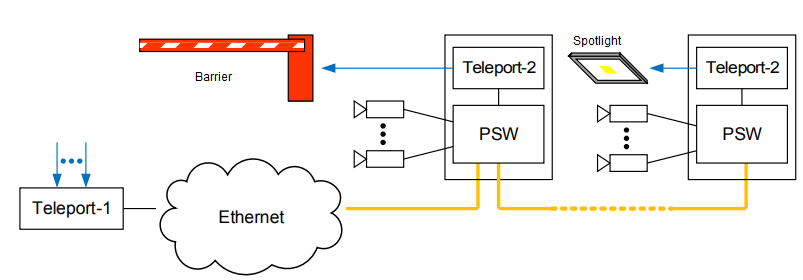


Fig. 1.8 Actuator control

1. **Transmission of alarm events from PSW switches**

TFortis switches form a series of events that can be transmitted to Teleport integration units:

• Camera hanging

• Loss of power 230VAC

• Disconnection of fiber optics, etc.

On the server side these events are converted into logical states of the outputs of the Teleport unit, which can be connected to the security controller.

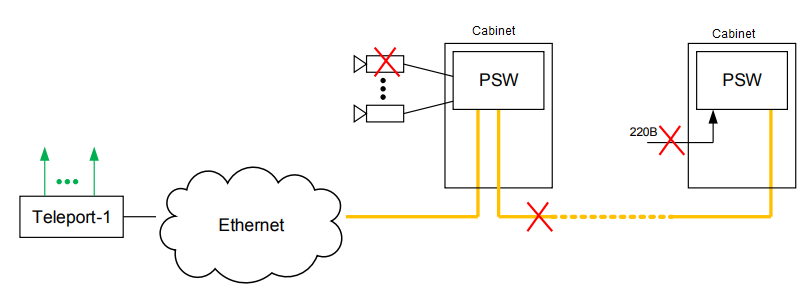


Fig. 1.9 Transmission of alarm events

1. Technical characteristics

2.1 Teleport 1 integration unit

* + Ethernet
    - 10/100Base-Tx with RJ-45 connector – 1;
    - supports Auto-MDIX;
    - supports IEEE 802.3x flow control.
  + **RS-485** – 1 pc
  + up to 115 200 bit/sec rate
  + up to 100 m length
  + built-in terminator – 120 Ohm
  + no galvanic isolation
  + **Inputs** – 3 pcs
  + Closed state – less than 200 Ohm
  + Open state – more than 50 kOhm
  + No galvanic isolation
  + **Outputs** – 9 pcs
  + Normally open contact
  + Switching voltage – 30V
  + Switching current – 50 mA
  + Channel resistance – 10 Ohm
  + Galvanic isolation
  + **Power supply**
  + Power supply voltage: 12/24VDC (9V..27V)
  + Maximum power consumption – 3V
  + **Design**
  + 106x90x58 mm (width of 6 modules)
  + Max weight 0.3 kg
  + DIN-rail mounting (35 mm)
  + **Meantime between failures** – 50 000 hours
  + **Operating conditions**
  + Temperature +5 C .. +40 C
  + Humidity up to 80%
  + **Storage**
  + Temperature -50 C .. +50 C
  + Humidity up to 80%

2.2 Teleport 2 integration unit

* + Ethernet
    - 10/100Base-Tx with RJ-45 connector – 1;
    - supports Auto-MDIX;
    - supports IEEE 802.3x flow control.
  + **RS-485** – 1 pc
  + up to 115 200 bit/sec rate
  + up to 100 m length
  + built-in terminator – 120 Ohm
  + with galvanic isolation
  + **Inputs** – 5 pcs
  + Closed state – less than 200 Ohm
  + Open state – more than 50 kOhm
  + with galvanic isolation
  + **Outputs** – 1 pc
  + Normally open contact
  + Switching voltage – 250V
  + Switching current – 150 mA
  + With galvanic isolation
  + **Power supply**
  + IEEE802.3af Class 3 (13 W)
  + Power output for external devices: 24VDC (6W)
  + With galvanic isolation and short circuit protection
  + **Design**
  + IP66 casing
  + 240x160x90 mm (excluding cable glands)
  + **Meantime between failures** – 50 000 hours
  + **Operating conditions**
  + Temperature -55 C .. +70 C
  + Humidity up to 80%
  + **Storage**
  + Temperature -50 C .. +50 C
  + Humidity up to 80%

**Supported functions and protocols:**

* + Transfer the state of the inputs to the outputs of the remote device
  + Transfer data from RS485 via Ethernet to a remote device or to the TFortis Administrator application (Virtual extension of the RS485 line)
  + Support of up to 32 remote devices
  + Integrated web interface
  + Modbus RTU, ASCII, TCP client
  + Telnet
  + monitoring by SNMP v1, v3
  + SNTP
  + SMTP
  + Syslog
  + system log
  + DNS
  + remote Ping function
  + event notification settings
  + firmware update using TFTP

1. Description
   1. Appearance

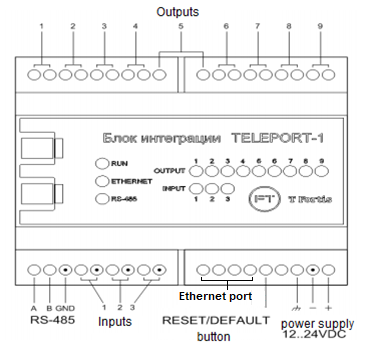


Fig. 3.1 Teleport-1 appearance

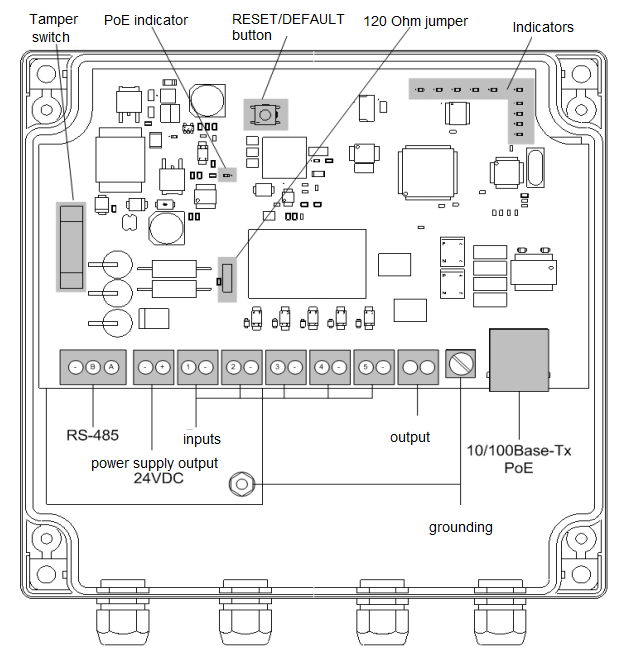


Fig.3.2 Teleport-2 appearance (with removed cover)

3.2 LED indication

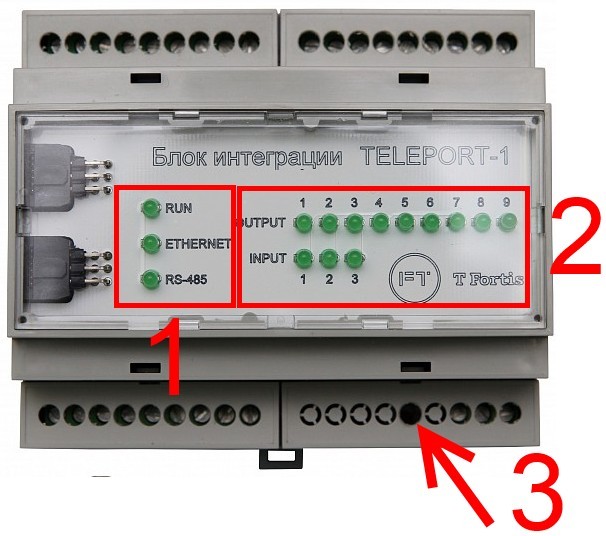


Figure 3.3. Teleport-1 indicators

Integration units Teleport-1 and Teleport-2 have LED indication on the front panel (Teleport-1) or on the printed board (Teleport-2) that displays the operating parameters of the device (**1** ) or the state of inputs and outputs ( **2** ).

**RUN** indicator displays the operating mode of the device.

**ETHERNET** indicator combines the link indicator and indicator of activity through the Ethernet port.

**RS485** indicator displays activity on the RS485 interface.

The indicators from group **(2)** – **INPUT** and **OUTPUT -** show the current state of the inputs and outputs (if the input or output is closed, the LED is ON, if open – OFF). These indicators can be useful in the configuration and setup process.

Table 3.1. Purpose of the indicators

|  |  |
| --- | --- |
| **Indicator status** | **Device status** |
| **RUN** indicator flashing (4 seconds interval) | The device operates with the factory settings. |
| **RUN** indicator flashing (1 second interval) | The device operates normally, the settings are different from the factory settings |
| **ETHERNET** indicator  continuously ON | The Ethernet interface link is picked up, but there is no data exchange |
| **ETHERNET** indicator  flashing | Data is exchanged via Ethernet |
| **RS485** indicator  flashing | Data is exchanged via RS485 |
| **RUN** and **RS485** indicators flashing in sync | Hardware or software fault is detected. Contact technical support. |

3.3 Reset and restart buttons

TFortis Teleport integration unit has **RESET** hard button.

The button is located in **(3)** (see Figure 3.1) and is sunken in the housing. To press the button, use any thin non-metallic object.

* + To restart the integration unit, press **RESET** button and hold it down for 3-5 seconds.
  + To restore default settings, press RESETbutton and hold it down for 15-20 seconds.

1. **Mounting and connection**

**4.1 Mounting of Teleport-1 unit**

Teleport-1 integration units are designed for installation on the standard 35 mm DIN rail. For installation it’s necessary to use a DIN rail with a length at least 106 mm (width of 6 standard modules). The DIN rail is horizontal.

Teleport-1 should be located in a heated room at some distance from sources of strong heating or cooling. Since the device does not have galvanic isolation and serious protection against pulse overvoltage over Ethernet, inputs and RS-485, it is recommended to minimize the length of connected cable lines. It is recommended to use power from uninterruptible power supplies with an output of 12..24V.

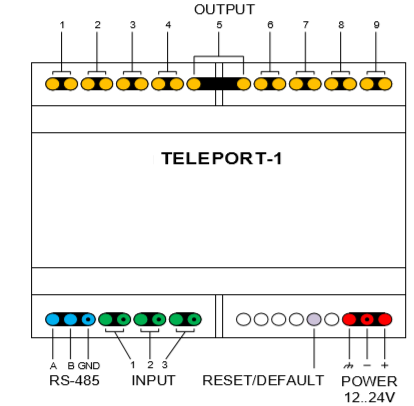
Grounding is recommended. The presence of grounding increases the noise immunity of the device.

**Connecting dry contact lines and Ethernet**

The inputs of the device do not have galvanic isolation (both between the control microcontroller and between themselves). Therefore, when connecting sensors, it should be kept in mind that all inputs have 2 contacts, one of which is common. In fig. 4.1 and on the unit the total potential is indicated by a dot. Contacts marked with a dot are connected with each other.

The outputs of the device are galvanically isolated, this requirement does not apply to them.

To reduce the effect of interference, it is recommended to reduce the length of the input, output and Ethernet lines.



*Fig. 4.1 Inputs and outputs arrangement.*

RS-485 connections are made using a twisted pair cable. The presence of a line for potential compensation (GND) is mandatory with a long line length. Termination resistors (120 Ohm) are already installed inside the enclosure, installation of additional resistors is not required.

Connecting to a server or central switch is performed by UTP or FTP patch cord.

 It is forbidden to lay lines along high-voltage power lines.

**4.2 Mounting of Teleport-2 unit**

Teleport-2 allows installation outdoors on any metal / non-metallic surfaces, next to perimeter security controllers, as the enclosure of the device provides IP66 protection rating against dust and moisture. However, installation next to PSW switches in outdoor metal cabinets with at least IP54 protection allows for increased ease of installation and provides good vandal protection.

Teleport-2 provides for fastening to the rear false wall of a TFortis CrossBox-2 and CrossBox-3 outdoor cabinet through the “PSW-11 Mounting Panel”.



*Fig. 4.1. Unit mounting in a cabinet.*

The unit is attached to the adapter plate using M4 screws (not supplied). Mounting screws are supplied with the mounting plate.

Mounting outside the cabinet is also allowed. For installation, M4 screws or universal screws with a diameter of 4 mm are used.

**Grounding**

Grounding is required. In case there is no grounding, as well as poorly made grounding, lightning protection components do not work or do not work in full. The grounding can significantly increase the resistance of the device to electromagnetic impulse interference.

Grounding is carried out through the ground terminal or ground stud (Fig. 3.2). Grounding through the screen of an FTP cable **is not allowed**!

Ground resistance **no more than 4 Ohm**.

**Connection of dry contact lines and Ethernet**

The inputs and outputs of the device are galvanically isolated and are resistant to impulse noise. However, in order to reduce the influence of interference, it is recommended to reduce the length of the input, output, RS-485 and Ethernet lines.

RS-485 connections are made using a twisted pair cable. A line for potential equalization (GND) is mandatory. Termination resistors (120 Ohm) are already installed inside the device, installation of additional resistors is not required. It is possible to disable termination resistors. By default, resistors are connected.

Connecting to the PoE switch is performed using high-quality outdoor FTP cable.

It is forbidden to lay lines along high-voltage power lines.

The outputs of the device are not designed for switching a powerful load. The maximum load on the port is 150mA 250V.

**Sealing of inputs**

The device is supplied with a set of cable glands. When installing the glands, they must be tightened securely. Unused entries must be sealed with a sealant or plastic fungus. Violations in the installation of cable glands do not guarantee compliance of the device with IP66 protection rating.

1. Configuration
   1. Management Interfaces

TFortis Teleport integration units have the following options of remote management: Web interface, Telnet, SNMP, **TFortis Device Manager** software.

Web interface contains a full set of managed parameters with a detailed explanation and a short summary. The interface is available in Russian and in English. You may connect to it via a standard web browser.

Telnet is an alternative way of device configuring using a console application, such as Microsoft Telnet, PuTTY, Hyper Terminal, etc.

SNMP is used for state and parameter monitoring.

By means of **TFortis Device Manager** you can broadcastly search for devices and configure remotely. The software can be useful when the network settings of Teleport integration units are unknown, and when there is duplication of IP addresses (in case when there are several devices with the same IP addresses in a network, standard configuration methods such as configuration via the WEB interface are not applicable)

* 1. What you need to know before connection

**Attention!**

The device outputs are not designed to switch to powerful load. Maximum port load is 100mA 250V (for Teleport-2) and 50mA 30W (for Teleport-1).

Teleport-2 integration unit includes 24 VDC output to provide power supply for peripheral devices. Maximum power of the output is 6W.

* 1. Management via web interface
     1. First connection, quick start

When switched on for the first time, the integration unit has the following default settings:

IP address: 192.168.0.1

Subnet mask: 255.255.255.0

Login/Password not specified

DHCP client off

Telnet on

SNMP off

Before connecting, make sure that the network card of the computer is on the same subnet as Teleport integration unit (192.168.0. \*).

Start the web browser and enter the IP address **192.168.0.1** in the address bar

(Figure 5.3.1.1)

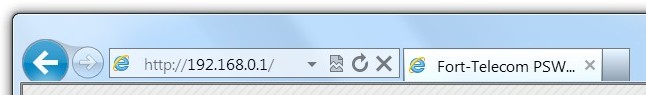


Figure 5.3.1.1. Connection to the integration unit

After connection, main web interface page should display (Figure 5.3.1.2).

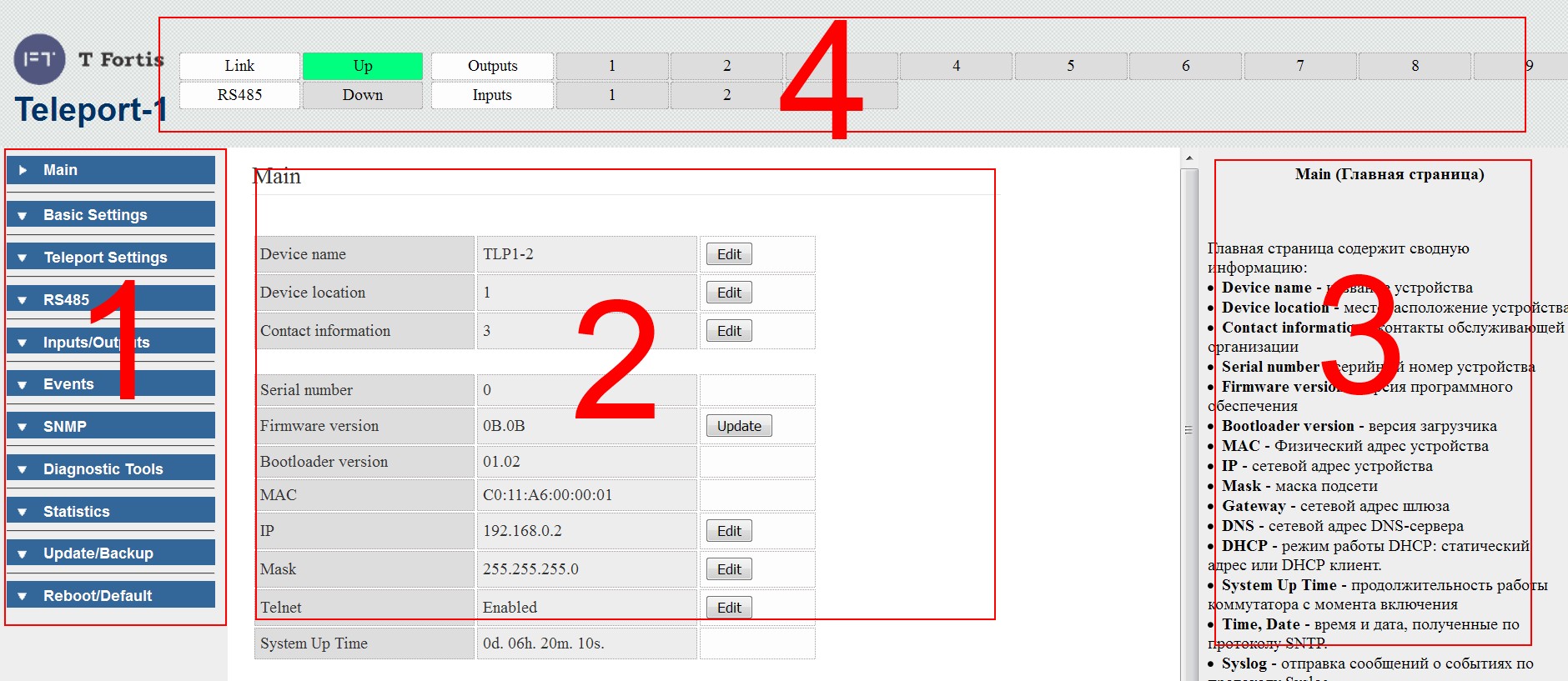


Figure 5.3.1.2. Web interface

The web interface can be divided into 4 frames shown in Figure 5.3.1.2:

* + - 1. – side menu that provides access to various groups of settings
      2. – the main frame containing the group of settings
      3. – help for these settings

4 – header with input and output state (automatically updated every 10 seconds)

**Note:** by default, access to web interface is available without login and password. It is recommended to restrict access in the future by setting login and password. In this case each subsequent connection will be accompanied by a standard authentication dialog box.

After connecting to web interface, proceed with configuration. To start the configuration, you should have a deep knowledge of the network map including location and functions of all units.

Consider the structure displayed in Figure 5.3.1.3.

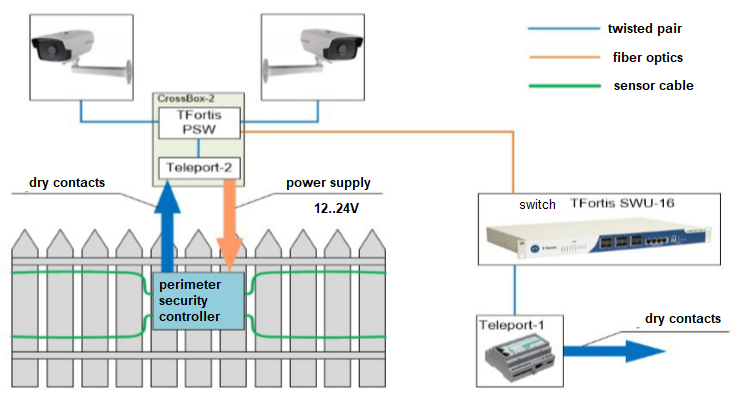


Figure 5.3.1.3. Structure of the system

This example shows the perimeter surveillance system that is remote from the data collection and processing server (DCPS). The perimeter surveillance controller checks sensitive cable elements and warns of the system response via the standard two-wire interface RS-485. Around the perimeter, there are also surveillance cameras connected to TFortis PSW switch. This bundle of equipment makes up the Security node. To use this system, connect the Server and the Security node However, the Security node may be located too far away from the Server. The only solution may be the use of fiber optic lines for the Ethernet network. In this case you can implement a virtual channel – pipe – via Ethernet for RS-485.

Teleport-2 converts RS-485 to Ethernet. Data goes through the nodal switch TFortis PSW, then by fiber optics through the core switch, then to Teleport-1 integration unit, where the reverse conversion Ethernet → RS-485 is performed.

To create a virtual RS-485 channel between two Teleport-1 and Teleport-2 units, they must be configured.

In general, the configuration process looks like this:

1. Configure the network settings
2. Register a remote device (For Teleport-1 it is Teleport-2 and vice versa)
3. Setting the RS-485 port to paired mode with a remote device.

**Network settings**

In the network settings of the integration unit, you should specify a unique IP address within the subnet. Let's say, the IP of Teleport-1 is 192.168.0.1, and the IP of Teleport-2 is 192.168.0.2. Change these fields as shown in Figure 5.3.1.4. To do that, select **Basic Settings → Network Settings** in the side menu

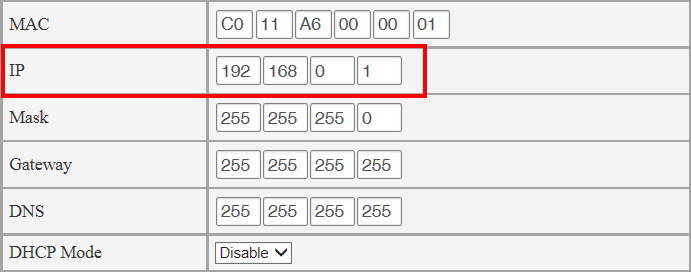


Figure 5.3.1.4. Network settings of Teleport-1

List of remote devices

To make Teleport-1 visible to Teleport-2, and Teleport-2 visible to Teleport-1, you should introduce them to each other. To do that, each unit has a list of remote devices. It stores all the devices that a local device can interact with.

Let's take Teleport-1 as an example. For it, the remote device is Teleport-2. Therefore, go to Teleport-1 web interface, tab **Teleport Settings → Remote Devices**. As we see, the list is empty yet. Add Teleport-2 to the list indicating its IP address, type (Teleport-2) and a user-defined description to ease the identification. Press **Apply**.

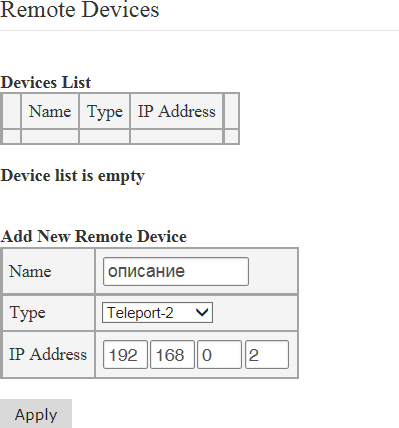


Figure 5.3.1.5 Configuration of remote devices of Teleport-1

As we see in Figure 5.3.1.6, Teleport-2 has been added to the list.

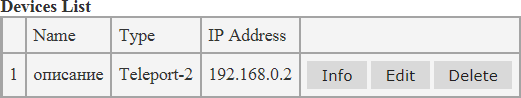


Figure 5.3.1.6 List of remote devices of Teleport-1

A similar setting is made on Teleport-2 web interface.

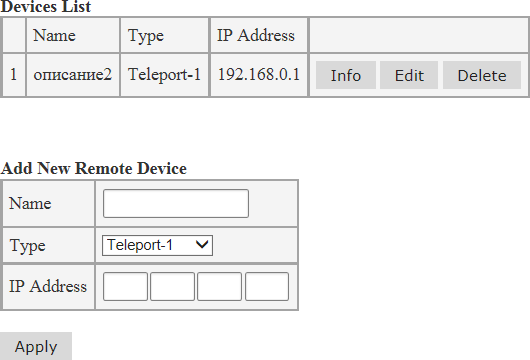


Figure 5.3.1.7 Configuration of remote devices of Teleport-2

Configuring RS-485 port

To configure RS-485 port, go to **RS-485 → RS-485 Settings** tab

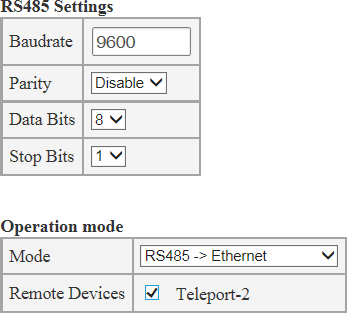


Figure 5.3.1.7 Configuration of RS-485 port of Teleport-1

In **RS485 Settings** section enter the same port settings as for the perimeter surveillance controller. Enter operating mode of the port in **Operation mode** section. We need to transfer data via Ethernet, so we select **RS485->Ethernet mode**. Indicate all the devices to which the data will be broadcast in the list of Remote Devices. In our case there is only one entry – Teleport-2. So we select it by setting a check mark. Click **Apply** to apply the settings. Select the same settings on the other device.

Configuration is completed. Data from RS485 port of the perimeter surveillance controller will be transparently delivered to RS485 port of the data collection and processing server.

**5.3.1.1 Configuration strategy**

In the previous section we examined the configuration process using a specific example, but the entire configuration process can be divided into several steps.

1. Network settings (setting a unique IP address within the subnet, mask and gateway)
2. Set login and password to restrict access
3. Creating a list of remote devices
4. Configuring inputs, outputs, RS-485. Indication of operating modes, remote devices.
5. Monitoring setup. For ease of administration you can configure sending events through the Syslog, SMTP, SNMP protocols, and synchronize the internal clock via SNTP protocol.  
   * 1. Network settings

*Basic Settings → Network Settings*

This section describes the basic network settings of the integration unit.

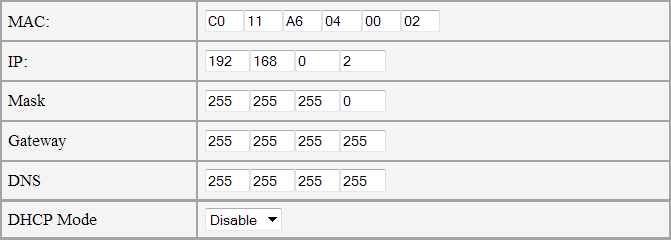


Figure 5.3.2.1 Network settings

**MAC** is the physical address of the device used to identify the device in the network. It is not recommended to change the MAC address otherwise than in extreme cases, since it ensures uniqueness of the device in the network. The last 2 bytes of the factory MAC address are the serial number of the device. See the factory MAC address on the label attached to the enclosure.

**IP** is the network address of the device. When working within the same subnet, it is necessary to ensure the uniqueness of the network address.

**Mask** is the subnet mask.

**Gateway** is the gateway network address. If the gateway is not used, leave the default value: *255.255.255.255*

**DNS** is the network address of the DNS resolver. It is used in some functions to convert the host name to its network address. If not used, leave the default value: *255.255.255.255*

**DHCP Mode** is selecting the operating mode of the DHCP protocol:

1. *Disable* – DHCP disabled. The integration unit uses static network settings (IP, Mask, Gateway, etc.).
2. *Client* – DHCP mode enabled. The integration unit receives network settings automatically using broadcast request to the DHCP server.
   * 1. Configuring user accounts

*Basic Settings → User Accounts*

This section contains the settings of user accounts.

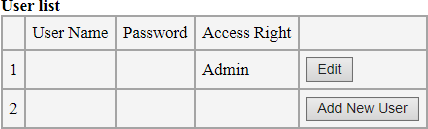


Figure 5.3.3.1 List of users

By default, the only account is the administrator account with an unset user name and password. It means that access to web interface and Telnet is available without authentication.

To restrict access, it is necessary to create at least one user with **Admin** rights and, if necessary, one or more users with **User** rights.

Access rights are separated by selecting the Access Right field.

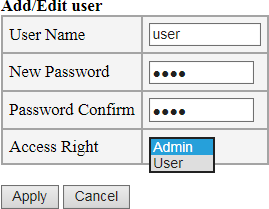


Figure 5.3.3.2 Configuring user name and password

A user with **Admin** rights has maximum authorities.

A user with **User** rights has limited authorities, cannot change settings, and has access to statistics and diagnostic tools (Ping).

If setting was successful, the message *"Parameters accepted"* will be displayed and it will be necessary to log in using the login and password.

If an error message is displayed, enter the parameters again.

**Note 1:** These fields are mandatory. The maximum length is 20 characters. Input language is English.

**Note 2:** The fields are case sensitive, i.e. there is a difference between "Admin" and "admin".

**Note 3:** Up to 4 accounts are supported.

* + 1. Device description

*Basic Settings → Device Description*

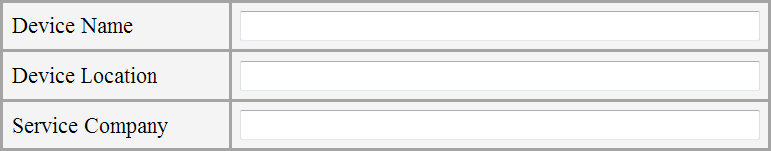


Figure 5.3.4.1 Device description

**Device Name** – device name

**Device Location** – device location

**Service Company** – contact information of the service company or responsible person

These fields are optional and only serve to simplify the identification of the device. The maximum length of entries is 64 characters in English and 32 characters in Russian.

* + 1. Telnet configuration

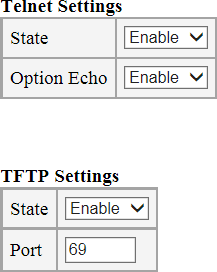
*Basic Settings → Telnet*

Figure 5.3.5.1. Enabling Telnet and TFTP

**Telnet** – protocol used for remote management of network equipment based on port 23 TCP protocol.

By default, Telnet is enabled. If necessary, it may be disabled.

The login and password for Telnet access are the same as for the web interface access.

**Option Echo** is an option of Telnet protocol, enabled by default.

In addition, the firmware may be upgraded using Telnet, in this case TFTP protocol is used.

Since TFTP protocol is not secure, it is disabled by default. If necessary, it is possible to enable it, or change the standard UDP port (69) for another one.

For more details on configuring with Telnet, see Section 5.4.

* + 1. Configuring SNTP

*Basic Settings → SNTP*

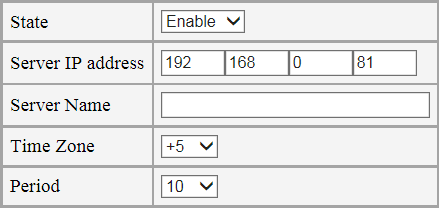


Figure 5.3.6.1. Configuring SNTP

**SNTP** (Simple Network Time Protocol) is the protocol by which the integration unit synchronizes its internal clock with an external time server.

Teleport does not contain a built-in real-time clock, so it is necessary to use SNTP protocol to get information about the current time. The use of SNTP protocol is not mandatory, the main functions of the integration unit are not connected with SNTP. However, to simplify administration, Teleport supports the recording of the event log in the "black box" and sending syslog and e-mail messages about the events to the network administrator. With SNTP protocol enabled, these messages will include a time stamp, which can be helpful for the administrator servicing the network.

**Settings: State —** state

**Server IP address** – IP address of SNTP server

**Server Name** – domain name of SNTP server. If both IP address and domain name of the server are set, IP address will prevail

**Time Zone** – time zone (difference from UTC)

**Period** – time period of synchronization with the server (in minutes)

**Synchronize** – forced synchronization of time (to check the settings)

* + 1. Web interface language setting

*Basic Settings → Language*

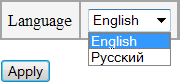


Figure 5.3.7.1. Language selection

The web interface of Teleport

supports 2 languages: Russian and English. The default language is English. You may change it to Russian, if necessary. To do that, make sure there are no problems with text encodings in the browser.

The web interface uses **UTF-8** encoding.

* + 1. Configuring the transfer mode

Teleport integration units perform the following transfer modes:

* + RS-485 transfer via Ethernet. To do this, an Ethernet connection is established between two or more (up to 32 devices) Teleport units, and data is transferred between the RS-485 ports of all units included in one group.
  + conversion of RS-485 to Ethernet. On the server side, the TFortis Administrator application is launched, which provides a virtual COM port interface associated with one or more Teleport integration units. (up to 32 devices). In other words, a “virtual channel” is organized between the virtual COM port and the integration unit.
  + Transferring “dry contacts” via Ethernet and transmitting alarm events from PSW switches. In this mode, the status of the inputs on the Teleport units or the inputs of the TFortis switches are transmitted to the outputs of other Teleport units. (Up to 32 devices)

When transferring RS-485 via Ethernet, it should be noted that delays inevitably occur due to data conversion. In order not to cause malfunctions in the system, you should take this into account when setting timeouts. For more details on the methodology for calculating timeouts, see page 95.

5.3.8.1 Setting the list of remote devices

*Teleport Settings → Remote Devices*

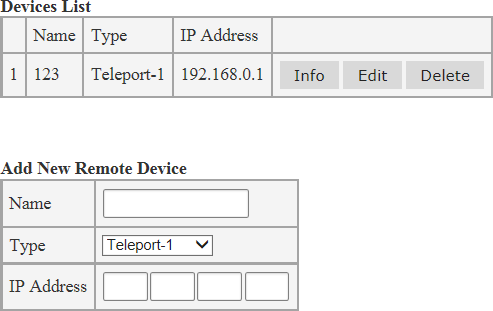


Figure 5.3.8.1. Adding remote devices

To configure a bundle of devices used to broadcast the state of dry contact inputs and RS-485 data, first create a list of devices to send data to. Fill in the list of remote devices only in this tab.

The list stores all the devices a local device can interact with.

To add a new device, fill in the following fields:

**Name** — description of the device. This field is optional bit it may simplify further identification of the device.

**Type** – type of remote device

**IP Address**— IP address of remote device. Press **Apply** to save the settings.

Press **Edit** to edit the settings of the remote device. To delete the settings, press **Delete** .

Pressing the **Info** button will display detailed information about the device, connection status, number of inputs and outputs, etc.

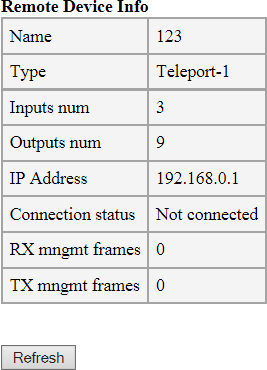


Figure 5.3.8.2. Detailed information about the device

* + 1. Configuring RS-485 port

*RS-485 → RS-485 Settings*

This section describes RS-485 port configuration. The configuration processes consists of two stages: setting physical parameters of the interface and setting the operating mode.

Setting the interface parameters:

* + - * **Baudrate** – speed of the port (bits per second)
      * **Parity** – parity check: **Disable** – disabled; **Even** – even; **Odd** – Odd.
      * **Data Bits** – number of data bits
      * **Stop Bits** – number of stop bits

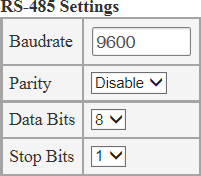


Figure 5.3.9.1. Setting RS-485

Setting the operating mode

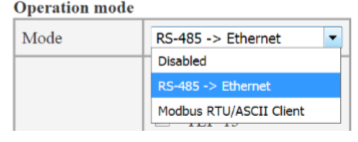
****

Figure 5.3.9.2. Setting the operating mode

Two operating modes are supported for the interface: RS-485 data transmission via Ethernet and Modbus RTU / ASCII client.

**RS-485 transfer mode**

In this mode you have to set the appropriate checkboxes to indicate which remote devices are communicating with.

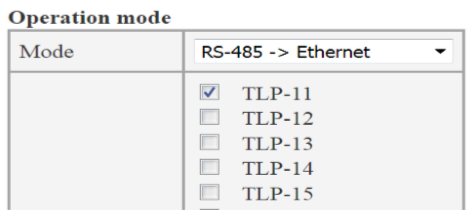


Figure 5.3.9.3 Setting the list of remote devices

In this case data from the local port of the device are transferred to RS-485 port of the remote device that is chosen (TLP-11 in a Fig. 5.3.9.3)

See an example of setting in Section 5.3.1 (First connection, quick start)

**Modbus RTU/ASCII client mode**

In this mode Teleport is a client of Modbus RTU or Modbus ASCII protocols. Configuration of Modbus protocol is performed in section “Modbus configuration”.

* + 1. Configuring digital inputs

*Inputs/Outputs → Inputs*

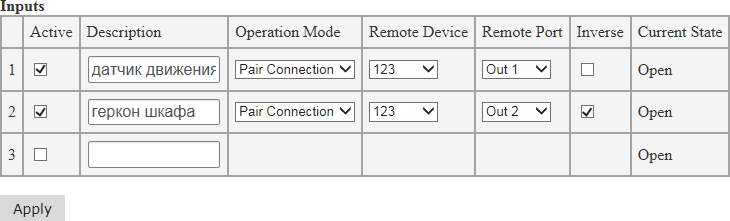


Figure 5.3.10.1 Configuring inputs

The inputs of the integration unit may be broadcast to the remote device output.

* + - * **Active** – enables input operation. If this box is checked, the input is active and its state may be broadcast to the remote device.
      * **Description** – the device description. Use this to simplify the setting process.
      * **Pair Connection** – pair connection mode. The input state will be broadcast to the remote device output. This is currently the only operating mode of the input.
      * **Remote Device** – the remote device to which the input state will be broadcast. If the input is active, you should specify the place for transfer, i.e. set the remote device.
      * **Remote Port** – the number of the remote device output to which the input state will be broadcast
      * **Inverse** – the input inversion. The inverse state of the input will be broadcast to the remote device. For example, if the sensor connected to this device is closed the output relay on the remote device will open.

**Current State** – current input state:

**Open** – the input is open, logic "0"

**Short** – the input is closed, logic "1"

Press **Apply** to apply and save the settings.

In case there is no need to broadcast the input but it is required to

get information about the input state, use the following methods:

1. receiving messages about changes in the input state via Syslog, SMTP, SNMP-Traps protocol
2. sending requests via the SNMP protocol
3. sending requests via the Modbus protocol
   * 1. Configuring digital outputs

*Inputs/Outputs → Outputs*

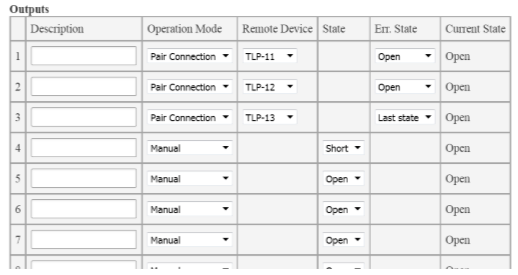
**

Figure 5.3.11.1. Configuring outputs

The integration unit contains several managed solid-state relays. The outputs support several management modes (**Operation Mode**)

1. **Pair Connection** – pair connection mode. In this mode the output is used to broadcast the state of the remote device input. The input on the remote device from which the input is to be broadcast also switches to **Pair Connection**. For this mode specify the remote device in the **Remote Device** field.

If the remote device is not specified, the output will not respond to control commands. In this mode, you may change the output only by the control command from the input.

If during operation the connection with the remote device is lost, the output state is transferred to the **Err. State.**

1. **Manual** – Manual control mode. You may set the necessary output state via the web interface or Telnet.

**Open** – the output relay is open.

**Short** – the output relay is closed.

In this mode the port can be also set to the appropriate state via SNMP, Modbus, or in the I/O network controller mode.

Due to the restriction of the output management mode only one managing protocol may be used at a certain time point. However, you may use a variety of options to monitor the state of inputs as there are no restrictions in this respect:

1. receiving messages about changes in the output state via Syslog, SMTP, SNMP-Traps protocol
2. sending requests about the output state via the SNMP protocol
3. sending requests about the output state via the Modbus protocol
   * 1. Configuring Modbus

*Inputs/Outputs → Outputs*

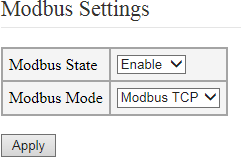


Figure 5.3.12.1. Configuring outputs

The Teleport integration unit can be a Modbus client. The following modes are supported:

Modbus TCP

Modbus RTU

Modbus ASCII

Use the Modbus protocol to read the state of inputs and outputs and manage the outputs.

Address space for the Modbus protocol

|  |  |
| --- | --- |
| address | value |
| 00001-00009  (00001) | The state of digital outputs for Teleport-1 (Teleport-2) |
| 10001-10003  (10001-10005) | The state of digital inputs for Teleport-1 (Teleport-2) |

The integration unit supports the following protocol functions:

* + - * (0x01) Read Coil Status – read the digital input
      * (0x02) Read Discrete Inputs — read the digital output
      * (0x05) Write SingleCoil Status — write a single output
      * (0x0F) Write Coil Status — write the group of outputs

5.3.13 I/O network controller mode configuration

*Teleport→ PLC*

Teleport integration unit supports the functions of network controller ( control of inputs and outputs)

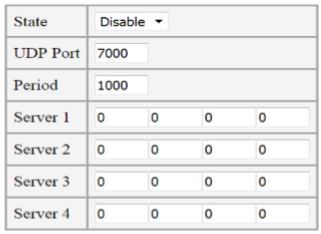


Figure 5.3.13.1 Network controller mode configuration

State – the state. Enable – enabling the function, Disable – disabling the function.

Control of outputs is performed via http-request :

xx.xx.xx.xx/digitaloutput/all/value?DO0=0&DO1=1&DO2=0  
xx.xx.xx.xx – IP address of the unit

DO0=0 – setting output 0 into 0 state (open)

DO1=1 for output 1 in state 1 (closed)

Etc.

Obtaining the status of inputs is carried out by periodic sending (with a period of Period, specified in ms.) of UDP packets to the UDP port and server addresses (Server 1 - Server 4). The format of sending matches the format in Advantech ADAM6066 controllers.

* + 1. Configuring the event list

*Events → Event List*

The Teleport integration unit has a wide range of capabilities to ensure convenient administration. The key feature is the ability to provide an administrator with instant notifications about the events through various tools, such as Syslog, SMTP (e-mail) or SNMP Trap.

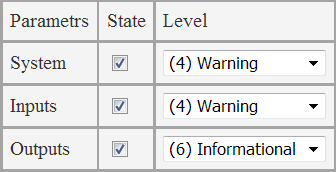
The integration unit may be adjusted to respond only to certain events to which an appropriate level of significance is assigned (only for the Syslog protocol). Levels range from 0 to 7, where 0 is the highest level of significance.

Figure 5.3.13 Event list

The following range of levels is generally accepted:

* + - 1. **(0) Emergency**: the system is inoperable
      2. **(1) Alert**: the system requires immediate intervention
      3. **(2) Critical**: the state of the system is critical
      4. **(3) Error**: error messages
      5. **(4) Warning**: warnings about possible problems
      6. **(5) Notice**: messages of normal, but important events
      7. **(6) Informational**: information messages
      8. **(7) Debug**: debugging messages

Such separation of events significance levels allows to process the events differently on the server side. For example, messages about level 6 and 7 events can simply be recorded in the event log, while messages about level 0-3 events will be shown to the operator.

The settings are divided into subgroups by the following categories:

* + - 1. **System** – change the system state (restart, update, reset to factory settings, etc.)
      2. **Inputs** — event in case of changing the state of inputs
      3. **Outputs** — event in case of changing the state of outputs
    1. Configuring Syslog

*Events → Syslog*

**Syslog** – the standard for sending messages about the events occurring in the system (logs) used in IP networks. Syslog protocol is simple: when certain events occur, Teleport sends a short text message, less than 1024 bytes in size, to the recipient of the message. Messages are sent by UDP (port 514). Syslog is used for ease of administration and information security.

Certain events may be flexibly adjusted and provided with an appropriate level of significance is assigned (Events → Event List tab). Levels range from 0 to 7, where 0 is the highest level of significance.

The following range of levels is generally accepted:

* + - 1. **(0) Emergency**: the system is inoperable
      2. **(1) Alert**: the system requires immediate intervention
      3. **(2) Critical**: the state of the system is critical
      4. **(3) Error**: error messages
      5. **(4) Warning**: warnings about possible problems
      6. **(5) Notice**: messages of normal, but important events
      7. **(6) Informational**: information messages
      8. **(7) Debug**: debugging messages

Such separation of event significance levels allows processing the events in different ways on the recipient side. For example, messages about level 6 and 7 events can simply be recorded in the event log, while messages about level 0-3 events will be shown to the operator.

Syslog message format

According to the Syslog standard, the message has the following format:

<significance level> <date and time> <sender's IP address> <message>

**Note:** the <date and time> field shows the date and time received by the SNTP protocol. If no time data is received or SNTP is not configured, the <date and time> field will show the time in seconds after power supply.

Here is an example to illustrate that: We have a message**,** received over Wireshark:



Figure 5.3.14.1. SNTP is not configured

As we see, the time has not been set. The time after start is shown.



Figure 5.3.14.2. SNTP is configured

Now the message has a standard time stamp.

Configuring Syslog on the integration unit

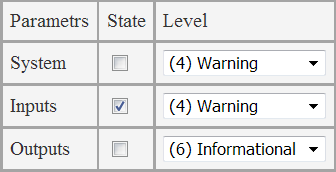
Configuring is rather simple. First, select the necessary events in the Events → Event List tab. For example, we are interested in the input change event.

Figure 5.3.14.3. Select the event

Then go to the Events → Syslog Settings tab and enable the Syslog protocol and set the IP address of the server to which messages will be sent.

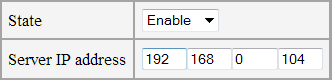


Figure 5.3.14.4. Configuring Syslog

Getting Syslog messages

After configuring the integration unit, proceed to configure the server. Let's consider an example for Windows OS. There are a lot of programs for working with syslog-messages. Here are some of them:

* + - 1. Kiwi Syslog
      2. Syslog Watcher
      3. Datagram SyslogServer Suite
      4. syslogbroadband
      5. LogZilla
      6. Syslog Server Free Tool

Let's choose Kiwi Log Viewer. This is a free simplified version of Kiwi Syslog Server. Nevertheless, it is fit for purpose in our case.

Download address is <http://www.kiwisyslog.com/downloads.aspx>

The installation of the program is rather simple. The main thing is to choose 'Install as Service' in the 'Choose Operating Mode' window (in this case, Kiwi Syslog will be installed as a service: it will start as the OS starts and will reside in the tray).



Figure 5.3.14.5. Kiwi Syslog installation

After installation, start the program. By default, all received messages will be displayed in the main window. These messages are recorded to a text file. It is also possible to configure forwarding by email.

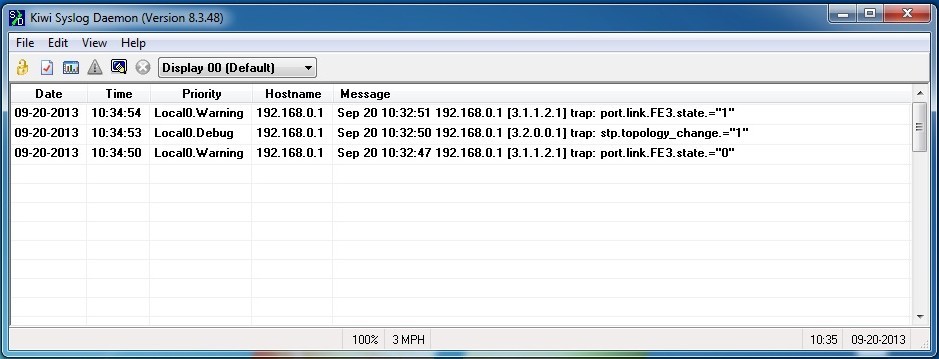


Figure 5.3.14.6. Kiwi Syslog interface

5.3.15.1 Syslog message list

Table 5.3.14.1 Syslog message list

|  |  |
| --- | --- |
| Web interface authentication: Ok | Login to the web interface with a password |
| Update firmware x.x.x | Firmware update |
| Default settings | Reset to factory settings |
| Clear ARP cash | Clear the ARP cache |
| Start after power reset | Start after power reset |
| Start after reset | Start after reset |
| Output 1 is changed | Output 1 has changed its state |
| Input 1 is changed | Input 1 is active (with indication of the current state) |
| Tamper is changed | The tamper sensor is tripped (for Teleport-2) |
|  |  |

* + 1. Configuring SMTP

*Events → SMTP*

Short list of terms.

**SMTP** – (Simple Mail Transfer Protocol) protocol for sending e-mail messages over the network. SMTP is used to send messages to a mail server. To receive messages from the mail server, client applications typically use POP or IMAP protocols.

Settings:

**State** — SMTP state

**Server IP address** - IP address of the mail server

**Server domain name** – domain name of the mail server

**Port** – number of TCP port through which messages are sent (0 – 65534). By default 25.

**Sender e-mail address** – e-mail address of the sender shown in the **From** field in the e-mail

**Receiver e-mail address** – e-mail address of the receiver shown in the **To** field in the e-mail.For additional user opportunities, up to 3 receivers are available.

**Subject** – subject of the e-mail.

**Login, Password** – login and password if the server requires authentication.

If these fields are filled in, the authentication with the server will be automatically activated. If these fields are empty, authentication will not be required.

The Teleport integration unit supports **AUTH PLAIN** and **AUTH LOGIN** authentication.

If server IP address is not specified, messages are sent to this address by default. To use the domain name, set **Server IP address** in **0.0.0.0** and specify the domain name in the **Server domain name** field.

Examples of SMTP configuration

There are two options for configuring e-mail:

* + - 1. A dedicated mail server is located on the local network.
      2. An external mail server is used.

Each option has its advantages and disadvantages. A dedicated mail server can be recommended if video surveillance network is physically separated from the Internet and it is impossible to use external mail services, or there is already a mail server on the network and no additional efforts are required to create and maintain the server. Using external mail services makes configuration easier and faster, eliminates the need to maintain a mail server, but in this case you need a permanent connection to the Internet, which may not always be possible because of enterprise security policies.

* + - 1. Example of configuration with a dedicated mail server on the local network

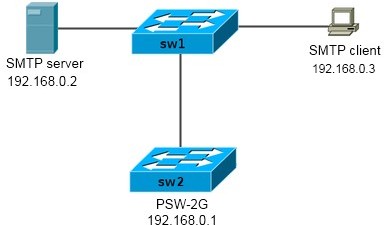


Figure 5.3.16.1.1 Network structure

Let's formulate the task as follows:

We need to configure SMTP on switch SW2 (PSW-2G) with IP 192.168.0.1 to send messages about the link change on the ports of PSW-2G switch to operator's computer 192.168.0.3.

Since the SMTP protocol does not involve storing messages and issuing them to the mail client, we need to include a mail server (192.168.0.2) into the network.

We select the domain name companyname.com for the network, the e-mail address [psw2g@companyname.com](mailto:psw2g@companyname.com) for PSW-2g, [server@companyname.com](mailto:server@companyname.com) for the SMTP server,

and [client@companyname.com](mailto:client@companyname.com) for the client.

Configuring Teleport

First, specify the event that will send a message when it occurs. In our case, this event is a link change. To do this, tick the appropriate event in the Events → Event List tab.

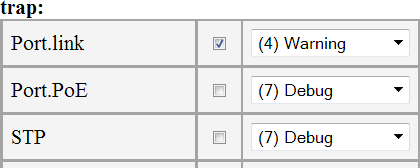


Figure 5.3.16.1.2 Select the event

Now let's configure the SMTP

Go to Events → SMTP tab.

Enable SMTP, set the IP address of the server,

set the e-mail address of the sender (i.e. PSW) [psw@companyname.com](mailto:psw@companyname.com), set the e-mail address of the main receiver [server@companyname.com](mailto:server@companyname.com), and also set the backup address [server2@companyname.com](mailto:server2@companyname.com) to which the messages swill be duplicated.

E-mail subject is "TFortis Teleport-1".

Leave the Login and Password fields empty since we are not going to use authentication.

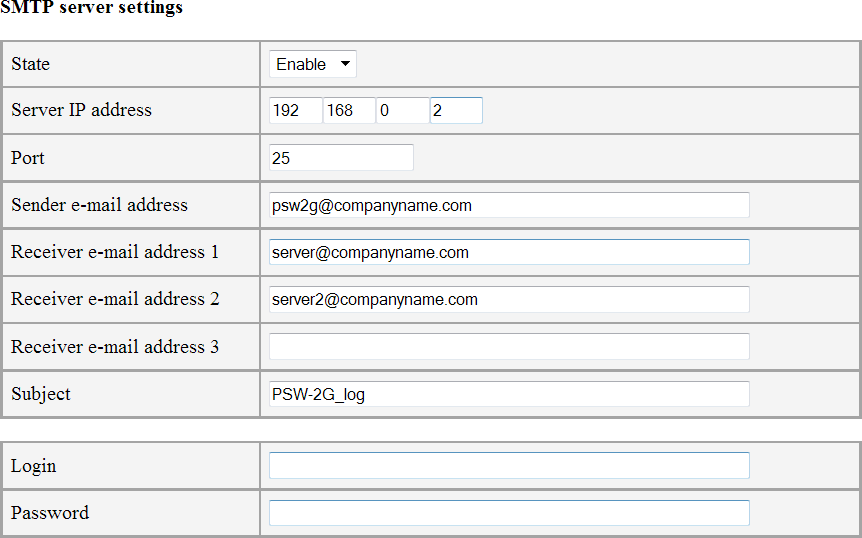


Figure 5.3.16.1.3 Configuring SMTP in Teleport

Press "Apply". Now the settings are applied. Now let's configure the mail server.

There are a number of mail server programs for various operating systems that support various protocols. We need a program that supports SMTP and POP3.

As an example of mail server for Windows, let's see Office Mail Server (<https://www.box.com/oms>). This is a free program with simple configuration.

Technical support and instructions are available on the website: <http://oficemailserver.livejournal.com/>

Install the program. After startup, the main window will be available:

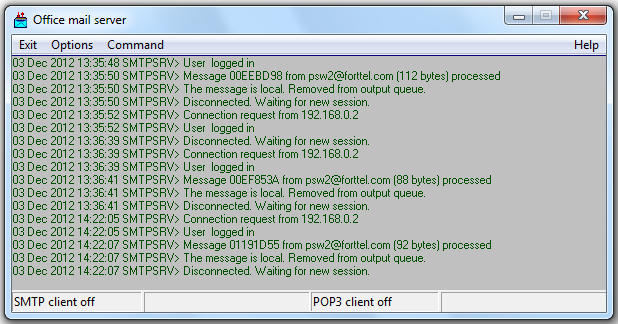


Figure 5.3.16.1.4 Office Mail Server main window

Go to menu **Options->SMTP/POP3 server options** and select

**Local domain name:** companyname.com

In the Users field add the user **client.** Then select user type [BOSS].

Office Mail Server support the following types of users:

* + - * 1. Postmaster — a user responsible for Office Mail Server operation and maintenance. This user receives special messages generated by the system in case of an error.
        2. Daemon – this is used to remotely connect to an external SMTP/POP3 server, send and receive messages
        3. Boss – this is the user who gets copies of all messages sent over the SMTP server.

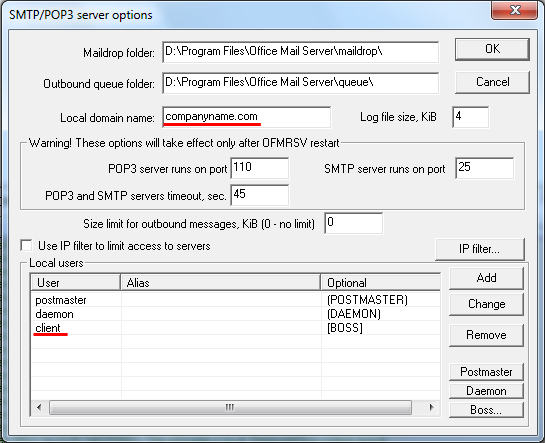


Figure 5.3.16.1.5 Office Mail Server configuration

In **Options->Transaction options** tab:

Set the IP address of the server, check the box "Automatically send outbound message if found", disable SMTP authorization (SMTP login button)

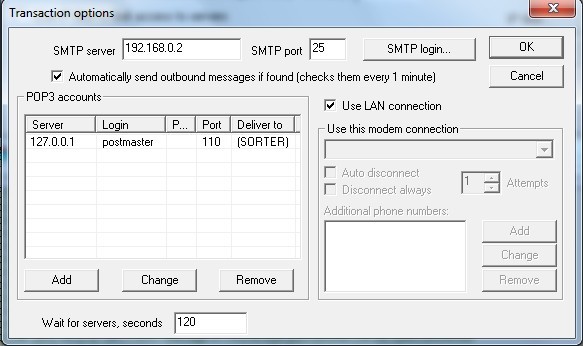


Figure 5.3.16.1.5 Office Mail Server configuration

Now all the messages coming to the server will be forwarded to [client@companyname.com](mailto:client@companyname.com)

Configuring client

Configuring client is rather simple. Example of configuring using Mozilla Thunderbird:

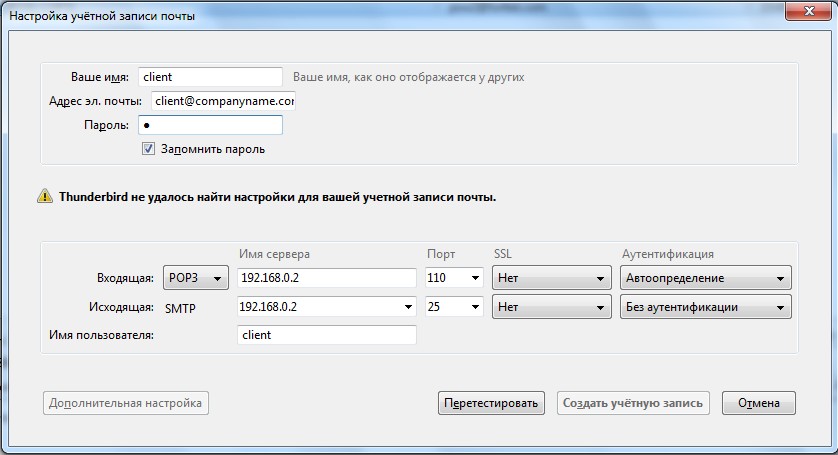


Figure 5.3.16.1.5 Configuring the Mozilla Thunderbird mail program

After finishing all the settings, you can go to the web interface to the SMTP Settings tab and check by sending a test message. Fill in Subject and Message fields and send out the message. If the settings are correct, Mozilla Thunderbird will notify of the new message.



Figure 5.3.16.1.6 Sending a test message

5.3.16.2. Example of setting with an external mail server

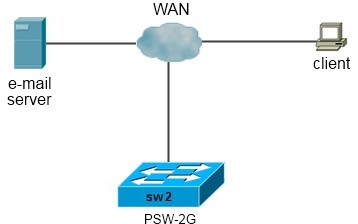


Figure 5.3.16.2.1 Sample network topology

In this example we will see how to configure PSW when an external mail server is used.

Let it be a mail server mail.ru. The procedure will be similar for other servers that support AUTH PLAIN or AUTH LOGIN authentication.

We will need to create a mail account and select the SMTP connection settings. For mail.ru the SMTP server address is as follows: smtp.mail.ru and port 25.

Now we can start configuring.

Fill in the information according to Figure 5.3.16.2.2.

Address for sending messages is [companyname@mail.ru](mailto:companyname@mail.ru).

Let the recipient address be the same, as if we are sending an e-mail to ourselves.

Login: [companyname@mail.ru](mailto:companyname@mail.ru) (at mail.ru login is the address itself) Password: password

**Note:** in this example we fill in the **Server domain name** field and fill the **Server IP address** with zeros. In this case, the switch will receive the IP address of the server automatically through the DNS query, but for this purpose the DNS address of the resolver must be configured. If DNS is not configured, it will be necessary to directly specify the IP address of the SMTP server.

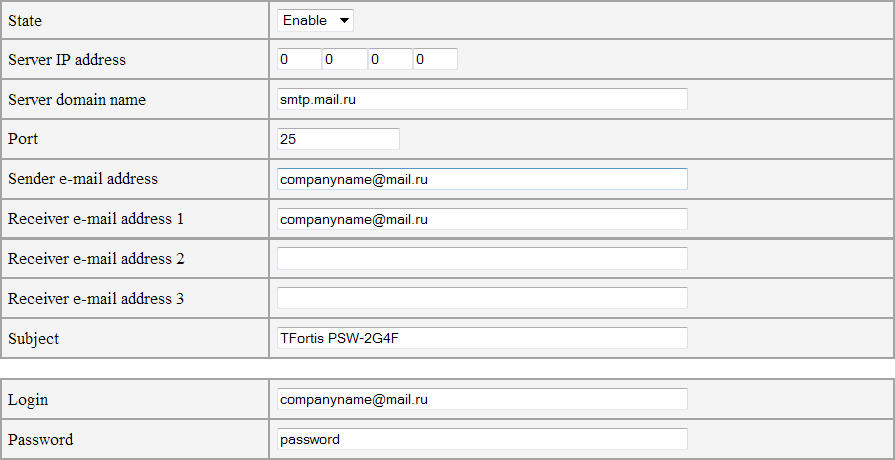


Figure 5.3.16.2.2 Configuring SMTP in PSW

After finishing all the settings, you can go to the web interface to the SMTP Settings tab and check by sending a test message. Fill in Subject and Message fields and send out the message.



Figure 5.3.16.2.3 Sending a test message

5.3.17 Configuring SNMP

*SNMP → SNMP*

**SNMP** (**Simple Network Management Protocol**) is a protocol used to manage and monitor network devices. Using the SNMP protocol, the software can access information that is stored on managed devices (for example, on a switch). On managed devices, SNMP stores information about the device on which it operates in a database called MIB.

The integration unit supports SNMP v1 and SNMP v3.

* + - 1. Configuring SNMP v1

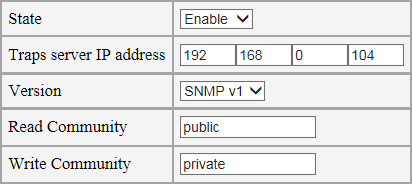


Figure 5.3.16.1 Configuring SNMP v1

* + - * + **State** — state.
        + **Traps Server IP address** – the IP address of the server to which SNMP Traps are sent.
        + **Version** – SNMP protocol version.
        + **Read Community** – read-only community, the string used for authentication in SNMP v1. Also, **Read Community** is used to send SNMP Taps.
        + **Write Community** – community for recording, the string used for authentication in SNMP v1.

SNMP Traps will be sent only when events occur that are specified in the **Event List** tab

* + - 1. Configuring SNMP v3

SNMP v3 provides a higher level of security compared to SNMP v1.

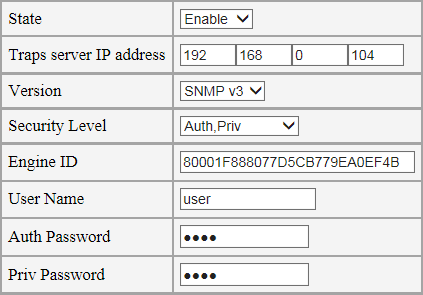


Figure 5.3.16.2 Configuring SNMP v3

To configure SNMP v3, set the Version switch to "SNMP v3".

SNMP v3 allows to flexibly configure the security level. The level is selected by the **"Security Level"** switch:

* + - * 1. **NoAuth, NoPriv** – authorization only on the User Name line, without encryption (this mode is similar to SNMP v1)
        2. **Auth, NoPriv** – Auth Password authentication (method HMAC-MD5-96), without encryption.
        3. **Auth, Priv** – Auth Password authentication (method HMAC-MD5-96), AES-128 encryption using the Priv Password key.

**Engine ID** – identifier in SNMP v3. For each device **Engine ID** is unique, it is generated based on the MAC address of the device. That is, you do not need to change it, but you can set your own value if necessary.

* + 1. Remote Ping function

*Diagnostic Tools → Ping*

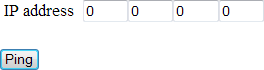


Figure 5.3.17.1 Remote PING interface

**PING** is a software utility used to test connection in TCP/IP-based networks. This utility sends four 32-bytes packages and waits for echo replies.

This utility helps you "ping" the remote device directly from the integration unit. It may be useful to resolve problems.

* + 1. Statistics

The Teleport integration unit provides a variety of statistic information that can be useful to solve network issues and for network administration.

5.3.19.1 Summary information

*Statistics → Main Statistics*

This section displays statistics on the state of inputs and outputs, RS-485 and the list of connected devices.

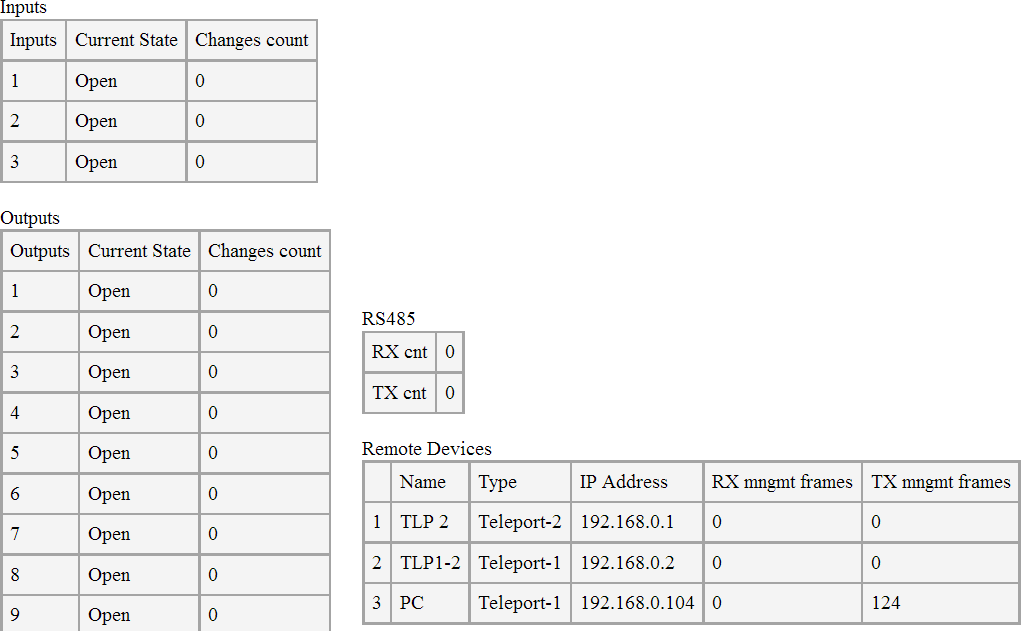


Figure 5.3.19.1.1 Summary statistics for the entire device

Interpretation of this table allows you to verify the correct operation and configuration of the device.

**Inputs** - a table of the current state of the inputs and the number of changes. If the input state changes very often, and the connected device does not imply a frequent change of state (for example, a reed switch for opening the cabinet), then this can be interpreted as a sensor malfunction or an alternating contact in the line.

**Outputs**- output status table

**RS-485** - RS-485 port counters. If the port is active and in use, the transmit and receive counters should increment.

**Remote Devices** - a table of statistics on remote devices.

If the device translates the state of its inputs to the outputs of the remote devices, then the TX mngmt frames counter should increment. If the status of the inputs of the remote devices is transmitted to the device outputs, then the RX mngmt frames counter should be incremented. If the device operates in RS-485 broadcast mode, then both counters must be incremented.

5.3.19.2 ARP table

*Statistics → ARP Table*

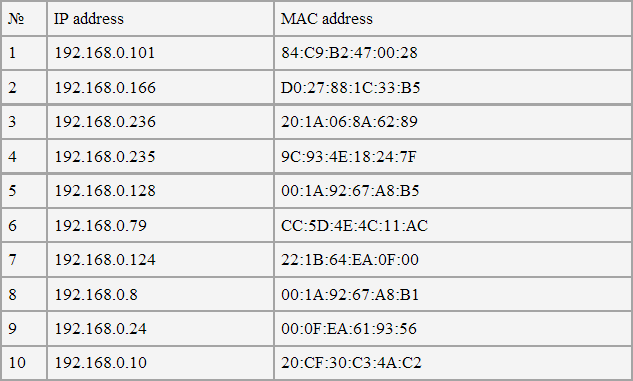
The page contains the ARP cache of the processor represented as a table.

Figure 5.3.19.2.1 ARP table

5.3.19.3 DNS table

*Statistics → DNS Table*

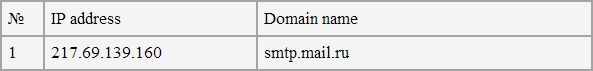
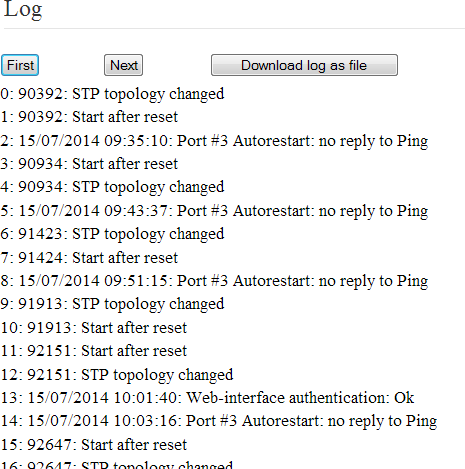
The tab contains the output of the DNS protocol: matching hostname with its IP address.

Figure 5.3.19.3.1 DNS table

5.3.19.4 System log

*Statistics → Log*

The tab contains the integration unit log. There are 10000 entries per page. In order to go to the next page, click **Next**.

To save this log in a .txt file, press **Download log as file.**

* + 1. Firmware update

Figure 5.3.19.4.1 Log

*Update/Backup → Update Firmware*

The Teleport integration unit supports firmware update. The latest firmware is always available on website tfortis.com

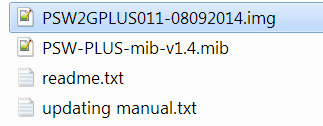
To update the firmware, download the firmware archive file. Unpack. The firmware file has a \*.img file extension.

Figure 5.3.20.1. \*.img file

In web interface, go to **Update Firmware** tab and pick a firmware file by pressing the **Browse** button.

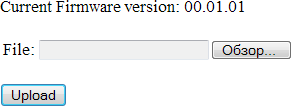


Figure 5.3.20.2. Press Browse

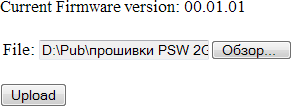


Figure 5.3.20.3. Pick a \*.img file

Press the Upload button and wait until the file is copied into device internal storage.

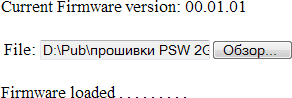


Figure 5.3.20.4. Wait when the file upload is finished

When the file is uploaded, press **Update** to update or

**Cancel** to cancel.



Figure 5.3.20.5. Press Update

After pressing Update, the update process will start. Do not reboot the integration unit, do not turn off the power.



Figure 5.3.20.6. Wait while firmware update process finishes

**Note**: the integration unit also supports updating via Telnet from an external TFTP server. For more information take a look at "Manage using Telnet" section.

* + 1. Saving and restoring settings

*Update/Backup → Backup/Recovery*

The Teleport integration unit support saving current settings to a configuration file, this file editing and restoring settings from the file.

5.3.21.1 Save settings to file

In the side menu, select Update/Backup → Backup/Recovery

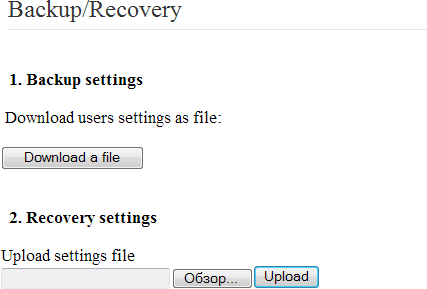


Figure 5.3.21.1.1 Save and Restore settings interface

In section 1 press the button «Download a file». You will be asked if you want to save or open the file, Save.

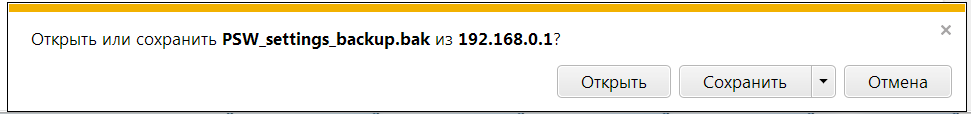


Figure 5.3.21.1.2 Saving the settings file

5.3.21.2. Restore settings from the file.

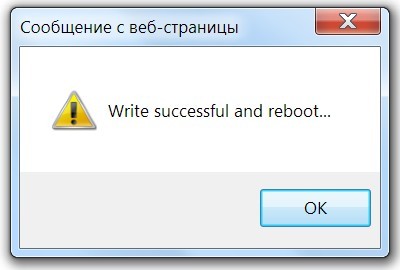
If you want to restore previously saved settings from the file, then in Update/Backup → Backup/Recovery tab, choose in section 2 (Recovery settings) \*.bak configuration file and press **"Upload"** for upload.

Figure 5.3.21.2.1 Reboot

After uploading the file, the device will reboot and the settings will be applied.

5.3.21.3 Editing configuration file

Changing the configuration file can be useful, when a group of devices has similar settings. In this case you can create a universal configuration file for these devices and change only a small set of parameters for each device, for example, the IP address. Other parameters will be taken from the configuration file.

The configuration file generated by the integration unit when saving settings to a file is a file with \* .bak extension with settings in text form.

This file can be opened with any text editor.

The structure of the records has a strictly defined form of recording. In general, it looks like this:

**#***<variable name>***=[***<variable value>***]**

**Example:** # IPADDRESS = [192.168.0.1], where the value of IPADDRESS variable is 192.168.0.1

Description of settings with default parameters is shown in Table 5.3.2.

Table 5.3.2. Configuration file variables

|  |  |
| --- | --- |
| **Сommand syntax** | **Description** |
| #IPADDRESS=[192.168.0.1] | IP address |
| #NETMASK=[255.255.255.0] | Subnet mask |
| #GATEWAY=[255.255.255.255] | default gateway |
| #USER\_MAC=[c0:11:a6:0:0:0] | user's MAC address |
| #DNS=[255.255.255.255] | IP address of the DNS server |
| #DHCPMODE=[0] | DHCP mode (0 — disabled, 1  — DHCP client) |
| #LANG=[0] | interface language (0 – English, 1 — Russian) |
| #HTTP\_USERNAME=[] #HTTP\_PASSWD=[] | login and password for the default account (**Admin** access rights) |
| #USER1\_USERNAME=[] | User name |
| #USER1\_PASSWD=[] | Account password |
| #USER1\_RULE=[0] | Access rights (0 – account disabled, 1 – Admin, 2 – User) |
| #SYSTEM\_NAME=[] | device description |
| #SYSTEM\_LOCATION=[] | device location |
| #SYSTEM\_CONTACT=[] | contact information |
| #SMTP\_STATE=[0] | SMTP protocol (0 – disabled, 1 — enabled) |
| #SMTP\_SERV\_IP=[0.0.0.0] | IP address of the SMTP server |
| #SMTP\_TO1=[] | mailing address of recipient 1 |
| #SMTP\_TO2=[] | mailing address of recipient 2 |
| #SMTP\_TO3=[] | mailing address of recipient 3 |
| #SMTP\_FROM=[] | mailing address of the sender |
| #SMTP\_SUBJ=[TFortis Teleport-1] | e-mail subject |
| #SMTP\_LOGIN=[] | login to access the mailbox |
| #SMTP\_PASS=[] | password to access the mailbox |
| #SMTP\_PORT=[25] | SMTP port |
| #SMTP\_DOMAIN\_NAME=[] | mail server domain name |

|  |  |
| --- | --- |
| #SNTP\_STATE=[0] | SNTP protocol state |
| #SNTP\_SETT\_SERV=[0.0.0.0] | IP address of SNTP server |
| #SNTP\_SERV\_NAME=[] | Domain name of SNTP server |
| #SNTP\_TIMEZONE=[0] | time zone, relative to UTC (from  -12 to +13) |
| #SNTP\_PERIOD=[10] | server synchronization period (1, 10 or 60 minutes) |
| #SYSLOG\_STATE=[0] | Syslog protocol state |
| #SYSLOG\_SERV\_IP=[0.0.0.0] | IP address of the Syslog server |
| #EVENT\_LIST\_SYSTEM\_T=[7] | event in the EventList (7 – disabled) |
| #EVENT\_LIST\_INPUTS\_T=[12] | event in the EventList (7 – disabled) |
| #EVENT\_LIST\_OUTPUTS\_T=[12] | event in the EventList (7 – disabled) |
| #SNMP\_STATE=[0] | SNMP (0 – disabled, 1 — enabled) |
| #SNMP\_SERVER=[0.0.0.0] | IP address of the SNMP Traps server |
| #SNMP\_VERS=[0] | SNMP protocol version (0 – SNMP v1, 3– SNMP v3) |
| #SNMP\_COMMUNITY1=[public] | reading community |
| #SNMP\_COMMUNITY2=[private] | writing community |
| #SNMPV3\_USER1\_LEVEL=[0] | Security level (0 — NoAuth,NoPriv, 1 – Auth,NoPriv, 2 – Auth,Priv) |
| #SNMPV3\_USER1\_USER\_NAME=[] | User name for SNMP v3 |
| #SNMPV3\_USER1\_AUTH\_PASS=[] | Auth Password for SNMP v3 |
| #SNMPV3\_USER1\_PRIV\_PASS=[] | Priv Password for SNMP v3 |
| #SNMP3\_ENGINE\_ID=[] | Engine ID for SNMP v3 |
| #TELNET\_STATE=[1] | Telnet state (0 – disabled, 1 — enabled) |
| #TFTP\_MODE=[0] | TFTP mode (0 – disabled, 1 — enabled) |

|  |  |
| --- | --- |
| #TFTP\_PORT=[69] | UDP port on TFTP |
| #SERIAL\_STATE=[1] | Enabling the RS-485 port |
| #SERIAL\_BAUDRATE=[9600] | The RS-485 port speed |
| #SERIAL\_PARITY=[0] | RS-485 parity (0 – Disable, 1 – Even, 2 – Odd) |
| #SERIAL\_DATABITS=[8] | Number of data bits |
| #SERIAL\_STOPBITS=[1] | Number of stop bits |
| #SERIAL\_MODE=[0] | Port operating mode: 0 – Disable, 1 – Pair Connection |
| #SERIAL\_REMDEV=[[1][0][0][0][0] [0][0][0]] | List of remote devices for Pair Connection port |
| #OUTPUT1\_STATE=[0] | State of output 1 (0 – short, 1 – open) |
| #OUTPUT1\_ACTION=[0] | Not used |
| #OUTPUT1\_MODE=[0] | Output management mode: 0 – Pair Connection, 1 – Manual, 2 – SNMP, 3 – Modbus |
| #OUTPUT1\_DESCR=[] | Description of output 1 |
| #OUTPUT1\_REMDEV=[0] | Remote device for output 1, if it is operating in Pair Connection mode |
| #INPUT1\_STATE=[0] | Enable input operation 1. 0 – inactive, 1 – active |
| #INPUT1\_ALARM=[1] | Not used |
| #INPUT1\_DESCR=[] | Description of input 1 |
| #INPUT1\_MODE=[1] | Operating mode of input 1. 1 – Pair Connection |
| #INPUT1\_REMDEV=[0] | Remote device for input 1 |
| #TLP1\_VALID=[1] | Entry 1 in the list of remote devices is active |
| #TLP1\_MODE=[0] | Not used |
| #TLP1\_TYPE=[0] | Type of device 1 in the list of remote devices |
| #TLP1\_DESCR=[] | Description of device 1 |

|  |  |
| --- | --- |
| #TLP1\_IP=[0.0.0.0] | IP address of device 1 |
| #TLP1\_GATE=[0.0.0.0] | Not used |
| #TLP1\_MASK=[0.0.0.0] | Not used |
| #TLP\_NET\_MODE=[0] | Not used |
| #MODBUS\_STATE=[1] | State of the Modbus protocol |
| #MODBUS\_ID=[0] | Not used |
| #MODBUS\_MODE=[2] | Operating mode: only 2-Modbus TCP |

* + 1. Reset to factory settings

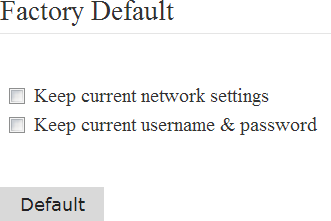
*Reboot/Default → Factory Default*

Figure 5.3.21.1 Restoring default settings

If necessary, it is possible to reset the settings to the factory settings. The resetting can be selective:

**Keep current Network settings** — Reset all settings, but keep current network settings: IP, MAC, Gateway, Mask

**Keep current username & password** — Reset all settings, but keep current access settings: Username, Password

* + 1. Reboot

*Reboot/Default → Reboot*

If necessary, Teleport can be remotely rebooted.

* + - 1. **Reboot CPU** – Rebooting the processor only.
      2. **Reboot All** – Complete reboot (processor, switching part)



Figure 5.3.22.1 Reboot

* 1. Management via Telnet

Telnet is used for remote management of equipment through the command line. Telnet uses TCP protocol and port 23. In TFortis Teleport integration units, Telnet is enabled by default. If necessary, you may disable it: go to Basic Settings → Telnet



Figure 5.4.1 Configuring Telnet

Telnet supports the following **extra modes**:

* + 1. **Short commands**. It is possible to work with short commands (you do not need to enter the command to the end).

**Example**: if you need to enter the command ***config ports 1-2 state enable***, you can reduce it to the minimum: ***co po 1-2 st en***

* + 1. **Auto-completion of commands**. The ability to press the **TAB** key

to complete the command entered.

Example: If you enter **con** and press TAB, the command will complete to **config**

* + 1. **Command history**. The history of the entered commands is available. Switching is done with the UP, DOWN keys

You can connect to the device using any terminal program. In this document, the configuration will be based on the example of Microsoft Telnet. Connect using the command "*open <IP address>*"

After connection it is required to enter login and password. Login and password for Telnet are the same as for accessing the web interface. If the login and password are not set, press Enter twice.



**Note:** if login / password were entered incorrectly 30 times in a row, access to Telnet is blocked for 1 hour.

The **#** symbol and the device name indicate that the authentication was successful and the integration unit went into configuration mode. (Access rights – **Admin**)

If you have entered the login / password for an account with limited rights, you will enter the viewing mode. (Access rights – **User**)



The list of commands can be obtained using the command "?" or "help"

The following designations are used as command arguments:

* <IP> – IP address in **XX.XX.XX.XX** format
* <STATE> – state, either **enable** or **disable**
* <VALUE> – any signed or unsigned integer
* <STRING> – text line
* <LIST> – list in the following form: **begin element-end element Example:** For outputs 1, 2, 3: **"1-3"** ; only for port 2: «**2**»

**Setting process** via Telnet includes several steps:

1. Using the subset of commands from the **config** group, the required configuration is set.
2. This configuration is saved into memory with the **save command, after which the settings are applied**

Attention:

If after setting the parameters the device is rebooted without using the **save** command, the settings will not be saved.

* + 1. Configuration example

Let's look at the process of Teleport-1 configuring. For example, we need to set the following settings:

* IP address 192.168.0.100
* Gateway 192.168.0.1

Now let's connect to the device. If the device has not yet been configured, then its IP address 192.168.0.1, login and password for access are not specified.

Let's go to the management mode



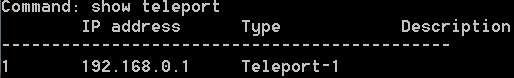
Change the IP address by the command **config ipif System ipaddress 192.168.0.100**



Add a default gateway: **config ipif System gateway 192.168.0.100**

Add a new remote device: **config teleport add 192.168.0.1**

Check that the device is added: **show teleport**

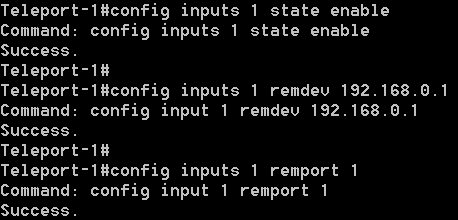


Configure input 1 for further transfer to output 1 of the Teleport-1 device from IP 192.168.0.1

config inputs 1 state enable

**config inputs 1 remdev 192.168.0.1**

**config inputs 1 remport 1**



Now the setup is complete, let's save the settings

save

* + 1. Description of Telnet commands

The integration units support the following set of Telnet commands:

1. The **config** command group:
   * ipif – network settings (IP address, subnet mask, gateway)
   * snmp – SNMP setting
   * syslog – Syslog setting
   * sntp – SNTP setting
   * smtp – SMTP setting
   * user\_account – setting user name / password
   * tftp — TFTP setting
   * events – events setting
   * description – specify the description of the device
   * inputs – setting the inputs of the expansion board
   * outputs – setting the outputs of the expansion board
   * rs485 – setting RS485
   * modbus – setting Modbus
   * teleport – setting remote devices
2. The **show** command group
   * system — summary information about the device
   * snmp — information about SNMP
   * syslog – information about SYSLOG protocol
   * sntp — information about SNTP
   * smtp — information about SMTP
   * firmware — information about current firmware version
   * arpentry — ARP table
   * tftp — information about TFTP
   * events – information about configured events
   * config – displays the entire configuration
   * inputs – information about the inputs of the expansion board
   * outputs – information about the outputs of the expansion board
   * rs485 – RS485 configuration information
   * modbus – information about Modbus configuration
   * teleport – information about remote devices
3. Firmware upgrade and configuration download from TFTP server

download

1. Save settings and system log to TFTP server

upload

1. Ping utility

ping

1. Save and apply settings

save

1. Reboot

reboot

1. Display help on commands

**help** or **?**

1. Exit Telnet management mode

exit

* + 1. config group
       1. Network settings (config ipif)
          1. IP address of the Teleport integration unit

config ipif System ipaddress <IP>

**Example:** *config ipif System ipaddress 192.168.0.100*

* + - * 1. Subnet mask.

config ipif System netmask <IP>

**Example:** *config ipif System netmask 255.255.255.0*

* + - * 1. Gateway address

config ipif System gateway <IP>

**Example:** *config ipif System gateway 192.168.0.1*

* + - * 1. Address of the DNS server

config ipif System dns <IP>

**Example:** *config ipif System dns 192.168.0.1*

* + - * 1. DHCP client mode

config ipif System dhcp <STATE>

**Example:** *config ipif System dhcp enable – DHCP client mode enabled*

* + - 1. Configuring SNMP
         1. Enabling SNMP

**config snmp state <STATE> Example:** *config snmp state enable*

* + - * 1. IP address of the server (for SNMP Traps)

config snmp host <IP>

**Example:** *config snmp host 192.168.0.1*

* + - * 1. Read Community string **config snmp read\_community <STRING> Example:** *config snmp read\_community public*
        2. Write Community string (Write Community) **config snmp write\_community <STRING> Example:** *config snmp write\_community private*
        3. Protocol version (SNMPv1 and SNMPv3 are supported)

config snmp version <VALUE> where <VALUE> : 1, 3

**Example:** *config snmp version 1*

* + - * 1. Security Level for SNMP v3

config snmp level <VALUE> where <VALUE> :

0 – NoAuth, NoPriv 1 – Auth, NoPriv

2 – Auth, Priv

**Example:** *config snmp level 2*

* + - * 1. User name for SNMP v3

config snmp user\_name <STRING>

**Example:** *config snmp user\_name administrator*

* + - * 1. Auth Password for SNMP v3 (required if the security level is Auth, NoPriv or Auth, Priv)

**config snmp auth\_pass <STRING> Example:** *config snmp auth\_pass test*

* + - * 1. Priv Password for SNMP v3 (required if the security level is Auth, Priv)

**config snmp priv\_pass <STRING> Example:** *config snmp priv\_pass test*

9. Engine ID for SNMP v3, unique identifier

config snmp engine\_id <STRING>

**Example:** *config snmp engine\_id 8000A42303C011A6050001*

* + - 1. Configuring Syslog
         1. Enabling Syslog

**config syslog state <STATE> Example:** *config syslog state enable*

* + - * 1. IP address of the server

config syslog host <IP>

**Example:** *config syslog host 192.168.0.1*

* + - 1. SNTP setting
         1. Enabling SNTP

**config sntp state <STATE> Example:** *config sntp state enable*

* + - * 1. IP address of SNTP server

config sntp primary <IP>

**Example:** *config sntp primary 192.168.0.1*

* + - * 1. Time zone (relative to UTC) **config sntp timezone <VALUE> Example:** *config sntp timezone +6*
      1. Configuring TFTP
         1. Enabling *TFTP*

**config tftp state <STATE> Example:** *config tftp state enable*

* + - * 1. configuring UDP port (by default port 69)

**config tftp port <NUM> Example:** *config config tftp port 69*

* + - 1. Configuring events

It is necessary to configure events that will be sent to the monitoring server. If Syslog protocol is used, it is also necessary to indicate event significance.

<STATE> variable takes the value enable/disable, <NUM> variable shows the significance level 0..7

* + - * 1. system events

**config events system state <STATE> level <NUM> Example:** *config events system state enable level 4*

* + - * 1. changes in the state of inputs

config events inputs state <STATE> level <NUM>

***Example:*** *config events inputs state enable level 4*

* + - * 1. changes in the state of outputs

config events outputs state <STATE> level <NUM>

***Example:*** *config events outputs state enable level 4*

* + - 1. Configuring user accounts
         1. Creating a new account

config user\_account add <USERNAME> <PASSWORD> <MODE>

where **<USERNAME>** is the user name (maximum 20 characters),

**<PASSWORD>** is the password (maximum 20 characters),

**<MODE>** is the access rights level:

admin\_rule

**user\_rule**

**Example:** *config user\_account add username password admin\_rule*

Create an administrator account with username "username" and password

"password"

* + - * 1. Editing user data

config user\_account add <USERNAME> <PASSWORD> <MODE>

where **<USERNAME>** is the user name (maximum 20 characters),

**<PASSWORD>** is the password (maximum 20 characters),

**<MODE>** is the access rights level:

admin\_rule

**user\_rule**

**Example:** *config user\_account add username password user\_rule*

"Username" account has different access rights now (User)

* + - * 1. Deleting a user

config user\_account delete <USERNAME>

**where <USERNAME>** is the user name (maximum 20 characters)

**Example:** *config user\_account delete username*

Account "username" has been deleted.

* + - 1. Configuring device description
         1. configuring device name

**config description name <STRING> Example:** *config description name psw-2g4f*

* + - * 1. configuring device location **config description location <STRING> Example:** *config description location servernaya*
        2. configuring contacts of the service company

config description location <STRING>

**Example:** *config description company superpuper-telecom*

* + - 1. Configuring inputs
         1. enable input operation

config inputs <INPUT> state <STATE>

where **<INPUT>** is the input number,

**<STATE>** is the input state:

enable – input active

disable — input inactive

**Example:** *config inputs 1 state enable*

* + - * 1. Specifying the input description

config inputs <INPUT> description <STRING>

where **<INPUT>** is the input number,

**<STRING>** is the line, description of the input

**Example:** *config inputs 1 description some\_name*

* + - * 1. Specifying a remote device for the input

config inputs <INPUT> remdev <IP>

where **<INPUT>** is the input number,

**<IP Address>** – IP address of the remote device

**Note:** First add the remote device to the list (***config teleport add ..***). If you add a device with an unknown IP address, an error will occur.

**Example:** *config inputs 1 remdev 192.168.0.2*

* + - * 1. Specifying the output port of the remote device

config inputs <INPUT> remport <NUM>

where **<INPUT>** is the input number,

***<NUM>*** *– the number of the remote device output to which the input state will be broadcast*

**Example:** *config inputs 1 remport 5*

* + - * 1. Inversion of the input state

config inputs <INPUT> inverse <STATE>

where **<INPUT>** is the input number,

***<STATE>*** *– the state of the input inversion*

enable – input inverted

*disable* – input is not inverted, normal mode

**Example:** *config inputs 1 inverse enable*

* + - 1. Configuring outputs

1. Setting the initial state of the output in the manual mode

config outputs <OUTPUT> state <STATE>

where **<OUTPUT>** is the output number,

**<STATE>** is the output state:

* + short — closed
  + open – open

**Example:** *config outputs 1 state short*

1. Configuring the output management mode **config outputs <OUTPUT> mode <STATE>** where **<OUTPUT>** is the output number,

**<STATE>** – operating mode:

* + pair – Pair Connection mode**/**"Pair connection", the input state from the remote Teleport can be broadcast to the ouput
  + manual – manual control mode.
  + snmp – the output is controlled only via the SNMP protocol
  + modbus – the output is controlled only via the Modbus TCP protocol

**Example:** *config outputs 1 mode pair*

1. Configuring the output description

config outputs <OUTPUT> description <STRING>

where **<OUTPUT>** is the output number,

**<STRING>** is the line, description of the input

**Example:** *config outputs 1 description some\_name*

1. Specifying the remote device for the output (if the output is operating in "pair connection" mode)

config outputs <INPUT> remdev <IP>

where **<OUTPUT>** is the output number,

**<IP Address>** – IP address of the remote device

**Note:** First add the remote device to the list (***config teleport add ..***). If you add a device with an unknown IP address, an error will occur.

**Example:** *config outputs 1 remdev 192.168.0.2*

* + - 1. Configuring RS485

1. Port speed

config rs485 baudrate <BR>

where **<BR>** is the speed, selected from 1200, 2400, 4800, 9600, 14400, 19200,

38400, 57600, 115200

**Example:** *config rs485 baudrate 9600*

1. Checking parity

config rs485 parity <PARITY>

where **<PARITY>** is parity check

* + disable – checking disabled
  + even — even
  + odd — odd

**Example:** *config rs485 parity even*

1. Number of data bits

**config rs485 databits <DATABITS>** where **<DATABITS>**  is the number of data bits  **Example:** *config rs485 databits 7*

1. Number of stop bits

config rs485 stopbits <STOPBITS>

where **<STOPBITS>** is the number of stop bits

**Example:** *config rs485 databits 1*

1. Port operating mode

config rs485 mode <STATE>

where ***<STATE>*** is the operating mode

* + disable – port disabled
  + translate – the port is operating in the transfer mode

*Example: config rs485 mode translate*

1. Adding remote devices

config rs485 remdevs add <IP>

*where* ***<IP>*** *is the IP address of the remote device Example: config rs485 remdevs add 192.168.0.1*

1. Deleting the remote device

config rs485 remdevs del <IP>

*where* ***<IP>*** *is the IP address of the remote device Example: config rs485 remdevs del 192.168.0.1*

* + - 1. Configuring Modbus

1. Protocol state

config modbus state <STATE>

where ***<STATE>*** is the operating mode

* + disable – protocol disabled
  + enable – protocol enabled

*Example: config modbus state enable*

* + - 1. Setting the list of remote devices

1 Adding remote devices

config teleport add <IP>

*where* ***<IP>*** *is the IP address of a new remote device Example: config teleport add 192.168.0.1*

1. Deleting the remote device

config teleport del <IP>

*where* ***<IP>*** *is the IP address of the remote device Example: config teleport del 192.168.0.1*

* + 1. Show group

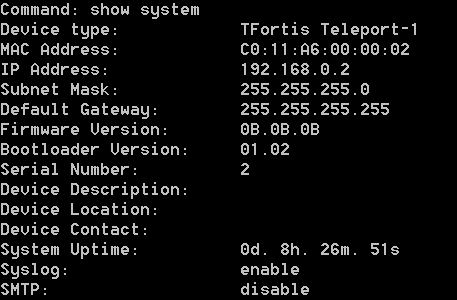
Possible commands:

* + - * system — summary information about the device
      * snmp — information about SNMP
      * syslog – information about SYSLOG protocol
      * sntp — information about SNTP
      * smtp — information about SMTP
      * firmware — information about current firmware version
      * arpentry — ARP table
      * tftp — information about TFTP
      * events – information about configured events
      * config – displays the entire configuration
      * inputs – information about the inputs of the expansion board
      * outputs – information about the outputs of the expansion board
      * rs485 – RS485 configuration information
      * modbus – information about Modbus configuration
      * teleport – information about remote devices

All commands in this group can be divided into several subgroups:

* + - * + View summary information
        + View settings
      1. View summary information
         1. Display full information about the device and its configuration

show system



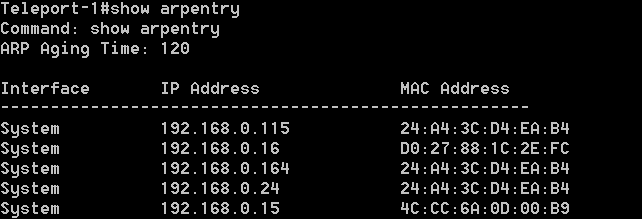
* + - * 1. Display information about integrated firmware

show firmware



* + - * 1. Display ARP table

show arpentry



* + - 1. View the settings of the Teleport integration unit
         1. Display information about SNMP

show snmp

For SNMP v1:



For SNMP v3:

* + - * 1. Display information about Syslog protocol

show syslog



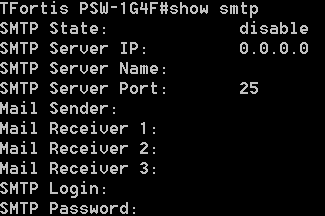
* + - * 1. Display information about SNTP settings

show sntp



* + - * 1. Display information about SMTP settings

show smtp



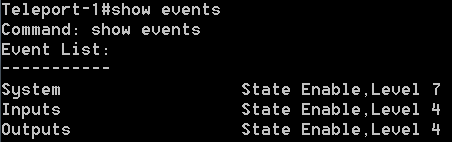
* + - * 1. Display information about TFTP settings

show tftp



* + - * 1. Display information about event list setting

show events



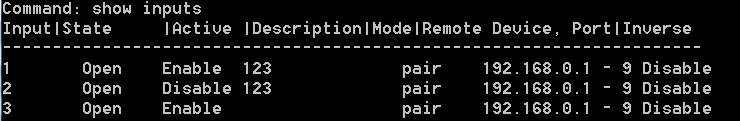
* + - * 1. Display full configuration (information is displayed in the same form as the configuration file)

show config



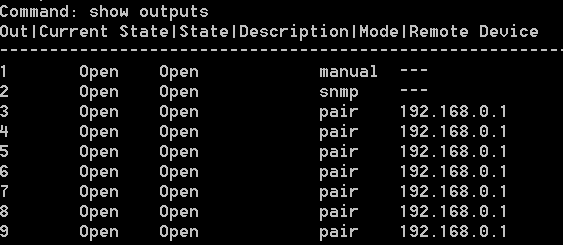
* + - * 1. Information about the state of inputs

show inputs



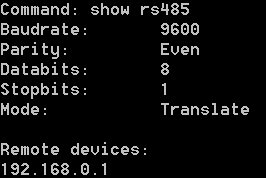
* + - * 1. Information about the state of outputs

show outputs



* + - * 1. RS485 configuration information

show rs485



* + - * 1. Modbus configuration information

show modbus



* + - * 1. Information about remote devices

show teleport



* + 1. Firmware update using TFTP

TFortis Teleport integration units support firmware update via Telnet using the external TFTP server.

Command for firmware update:

download firmware\_fromTFTP <IP> <PATH>

where **<IP>** is the IP address of the TFTP server

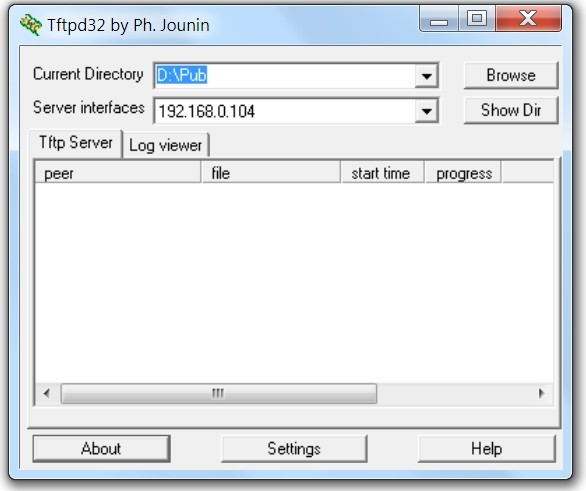
**<PATH>** is the path to the firmware file

Let's consider the update process in detail.

1. First make sure, that the TFTP server has been started. If not, start it. A common application for Windows OS is Tftpd32. That is why we will consider the update process based on Tftpd32.

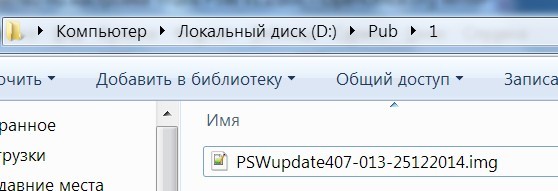
The distribution file is available on the website: <http://tftpd32.jounin.net/tftpd32.html>

Start in TFTP server mode



As you can see, the TFTP server will be accessible at the address 192.168.0.104, and the root directory of the server is D:\Pub

1. We put the firmware file in the root directory of the server
2. On the server side, everything is ready, let's proceed to the switch settings.



By default, the TFTP protocol on the integration units is disabled, enable it using the following command:

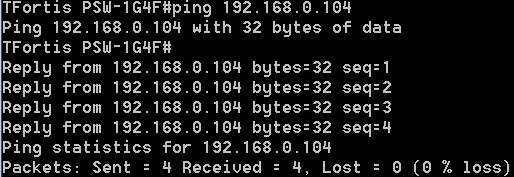
config tftp state enable



The protocol support will be enabled. In order to save this setting in the non-volatile memory, we execute the **save** command, otherwise after the reboot this setting will not be saved.

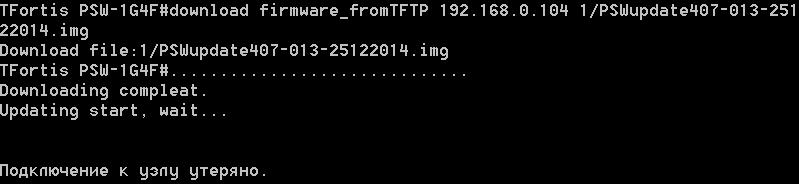


Check that Teleport "sees" the TFTP server. To do this, you can ping

192.168.0.104

1. Proceed to update. Enter the command:

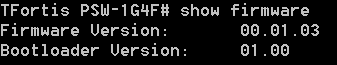
**download firmware\_fromTFTP 192.168.0.104 1/PSWupdate407-013-25122014.img** The file will start uploading the file to the internal memory, after that the update process will start



After that the integration unit will update the firmware and reboot, and

the Telnet connection will be interrupted.

The update process lasts about 1 minute. After that, you can reconnect via Telnet and check the firmware version, making sure that the update was successful.



* + 1. Saving and loading configuration and log via TFTP

Teleport supports saving current settings to a configuration file, this file editing and restoring settings from the file.

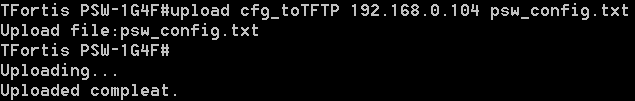
* + - 1. Saving configuration

Configuration is saved to the specified TFTP server

upload cfg\_toTFTP <IP> <PATH>

where **<IP>** is the IP address of the TFTP server

**<PATH>** is the name and path of configuration



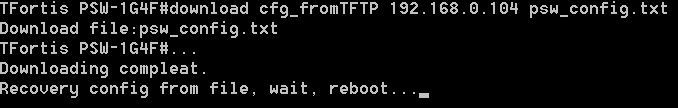
* + - 1. Restoring configuration

Configuration is restored from the specified TFTP server

download cfg\_fromTFTP <IP> <PATH>

where **<IP>** is the IP address of the TFTP server

**<PATH>** is the path to the configuration file



After configuration is installed, the integration unit will restart with the new settings.

* + - 1. Saving system log

In some cases, it may be necessary to save the log of the device for later analysis.

upload log\_toTFTP <IP> <PATH>

where **<IP>** is the IP address of the TFTP server

**<PATH>** is the path to the configuration file

* + 1. Saving settings

Saving settings to a non-volatile memory.

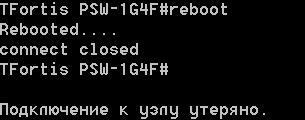
Save



* + 1. Reboot

The integration unit is rebooted

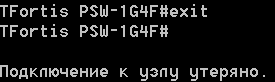
reboot



* + 1. Exit the management mode

Exit Telnet management mode

exit



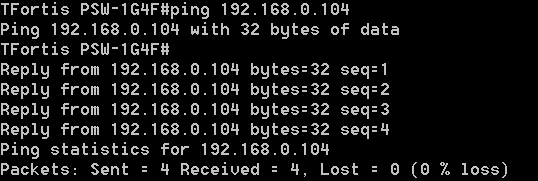
* + 1. Diagnostic functions

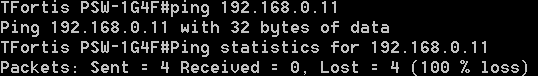
5.4.10.1 Ping utility

It allows to ping the remote node

ping <IP>

where **<IP>** is the node IP address

If the node is available:

If the node is not available:

1. Troubleshooting

Table 6. Malfunction list and diagnostics

|  |  |
| --- | --- |
| Problem occurred | Problem solution |
| Device is not working, no RUN indication | 1. For Teleport-1:   Check the presence of power supply   1. For Teleport-2   Check the connection to PoE switch, check PoE indicator. If it’s off make sure that the PoE switch can provide power according to IEEE 802.1af standard, option A (for pairs with data: 1-2, 3-6) |
| Errors in RS-485 transfer | For diagnostic open *Statistics->Main Statistics* using web-interface.     1. verify that data is being received on the RS-485 interface: the RX cnt field (the number of received packets on the interface) should be increased when the interface is active. If the field does not change, check the settings of the RS-485 port, physical connection to the port. 2. RX mngmt frames and TX mngmt frames fields are counters of received and sent UDP control packets. If only RS-485 transfer is configured, then the RX mngmt frames and TX Cnt counters should match. The TX mngmt frames and RX Cnt counters should match. The values ​​of RX mngmt frames and TX mngmt frames, RX cnt and TX cnt can be the same when a device connected to the local RS-485 port answers all requests from the remote port. In the case an address protocol is used, for example, Orion, Modbus RTU, the local device can only respond to requests with its own address, so the value of the TX cnt field can be greater than RX cnt. 3. To check the Ethernet connection between two devices, you need to compare the RX mngmt frames and TX mngmt frames counters.   If the counter RX mngmt frames of one device is equal to TX mngmt frames of another device and vice versa, then we consider that there are no problems in the Ethernet lines. |
| Errors in RS-485 transfer: polling timeout exceeded  (Single-code communication) | In the RS-485 - Ethernet transfer mode delays inevitably occur during data transmission. For the correct operation of the entire system you need to correctly calculate the delays and configure timeouts.  If the transmission delays are greater than the established response timeout, this will lead to either partial or complete discarding of the packets, and as a result, the system will not work.  Calculation of transfer delays when transmitting via Teleport unit  *t = 15000 ∗ length / baudrate + 1*  t - delay in milliseconds that occurs when transmitting via Teleport unit  length - packet length in RS-485 protocol in bytes, if this specification is not in the protocol specification then use the value 128.  baudrate - port speed  When transmitting RS-485 via Ethernet, 4 conversions occur (RS-485 → Ethernet and vice versa)  Therefore, it is necessary to set the response timeout longer than the estimated delay:  *T≥4 ∗ t + δ*  T - timeout  t - delay during conversion  δ - some margin |
| 24V indicator is flashing | The flashing 24V indicator on the Teleport-2 unit board indicates an overload or short circuit on the 24V output. Disconnect the powerful load from the output. |

1. Warranty

Warranty period for the device – 36 months from the sale date. The device is accepted for warranty maintenance and repair only in full completeness.

Warranty repair is not performed in following cases:

* if warranty period has expired;
* if there is no label with serial number on the product housing, and also if serial number was changed, removed or illegible;
* if there are external and internal mechanical damages (chips, cracks, deformation, damage to the power cord, breaks and cracks of connectors), traces of chemicals, corrosive environments, liquids, heavy contamination, as well as the presence of insects or traces of their presence;
* due to non-compliance with the rules of connection and operation, as well as non-compliance of power specified in the operating manual;
* due to force majeure, third party action and other reasons that doesn’t depend on manufacturer.

1. Technical support

To get technical support for the design of systems, operation and adjustment of equipment:

* call (8 a.m. to 4 p.m. Moscow time) +7 (342) 260 20 30
* e-mail at:

[tfortis@fort-telecom.ru](mailto:tfortis@fort-telecom.ru)

* use Help-Desk

<http://support.fort-telecom.ru/>

All technical documents are available at: <http://www.tfortis.com>

If you have any ideas for improvement or creating new devices, you can send us a request at [tfortis@fort-telecom.ru](mailto:tfortis@fort-telecom.ru)