

# Firmware version 2.4.6 WB-2P-LR2. User manual

User station  
WB-2P-LR2  
User manual, firmware version 2.4.6

IP address: <http://192.168.1.1>  
Login: admin  
Password: password

## Introduction

### Annotation

Modern tendencies of telecommunication development necessitate operators to search for the most optimal technologies, allowing you to satisfy drastically growing needs of subscribers, maintaining at the same time consistency of business processes, development flexibility and reduction of costs of various services provision. Wireless technologies are spinning up more and more and have paced a huge way for a short time from unstable low-speed communication networks of low radius to broadband networks equitable to speed of wired networks with high criteria for the quality of provided services.

WB-2P-LR2 is a user station designed for connection to Wi-Fi access network which might be constructed using base stations within long distances. The case of WB-2P-LR2 is sealed, that is allows to install the device outdoor with different climate conditions.

This manual specifies intended purpose, main technical parameters, design, installation procedure, safe operation rules and installation recommendations for WB-2P-LR2.

### Symbols

#### Notes and warnings



Notes contain important information, tips or recommendations on device operation and setup.



Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

## Device description

### Purpose

User station WB-2P-LR2 (herein after 'the device') is designed for access provision to secure wireless network.

WB-2P-LR2 connects to a base station via Wi-Fi technology and operates at 2.4 GHz (the frequency range – 2402–2482 MHz). The device is supposed to operate with WOP-2ac-LR2. WB-2P-LR2 might be also used for wireless bridge organization.

WB-2P-LR2 supports up-to-date requirements to service quality and allows transmitting more important traffic in higher priorities queues. Prioritization is based on QoS technologies: CoS (special tags in VLAN packet field) and ToS (tags in IP packet field).

The device is capable to operate in wide temperature range and in high-humidity conditions (parks, factories, stadiums, etc.).

Power to the device is supplied via Passive PoE technology 24V.

### Device specification

#### Interfaces:

- 1 port of Ethernet 10/100/1000BASE-T (RJ-45);
- Wi-Fi 2.4 GHz IEEE 802.11b/g/n.

The power is supplied via PoE injector 24V connected to 220V network.

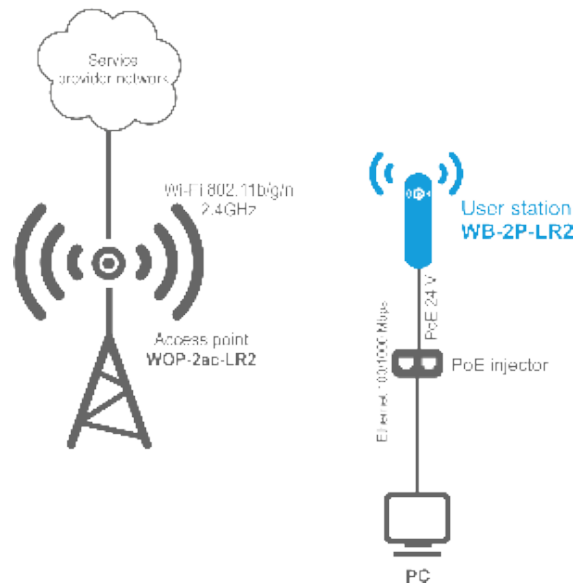


Do not use an injector with voltage different from 24V so as not to break down the device!

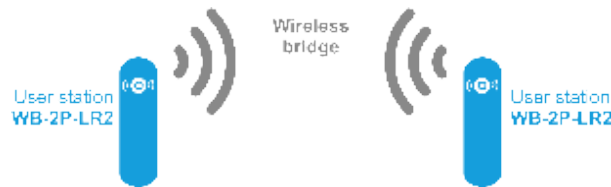
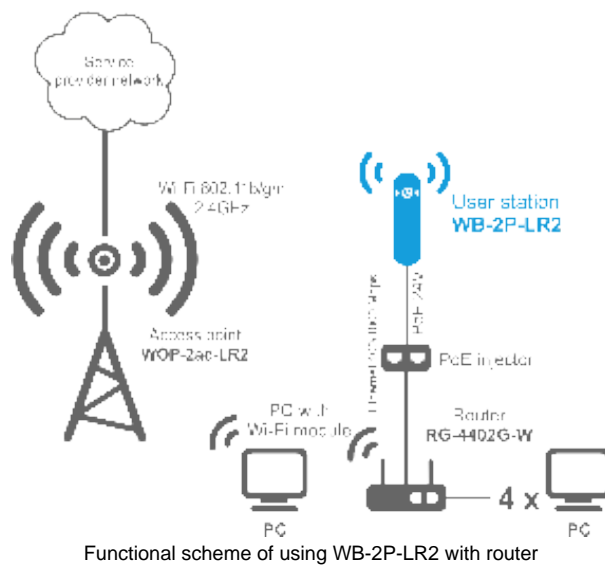
### Network functions:

- operating in bridge and router modes;
- operating in 'Wi-Fi Station' and 'Wireless bridge' modes;
- support for VLAN Trunk;
- support for Management VLAN;
- support for General VLAN;
- support for Transparent Mode;
- static routing;
- support for Transparent wireless bridge function;
- support for PPPoE client;
- time synchronization via NTP;
- support for static address and DHCP (DHCP client on WAN side, DHCP server on LAN side);
- support for DNS;
- support for D-DNS;
- support for NAT;
- support for UPnP;
- firewall;
- support for cloning of MAC address on WAN interface;
- support for quality of service mechanisms (QoS through DSCP and 802.1P).
- support for IPTV functions (IGMP-proxy, UDP-to-HTTP proxy);
- firmware update via web interface;
- support for DHCP-based autoprovisioning;
- support for TR-069;
- remote monitoring, configuration and setup: SNMP, web interface, Telnet, SSH.

The figures below illustrate applications schemes of WB-2P-LR2.



Functional scheme of using WB-2P-LR2 without router



## Technical features

Table 1 shows main specifications of the device.

Table 1 – Main specifications

LAN Ethernet interface parameters	
Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100/1000, auto-negotiation
Standards	BASE-T
Wireless interface parameters	
Standards	802.11b/g/n
Frequency range	2402–2482 MHz
Modulation	DSSS, CCK, BPSK, QPSK, 16QAM, 64QAM
Speed of data transmission	<b>802.11b:</b> up to 11 Mbps <b>802.11g:</b> up to 54 Mbps <b>802.11n:</b> up to 300 Mbps
Maximum output power of the transmitter	<b>2.4 GHz:</b> 26 dBm
Receiver sensitivity	<b>2.4 GHz:</b> -98 dBm
Security	64/128/152-bit WEP encryption, WPA/WPA2, centralized authorization via RADIUS server (WPA/WPA2 Enterprise)
Antenna's parameters	

Gain	2x10.5 dBi
Polarization	dualpolarized antenna
Beam angle (horizontal polarization)	60°
Beam angle (horizontal polarization)	40°
SWR	2.0 max.
Impedance	50 Ohm
Front to back ratio	> 20 dB
<b>Control</b>	
Remote control	web interface, Telnet, SSH, SNMP (monitoring), TR-069
Access restriction	by password
<b>General parameters</b>	
Processor	Realtek RTL8197FS 1 GHz
RAM	128 MB
Flash	32 MB
Power supply	Passive PoE 24 V
Power consumption	9 W max.
Operating temperatures	from -45 to +65°
Operating humidity	95% max.
Ingress Protection Marking	IP54
Dimensions	80x66x282 mm
Weight	0,35 kg

## Design

WB-2P-LR2 housed in a plastic case, industrial version. The size of the device: 80x66x282 mm.

The layout of WB-2P-LR2 is shown in the figure below.



WB-2P-LR2 layout

LAN port 10/100/1000Base-T (RJ-45 connector) for local network connection and power supply via PoE, grounding connector and the button for resetting to factory settings ('Reset') are located on the bottom panel of the device.



WB-2P-LR2 bottom panel's elements

## Light indication







The light indication panel of WB-2P-LR2 is shown below.



WB-2P-LR2 light indication panel

The current state of the device is shown with the help of light indicators located on the back panel of WB-2P-LR2. The list of indicators and their description is shown in the table below.

Table 2 – Description of rear panel LED indicators

	LED	LED status	Description
	<b>Power</b> – Device power and operation status LED	solid green	the device power supply is enabled, normal operation
		solid orange	the device is loaded but IP address is not received via DHCP
		solid red	the device is loading
	<b>LAN</b> – LAN interface indicator	solid green (10, 100 Mbps)/solid orange (1000 Mbps)	the channel between LAN interface of WB-2P-LR2 and connected device is active
		flashes	packet data transmission between LAN interface of WB-2P-LR2 and connected device
	<b>WLAN</b> – received signal strength indicator (RSSI)	solid red	the device is connected to a base station. The base station signal level is more than -98 dBm
		solid yellow	the device is connected to a base station. The base station signal level is more than -80 dBm
		solid green	the device is connected to a base station. The base station signal level is more than -70 dBm
		solid green	the device is connected to a base station. The base station signal level is more than -60 dBm
		none of the indicators is on	the device is not connected to the base station

## Reset to the default settings

There are two ways to reset the device to factory settings:

1. Using 'Reset' button on the device. When the device is loaded, press and hold 'Reset' button located on the bottom panel (approximately 10–15 seconds) until 'Power' indicator is flashing orange.
2. Using PoE injector supplied with the device. When the device is loaded, press and hold 'RST' button of the injector (approximately 10–15 seconds) until 'Power' indicator of WB-2P-LR2 is flashing orange.

Device will be rebooted automatically. DHCP client will be launched by default. If the address is not received via DHCP the device will have IP address — *192.168.1.1*, subnet mask — *255.255.255.0*, User Name/Password to access via Web interface: admin/password.

## Delivery package

The basic supply package of WB-2P-LR2 includes:

- User station WB-2P-LR2;
- Mounting kit: 2 clamps for attaching;
- PoE injector 24 V;
- Patch cord RJ-45, 5e cat. 1.5 m;
- Cord for europlug - C13-F-1.8 m;
- Sheet with light indication description;
- Conformity certificate;
- Technical passport.

A bracket with horizontal and vertical adjustment might be included to the supply package upon a request.

## Installation order

This section defines safety rules, installation recommendations, setup procedure and the device starting procedure.

### Safety rules

1. Do not open the device case. There are no user serviceable parts inside.
2. Do not install the device during a thunderstorm. There is a risk of lightning stroke.
3. You must follow requirements for voltage, current and frequency specified in the user manual.
4. Measuring devices and computer must be grounded before connecting to the device. The electric potential difference between devices' cases should not exceed 1 V.
5. Make sure that all the cables are intact and they are reliably attached to connectors.
6. You should satisfy established standards and requirements for working at height during the device installation on the high-rise constructions.
7. The device exploitation should be performed by specially prepared engineering and technical personnel.
8. Connect only to operational service equipment.

### Installation recommendations

1. Recommended location for device installation: communications mast/pole.
2. Before you install and enable device, check the device for visible mechanical defects. If defects are observed, you should stop the device installation, draw up corresponding act and contact the supplier.
3. Install the device vertically on communications mast or pole in the way that the LAN port is pointed down.
4. In order to provide better receiving signal level, the sectoral antenna of a base station should be in line of sight of WB-2P-LR2. You may achieve the highest signal level by antenna alignment with the help of RSSI indicators.
5. The transmitting part of the device is located on the other side from brackets. This area should be directed to base station sectoral antenna.

After adjusting, make sure that level of the received signal from the base station should be no more than  $-65 \div -70$  dBm.



**Install the device on communications mast/pole so that the device is directed to base station sectoral antenna as much as possible. There should also be direct visibility to the base station.**

## WB-2P-LR2 mounting

### Pre-tuning

Before installing, proceed pre-tuning of the device (see section [Configuration example](#)). For this, power on the device (paragraph 2-7, section [Mounting algorithm](#)) and follow the instructions given in the section [Configuration example](#). Make sure that the user station connects required wireless network: RSSI indicators should be on.

### Mounting order

1. Install the device on communications mast/pole pointing LAN port down as it is shown on the figure below. Attach the device using clamps supplied in the device package. Comply the safety rules and recommendations given in [Safety rules](#) and [Installation recommendations](#).



2. Remove the bottom cover which close LAN-port. Ground the device through a grounding connector.



3. Connect Ethernet cable to LAN port.



4. Close the bottom cover.
5. Connect Ethernet cable connected to WB-2P-LR2 to PoE port of injector.



6. Connect Ethernet cable of your LAN network or PC to LAN port of PoE injector.





7. Connect PoE injector to 220V socket with the help of power line cord.



8. Align the position of the device for best signal level receiving. The level of received signal is shown by the indication located on the back panel of the device.
9. Fasten the clamps.

## Switching on

1. Plug the injector into 220 V outlet. Connect a PC to LAN port of the injector.
2. WB-2P-LR2 loads in a minute after switching on. Connect to the web configurator of WB-2P-LR2 through a browser.

✓ IP address by default: 192.168.1.1.  
Login: *admin*, password: *password*.

3. Network configuration is described in section [5.1 The 'Network' menu](#).

## Managing the device through web configurator

### Getting started

To start, you need to connect the device through a browser:

1. Open a web browser (web-page explorer), for example, Firefox, Opera, Chrome.
2. Enter IP-address of the device to the browser address line.

✓ IP address by default: 192.168.1.1, subnet mask: 255.255.255.0. The device is capable to obtain an IP address via DHCP.

If connection is successful, request form with user name and password will be displayed on a browser window.

Login:

Enter login

Password:

Enter password

✓ Log In

✔ Factory settings: login: *admin*, password: *password*.

- Enter your username into 'Login' and password into 'Password' field. Click the 'Log in' button. Device Web configurator home page will be opened in the browser window.

WB-2P-LR2

admin

Test Changes
EN
Logout

Monitoring
Network
System

Internet
Ethernet Ports
ARP
PPPoE Relay
Device
Conntrack
Routes

Internet Connection

Network Connection	Wi-Fi Client
Connection Status	Authenticated
SSID	WOP-2ac-LR2
Access Protocol	DHCP
IP Address	100.110.0.243
Link Capacity	31
Link Quality	69 (not changed)
Link Quality Common	69
RSSI Vertical/Horizontal	-42/-39 dBm
SNR	48/53 dB
TxRate	39 Mbit/s
RxRate	117 Mbit/s

Refresh

✔ You may select languages on the top-right of the page. Russian and English languages are available for WB-2P-LR2.

WB-2P-LR2

admin

Test Changes
EN
Logout

Monitoring
Network
System

Internet
Ethernet Ports
ARP
PPPoE Relay
Device
Conntrack
Routes

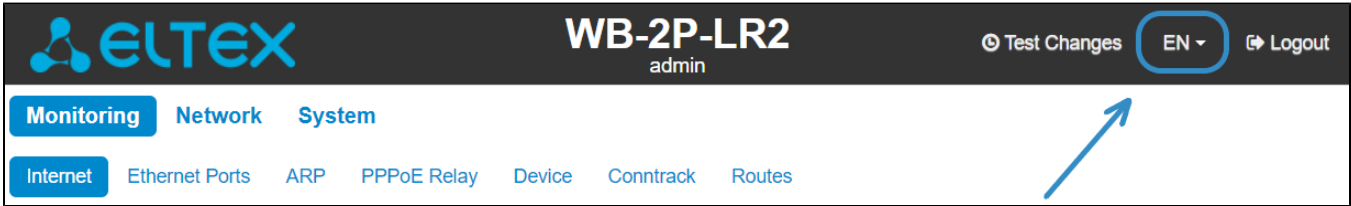
Internet Connection

Network Connection	Wi-Fi Client
Connection Status	Authenticated
SSID	WOP-2ac-LR2
Access Protocol	DHCP
IP Address	100.110.0.243
Link Capacity	31
Link Quality	69 (not changed)
Link Quality Common	69
RSSI Vertical/Horizontal	-42/-39 dBm
SNR	48/53 dB
TxRate	39 Mbit/s
RxRate	117 Mbit/s

# Changing user

There are two user types for the device: **admin** and **viewer**:

- **admin** (password by default: **password**) has the full access to the device: read/write any settings, full device status monitoring.
- **viewer** may only view full device configuration without editing privileges; may access full device status monitoring.



When you click the «Logout» button, the current user session will be terminated; login window will be displayed:

A login window form with two input fields: 'Login:' with a placeholder 'Enter login' and 'Password:' with a placeholder 'Enter password'. Below the fields is a blue button with a checkmark icon and the text 'Log In'.

To change the access, you should specify the corresponding username and password and click the *Log in* button.

## Applying configuration and discarding changes

### 1. Applying configuration

Press 'Apply' to save configuration to flash memory and apply new settings. All the settings come into operation without device rebooting.

The visual indication of the settings applying is realized in the web interface.  
The visual indication of the settings applying:

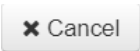
Image	State description
	After clicking 'Apply', the process of settings saving to device memory is launched. This is indicated by the  icon in the tab name and on the Apply button.
	Successful settings saving and application are indicated by the  icon in the tab name.
	If any parameter value have been set incorrectly, the error notification with description will be displayed after pressing 'Apply' button. The  mark will be displayed next to the tab name and on 'Apply' button.



The 'Apply' button in the menu appears as follows:

### 2. Discarding changes

You can discard changes only before clicking the 'Apply' button. If you click the 'Apply' button, all the changed parameters will be applied and saved to device memory. You will not be able to return to previous configuration after clicking 'Apply'.



The button for discarding changes appears as follows:

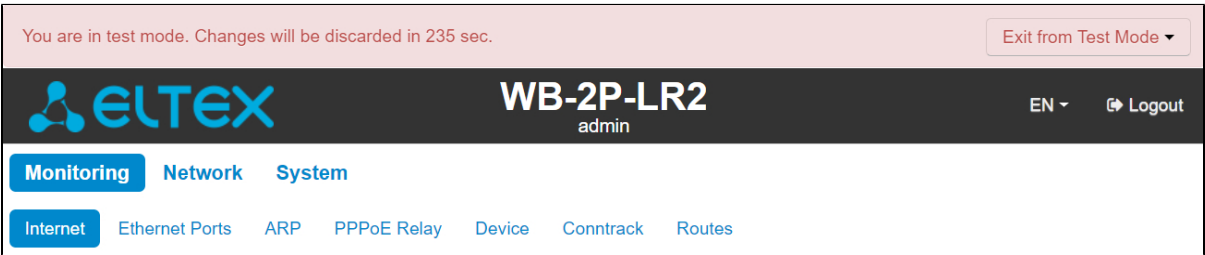
## Test changes mode

The device has a test mode for a test configuration application.

To activate it, press the 'Test changes' button on the top panel of the web interface.



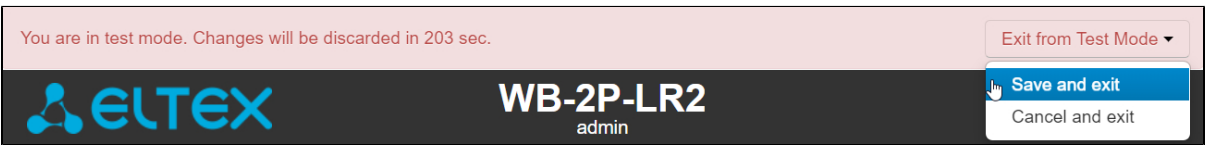
Test mode operating time is 300 seconds (5 minutes). During this time you can navigate through the web configurator tabs and make any changes by applying them on each page using the 'Apply' button.



After checking the required configuration, press the 'Exit from Test Mode' button and select the desired action:

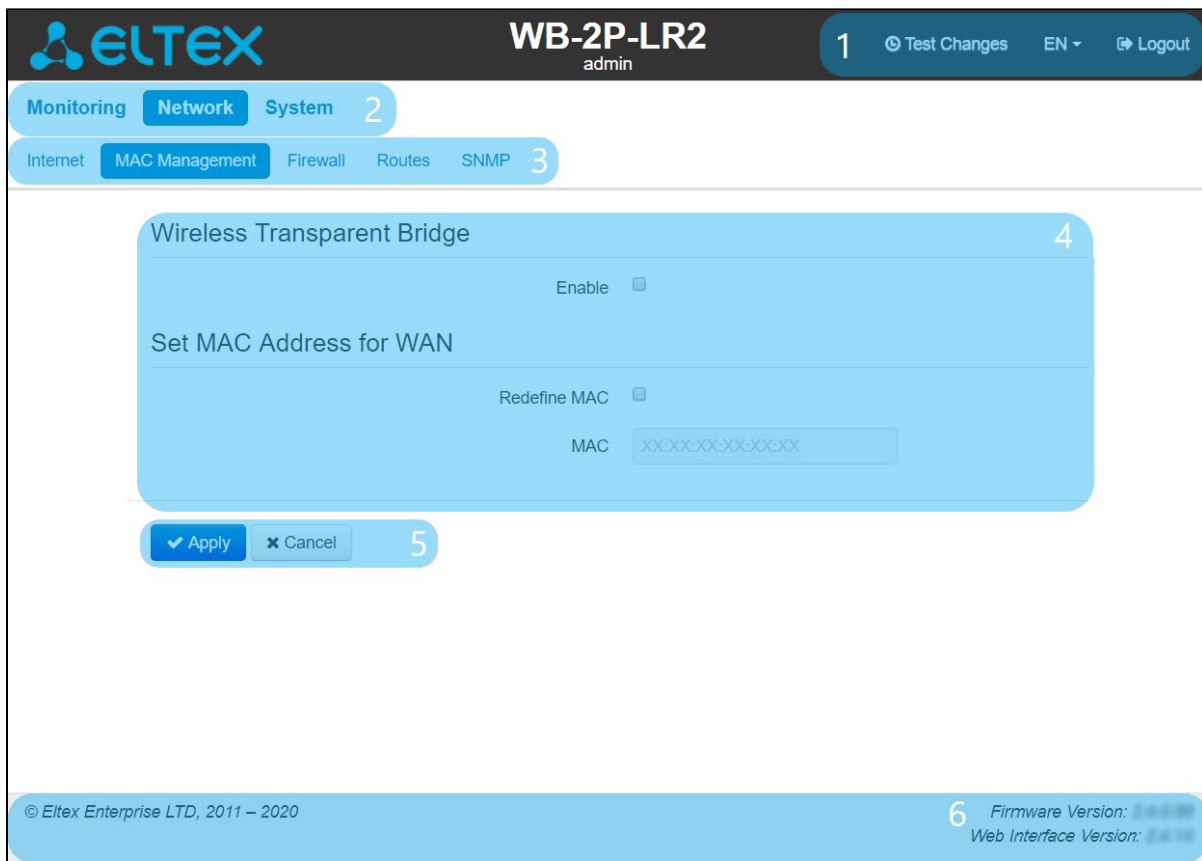
- 'Save and exit' – pressing this button will exit the test mode and save to the non-volatile memory all configuration changes that were made and applied in this mode. It will be impossible to undo changes made in the test mode.
- 'Cancel and exit' – pressing will exit the test mode and cancel all changes made in this mode. The configuration in effect on the device before the test mode is activated will be restored.

If the administrator does not exit the test mode within 300 seconds, this will happen automatically along with a rollback of all changes that have been made in this mode. After the specified time, the configuration will be restored even if access to the device is lost as a result of the changes made.



## Main elements of the web interface

The figure below shows navigation elements of the web configurator.



The user interface is divided into seven areas:

1. Username, which was used to enter the system and 'logout' button to finish the user session.
2. Menu tabs which contain submenu tabs are divided into categories: **Monitoring, Network, IPTV, System**.
3. Submenu tabs manage the settings field below.
4. Settings field, which is based on the user select. The field is dedicated to view device settings and setting configuration data.
5. Configuration management buttons, the detailed description is given in section [Applying configuration and discarding changes](#).
6. Information field. The field contain information on firmware version and web interface version.


## The 'Monitoring' menu

To move to monitoring mode, select 'Monitoring' on the left panel.

Some pages are not updated automatically. To obtain current information from the device, click the [Refresh](#) button.

## The 'Internet' submenu

In the Internet submenu, you may view main network settings of the device.



**WB-2P-LR2**  
 admin

Test Changes
 EN
 Logout

Monitoring
 Network
 IPTV
 System

Internet
 Ethernet Ports
 DHCP
 ARP
 PPPoE Client
 Device
 Conntrack
 Routes

### Internet Connection

Network Connection	Wi-Fi Client
Connection Status	Authenticated
SSID	WOP-2ac-LR2
Access Protocol	DHCP
IP Address	100.110.0.243
Link Capacity	46
Link Quality	64
Link Quality Common	56
RSSI Vertical/Horizontal	-40/-38 dBm
SNR	32/34 dB
TxRate	39 Mbit/s
RxRate	78 Mbit/s

Refresh

#### Internet Connection

- *Network connection* – the parameter shows the type of connection to external network;
- *Connection Status* – the parameter shows state of connection to external network;
- *SSID* – a name of wireless network, to which the device is connected;
- *Access Protocol* – protocol, used for network access;
- *IP address* – device IP address in external network;
- *Link Capacity* – parameter that reflects the effectiveness of the use of a modulation by the device on the transmission. It is calculated based on the number of packets transmitted on each modulation, and the reduction factors. The maximum value is 100% (means that all packets are transmitted at maximum modulation for the maximum nss type supported by the device). The minimum value is 2% (in the case when the packets are transmitted to the modulation nss1mcs0 for the device with MIMO 3x3 support). The parameter value is calculated for the last 10 s;
- *Link Quality* – parameter that displays the status of the link, calculated based on the number of sent retransmit packets. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent). The parameter value is calculated for the last 10 s;
- *Link Quality Common* – parameter that displays the status of the link, calculated based on the number of sent retransmit packets. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent). The parameter value is calculated for the entire connection time;
- *RSSI Vertical/Horizontal* – level of signal received from base station, dBm;
- *SNR* – signal/noise ratio, dB;
- *TxRate* – data rate of transmission, Mbps;
- *RxRate* – data receive rate, Mbps.

Press 'Refresh' button to update the page.

### The 'WDS' submenu



The 'WDS' submenu is available only in the 'Wireless bridge' mode.

You may view radio interface settings and wireless bridge state in the WDS submenu

Monitoring

Network

System

Internet

WDS

Ethernet Ports

ARP

Device

Conntrack

Routes

Radio

Channel

1

Channel Bandwidth

20 MHz

Network Mode

80211bgn

WDS

MAC	Client Name	IP Address	Link Capacity	Link Quality	Link Quality Common	RSSI	SNR	Uptime	TxRate	RxRate
E0:D9:E3:49:C1:80	WB-2P-LR2	10.24.80.74	30	73	56	-63	21	3 min 40 s	58.5 Mbit/s	39.0 Mbit/s

#### Radio:

- *Channel* – a channel of wireless bridge;
- *Channel Bandwidth* – channel bandwidth used for wireless bridge;
- *Network mode* – the current network mode of the radio interface.

#### WDS:

- *MAC address* – MAC address of the opposite device;
- *Client Name* – network name of the opposite device;
- *IP address* – IP address of the opposite device;
- *Link Capacity* – parameter that reflects the effectiveness of the use of a modulation by the device on the transmission. It is calculated based on the number of packets transmitted on each modulation, and the reduction factors. The maximum value is 100% (means that all packets are transmitted at maximum modulation for the maximum nss type supported by the device). The minimum value is 2% (in the case when the packets are transmitted to the modulation nss1mcs0 for the device with MIMO 3x3 support). The parameter value is calculated for the last 10 s;
- *Link Quality* – parameter that displays the status of the link, calculated based on the number of sent retransmit packets. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent). The parameter value is calculated for the last 10 s;
- *Link Quality Common* – parameter that displays the status of the link, calculated based on the number of sent retransmit packets. The maximum value is 100% (all transmitted packets were sent on the first attempt), the minimum value is 0% (no packets were successfully sent). The parameter value is calculated for the entire connection time;
- *RSSI* – level of signal received from the opposite device, dBm;
- *SNR* – signal/noise ratio, dB;
- *Uptime* – time of wireless bridge operation;
- *TxRate* – channel data rate of transmission, Mbps;
- *RxRate* – channel data rate of receiving, Mbps.

## The 'Ethernet ports' submenu

You may view Ethernet ports' state in the Ethernet Ports submenu.

Monitoring

Network

IPTV

System

Internet

Ethernet Ports

DHCP

ARP

PPPoE Client

Device

Conntrack

Routes

State

Port	Connection	Speed	Mode	Transmitted	Received
LAN	On	1000 Mbit/s	Full-duplex	143.9 K (147 345 B)	66.4 K (68 032 B)

Refresh

#### State

- *Port* – port name:
  - *LAN* – local network port.
- *Connection* – port connection state:
  - *On* – network device is connected to the port (connection is active);
  - *Off* – network device is not connected to the port (connection is inactive).
- *Speed* – speed of the external network device connection to this port (10/100/1000 Mbit/s);
- *Mode* – data transmission mode:

- *Full-duplex* – full duplex;
- *Half-duplex* – half duplex;
- *Transmitted* – the quantity of bytes transmitted from the port;
- *Received* – the quantity of bytes received by the port.

To obtain current information on Ethernet ports states, press 'Refresh' button.

## The 'DHCP' submenu

The list of network devices connected to LAN interface of the device, whose IP addresses were assigned by local DHCP server, is given in the DHCP submenu. The expire time of address lease is shown in the table as well.

Monitoring	Network	IPTV	System
Internet	Ethernet Ports	DHCP	ARP
PPPoE Client	Device	Conntrack	Routes

List of DHCP Clients			
MAC	Client Name	IP Address	Lease Expires
30:65:EC:90:FB:E1	DESKTOP-PMJLVM9	192.168.1.2	11 h 55 min

Refresh

### List of DHCP Clients

- *MAC Address* – MAC address of the connected device;
- *Client Name* – network name of the connected device;
- *IP Address* – IP address assigned to client from address pool;
- *Lease Expires* – the period after which the lease of the dedicated address expires.

To obtain current information on DHCP clients, click the 'Refresh' button.

## The 'ARP' submenu

You may view ARP table in the ARP submenu. ARP table contain information on IP and MAC addresses mapping.

Monitoring	Network	System
Internet	Ethernet Ports	ARP
PPPoE Relay	Device	Conntrack
Routes		

ARP Table			
IP Address	MAC	Client Name	Interface
10.24.80.29	3C:1E:04:46:97:1F		Bridge
10.24.80.1	E0:D9:E3:E8:E1:40		Bridge

Refresh

### ARP Table

- *IP address* – the device IP address;
- *MAC address* – the device MAC address;
- *Client name* – device hostname (if one is present);
- *Interface* – interface from which the device is active: WAN, LAN or Bridge.

To get current information, click the 'Refresh' button.

## The 'PPPoE Relay' submenu



The 'PPPoE Relay' submenu is only available in the 'Wi-Fi Client' device mode in the 'Bridge' operation mode.



Internet
Ethernet Ports
ARP
**PPPoE Relay**
Device
Conntrack
Routes

### PPPoE Relay Sessions

Sessions Count
0

### Sessions List

Status	Session ID	Uptime	Client MAC	Client Timeout	Server MAC	Server Timeout
--------	------------	--------	------------	----------------	------------	----------------

Refresh

- *Sessions Count* – the quantity of PPPoE sessions established through the device. The maximum value – 64;
- *Status* – active or inactive session;
- *Session ID* – number of session;
- *Uptime* – session uptime;
- *Client Timeout* – time since the last packet from the client is received;
- *Server Timeout* – time since the last packet from the server is received.

You can also see information about the MAC address of the client and server.

## The 'PPPoE Client' submenu

✓ The 'PPPoE Client' submenu is available only in 'Router' mode.

On the page you can see information about the MAC address and the IP address of the client and server. The 'Status' parameter displays the session state - whether session is active or inactive.

Monitoring
Network
IPTV
System

Internet
Ethernet Ports
DHCP
ARP
**PPPoE Client**
Device
Conntrack
Routes

### PPPoE Client Info

Status	ACTIVE
Client MAC	E0:D9:E3:7A:BE:40
Server MAC	5C:D9:98:F5:8C:9B
Client IP	10.10.1.10
Server IP	10.10.1.1

## The 'Device info' submenu

General information on the device is given in the Device submenu.

Monitoring

Network

IPTV

System

Internet

Ethernet Ports

DHCP

ARP

PPPoE Client

Device

Conntrack

Routes

Device Info

Product

WB-2P-LR2

Firmware Version

2.4.0.50

Factory MAC Address

E0:D9:E3:49:C1:A0

Serial Number

WP36000038

System Time

20:47:10 05.04.2020

Uptime

9 d, 04:15:22

#### Device info

- *Product* – device model name;
- *Firmware Version* – device firmware version;
- *Factory MAC Address* – device WAN interface MAC address, setted by manufacturer;
- *Serial Number* – device serial number, setted by manufacturer;
- *System Time* – current time and date, setted in system;
- *Uptime* – the time since the last turn on or restart of the device.

### The 'Conntrack' submenu

In the 'Conntrack' submenu you may find the current active network connections of the device.

Monitoring
Network
IPTV
System

Internet
Ethernet Ports
DHCP
ARP
PPPoE Client
Device
Conntrack
Routes

### Active NAT Session

Active Connections	19
Shown Connections	19

### Connections List

Protocol	Source Address	Destination	Timeout
UNKNOWN	192.168.1.1	224.0.0.1	9 min 56 s
UDP	127.0.0.1:58279	127.0.0.1:53	14 s
UDP	0.0.0.0:88	255.255.255.255:87	22 s
TCP	100.110.0.13:56823	100.110.0.243:80	4 min 32 s
UDP	100.110.0.243:38840	172.16.0.100:53	3 s
TCP	100.110.0.13:56834	100.110.0.243:80	1 min 56 s
UDP	100.110.0.243:38840	100.110.1.253:53	3 s
TCP	100.110.0.13:56836	100.110.0.243:80	4 d 23 h 59 min 58 s
TCP	100.110.0.13:56835	100.110.0.243:80	4 d 23 h 59 min 57 s
TCP	100.110.0.13:56837	100.110.0.243:80	4 d 23 h 59 min 59 s
UDP	127.0.0.1:35513	127.0.0.1:53	3 s
TCP	100.110.0.13:56824	100.110.0.243:80	1 min 31 s
UNKNOWN	100.110.0.238	239.255.255.250	9 min 38 s
UNKNOWN	100.110.0.238	224.0.0.251	9 min 38 s
TCP	100.110.0.13:56838	100.110.0.243:80	4 d 23 h 59 min 58 s
TCP	100.110.0.13:56839	100.110.0.243:80	4 d 23 h 59 min 57 s
UDP	100.110.0.243:38840	172.16.0.250:53	3 s
UNKNOWN	100.110.0.238	224.0.0.252	9 min 38 s
TCP	100.110.0.13:56833	100.110.0.243:80	4 d 23 h 59 min 56 s

Refresh

#### Active NAT Session

- *Active Connections Count* – total number of active network connections;
- *Shown Connections* – number of connections shown in the WEB interface. In order to maintain high performance of the WEB interface, the maximum number of connections shown is limited to 1024. You may view other connections through the device console

#### Connections List

- *Protocol* – protocol by which the connection has been established;
- *Source Address* – connection initiator IP address and port number;
- *Destination IP* – connection destination IP address and port number;
- *Timeout* – time period before the disconnection.

To get current information, click the 'Refresh' button.

## The 'Routes' submenu

In the Routes submenu you may view the device route table.

Internet	Ethernet Ports	DHCP	ARP	PPPoE Client	Device	Conntrack	Routes
----------	----------------	------	-----	--------------	--------	-----------	--------

Routes							
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	100.110.0.1	0.0.0.0	UG	0	0	0	wlan0
100.110.0.0	0.0.0.0	255.255.254.0	U	0	0	0	wlan0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

Refresh

- *Destination* – IP address of destination host or subnet that the route should be established to;
- *Gateway* – gateway IP address that allows for the access to the Destination.
- *Netmask* – subnet mask;
- *Flags* – certain route characteristics. The following *flag* values exist:
  - **U** – means that the route is created and passable.
  - **H** – identifies the route to the specific host;
  - **G** – means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. G flag is used for all routes except for the routes in the direct connection networks.
  - **R** – indicates that the route was most likely created by a dynamic routing protocol running on the local system using the reinstate parameter;
  - **D** – indicates that the route was added as a result of receiving an ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination.
    - – means that the route was modified – likely by a dynamic routing protocol running on a local system with the 'mod' parameter applied;
    - – points to a buffered route to which an entry in the ARP table corresponds.
    - – means that the route source is the core routing buffer.
  - **L** – indicates that the destination of the route is one of the addresses of this computer. Such 'local routes' exist in the routing buffer only.
  - – means that the route destination is a broadcasting address. Such 'broadcast routes' exist in the routing buffer only.
  - **I** – indicates that the route is connected to a ring (loopback) interface for a purpose other than to access the ring network. Such 'internal routes' exist in the routing buffer only.
  - **!** – means that datagrams sent to this address will be rejected by the system.
- *Metric* – determines route 'price'. Metrics allows you to sort the duplicate routes, if they are exist in the table.
- *Ref* – fixed number of calls to the route to create a connection (not used in the system);
- *Use* – number of route detections performed by IP protocol.
- *Interface* – the name of the network interface through which this route runs.

To get current information, click the 'Refresh' button.

## The 'Network' menu

You may implement main network settings in the 'Network' menu.

### The 'Internet' submenu

In 'Internet' submenu, you may configure parameters to connect to a base station via Wi-Fi and select connection mode.

#### Wi-Fi Client mode

MonitoringNetworkSystem

InternetMAC ManagementFirewallRoutesSNMP

Common Settings

Hostname

WAN

Device ModeWireless Station

Connection Settings

SSIDWOP-2ac-LR2Scan Environment

802.11 Mode802.11bgn

Channel Bandwidth40 MHz

Security ModeWPA2

WPA Key

Tx Power (dBm)26

Short Guard Interval

Fixed Center Frequency

Limit Channels

Fixed Transmit RateAuto

Maximal Transmit RateAuto

ACK Timeout, μs64

Network ModeBridge

PriorityDSCP

ProtocolDHCP

VLAN Trunk Mode

Alternative Vendor ID (option 60)

Vendor ID (option 60)

Primary DNS Server

Secondary DNS Server

Tx Broadcast Rate Limit (packets/sec)0

Traffic Shaper

ApplyCancel

- *Hostname* – a name of the network device;
- *Device mode* – a mode of device connection;

WAN

Device ModeWireless Station

Connection Settings

SSIDWOP-2ac-LR2Scan Environment

802.11 Mode802.11bgn

Channel Bandwidth40 MHz

Security ModeWPA2

WPA Key

Tx Power (dBm)26

Short Guard Interval

Fixed Center Frequency

Limit Channels

Fixed Transmit RateAuto

Maximal Transmit RateAuto

ACK Timeout, μs64

Network ModeBridge

SSID	Security	MAC	Channel	Bandwidth, MHz	Frequency, MHz	RSSI, dBm
WOP-2ac-LR2	WPA/WPA2	E0:D9:E3:91:23:11	4	40L	2437	-58
I-OTT-ent-05	WPA_1X/WPA2_1X	E0:D9:E3:70:59:20	6	20	2437	-84
I-OTT-05-portal	Open	E0:D9:E3:70:59:21	6	20	2437	-86
Hotspot-GRE-Test	Open	E8:28:C1:01:27:70	6	40L	2447	-86
proverkasy	Open	E8:28:C1:01:27:71	6	40L	2447	-90

- ***SSID*** – wireless network ID, which is used for base station connection. The maximum name length – 32 symbols, the keyboard register is important. The name may consist of digits, latin letters and symbols '!', '\_', ':', ';', '\', '/', '#', '\$' and space, although it is forbidden to start with the symbols '!', ':', '#' and space;
- ***Scan Environment*** – click the button to start scanning at the defined range. The list of found access points will be displayed. The list of access points consists of seven columns: access point SSID, security mode, MAC address, channel, channel bandwidth, frequency, signal level. If you select any access point from the list, SSID field will be filled automatically, and the corresponding mode will be selected;
- ***802.11 Mode*** – operation mode according to the standard:
  - ***802.11bg*** – maximum rate is up to 54 Mbps;
  - ***802.11bgn*** – maximum rate is up to 300 Mbps;
  - ***802.11n*** – maximum rate is up to 300 Mbps.
- ***Channel Bandwidth*** – channel bandwidth, on which a Wi-Fi client operates. The parameter may take values from 5, 10, 20 and 40 MHz. If the base station has 5 or 10 MHz bandwidth, you should select the same bandwidth on the user station.
- ***Security mode*** – select security mode for wireless network:
  - ***Off*** – encryption of the wireless network is off, low security;
  - ***WEP*** – WEP encryption. WEP-key should consist of hexadecimal digits and be of 10 or 26 symbols length or it might be a string (a-z, A-Z, 0-9, ~!@#%&\*()\_-=+ symbols) with length of 5 or 13 symbols. The mode is hidden in the web interface;
  - ***WPA, WPA2*** – WPA and WPA2 authentication. The key length is from 8 to 63 symbols. Only the following characters can be used: a-z, A-Z, 0-9, ~!@#%&\*()\_-=+;./?.,<>"' or space. It is recommended to use WPA and WPA2 encryption modes as the safestest;
  - ***WPA-Enterprise, WPA2-Enterprise*** – WPA and WPA2 encryption with client authentication via 802.1x. Enter username and password as authentication data.
- ***Tx Power (dBm)*** – transmitting Wi-Fi signal power adjustment, dBm.
- ***Short Guard Interval*** – support for shortened guard interval. 400 ns interval is used (instead of 800 ns).
- ***Fixed center frequency*** – when the flag is checked, all traffic (data and management packets) will be transmitted on the specified center channel frequency with a given bandwidth (40 MHz). The function is proprietary, the transmission is not carried out according to IEEE 802.11 standards, where it is supposed to use different center frequencies for data and management traffic with 40 MHz bandwidth. When using the WB-2P-LR2 with WOP-2ac-LR2 devices with enabled fixed center frequency, activation at the subscriber station is not required, because happens automatically at the moment of connection to the base station.
- ***Limit Channels*** – the list of frequencies on which the air is scanned to connect to the base station.

WAN

Device Mode

Wireless Station

Connection Settings

SSID

WOP-2ac-LR2

Q Scan Environment

802.11 Mode

802.11bgn

Channel Bandwidth

20 MHz

Security Mode

WPA2

WPA Key

••••••••

Tx Power (dBm)

26

Short Guard Interval

☒

Limit Channels

☒

1 (2412 MHz) ✕ 2 (2417 MHz) ✕ 3 (2422 MHz) ✕ 4 (2427 MHz) ✕ 5 (2432 MHz) ✕ 6 (2437 MHz) ✕ 7 (2442 MHz) ✕

If the parameter Alternative Vendor ID (Option 60) is not checked, the default value will be transmitted in option 60. The default value has the following format:

[VENDOR:device vendor][DEVICE:device type][HW:hardware version] [SN:serial number][WAN:WAN interface MAC address]  
[LAN:LAN interface MAC address][VERSION:firmware version]

Example:

[VENDOR:Eltex][DEVICE:WB-2P-LR2][HW:1.2][SN:WP29000038] [WAN:E0:D9:E3:75:55:60] [LAN:E0:D9:E3:75:55:60]  
[VERSION:2.0.0.161]

- *PPPoE (available in the router mode)* – operation mode when PPP session is established on WAN interface; When PPPoE is selected, the following parameters will be available for editing:
  - *Username* – user name for authorization on PPP server;
  - *Password* – password for authorization on PPP server;
  - *MTU* – the maximum packet size that can be transmitted through a PPP session without fragmentation;
  - *Service-Name* – service provider name. Service-Name tag value in PADI message for PPPoE connection (this parameter is optional, and configured only on the provider's request);
  - *Secondary access* – type of access to local network resources.
    - *DHCP* – operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server;
    - *Static* – operation mode, when IP address and other necessary parameters of WAN interface are set statically. If 'Static' is selected, the following parameters will be available to set:
      - *External IP address* – specify device WAN interface IP address in the provider network;
      - *Netmask* – set subnet mask of device's WAN interface in service provider network;
      - *Default gateway* – address where the packet will be sent to, when route for it is not found in the routing table;
      - *Primary DNS, Secondary DNS* – DNS IP address – if DNS addresses are not automatically assigned via DHCP, you should defined them manually.
- *Disable sender address translation (available in router mode)* – the option allows you to disable sender address broadcasting (masquerade);
- *Tx Broadcast Rate Limit (packets/sec)* – limits transmission to external Wi-Fi network;
- *Traffic Shaper* – rate limit of both Downlink and Uplink directions. The maximum limit is 200 Mbps.

### VLAN trunk in bridge mode

- *VLAN Trunk* – if checked, the trunk port is activated for connected devices. The device will transparently transmit all VLANs (including 'Restrict VLAN list' option) received from the base station to wired clients and vice versa. At the same time, the passage of untagged traffic depends on the "Transparent mode" option;
  - *Use Management VLAN* – when checked, management VLAN used for access to the device is enabled:

- *Management VLAN ID* – VLAN identifier, which is used to access the device;
- *Management 802.1P* – 802.1P attribute (also called CoS – Class of Service), which is attached to egress packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority);
- *Management VLAN Access* – restrict access to the management network. Possible values:
  - *Ethernet and wireless* – access to the management network is possible from the wireless and Ethernet interfaces;
  - *Wireless* – access to the management network is only possible from the wireless interface side.



If the "Use Management VLAN" flag is checked and the Management VLAN is configured incorrectly, access to the device may be lost. When connected via Ethernet, the device will be available at 192.0.3.1.

- *Limit VLAN-list* – when checked, the device in VLAN trunk mode will pass only a limited number of VLANs, which are specified in the "VLAN list" field.
  - *VLAN list* – contains VLAN identifiers that are allowed for transmission. Accepts values from 1 to 4094, it is possible to specify a range, for example "2000-2010".

- *Use General VLAN* – when checked, one VLAN specified in the General VLAN ID field will be removed and the traffic of this VLAN will go to the client without a tag. When traffic flows in the opposite direction, untagged traffic will be tagged with General VLAN ID:
  - *General VLAN ID* – VLAN identifier;

- *General 802.1P*– 802.1P attribute (also called CoS – Class of Service), which is attached to egress packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority).
- *Transparent mode*– when checked, the device will pass untagged traffic in the VLAN trunk mode.

Use General VLAN	<input checked="" type="checkbox"/>
General VLAN ID	<input type="text"/>
General 802.1P	0 ▼
Transparent Mode	<input type="checkbox"/>

#### VLAN Trunk in router mode

- *VLAN Trunk*– if checked, the trunk port is activated for connected devices. There is an opportunity to use Management VLAN and Internet VLAN:

VLAN Trunk Mode	<input checked="" type="checkbox"/>
Use Management VLAN	<input checked="" type="checkbox"/>
Management VLAN ID	<input type="text"/>
Management 802.1P	0 ▼
Management Protocol	Static ▼
Management IP Address	192.168.15.200
Management Netmask	255.255.255.0
Management Default Gateway	192.168.15.1

- *Use Management VLAN*– when checked, management VLAN used for access to the device is enabled:
  - *Management VLAN ID*– VLAN identifier, which is used to access the device;
  - *Management 802.1P*– 802.1P attribute (also called CoS – Class of Service), which is attached to egress packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority).
  - *Management Protocol*– defines management interface operation mode:
    - *DHCP*– operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.
    - *Static*– operation mode where IP address and all the necessary parameters for interface are assigned statically. If 'Static' is selected, the following parameters will be available to set:
      - *Management IP*– set IP address of interface of the device in service provider network;
      - *Management netmask*– set subnet mask of device's interface in service provider network;
      - *Management Default Gateway*– address, to which a packet will be transmitted in case the route has not been found in the route table;

VLAN Trunk Mode	<input checked="" type="checkbox"/>
Use Management VLAN	<input type="checkbox"/>
Use Internet VLAN	<input checked="" type="checkbox"/>
Internet VLAN ID	<input type="text"/>
Internet 802.1P	0 ▼
Internet Protocol	Static ▼
Internet IP Address	192.168.12.200
Internet Netmask	255.255.255.0
Internet Default Gateway	192.168.12.1



- *Use Internet VLAN*— when checked, the VLAN is enabled to transmit user traffic.
  - *Internet VLAN ID*—VLAN identifier;
  - *Internet 802.1P*— 802.1P attribute (also called CoS – Class of Service), which is attached to egress packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority);
  - *Internet Protocol*— select operation mode of the device interface, used to transmit user traffic in a separate VLAN:
    - *DHCP*— operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server;
    - *Static*— operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. If 'Static' is selected, the following parameters will be available to set:
      - *Internet IP*— set IP address of WAN interface of the device in service provider network;
      - *Internet Netmask*— set subnet mask of device's WAN interface in service provider network;
      - *Internet Default Gateway*— address, to which a packet will be transmitted in case the route has not been found in the route table.

If *PPPoE* is selected as the Internet protocol, then you can specify the secondary access settings:

VLAN Trunk Mode	<input checked="" type="checkbox"/>
Use Management VLAN	<input type="checkbox"/>
Use Internet VLAN	<input checked="" type="checkbox"/>
Internet VLAN ID	<input type="text"/>
Internet 802.1P	0 ▼
Internet Protocol	PPPOE ▼
User Name	admin
Password	.....
MTU	1492
Service-Name	<input type="text"/>
Secondary Access	Static ▼
WAN IP Address	192.168.12.200
Netmask	255.255.255.0
Default Gateway	192.168.12.1
DNS Server	<input type="text"/>

- *Secondary access*— defines the method of setting the IP address on the interface for accessing the device if the management VLAN is not used:
  - *DHCP*— operation mode, when IP address, subnet mask, DNS server address, default gateway and other parameters required for operation are obtained from DHCP server automatically;
  - *Static*— operation mode, when IP address and other necessary parameters of WAN interface are set statically (manually). If 'Static' is selected, the following parameters will be available to set:
    - *External IP address*— specify device WAN interface IP address in the provider network;
    - *Netmask*— set subnet mask of device's WAN interface in service provider network;
    - *Default Gateway*— address, to which a packet will be transmitted in case the route has not been found in the route table;
    - *DNS server*— domain name server address (allows identifying the IP address of the device by its domain name).

**VLAN** is a virtual local area network. VLAN consists of a group of hosts combined into a single network regardless of their location. The devices grouped to a VLAN have the same identifier VLAN-ID.

#### Wireless bridge mode

Common Settings

Hostname

WAN

Device Mode

Wireless Bridge

Connection Settings

Priority

DSCP

Protocol

DHCP

VLAN Trunk Mode

☐

Alternative Vendor ID (option 60)

☒

Vendor ID (option 60)

Primary DNS Server

Secondary DNS Server

WDS Settings

Security Mode

Off

MAC Setting

Link 0

☐

XXXXXXXXXXXX

Link 1

☐

XXXXXXXXXXXX

Link 2

☐

XXXXXXXXXXXX

Link 3

☐

XXXXXXXXXXXX

Link 4

☐

XXXXXXXXXXXX

Link 5

☐

XXXXXXXXXXXX

Link 6

☐

XXXXXXXXXXXX

Link 7

☐

XXXXXXXXXXXX

✓ Apply

✕ Cancel

## WAN


- *Hostname* – a name of the network device;
- *Device mode* – a mode of device connection;
- *Priority* – select prioritization means. Defines a field based on which traffic transmitted to the radio interface will be distributed among WMM queues:
  - *DSCP* – enables analization of priority from the DSCP field of IP packet header;
  - *802.1p* – enables analization of priority from the CoS (Class of Service) field of tagged packets.
- *Protocol* – defines operation mode of the interface through which the connection of the device to service provider network will be performed:
  - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. If 'Static' is selected, the following parameters will be available to set:
    - *WAN IP* – set IP address of WAN interface of the device in service provider network;
    - *Netmask* – set subnet mask of device's WAN interface in service provider network;
    - *Default gateway* – address where the packet will be sent to, when route for it is not found in the routing table.
- *DHCP* – operation mode where IP address, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server. Before obtaining the parameters via DHCP, the access to the device is implemented via address set in IP address field:
  - *Alternative Vendor ID (Option 60)* – when selected, the device transmits *Vendor ID (Option 60) in Option 60 DHCP messages (Vendor class ID)*. If the field is empty, Option 60 will not be transmitted in DHCP messages. If the parameter Alternative Vendor ID (Option 60) is not checked, the default value will be transmitted in option 60. The default value has the following format:  
[VENDOR:device vendor][DEVICE:device type][HW:hardware version] [SN:serial number][WAN:WAN interface MAC address][LAN:LAN interface MAC address][VERSION:firmware version]  
Example:  
[VENDOR:Eltex][DEVICE:WB-2P-LR2][HW:1.2][SN:WP29000038] [WAN:E0:D9:E3:75:55:60] [LAN:E0:D9:E3:75:55:60][VERSION:2.0.0.161]
  - *Primary DNS, Secondary DNS* – DNS Ip address – if DNS addresses are not automatically assigned via DHCP, you should defined them manually.
- *VLAN Trunk* – if checked, the trunk port is activated for connected devices. There is an opportunity to use Management VLAN:
  - *Use Management VLAN* – when checked, management VLAN used for access to the device is enabled:

- *Management VLAN ID* – VLAN identifier, which is used to access the device;
- *Management 802.1P* – 802.1P attribute (also called CoS – Class of Service), which is attached to egress packets transmitted from this interface. The value is from 0 (the least priority) to 7 (the highest priority).
- *Management VLAN Access* – restrict access to the management network. Possible values:
  - *Ethernet and wireless* – access to the management network is possible from the wireless and Ethernet interfaces;
  - *Wireless* – access to the management network is only possible from the wireless interface side.
- *Limit VLAN-list* – when checked, the device in VLAN trunk mode will pass only a limited number of VLANs, which are specified in the "VLAN list" field.
  - *VLAN list* – contains VLAN identifiers that are allowed for transmission. Accepts values from 1 to 4094, it is possible to specify a range, for example "2000-2010".

### WDS Settings

- *Security mode* – select security mode for wireless bridge:
  - *Off* – wireless network encryption is off, low security;
  - *WPA2* – WPA2 authentication. The length of the key makes from 8 to 11 characters. Only the following characters can be used: a-z, A-Z, 0-9, ~!@#\$%^&\*()\_+=;:|/?.,<>"' or space.
- *Link X (where X=0..7)* – enable wireless bridge link. Enter MAC address of the device, to which you want to configure the wireless bridge, to a corresponding field next to Link checkbox.

## The 'Radio' submenu

 The 'Radio' submenu is available only in the 'Wireless bridge' mode.

In the 'Radio' submenu, you may configure the radiointerface to organize wireless bridge.

### Basic settings:

Monitoring
Network
System

Internet
Radio
MAC Management
Firewall
Routes
SNMP

Wi-Fi 2.4 GHz

Basic Settings
Advanced Settings

802.11 Mode802.11bgn

Channel1 (2412 MHz)

Channel Bandwidth20 MHz

Tx Power (dBm)26

Fixed Transmit RateAuto

Maximal Transmit RateAuto

ACK Timeout, μs64

✓ Apply

✕ Cancel

🔍 Scan Environment

- *Scan Environment* – press the button to start scanning at the defined range. The list of found access points will be displayed. The list of access points consists of seven columns: access point SSID, security mode, MAC address, channel, channel bandwidth, frequency, signal level.
- *802.11 Mode* – operation mode according to the standard:
  - *802.11bg* – maximum rate is up to 54 Mbps;
  - *802.11bgn* – maximum rate is up to 300 Mbps;
  - *802.11n* – maximum rate is up to 300 Mbps.
- *Channel* – select channel for data transmission.
- *Channel Bandwidth* – channel bandwidth, on which the radiointerface operates. The parameter may take values from 5, 10, 20 and 40 MHz according to selected mode.
- *Fixed center frequency* – when the flag is checked, all traffic (data and management packets) will be transmitted on the specified center channel frequency with a given bandwidth (40 MHz). The function is proprietary, the transmission is not carried out according to IEEE 802.11 standards, where it is supposed to use different center frequencies for data and management traffic with 40 MHz bandwidth;

- *Tx Power (dBm)* – transmitting Wi-Fi signal power adjustment, dBm.
- *Fixed Transmit Rate* – fixed wireless data transmission rate which is defined by IEEE 802.11 g/n standards;
- *Maximum Transmit Rate* – maximum allowed wireless data transmission rate which is defined by IEEE 802.11 g/n standards.

Advanced settings:

Monitoring
Network
System

Internet
Radio
MAC Management
Firewall
Routes
SNMP

Wi-Fi 2.4 GHz

Basic Settings
Advanced Settings

Fragmentation Threshold
2346
(256-2346)

RTS Threshold
2347
(0-2347)

Beacon Interval, ms
100
(20-1024)

Aggregation
☒

Short Guard Interval
☒

STBC
☐

Coexistence 20/40 MHz
☐

Apply
Cancel

- *Fragmentation Threshold* – frame fragmentation threshold, bytes. The parameter takes values 256-2346, by default – 2346;
- *RTS Threshold* – after what quantity of bytes the Request to Send will be sent. Decreasing of the parameter's value might improve access point operation when there are a lot of clients connected. However, decreasing of the parameter's value will reduce general bandwidth of wireless network. The parameter takes values from 0 to 2347, by default – 2347;
- *Beacon Interval, ms* – beacon frames transmission period. The frames are sent to detect access points. The parameter takes values from 20 to 2000 ms, by default – 100 ms;
- *Aggregation* – enable support for AMPDU/AMSDU;
- *Short Guard interval* – support for shortened guard interval. 400 ns interval is used (instead of 800 ns).
- *STBC* – Space-Time Block Coding method dedicated to improve data transmission reliability. When checked, the device transmits one data flow through several antennas. When unchecked, the device does not transmit one data flow through several antennas;
- *Coexistence 20/40 MHz* – automatic bandwidth changing when environment is loaded.

✔ For wireless bridge operation, radiointerface parameters should be configurate identically on all the devices.

## The 'LAN' submenu

✔ The 'LAN' submenu is available only in the 'Router' mode.

In DHCP server settings section you may configure local network, DHCP server, set static addresses bindings.

The device is capable to assign IP addresses and other parameters required to the Internet access to computers connected to LAN interface through DHCP (Dynamic Host Configuration Protocol). The use of DHCP allows to avoid manual configuration of TCP/IP.

Monitoring
Network
IPTV
System

Internet
LAN
MAC Management
Local DNS
NAT and Port Forwarding
Firewall
Routes
Dynamic DNS
SNMP

### LAN

IP Address
192.168.1.1

Netmask
255.255.255.0

### DHCP Server Settings

Enable
☒

Start IP Address
192.168.1.2

Pool Size
250

Lease Time (min)
720

### Static Leases

Name	MAC	IP Address
<input type="button" value="+ Add"/> <input type="button" value="Remove"/>		

#### LAN:

- *IP address* – IP address of the device in a local network;
- *Netmask* – subnetmask in local network.

#### DHCP server settings:

- *Enable* – when checked, a local DHCP server is enabled, otherwise the server is disabled;
- *Start IP address* – the initiate address of the IP addresses pool;
- *Pool size* – number of addresses in the pool;
- *Lease time (min)* – set the maximum time range for using an IP address assigned by DHCP server, lease time is set in minutes.

To apply a new configuration and store settings into the non-volatile memory, click the *'Apply' button*. To discard changes click the *'Cancel' button*.



When you try to change the starting address of the DHCP pool to an address from a different subnet with respect to the subnet of the LAN interface, the pool is automatically set in accordance with the specified local subnet.

#### Static leases

To set new static lease, press the *'Add'* button and fill the following fields:

- *Name* – lease name
- *MAC address* – specify a static address. It is assigned in XX:XX:XX:XX:XX:XX format;
- *IP address* – define a static IP address for the specific MAC address.

Configuring of static leases is helpful when you need that the certain computer always obtains certain IP address.

Press *'Apply'* to add IP address to the list of static IP addresses for DHCP server. To discard changes click the *'Cancel' button*. To delete an address from the list, select the corresponding checkbox and press *'Remove'*.

## The 'MAC Management' submenu

In the MAC address Management submenu, you may set MAC address of the device's WAN interface.

Monitoring **Network** IPTV System

Internet LAN **MAC Management** Local DNS NAT and Port Forwarding Firewall Routes Dynamic DNS SNMP

Wireless Transparent Bridge

Enable ☐

Set MAC Address for WAN

Redefine MAC ☐

MAC XX:XX:XX:XX:XX:XX

#### Wireless transparent bridge

'Wireless transparent bridge' settings are available for Bridge mode of Wi-Fi station only.

When you enable Wireless transparent bridge, WB-2P-LR2 will not substitute client MAC addresses from LAN with own MAC address. The limit is 15 MAC addresses without substitution. When the value is exceeded client's MAC address will be substituted. The section of connected clients on a base station will include MAC addresses of client devices from LAN.

#### Set MAC address for WAN

- *Redefine* – when checked, the MAC address from the field MAC is used.

To apply a new configuration and save setting to non-volatile memory, press 'Apply'. Press 'Cancel' to discard the changes.

## The 'Local DNS' submenu

The local DNS submenu is available only in router mode.

You may configure Local DNS server of the device by adding IP address and domain name in the 'Local DNS' submenu.

ocal DNS allows to obtain an IP address of the device using its domain name (host) in case of lack of DNS server in a network segment. To implemet this, you should know concordances between nodes names (hosts) and their IP addresses.

Monitoring **Network** IPTV System

Internet LAN MAC Management **Local DNS** NAT and Port Forwarding Firewall Routes Dynamic DNS SNMP

List of Domain Names

Domain Name	IP Address
-------------	------------

#### Configuring nodes

To add the address into the list, click the *Add* button in the 'New domain name' window and fill in the following fields:

Monitoring
Network
IPTV
System

Internet
LAN
MAC Management
Local DNS
NAT and Port Forwarding
Firewall
Routes
Dynamic DNS
SNMP

### New Domain Name

Domain Name

IP Address

- *Domain name* – host name;
- *IP Address* – IP address of the host.

Press *'Apply'* to create concordance IP address – domain name. To discard changes click the *'Cancel'* button. To delete an entry from the list, select corresponding checkbox and press *'Remove'*.

## The 'NAT and Port Forwarding' submenu

✓ The NAT and Port Forwarding submenu is available only for router mode.

You may configure Port Forwarding from WAN interface to LAN interface in the NAT and Port Forwarding submenu.

NAT (Network Address Translation) mode allows to modify IP addresses and network ports of IP packets. Port forwarding is necessary when TCP/UDP connection with local PC (connected to LAN interface) is established via external network. The settings menu allows to set rules which permit packets transmission from external network to specified address in a local network, i.e. to establish connection. Port forwarding is also necessary when using torrent and p2p services. To implement the configuration, find TCP/UDP ports used by torrent or p2p clients in settings and set them for corresponding port forwarding rules to a PC IP address.

Monitoring
Network
IPTV
System

Internet
LAN
MAC Management
Local DNS
NAT and Port Forwarding
Firewall
Routes
Dynamic DNS
SNMP

### NAT Settings

Enable NAT
☒

### NAT Rules

	Name	LAN IP	LAN Ports	Protocol	WAN IP	WAN Ports
<input type="checkbox"/>	Rule-1	192.168.1.3	50002	TCP	76.44.23.56	50000
<input type="checkbox"/>	Rule-2	192.168.1.3	50005	UDP	213.45.66.89	50005

### NAT rules

To add a new NAT rule, click the *'Add'* button and fill in the following fields in the Add a new rule window:

Add a New Rule

Name

LAN IP Address

Destination Ports of LAN

Protocol

UDP

WAN IP Address

Destination Ports of WAN

Apply
Cancel

- *Name* – name of the rule (this field is mandatory);
- *LAN IP Address* – IP address of host in local network. Packets translated to this host will follow the rule;
- *Destination ports of LAN* – receiver TCP/UDP ports, via which packets are translated to local network (you may assign either single port or range of ports using dash);
- *Protocol* – selection of the packet protocol falling under this rule: TCP, UDP, TCP/UDP;
- *WAN IP address* – source IP address in external network which will be under the rule;
- *Destination Ports of WAN* – destination TCP/UDP ports in external network, packets from which will follow the rule (you may assign either single port or range of ports using dash).

Port forwarding rule will work as follows: a packet received via «*Protocol*» on a port defined in «*Destination Ports of WAN*» field and having source address defined in «*WAN IP address*» field (if the field is empty, source IP does not consider) undergoes address and Destination port substitute with the parameters defined in «*LAN IP Address*» and «*Destination Ports of LAN*» fields respectively.

Click '*Apply*' to create concordance IP address – domain name. To discard changes, click '*Cancel*'.

To delete an entry from the list, select corresponding checkbox and click '*Remove*'.

## The 'Firewall' submenu

The rules for incoming, outgoing and transit traffic transmission are set in the *Firewall* submenu. There is an opportunity to limit transmission of different types of traffic (incoming, outgoing, transit) depending on protocol type, source and destination IP, TCP/UDP source and destination ports, type of ICMP message.

Monitoring
Network
IPTV
System

Internet
LAN
MAC Management
Local DNS
NAT and Port Forwarding
Firewall
Routes
Dynamic DNS
SNMP

Rules for Input Traffic

Name	Protocol	Source IP Address	Source Ports	Destination Ports	Action
------	----------	-------------------	--------------	-------------------	--------

Rules for Output Traffic

Name	Protocol	Source Ports	Destination IP Address	Destination Ports	Action
------	----------	--------------	------------------------	-------------------	--------

Rules for Forward Traffic

Name	Protocol	Source IP Address	Source Ports	Destination IP Address	Destination Ports	Action
------	----------	-------------------	--------------	------------------------	-------------------	--------

+ Add
Remove

### Configuring firewall rules

To add a new NAT rule, click the '*Add*' button and fill in the following fields in the 'Add a new rule' window:



Add a New Rule

Name

Traffic Type

Input

Protocol

TCP

Source IP Address

Source Ports

0

Destination Ports

0

Action

Accept

✓ Apply

✕ Cancel

- *Name* – rule name;
- *Traffic type* – select the traffic type that will fall under this rule:
  - *Incoming* – incoming device traffic (recipient is one of the device network interfaces). If the parameter is selected, the following field will be displayed:
    - *Source address* – define starting source IP address. You may set subnet mask after '/' character. The subnet mask should be set in the following formats: xxx.xxx.xxx.xxx or xx, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0 to set addresses range (the subnet mask entry /24 coincides with /255.255.255.0 entry);
  - *Outgoing* – outgoing device traffic (traffic generated locally by the device from one of the network interfaces). If the parameter is selected, the following field will be displayed:
    - *Destination IP address* – set destination IP address. You may set subnet mask after '/' character. The subnet mask should be set in the following formats: xxx.xxx.xxx.xxx or xx, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0 to set addresses range (the subnet mask entry /24 coincides with /255.255.255.0 entry);
  - *Protocol* – packet protocol that will fall under this rule: TCP, UDP, TCP/UDP, ICMP, any.
  - *Action* – action to be performed on packets (reject/skip).

When TCP, UDP, TCP/UDP protocols are selected, the following settings will be available to configure:

- *Source ports* – the list of source ports, packets from which will follow the rule (it is acceptable to specify single port or port range with the help of '-' sign). To specify all the source ports, enter '0–65535';
- *Destination ports* – the list of destination ports, packets from which will follow the rule (it is acceptable to specify single port or port range with the help of '-' sign). To specify all the source ports, enter '0–65535'.

When ICMP is selected, the following settings will be available for editing:

- *Message type* – you can create the rule for the specific ICMP message type or for all ICMP message types.

Click the 'Apply' button to add a new rule. Press 'Cancel' to discard the changes. To delete a created rule, check the box next to the rule and click 'Remove'.

## The 'Routes' submenu

You may set static routes in the Routes submenu.

Monitoring

Network

IPTV

System

Internet

LAN

MAC Management

Local DNS

NAT and Port Forwarding

Firewall

Routes

Dynamic DNS

SNMP

Routes

Name

Destination

Netmask

Gateway

+ Add

Remove

Click the 'Add' button to add a new route. Fill the following fields:

Add Route

Name

Destination

Netmask

Gateway

✔ Apply
✕ Cancel

- *Name* – route name;
- *Destination IP* – IP address of destination host or subnet that the route should be established to;
- *Netmask* – a subnet mask. A subnet mask for a host is set to 255.255.255.255 value, for a subnet — depending on its size;
- *Gateway* – gateway IP address that allows for the access to the *Destination IP*.

To apply a new configuration and store settings into the non-volatile memory, click the *'Apply' button*. To discard changes click the *Cancel*/button.

## The 'Dynamic DNS' submenu

✔
The 'Dynamic DNS' submenu is available only in the 'Router' mode.

In the 'Dynamic DNS' submenu, you may configure the corresponding service.

*Dynamic DNS (D-DNS)* provides information on DNS server update in real time or automatically, if necessary. It is used to assign a permanent domain name to a device (PC, router) with dynamic IP address.

Dynamic DNS is often used in local networks, where clients obtain IP addresses via DHCP, and then register their names on local DNS server.

Monitoring
Network
IPTV
System

Internet
LAN
MAC Management
Local DNS
NAT and Port Forwarding
Firewall
Routes
Dynamic DNS
SNMP

Dynamic DNS

Enable D-DNS
☒

Server

dyndns.org
▼

User Name

Password

Domain Name 0

Domain Name 1

Domain Name 2

Domain Name 3

Domain Name 4

Domain Name 5

Domain Name 6

Domain Name 7

Domain Name 8

Domain Name 9

✔ Apply
✕ Cancel

- *Enable D-DNS* – when selected, D-DNS service is enabled; the following settings will be available for editing:
  - *D-DNS provider name* – select one of the available providers;
  - *User name* – user name used to access D-DNS server account;
  - *Password* – password used to access D-DNS service account;
  - *Domain name (0..9)* – you may register up to 10 domain names (usually only one is required). The update of data on IP address of the device is implemented once in 60 seconds on a provider server.

To apply a new configuration and store settings into the non-volatile memory, click the *'Apply' button*. To discard changes click the *'Cancel' button*.

### The 'SNMP' submenu

WB-2P-LR2 software allows monitoring of the device status and its sensors via SNMP. In The SNMP submenu, you can configure settings of SNMP agent. The device supports SNMPv1, SNMPv2c.

MonitoringNetworkIPTVSystem

InternetLANMAC ManagementLocal DNSNAT and Port ForwardingFirewallRoutesDynamic DNSSNMP

SNMP Settings

Enable SNMP☐

Read-only Community

public

Read-write Community

private

TrapSink

Trap2Sink

InformSink

System Name

Contact

Contact

Location

Russia

Trap Community

trap

✓ Apply

✕ Cancel

- *Enable SNMP* – when checked, SNMP is enabled;
- *roCommunity* – a password to read the parameters (by default: *public*);
- *rwCommunity* – a password to configure (write) parameters (by default: *private*);
- *TrapSink* – IP address or domain name of SNMPv1-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *Trap2Sink* – IP address or domain name of SNMPv2-trap message recipient in HOST [COMMUNITY [PORT]] format;
- *InformSink* – IP address or domain name of Inform message recipient in HOST [COMMUNITY [PORT]] format;
- *Sys Name* – device name;
- *Sys Contact* – device vendor contact information;
- *Sys Location* – device location information;
- *Trap community* – password enclosed in traps (default value: trap).

The list of objects which are supported for reading and configuration via SNMP is given below:

- eltexLtd.1.165.1 – WB-2P-LR2 parameters monitoring

where eltexLtd – 1.3.6.1.4.1.35265 is Eltex Enterprise identifier.

To apply a new configuration and save setting to non-volatile memory, click 'Apply'. Click 'Cancel' to discard the changes.

### The 'IPTV' menu

This menu is available only in the 'Router' mode.

### The 'IPTV' submenu

You may configure IPTV service in IPTV settings menu.

The screenshot shows the 'IPTV Settings' page. At the top, there are four tabs: 'Monitoring', 'Network', 'IPTV' (which is highlighted), and 'System'. Below the tabs, there is a sub-tab labeled 'IPTV'. The main content area is titled 'IPTV Settings'. It contains the following settings:

- Enable IPTV**: A checkbox that is checked.
- IGMP Version**: A dropdown menu showing '3'.
- Renew Subscription**: A checkbox that is unchecked.
- Fast Leave Mode**: A checkbox that is unchecked.
- HTTP Proxy Settings**: A checkbox that is checked.
- HTTP Port**: A text input field containing '1234'.

At the bottom of the settings area, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'X' icon).

- *Enable IPTV* – when checked, IPTV signals transmission via WAN interface (from provider network) to the devices connected to the LAN interface is enabled;
- *IGMP version* – IGMP version for IGMP messages sending from WAN interface (IPTV channel subscription activation/deactivation messages). Versions 2 and 3 are supported.

#### Renew subscription

- *Enable* – when option is enabled messages with active IPTV channel list are periodically sending from the WAN interface to higher server, that translating IPTV signals. Enabling of the function is necessary if a higher server disables IPTV channels translation in a certain period of time.
- *Renew Subscription Interval, s* – active IPTV channel list messages sending period, in seconds. Set the value of interval less than interval (timeout) of higher server signals translation disabling.

#### Fast leave mode

- *Enable* – when checked, the option for fast exit from the multicast group is enabled. The function is not recommended when more than one multicast traffic receiver is used.

#### HTTP Proxy Settings

- *Enable* – when checked HTTP proxy service is enabled. HTTP Proxy implements modification of UDP stream to HTTP stream using TCP (transmission control protocol), that allows to improve quality of transmitted image in case of poor communication channel quality in a local network. The function is useful when IPTV is watched via wireless Wi-Fi channel.
- *Port HTTP* – HTTP proxy port number that will be used for video streaming. Use this port to connect IPTV streams translated by the device.

For instance, if the device has the 192.168.0.1 address on the LAN interface, Proxy server's value is 1234 and you need to playback 227.50.50.100 channel broadcasted to UDP port 9000, set stream address for VLC programm in the form of: <http://@192.168.0.1:1234/udp/227.50.50.100:9000>.

To apply a new configuration and store settings into the non-volatile memory, click the *'Apply' button*. To discard changes click the *Cancel*/button.

## The 'System' menu

In the 'System' menu, you may configure system parameters: time, access via different protocols, change password, update software.

### The 'Time' submenu

The configuration of time synchronization protocol (NTP) is implemented in the 'Time' submenu.

Monitoring
Network
IPTV
**System**

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Advanced

### Time Settings

Time Zone
Moscow, Russia

Daylight Saving Time Enable
☒

DST Start
-
-
in
-
at
--:--

DST End
-
-
in
-
at
--:--

DST Offset (minutes)
60

Enable NTP
☒

NTP Server
pool.ntp.org

Apply
Cancel

#### Time settings

- *Time Zone* – allows to set the timezone according to the nearest city for your region from the list;
- *Daylight Saving Time Enable* – when selected, automatic daylight saving change will be performed automatically within the defined time period:
  - *DST Start* – day and time, when daylight saving time is starting;
  - *DST End* – day and time, when daylight saving time is ending;
  - *DST Offset (minutes)* – time period in minutes, on which time offset is performing.
- *Enable NTP* – check if it is needed to enable device system time synchronization from a certain NTP server;
- *NTP Server* – Time synchronization server IP address/domain name.

To apply a new configuration and store settings into the non-volatile memory, click the *'Apply'* button. To discard changes click the *Cancel* button.

## The 'Access' submenu

In the 'Access' submenu, you may configure access to the device via web interface, Telnet and SSH.

### Access Ports

In this section you may configure TCP ports for the access to the device via HTTP, HTTPS, Telnet, and SSH:

- *HTTP port* – number of the port for access to the device web interface via *HTTP*, default value is 80;
- *HTTPS port* – number of the port for access to the device web interface via *HTTPS* (*HTTP Secure* – secure connection), default value is 443;
- *Telnet Port* – number of port for access to WEB interface via *Telnet* (default is 23);
- *SSH Port* – number of port for access to WEB interface via *SSH* (default is 22).

You may use *Telnet* and *SSH* protocols in order to access the command line (Linux console).

### Access to Internet service

This section allows or denies access to the device with separate rules for local and external networks (router mode). For this you need to set the following permissions:

#### **Web:**

- *HTTP* – when selected, the WAN port connection to the device WEB configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, the WAN port connection to the device WEB configurator is enabled via HTTPS (insecure connection).

#### **Telnet:**

*Telnet* is a protocol that allows you to establish mechanisms for remote control of the devices. It allows you to connect to the device via network for configuration and management purposes.

To enable the device access via Telnet protocol, select the corresponding checkbox.

#### **SSH:**

*SSH* – secure protocol of device remote control. As opposed to Telnet, SSH encrypts all traffic being transferred including passwords;

To enable the device access via SSH protocol, select the corresponding checkbox.

To apply a new configuration and store settings into the non-volatile memory, click the '*Apply*' button. To discard changes click the '*Cancel*' button.

## The 'Log' submenu

The 'Log' submenu is designed to configure the output of various kinds of debugging messages of the system in order to detect the causes of problems in the operation of the device. Debug information may be provided by the following device firmware modules:

- Networkd Log – deals with the device configuration according to the configuration file;

- Configd Log – deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring data collection.

#### Networkd Log

- *Log Output* – log messages output direction:
  - *Disabled* – the output is disabled;
  - *Syslog* – messages are output to the remote server or local file via syslog protocol (protocol configuration is carried out below);
  - *Console* – messages are output to device console (connection via COM port adapter is needed);
  - *Telnet* – messages are output to the telnet session; create telnet protocol connection first.

Select types of messages to be output in Networkd Log:

- *Error* – check if it is needed to output 'Error' type messages;
- *Warning* – check if it is needed to output 'Warning' type messages;
- *Debug* – check to collect debug messages;
- *Info* – check to collect information messages.

#### Configd Log

- *Log Output* – log messages output direction:
  - *Disabled* – the output is disabled;
  - *Syslog* – messages are output to the remote server or local file via syslog protocol (protocol configuration is carried out below);
  - *Console* – messages are output to device console (connection via COM port adapter is needed);
  - *Telnet* – messages are output to the telnet session; create telnet protocol connection first.

Select types of messages to be output in Configd Log:

- *Error* – check if it is needed to output 'Error' type messages;
- *Warning* – check if it is needed to output 'Warning' type messages;
- *Debug* – check to collect debug messages;

- *Info* – check to collect information messages.

### Syslog settings

If there is at least a single log (Networkd Log or Configd Log) configured for Syslog output, you should enable Syslog agent that will intercept debug messages and send them to a remote server or save them to a local file in Syslog format.

- *Enable* – when checked syslog agent is running;
- *Mode* – Syslog agent operation mode:
  - *Server* – log information is sending to remote Syslog server;
  - *Local file* – log information is saving to local file;
  - *Server and file* – log information is sending to remote Syslog server and saving to local file.

According to Syslog agent mode, the following settings might be available:

- *Syslog server address* – Syslog server IP address or domain name (required for 'Server', 'Server and file' modes);
- *Syslog server port* – port for Syslog server incoming messages (default value is 514; required for 'Server', 'Server and file' modes);
- *File name* – name of the file to store log in Syslog format (required for 'Local file', 'Server and file' modes);
- *File size, KB* – maximum log file size (required for 'Local file', 'Server and file' modes).

## The 'Passwords' submenu

In the 'Passwords' submenu you may define passwords for administrator and viewer access.

The set passwords are used for access to the device via web interface, Telnet and SSH.

When logging in via WEB interface administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. A viewer (password by default: **viewer**) has rights to view configuration and device monitoring data. Viewer is not permitted to change settings.



**Administrator login: admin**  
**Viewer login: viewer**

- *Administrator Password* – type administrator password and confirmation in corresponding fields;
- *Viewer password* – enter user password in the corresponding field and confirm it.

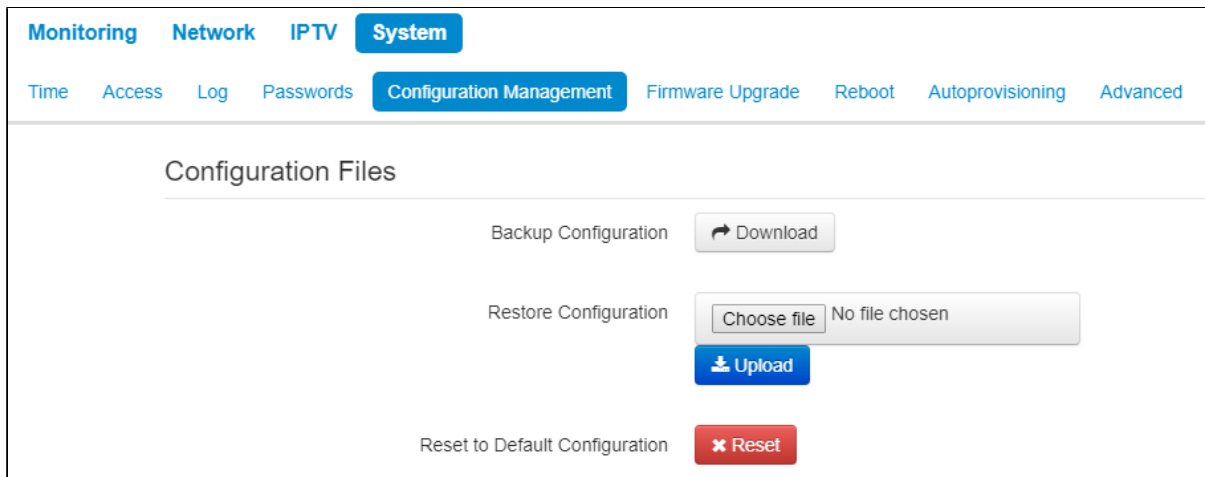
To apply a new configuration and store settings into the non-volatile memory, click the *'Apply' button*. To discard changes click the *'Cancel' button*.

## The 'Configuration management' submenu

In the 'Configuration management' submenu you may save and update the current configuration.

### Backup Configuration





The screenshot shows a web interface with a top navigation bar containing 'Monitoring', 'Network', 'IPTV', and 'System' (highlighted). Below this is a sub-navigation bar with 'Time', 'Access', 'Log', 'Passwords', 'Configuration Management' (highlighted), 'Firmware Upgrade', 'Reboot', 'Autoprovisioning', and 'Advanced'. The main content area is titled 'Configuration Files' and contains three sections: 'Backup Configuration' with a 'Download' button, 'Restore Configuration' with a 'Choose file' button, a 'No file chosen' status, and an 'Upload' button, and 'Reset to Default Configuration' with a 'Reset' button.

To save the current device configuration to a local PC, click 'Download' button.

#### Restore Configuration

- *Upload configuration archive to the device* – upload of configuration file saved on local computer. To update the device configuration click the 'Choose file' button, specify a file (in .tar.gz format) and click the 'Upload' button. Uploaded configuration will be applied automatically and does not require device reboot.



**Note that all the passwords of configuration are encrypted with a key depending on device MAC address. Before loading a configuration from one device to another, you should change all passwords in configuration file.**

To change the passwords open the configuration file in text editor and change passwords. Then save the changes in configuration archive. The example of password changing is shown below:

```
Passwords:
AdminPassword: "encrypted:7C607178736B7465"
ViewerPassword: "encrypted:7A68677C6176"
```

changes to

```
Passwords:
AdminPassword: "password"
ViewerPassword: "password"
```

#### Reset to Default Configuration

To reset all the settings to default values, click the 'Reset' button.

## The 'Firmware Upgrade' submenu

The 'Firmware Upgrade' submenu is dedicated to update firmware version of the device.

WB-2P-LR2 firmware upgrade:

Monitoring
Network
IPTV
System

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Advanced

Firmware Upgrade

Active Version2.3.0.213

Check for Update

Backup Version2.2.0.261

Set Active

Firmware upgrade is also available at <http://eltex-co.ru/support/downloads/>

Firmware Image

Browse...


Upload File

- *Active Version* – installed firmware version, which is operating at the moment;
- *Backup version* – installed firmware version which can be used in case of problems with the current active firmware version;
- *Check for upgrade* – click this button to check the availability of the latest firmware version. With this function, you may quickly check the latest firmware version and update the firmware, if necessary;
- *Make active* – a button that allows you to make a backup version of the firmware active, this will require a reboot of the device. The active firmware version will not be set as a backup.

 Firmware update check function requires access to the Internet.

You may update the device firmware manually by downloading the firmware file from the web site <http://eltex-co.com/support/downloads/> and saving it on the computer. To do this, click the 'Select file' button in the *Software update file* field and specify the path to the file in .tar.gz format.

To start the update process, you must click the 'Upload file' button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

 Do not switch off or reboot the device during the firmware update.

## The 'Reboot' submenu

In the 'Reboot' submenu you may reboot the device.

Monitoring
Network
IPTV
System

Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Advanced

Device Reboot

Reboot

Click the 'Reboot' button to reboot the device. Device reboot process takes approximately 1 minute to complete.

## The 'Autoprovisioning' submenu

In the 'Autoprovisioning' submenu you may configure DHCP-based autoprovisioning algorithm and subscriber device automatic configuration protocol TR-069.

Monitoring
Network
IPTV
System
Time
Access
Log
Passwords
Configuration Management
Firmware Upgrade
Reboot
Autoprovisioning
Advanced

### DHCP-based Autoprovisioning

Provisioning Mode
Configuration and Firmware
Parameters Priority from
DHCP options
Configuration File
Configuration Update Interval, s
300
Firmware File
Firmware Upgrade Interval, s
3600

### TR-069 Autoconfiguration

Common
Enable TR-069 Client
ACS Server Address
http://update.local:9595/
Enable Periodic Inform
Periodic Inform Interval, s
60
ACS Connection Request
User Name
acs
Password
acsacs
Client Connection Request
User Name
admin
Password
admin
NAT Settings
NAT Mode
Off

Apply
Cancel

#### DHCP-based Autoprovisioning:

- *Provisioning Mode* – select a mode for automatic device update. The followings are available:
  - *Disabled* – automatic update of configuration and firmware is disabled;
  - *Configuration and Firmware* – periodical configuration and firmware update is permitted;
  - *Configuration only* – only periodical update of configuration is permitted;
  - *Firmware only* – only periodical update of firmware is permitted.
- *Parameters Priority from* – this parameter determines where you need to get the names and location of configuration files and firmware:
  - *Static settings* – paths to configuration and firmware files are defined by the 'Configuration file' and 'Firmware file' settings correspondingly; more detailed information on the algorithm see in section [DHCP-based autoupdate algorithm](#);
  - *DHCP options* – paths to configuration and firmware files are defined by the DHCP Option 43, 66, and 67 (to do this, you should select DHCP for the Internet service); more detailed information on the algorithm see in section [DHCP-based autoupdate algorithm](#);
- *Configuration File* – full path to configuration file – set in URL format (there is an opportunity to load configuration files via TFTP):

tftp://<server address>/<full path to cfg file>

where < server address > – TFTP server address (domain name or IPv4),

< full path to cfg file > – full path to configuration file on the server;

- *Configuration Upgrade interval, s* – the time interval in seconds, after which the device configuration is periodically updated. If 0 is set, update of the device will be implemented once, right after reloading of the device;
- *Firmware File* – the full path to the firmware file is specified in the URL format (at the moment it is possible to download the software file using TFTP):

tftp://<server address>/<full path to firmware file>

where < server address > – TFTP server address (domain name or IPv4),

< full path to firmware file > – full path to configuration file on the server.

- *Firmware Upgrade Interval, s* – a time interval. The firmware update is implemented according to this period. If 0 is set, update of the device will be implemented once, right after reloading of the device.

More detailed information on the algorithm see in section [DHCP-based autoupdate algorithm](#).

#### Autoconfiguration via TR-069:

##### Common:

- *Enable TR-069 Client* – when checked, the operation of embedded TR-069 client is enabled, otherwise it is prohibited.

- *ACS Server Address* – autoconfiguration server address. The address should be entered in the following formats `http://<address>:<port>` or `https://<address>:<port>` (<address> – IP address or domain name of ACS server, <port> – ACS server port, the default port is 9595). The second format is to use the secure protocol – HTTPS for exchanging data with ACS server.
- *Enable Periodic Inform* – when checked, internal TR-069 client performs periodic ACS server polling with an interval equal to the '*Periodic Inform Interval*' in seconds. The poll aim is to detect device configuration changes.

#### ACS Connection Request:

- *User Name, Password* – user name and password for client to access ACS server.

#### Client Connection Request:

- *User Name, Password* – user name and password for ACS server to access TR-069 client.

#### NAT Settings:

If there is modification of network addresses between client and ACS server (NAT – network address translation), ACS server might not have the opportunity to establish connection with the client if certain technologies are not used to avoid it. The technologies help the client to define so called public address (NAT addresses – an address of external gateway, behind which the client is located). When the public address is defined, the client inform the server. Then, the server uses the public address (not the local) to establish connection with the client.

- *NAT Mode* – determines how the client should receive information about their public address. The following modes are available:
  - *STUN* – use STUN protocol for public address identification;
  - *Manual* – manual mode, when public address is explicit in configuration; in this mode, you should add a forwarding rule on a device that acts as a NAT for TCP port used by TR-069 client;
  - *Off* – NAT will not be used – this mode is recommended only when the device is directly connected to ACS server without network address translation. In this case, public address coincides with local one.

When *STUN* mode is selected you should configure the following settings:

- *STUN server address* – STUN server IP address or domain name;
- *STUN Server Port* – UDP port of STUN server (the value by default is 3478);
- *Minimum keep alive period, s* and *Maximum keep alive period, s* – define the time interval in seconds for periodic transmission of messages to STUN server for public address discovery and modification.

If *Manual* mode is selected, the client's public address is set manually via the *NAT Address* parameter (the address must be entered in IPv4 format).

Through TR-069, you may implement main configuration of the device, firmware update and reading the data on the device (firmware version, model, serial number, etc.), uploading/downloading of configuration file, remote reboot (TR-069, TR-098 specifications are supported). To apply a new configuration and store settings into the non-volatile memory, click the '*Apply*' button. To discard changes click the *Cancel* button.

## The 'Advanced' submenu

Use this menu to set reserved VLAN ID and enable UPnP.

UPnP

Enable UPnP
☒

Reserved VLAN ID

Start VLAN ID
1

End VLAN ID
6

Local management via Ethernet

Enabled
☒

Management IP-address
192.0.3.1

Netmask
255.255.255.0

#### UPnP

UPnP is used by some applications (e.g. DC clients such as FlylinkDC++) to create forwarding rules for TCP/UDP ports used by these applications on a higher router. It is recommended to enable UPnP for operation of file exchange services on a network.

- *Enable UPnP* – when checked, UPnP is enabled, otherwise – disabled.

#### Reserved VLAN ID

Reserved VLAN ID – the list of service VLANs, which are used for solving intrasystem tasks.

- *Start VLAN ID* – starting VLAN ID value in the reserved range;
- *End VLAN ID* – ending VLAN ID value in the reserved range.



When 'Use Management VLAN' is checked and Management VLAN configured incorrectly, there is a possibility of losing access to the device. The device will be available when connecting via Ethernet by address 192.0.3.1.

## Configuration example

1. Connect PC to LAN port of injector;
2. Enter IP address of the device to URL bar of a browser (192.168.1.1 by default, if address was not obtain via DHCP); When connection is established successfully, the window with Login and password fields will be displayed. Fill the fields and click 'Log in'. (By default, login: **admin**, password: **password**).

The screenshot shows a web-based login form. It has two input fields: the first is labeled 'Login:' and contains the placeholder text 'Enter login'; the second is labeled 'Password:' and contains the placeholder text 'Enter password'. Below these fields is a blue button with a white checkmark icon and the text 'Log In'.

If the window is not displayed, make sure that the PC and the device are in the same network.

Monitoring
Network
System

Internet
MAC Management
Firewall
Routes
SNMP

Common Settings

Hostname

WAN

Device Mode

Wireless Station

Connection Settings

SSID

shipovalov\_test1

Q Scan Environment

802.11 Mode

802.11ac

Channel Bandwidth

80 MHz

Security Mode

Off

Tx Power (dBm)

24

Short Guard Interval

☒

Fixed Center Frequency

☐

Limit Channels

☐

Fixed Transmit Rate

Auto

Maximal Transmit Rate

Auto

ACK Timeout

64

Network Mode

Bridge

Priority

DSCP

Protocol

DHCP

VLAN Trunk Mode

☐

Alternative Vendor ID (option 80)

☒

Vendor ID (option 80)

Primary DNS Server

Secondary DNS Server

Tx Broadcast Rate Limit (packets/sec)

0

Traffic Shaper

☐

Apply

Cancel

Implement configuration on the Internet tab. In Network Mode field, select the required mode: Bridge or Router. If static settings are used for connection to a provider network, choose «Static» value in «Protocol» field and fill the fields: «IP address», «Netmask», «Default gateway», «Primary DNS Server», «Secondary DNS Server» – the values are given by service provider.

Configure connection to a base station. Specify SSID of the wireless network, you want to connect to, in the corresponding field. Select security mode through which authentication in the selected wireless network is implemented and specify the key if using an encrypted network. After clicking on the 'Apply' button, the subscriber station will search for the specified SSID on the air and, upon detection, will attempt to connect to the base station with the specified parameters. If the parameters are specified correctly and the signal level is sufficient, a successful connection will occur.

## Spectrum Analyzer

To use the embedded spectrum analyzer on the WB-2P-LR2, you need to login to the device via telnet or ssh. Enter the **spectrum-analyzer** command to run it. The analysis time for all the radio channels in the range is approximately 5 minutes.



Please note that all clients will disconnect from the base station during spectrum analyzer operation. The subscriber stations will be connected again only when the spectrum analyzer finishes its work.

The result can be obtained using the **spectrum-analyzer-result** command. Information on the loading of each channel (in percent) will be displayed in the console:

```

root@WB-2P-LR2:~$ spectrum-analyzer
Spectrum analyzer scanning in progress
root@WB-2P-LR2:~$
root@WB-2P-LR2:~$ spectrum-analyzer-result
=====start dump config=====
node: Monitoring.Network.SpectrumAnalyzer
    name: 1, value: 13
    name: 2, value: 21
    name: 3, value: 1
    name: 4, value: 3
    name: 5, value: 20
    name: 6, value: 76
    name: 7, value: 9
    name: 8, value: 3
    name: 9, value: 3
    name: 10, value: 10
    name: 11, value: 28
    name: 12, value: 22
    name: 13, value: 10
=====end dump config=====

```

## Automatic DHCP-based update algorithm

The screenshot shows a web interface for configuring DHCP-based Autoprovisioning. The interface has a top navigation bar with tabs: Monitoring, Network, IPTV, and System (selected). Below the navigation bar are sub-tabs: Time, Access, Log, Passwords, Configuration Management, Firmware Upgrade, Reboot, Autoprovisioning (selected), and Advanced.

The main content area is titled "DHCP-based Autoprovisioning" and contains the following settings:

- Provisioning Mode:** Configuration and Firmware (dropdown)
- Parameters Priority from:** DHCP options (dropdown)
- Configuration File:** (text input)
- Configuration Update Interval, s:** 300 (text input)
- Firmware File:** (text input)
- Firmware Upgrade Interval, s:** 3600 (text input)

Below this section is the "TR-069 Autoconfiguration" section, which is divided into three sub-sections:

- Common:**
  - Enable TR-069 Client:** ☒
  - ACS Server Address:** http://update.local:9595/ (text input)
  - Enable Periodic Inform:** ☒
  - Periodic Inform Interval, s:** 60 (text input)
- ACS Connection Request:**
  - User Name:** acs (text input)
  - Password:** acsacs (text input)
- Client Connection Request:**
  - User Name:** admin (text input)
  - Password:** admin (text input)

At the bottom of the TR-069 Autoconfiguration section is the "NAT Settings" sub-section:

- NAT Mode:** Off (dropdown)

At the bottom of the page are two buttons: "Apply" (with a checkmark icon) and "Cancel" (with an X icon).

Automatic device update procedure algorithm is determined by the '*Parameters priority from*' parameter value.

1. If the '*Static settings*' value is selected, then the full path (including the access protocol and server address) to the configuration files and firmware is determined from the '*Configuration file*' and '*Firmware file*'. Full path should be specified in URL format: <protocol>://<server address>/<path to file>, where:

- <protocol> – protocol used for downloading corresponding files from the server (TFTP is supported);
- <server address> – address of the server with a file to be downloaded (domain name or IPv4);
- <path to file> – path to file on the server.

You may use the following macro in URL (reserved words substituted with the specific values):

- *\$MA* – MAC address – instead of this macro, the device inserts its own MAC address in the file URL;
- *\$SN* – Serial number – instead of this macro, the device inserts its own serial number in the file URL;
- *\$PN* – Product name – the macro is substituted with device's model name in file URL (e.g., WB-2P-LR2).

For MAC address, serial number and model name, see 'Device' section on the monitoring page.  
URL examples:

<ftp://download.server.loc/firmware.file>, <http://192.168.25.34/configs/WB-2P-LR2/my.cfg> ,

[ftp://server.tftp/\\$PN/config/\\$SN.cfg](ftp://server.tftp/$PN/config/$SN.cfg), [http://server.http/\\$PN/firmware/\\$MA.frm](http://server.http/$PN/firmware/$MA.frm) , etc.

Some URL parameters might be omitted. For example, configuration file may be specified in the following format:

<http://192.168.18.6>

or

config\_wb.cfg

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used:

- For protocol: tftp;
- For a server address: update.local;
- For a configuration file name WB-2P-LR2.cfg;
- For a firmware file name WB-2P-LR2.fw.

Thus, if the '*Configuration File*' and '*Software File*' fields are left empty, options 43 or 66, 67 with the location of these files will not be received via DHCP — the URL of the configuration file will look like:

<ftp://update.local/WB-2P-LR2.cfg> ,

and the firmware file URL:

<ftp://update.local/WB-2P-LR2.fw> .

2. If the 'DHCP options' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), thus, address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If URL parameters are not provided by DHCP options, default parameters values will be used:

- For protocol: tftp;
- For a server address: update.local;
- For a configuration file name WB-2P-LR2.cfg;
- For a firmware file name WB-2P-LR2.fw.

#### Option 43 format (Vendor specific info)

1|<acs\_url>|2|<rcode>|3|<username>|4|<password>|5|<server\_url>|6|<config.file>|7|<firmware.file>|8|<vlan\_tag>, where:

1 – TR-069 autoconfiguration server address code;

2 – 'Provisioning code' parameter specification code.

3 – code of the username for TR-069 server authorization;

4 – code of the password for TR-069 server authorization;

5 – server address code; server address is specified in URL format: <ftp://address> or <http://address> . The first version represents TFTP server address, the second version – HTTP server address;

6 – configuration file name code;

7 – firmware file name code;

8 – a code of VLAN tag for management;

'|' – mandatory separator used between codes and suboption values.

#### Algorithm of identification for configuration file and firmware file URL parameters from DHCP Options 43 and 66, 67.

1. DHCP exchange initialization  
Device initializes DHCP exchange after the startup.
2. Option 43 analysis  
When Option 43 has been received, suboption 8 is analyzed (vlan\_tag):
  - if there is a suboption and it is different from current VLAN tag, DHCP exchange is initiated in new VLAN;



- suboption is absent or present and does not differ from the current VLAN tag: suboptions with codes 5, 6, and 7 are analyzed to determine the server address and the names of the configuration files and software.

### 3. Option 66 analysis

If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be searched. If the system fails to obtain the firmware file name, Option 67 will be searched. They are used for TFTP server address and the firmware file path extraction respectively. Then, configuration and firmware files will be downloaded from Option 66 address via TFTP.

#### Special aspects of configuration updates

Configuration file should be in **.tar.gz** format (this format is used when configuration is saved from the web interface in the «System» – «Configuration management» tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

#### Special aspects of firmware updates

The firmware file must be in the **.tar.gz** format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in tar.gz archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.



**Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update that will lead to the device boot partition corruption. The device will become inoperable. To restore the device operation, use the instruction provided in [System recovering after firmware update failure](#).**

## System recovering after firmware update failure

If while the firmware update (through the web interface or through autoupdate mechanism based on DHCP) a failure occurred (e.g. due to power cutoff) and the device does not operate (the 'Power' indicator is constantly solid red), use the following algorithm to recover the device:

- Unpack the archive with firmware file;
- Connect PC to the device port. Set the following subnet mask on the network interface: 192.168.1.0/24;
- Run the TFTP client on the PC (for Windows, it is recommended to use the Tftpd32), specify 192.168.1.6 as the remote host address, and select the linux.bin file from the unpacked software archive for transfer;
- Run the command to send a file to a remote host (the **Put** command). The process of file transmission will be launched;
- If the transmission has started, please, wait for finishing. The device will write the firmware to its memory and launch the system automatically. The time of writing takes approximately 8 minutes. If the process is completed successfully, 'Power' indicator will be green or orange. The configuration of the device before failure is saved. If you can not connect the device, reset it to factory settings;
- If the process has not started, make sure that the network settings of PC are correct and try again. If it does not work, sent the device to maintenance service or proceed recovery using the connection via COM port through a special adapter (if available);

## Appendix . Launch user script when starting the system

Sometimes you need the device to implement certain actions when starting, which cannot be implemented through settings in configuration file. In this case you may configure a user script through a configuration file that will be launched when the system starting. You may set any needed commands sequence.

For user script launching, there is a settings section in the configuration file `cfg.yaml`:

```
UserScript:
Enable: "0"
URL: ""
```

The *'Enable'* option allows (if the value is 1) or denies (if the value is 0) the script launch, the path to which is specified in the *URL* parameter.

The userscript might be located on remote server as well as on the device. The script is loaded via HTTP or TFTP from remote server. Examples of configuration files for user script launching using different sources are given below:

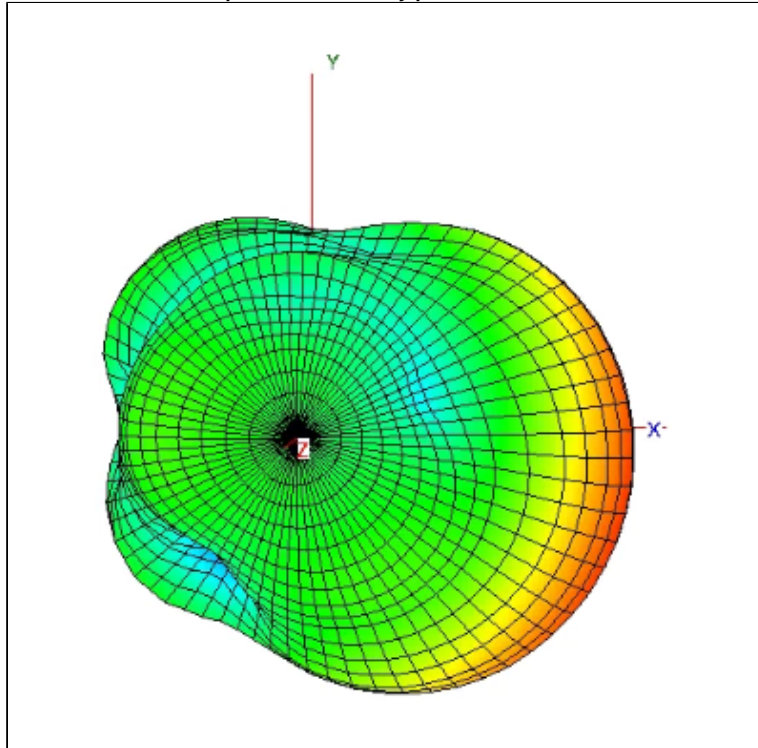
1. Launch from HTTP server  
To launch a script from HTTP server, enter the entire path to the file in HTTP-URL format to *URL* parameter:  
`URL: "http://192.168.0.250/user-script/script.sh"`  
In this case, after the device started, file `script.sh`, which is kept in the catalogue having 192.168.0.250 address, will be automatically loaded via HTTP from the defined server. Then it will be launched.
2. Launch from TFTP server  
To launch a script from TFTP server, enter the entire path to the file in TFTP-URL format to *URL* parameter:  
`URL: "tftp://192.168.0.250/user-script/script.sh"`  
In this case, after the device started, file `script.sh`, which is kept in the catalogue having 192.168.0.250 address, will be automatically loaded via TFTP from the defined server. Then it will be launched.
3. Local script launch  
Due to the peculiar properties of the file system, a local script should be stored in `/etc/config` catalogue as the content of the catalogue is saved after device reload. The script in the `/etc/config` directory can be created either using the vi editor, or download it from an external TFTP server

(using the `tfip -gl sh <TFTP-server address>` command). After creating a script, you should set rights for launching using the following command:  
`chmod 777 /etc/config/user.sh`  
In configuration file, URL for local script launching should be set as follows:  
URL: "[File:///etc/config/user.sh](#)"

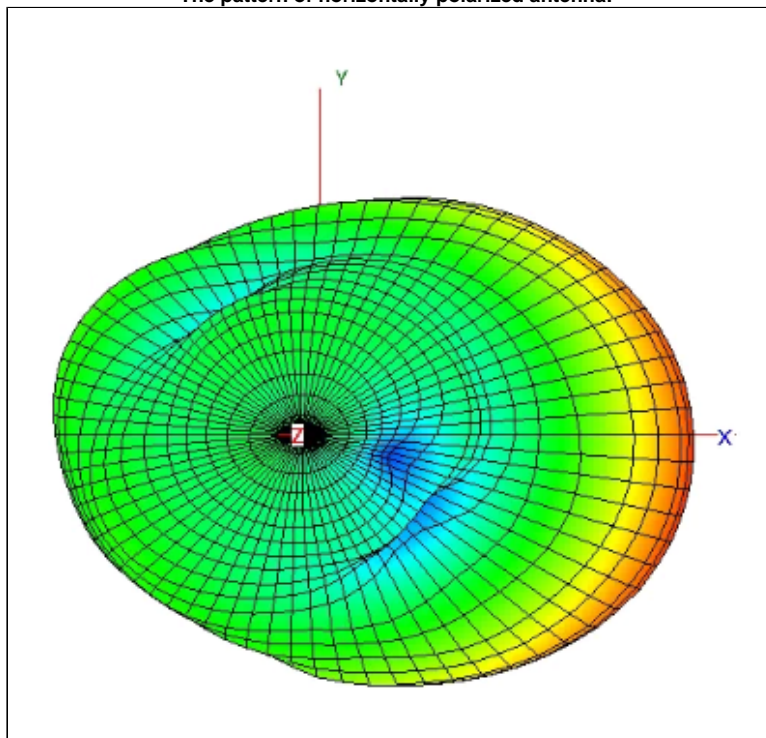
A user script should start from the `#!/bin/sh` directive.

## Application B. Antenna patterns

The pattern of vertically polarized antenna:



The pattern of horizontally polarized antenna:



# The list of changes

Document version	Issue date	Revisions
Version 1.2	25.06.2021	Synchronization with firmware version 2.4.6
Version 1.2	22.12.2020	Synchronization with firmware version 2.4.1
Version 1.1	07.04.2020	Synchronization with firmware version 2.4.0  Added: 4.4 Test changes mode  Changes in sections: 5.2.1 The «Network/Internet» menu
Version 1.0	06.11.2019	First issue
<b>Firmware version</b>		2.4.6