

# 1.19.3 WOP-12ac-LR. Quick guide for FBWA configuration via web interface

Wireless access point

WOP-12ac-LR

Application to the user manual

Quick guide for FBWA configuration via web interface

Firmware version 1.19.3 (04.2020)

IP:- <http://192.168.1.10>

User Name: admin

Password: password

## Annotation

This manual specifies the following:

- WOP-12ac-LR configuration via web interface;
- WB-1P-LR configuration via web interface;
- RG-4402G configuration via web interface.

The manual gives an example of device configuration without using a soft controller.

The following scheme is given as an example.

Figure 1 – Network structure

It is proposed to provide the subscriber with 3 types of services:

- Internet;
- VoIP;
- IPTV.

In the presented model, services (Internet, VoIP and STB +Multicast) operate in separate VLANs. All VLANs from provider network pass without change through the Wi-Fi base station to each subscriber station in tagged form. On the subscriber side of the client Wi-Fi equipment, traffic is received and terminated on a router (RG-4402G). In his turn, the subscriber can connect his equipment to the LAN port of the router to receive the «Internet» service, he can connect the telephone to the FXS port of the router to receive the «VoIP» service. Also, by connecting STB to the LAN port of the router, the subscriber receives the IPTV service.

To manage devices, static IP addresses are set. The «Internet» service is provided under the PPPoE protocol. For the «VoIP» service, the IP address is also issued via DHCP in a separate VLAN. Configuring and managing the STB is separate from the Multicast VLAN.

List of used VLANs:

- Management – VLAN 10;
- Internet – VLAN 11;
- VoIP – VLAN 12;
- IPTV – VLAN 13;
- STB – VLAN 14.

## WOP-12ac-LR configuration

### Connecting an access point to PC

PoE technology is used to power the WOP-12ac-LR, allowing it to transfer power through a UTP cable. A PoE injector is used to connect.

Connect the access point to the «Data & Power» connector of the injector, and the computer to the «Data» connector. Connect the injector to a 220V power supply.

### Configuring computer network interface settings

Install the following network interface settings on the computer:

- IP 192.168.1.5;
- Subnet mask: 255.255.255.0;
- Default gateway: 192.168.1.1.

### Connection to the WOP-12ac-LR web interface

To connect to the web interface of the WOP-12ac-LR, enter the following to the URL bar of your browser:

- **192.168.1.10**

In the window that appears, enter:

- User Name: **admin**
- Password: **password**

If the authorization page is not displayed after entering the device IP in the browser, check the IP address on the PC and switch settings. If the configuration on the device has been changed (is not a default one), reset the device to factory settings. To do this, press and hold the «F» button on the side panel of the device for 20 seconds, to access the «F» button, you must first unscrew the process screw.

## Firmware update:

Preliminary download the firmware file from <http://eltex-co.com/support/downloads/> and save it on your computer. After obtaining the relevant firmware version, open the menu «**Maintenance**», «**Upgrade**» tab and perform the following:



- Click the «**Switch**» button if you want to switch to an Alternative firmware image set in the «**Secondary Image**» field;
- **Upload Method** – check the «HTTP» box;
- **New Firmware Image** – click the «**Select file**» button and select relevant firmware version, click «**Open**»;
- Click «**Upgrade**». The update process will take several minutes (its current status will be indicated on the page), after which the access point will automatically reboot.



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

## Network settings:

You may check the current firmware version in the «**Basic Settings**» menu (Firmware Version).

For remote management of WOP-12ac-LR, you should set network parameters of the device according to the settings of the network that you intend to use. In the «**Manage**» menu, open «**Ethernet Settings**» tab and perform the following:

- 
- **Management VLAN ID** – set the number of VLAN that you are going to use for access point management. VLAN1 is used in the given example;
  - **Connection Type** – selection of the method for setting the IP address on the control interface, through which the device's WAN interface will be connected to the provider's services network:
    - DHCP – operation mode, when IP address, subnet mask, DNS server address, gateway are set by default and other parameters required for operation are obtained from DHCP server automatically;
    - Static IP – operation mode, when IP-address and all necessary parameters for WAN-interface are assigned as static.

In our case, a static IP address is used on the control interface. To assign an IP address to access points manually, select «**Static IP**». Specify the IP address of WOP-12ac-LR (in the example, it is 192.168.1.10) in the «**Static IP Address**» field. Enter the address of the default gateway in the «**Default Gateway**» field. Changing the network mask is optional. Click «**Update**».



Before changing the settings, make sure that the managing computer has the access to the access point. In case of erroneous changes, the settings can be rolled back by resetting the access point to the factory settings.

## Radio interface configuration

The access point has 3 radio interfaces that operate in the 5 GHz band.

To configure the radio interface, go to the «**Manage**» menu, open the «**Wireless Settings**» tab and perform the following:

- 
- **Country** – select settings according to the rules of selected country. Select «**Russia**» in the list;
  - **Radio Interface** – radio interface status:

- On – when checked, the radio interface is enabled;
- Off – when checked, the radio interface is disabled.
- **MAC Address**—MAC address of the radio interface;
- **Mode** – operating mode of the radio interface;
- **Channel** – channel number for work of wireless network. If you select «Auto», the channel with the least number of working access points on this channel is automatically determined taking into account the specified region;
- **Airtime Fairness** – technology of on-air fairness (limits data transfer to clients by equal transmission time):
  - On – when checked, the technology is enabled;
  - Off – when checked, the technology is disabled.

Radio1 configuration example:

- **Radio Interface** – check the «On» box;
- **Mode** – select value «IEEE 802.11a/n/ac».

Click «Update».

In the «Manage» menu, open the «Radio» tab and perform the following:

---

To go to the advanced settings, click «+» opposite «Advanced settings»:

---

- **Radio** – selects wireless Wi-Fi interface;
- **Status** – configurable Wi-Fi interface status:
  - On – when checked, the Wi-Fi interface is enabled;
  - Off – when checked, the Wi-Fi interface is disabled.
- **Mode** – operating mode of the radio interface:
  - IEEE 802.11a/n/ac – 5 GHz frequency range, maximum data rate of 867 Mbps in a 2x2 MIMO scheme.
- **Channel** – channel number for work of wireless network. If you select «Auto», the channel with the least number of working access points on this channel is automatically determined taking into account the specified region;
- **Channel Bandwidth** – channel bandwidth (available for 802.11n/ac modes). The 802.11n specification allows you to use a 40 MHz channel width in addition to the 20 MHz channel width used in other modes. Using channels with bandwidth of 40 MHz can increase the data transfer rate, but reduces the number of disjoint channels. The 802.11ac specification allows the use of a channel width of 80 MHz in addition to the possible values of 20 MHz and 40 MHz;
- **Transmit Chain** – antenna activity flags. When checked, the corresponding antenna is enabled;
- **VLAN list** – list of VLANs allowed for broadcasting. This setting is relevant for the VAP operating mode - VlanTrunk.

Radio1 configuration example:

- **Radio** – select value «1»;
- **Channel** – set «Auto»;
- **Channel Bandwidth** – set «80 MHz»;
- **VLAN list** – add each VLAN separately - 10, 11, 12, 13, 14.

Click «Update».

## VAP settings

On each wireless interface, you may configure up to 8 virtual access points. Each access point may have individual name of wireless network (SSID) and type of authentication/authorization. To configure VAP, go to the «Manage» menu, open the «VAP» tab and perform the following:

---

Access points configuration:

- **Radio** – selection of a configurable radio module;
- **VAP** – sequence number of the virtual access point;
- **Enabled** – when checked, the virtual access point will be enabled, otherwise it is disabled;
- **VLAN ID** – VLAN number to which the virtual access point is associated;
- **SSID** – wireless network name;
- **Broadcast SSID** – when checked, SSID broadcasting is on, otherwise it is disabled;
- **Station Isolation** – when checked, station traffic isolation from each other within the same VAP is enabled;
- **VLAN trunk** – when checked, the trunk port is used to connect the subscriber;
- **General Mode** - when checked, General port will be used to connect client equipment - receiving and transmitting tagged and untagged traffic;
- **General VLAN ID** - VLAN number, which will be removed in the direction of the client equipment/into which untagged traffic will be wrapped;
- **Security** – wireless access security mode:
  - None – do not use encryption for data transfer. The access point is available for any subscriber to connect;
  - WPA Personal – WPA and WPA2 authentication;
  - WPA Enterprise – certification mode of wireless devices, in which the client is authorized on a centralized RADIUS server.
- **MAC Auth Type** – authentication mode of clients by MAC address:
  - Disabled – do not use client authentication by MAC address;
  - RADIUS – use client authentication by MAC address using a RADIUS server;
  - Local – use client authentication by MAC address using the local address list generated on this access point.

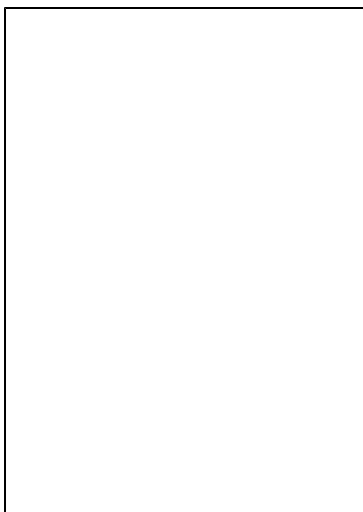
Radio1 VAP0 configuration example:

- **Radio** – select value «1»;
- **Enabled** – set the flags for VAP 0;
- **SSID** – enter the wireless network name«**Eltex VAP**»;
- **Broadcast SSID** – set the flag to enable broadcasting of the SSID name;
- **VLAN trunk** – set the flag to use the trunk port when connecting the WB-1P-LR;
- **Station Isolation** – set a flag to prohibit packet transfer between clients;
- **Security** – select the WPA Personal network security mode. Enter the password «**Eltex123**» in the «**Key**» field.

Click «**Update**».

## Enable WMF

In the «**Wireless Multicast Forwarding**» section multicast packet forwarding is configured:



- **Radio** – selection of a radio module;
- **VAP** – number of the virtual access point;
- **Enabled** – when checked, the virtual access point will be enabled, otherwise it is disabled;
- **WMF-Enabled** – when checked, the function of broadcasting multicast packets to unicast packets on a virtual access point will be enabled, otherwise it will be turned off.

WMF for Radio1 VAP0 configuration example:

- **Radio** – select value «1»;
- **WMF-Enabled** – set the flags for VAP 0.

Click «**Update**» to save changes.

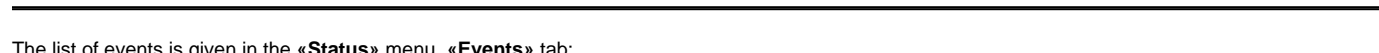
Configuration for Radio2 and Radio3 processes in the same way.

## Monitoring main parameters of wireless network

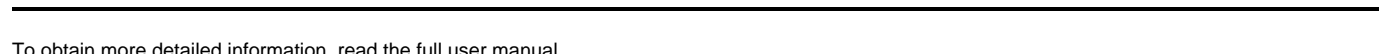
You may view the list of connected users in the «**Status**» menu, «**Client Association**» tab:



The list of third-party access points in WOP-12ac-LR area with data on wireless channel used and transmitted signal level is presented in «**Status**» menu, «**Rogue AP Detection**» tab:



The list of events is given in the «**Status**» menu, «**Events**» tab:



To obtain more detailed information, read the full user manual.

## WB-1P-LR configuration

## Connecting the device to PC

PoE technology is used to power the device, allowing it to transfer power through a UTP cable. A PoE injector is used to connect. Connect the device to the «**Data & Power**» connector of the injector, and the computer to the «**Data**» connector. Connect the injector to the household power supply.

## Configuring computer network interface settings

Install the following network interface settings on the computer:

- IP: 192.168.1.5
- Subnet mask: 255.255.255.0
- Default gateway: 192.168.1.1

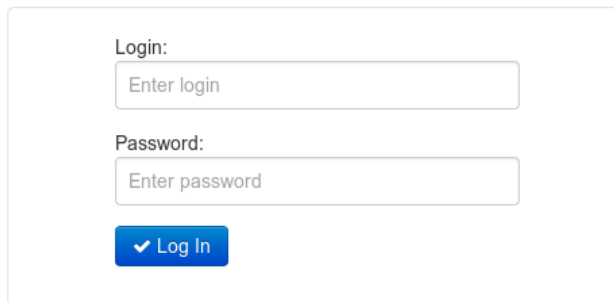
## Connection to the WB-1P-LR web interface

To connect to the web interface of the device, enter the following to the URL bar of your browser:

- **192.168.1.1**

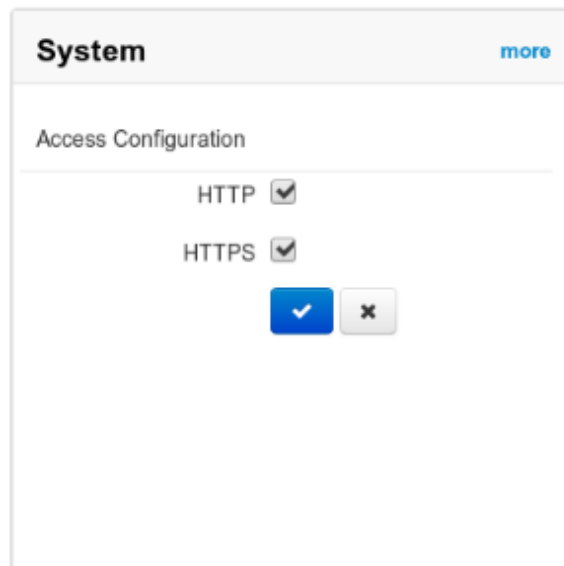
The authorization page will open, enter:

- Login: **admin**
- Password: **password**

A screenshot of a web interface login form. It contains 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 white checkmark and the text 'Log In'.

## Firmware update:

In the system settings, click on the link «**More**»:

A screenshot of the 'System' settings page. The title 'System' is at the top left, and a 'more' link is at the top right. Below the title is the 'Access Configuration' section. It shows 'HTTP' and 'HTTPS' both with checked checkboxes. At the bottom of this section are two buttons: a blue button with a white checkmark and a grey button with a white 'x'.

Go to the «**Update firmware**» tab. Preliminary download the firmware file from <http://eltex-co.com/support/downloads/> and save it on your computer. Firmware update for WB-1P-LR rev. M1:

## Firmware Upgrade

Active Version

1.13.1.69

Check for Update

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

Firmware Image

Обзор...

Файл не выбран.

Upload File

Firmware update for WB-1P-LR rev.B:

## Firmware Upgrade

Active Version

1.13.1.38

Check for Update

Backup Version

1.12.9.1

Set Active

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

Firmware Image

Обзор...

Файл не выбран.

Upload File

To do this, click the «**Select file**» button in the «**Firmware update file**» field and specify the path to the control program file in .tar.gz format.

- **Active Version** – installed firmware version, which is operating at the moment;
- **Backup Version** - the version of the firmware installed on the device, which can be accessed in case of problems with the active version of the firmware;
- **Check for update** – 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.

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.

## Attention! Do not power off the device!

File has been downloaded. Upgrading firmware is in progress. Please, wait about 3 min 26 sec

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

## Configure Wi-Fi connection to the base station

1. Connect to the web interface (see Section [Connection to the WB-1P-LR web interface](#)). In the Wi-Fi settings, click on the link «**More**»:

Wi-Fi Client

more

SSID

Eltex

Security Mode

WPA2

WPA Key

12345678

✓

✕

A page opens with a complete list of settings for Wi-Fi.

2. In the «**Network Identifier (SSID)**» field, enter the name of the Wi-Fi network to which the device will connect. If you use a Wi-Fi network without encryption to connect, then select «**Off**» in the «**Security mode**» field. If you use a Wi-Fi network with encryption for the connection, in the «**Security mode**» field, select the encryption mode that is configured on the base station and specify additional parameters (WPA key/username and password).

WAN

Connection Settings

SSID

Eltex

Q Scan Environment

802.11 Mode

802.11ac

Channel Bandwidth

80 MHz

Security Mode

WPA2

WPA Key

12345678

3. In the «**Operation mode**» field, select the operating mode of the «**Bridge**» device.

in the «**Protocol**» field select protocol for connection of the device via Wi-Fi interface to service provider network: Static or DHCP.

5. Set the flags in the options «**Use VLAN trunk**», «**Use Management VLAN**» and «**Use General VLAN**».

6. In the «**Management VLAN ID**» field, specify the VLAN number that will be used to manage the device. In the «**General VLAN ID**» field, specify the same VLAN number as in the «**Management VLAN ID**» field:

Network Mode	<input type="text" value="Bridge"/>
Priority	<input type="text" value="DSCP"/>
Protocol	<input type="text" value="Static"/>
IP Address	<input type="text" value="192.168.100.4"/>
Netmask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.100.1"/>
Primary DNS Server	<input type="text" value="8.8.8.8"/>
Secondary DNS Server	<input type="text" value="8.8.4.4"/>
VLAN Trunk Mode	<input checked="" type="checkbox"/>
Use Management VLAN	<input checked="" type="checkbox"/>
Management VLAN ID	<input type="text" value="10"/>
Management 802.1P	<input type="text" value="0"/>
Use General VLAN	<input checked="" type="checkbox"/>
General VLAN ID	<input type="text" value="10"/>
General 802.1P	<input type="text" value="0"/>

7. To apply the new configuration, click the **«Apply»** button.

For the example above, the following settings are used:

- In the field **«Network Identifier (SSID)»** specify **«Eltex»**;
- In the **«Security Mode»** field, select **«WPA2»**;
- In the **«WPA Key»** field, enter the key value **«Eltex123»**;
- Select the **«Bridge»** operation mode;
- In the **«Protocol»** field, select **«Static»**;
- In the **«IP address»** field specify the IP address: 192.168.100.4;
- In the **«Subnet mask»** field: 255.255.255.0;
- In the **«Default gateway»** field: 192.168.100.1;
- In the **«Management VLAN ID»** field specify the VLAN ID: 10;
- In the **«General VLAN ID»** field specify the VLAN ID: 10.

## Access the device from an external network

Go to the **«System»** submenu, **«Access»** tab. To get access to the device via external network set the following permissions:

### Web – External network:

- HTTP – when checked, connection to the device web configurator through WAN port via HTTP is enabled (insecure connection);
- HTTPS – when checked, connection to the device web configurator through WAN port via HTTPS is enabled (secure connection).

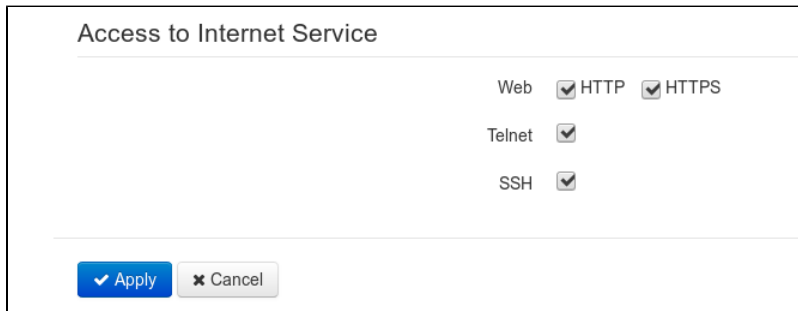
### Telnet – External network:

- Telnet – when checked, Telnet connection to the device through the WAN port is allowed.

### SSH – External network:



- SSH – when checked, SSH connection to the device through the WAN port is allowed.



Access to Internet Service

Web ☒ HTTP ☒ HTTPS

Telnet ☒

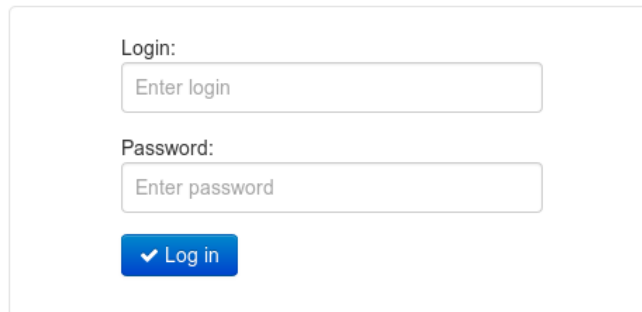
SSH ☒

To apply the new configuration, click the «**Apply**» button.

## RG-4402-G configuration

### Connection to RG-4402-G web interface

1. Turn on the computer to obtain network settings via DHCP and connect with a patch cord to one of the RG-4402G LAN ports.
2. To connect to the web interface of the device, enter the following to the URL bar of your browser:
  - **192.168.1.1**
3. In the window that appears, enter:
  - Login: **admin**
  - Password: **password**



Login:

Enter login

Password:

Enter password

### Firmware update:

1. In the system settings, click on the link «**More**»:

System

more

Access configuration

HTTP

☒

HTTPS

☐

✓

✗

2. Go to the «**Update firmware**» tab. Preliminary download the firmware file from <http://eltex-co.com/support/downloads/> and save it on your computer. To do this, click the «**Select file**» button in the «Firmware update file» field and specify the path to the control program file in .tar.gz format.

Firmware upgrade

Active version of firmware

1.14.1.527

Check for update

Firmware upgrade is also available at: <http://eltex.nsk.ru/downloads>

Firmware image

Обзор...

Файл не выбран.

If you return to version 1.9.x or later, configuration resets to default!

Upload file

3. 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.

Attention! Do not power off the device!

File has been downloaded. Upgrading firmware is in progress. Please, wait about 3 min 25 sec

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

## «Internet» service configuration

1. Connect to the web interface (see Section [Connection to the RG-4402-G web interface](#)).
2. In the «**Internet**» settings, click on the link «**More**»:

3. In the connection settings in the «**Operation mode**» field select «**Router**».

4. In the «**Protocol**» field, specify the type of protocol that is used to connect to the Internet. The following protocols are available:

- **Static** – operation mode, when IP address and other necessary parameters of WAN interface are set statically;
- **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;
- **PPPoE** – operation mode when PPP session is established on WAN interface;
- **PPTP** – operation mode when the Internet access is established via a tunnel, using PPTP.

5. Set the flag «**Use VLAN in external network**». In the «**VLAN ID**» field specify the VLAN number used for the Internet service.

6. To apply the new configuration, click the «**Apply**» button.

For the example above, the following settings are used:

- Select the «**Router**» operation mode;
- In the «**Protocol**» field, select «**PPPoE**»;
- In the «**Username**» field enter «**test**»;
- In the «**Password**» field: 12345678;
- In the «**Second access**» field select «**DHCP**»;
- In the «**VLAN ID**» field specify the VLAN ID: 11.

## VoIP service configuration

### *For VoIP, the Internet VLAN is used*

1. Go to the «**Settings**» section in the «**Network**» field to the «**Internet**» field.
2. Set the flag in the «**Use second access for VoIP**» field:

MTU 1462

Secondary access Static

Use the secondary access for VoIP ☐

IP address 192.168.15.100

3. Go to the «VoIP» menu To the «Network settings» tab. Set the flag in the «Use Internet settings» field:

VoIP network settings

Use internet settings ☒

IPSec settings

Enable ☐

✓ Apply ✕ Cancel

4. To apply the new configuration, click the «Apply» button.

### ***For VoIP, the separate VLAN is used***

1. Go to the «VoIP» menu, to the «Network settings» tab.
2. Remove the flag in the «Use Internet settings» field.
3. In the «VLAN ID» field specify the VLAN number used for VoIP.
4. In the «Protocol» field select the protocol for assigning the address to the VoIP service interface:
  - **Static** – operation mode, when IP address and other necessary parameters of WAN interface are set statically;
  - **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:

VoIP network settings

Use internet settings ☐

Use VLAN ☒

VLAN ID 10

802.1P 0

Protocol DHCP

Alternative vendor ID (option 60) ☐

DHCP Relay Agent Information (Option82) ☐

1st DNS-server

2nd DNS-server

IPSec settings

Enable ☐

✓ Apply ✕ Cancel

5. To apply the new configuration, click the «Apply» button.

In the example above, a separate VLAN is used for the VoIP service. To configure this operating mode, clear the «**Use Internet settings**» field, in the «**VLAN ID**» field, specify the value 12, in the «**Protocol**» field, select DHCP.

## Line parameters configuration

Go to the «**Line configuration**» tab. Select the first line. Set the flag in the «**Enable**» field. Then, fill in the following parameters:

- **Profile** – select SIP profile from the list of available profiles. To configure profiles, use the «**VoIP**» -> «**Profiles**» menu;
- **Phone number** – subscriber number assigned to the telephone port;
- **User name** – user name associated with this port (shown in Display-Name field of the From header in the outgoing SIP messages);
- **Use alternative number** – when selected, an alternative number will be inserted into the «**From**» header of SIP messages sent from this port (particularly, in order to hide the real number from the Caller ID system of the callee);
- **SIP port** – UDP port used to receive incoming SIP messages on the account and to transmit outgoing SIP messages from the account. It may take values from 1 to 65535 (the default value is 5060);
- **Calling party category** – enables transmission of outgoing messages in the From header; the latter is transmitted in Tel-URI format (see RFC3966);
- **Authentication username and password** – user name and password used for subscriber authentication on SIP server (and on registration server).

The screenshot shows the 'Edit line 1: Account settings' form. It includes an 'Enable' checkbox, a 'SIP profile' dropdown menu set to '1st profile', a 'Phone' text field with '001', an empty 'User name' text field, a 'Use alternative number' checkbox, a 'SIP port' spinner set to 5060, and a 'Calling party category' dropdown set to 'Off'. Under the 'Authentication' section, there is an empty 'Login' text field and a 'Password' text field with masked characters.

To apply the new configuration, click the «**Apply**» button.

The screenshot shows the 'Edit SIP profile' form. It includes a 'Profile includes' field set to 'Lines 1, 2', a 'Profile name' text field with '1st profile', a 'Proxy mode' dropdown set to 'Homing', an empty 'Proxy server' text field, a checked 'Registration' checkbox, an empty 'Registration server' text field, a 'Home server check method' dropdown set to 'Invite', and a 'Home server keepalive timeout, s' spinner set to 30.

## Profile configuration

1. Go to the «**Profiles**» tab.
2. Select the profile that was used in the line settings.
3. Specify the SIP server network address in the field «**SIP proxy server**». Set the flag in the «**Registration**» field.
4. Specify the network address of the device on which all subscribers of the telephone network are registered in order to provide them with the right to use communication services in the «**Registration server**» field.

5. To apply the new configuration, click the «**Apply**» button.

## IPTV service configuration

### *IPTV configuration*

1. Go to the «**IPTV**» menu, to the «**IPTV**» tab.
2. Set the flag «**Enable IPTV**».
3. In the «**IGMP Version**» field select the IGMP version.
4. Enable «**Periodic Subscription Update**» and specify the update period in the «**Update Period**» field.
5. Enable «**Fast leave**»:

Network VoIP **IPTV** Local interfaces System

**IPTV** STB

**IPTV settings**

Enable IPTV ☒

IGMP version 3

Renew subscription

Enable ☒

Renew subscription interval, s 30

Fast leave mode

Enable ☒

VLAN IPTV

Use VLAN ☐

HTTP proxy settings

Enable ☐

6. If a separate VLAN is used for IPTV, set the flag in the «**Use VLAN**» field. In the «**VLAN ID**» field specify the VLAN number used for IPTV.

**VLAN IPTV**

Use VLAN ☒

VLAN ID 0

802.1P 0

7. To apply the new configuration, click the «**Apply**» button.

To configure the «**IPTV**» service in accordance with the example above, the following settings must be performed:

1. Set the flag in the «**Use VLAN**» field;
2. In the «**VLAN ID**» field set the value **13**.

### *STB configuration*

1. Go to the «**IPTV**» menu, to the «**STB**» tab. Set the flag «**Enable STB**»:

Network VoIP **IPTV** Local interfaces System

IPTV **STB**

### STB VLAN Configuration

Enable STB ☒

Use VLAN ☐

*For binding of local interfaces to STB service go to page "Local interfaces - Functional assignment".*

2. If a separate VLAN is used for STB connection, set the flag in the «**Use VLAN**» field;
3. In the «**VLAN ID**» field specify the VLAN number used for IPTV;

### STB VLAN Configuration

Enable STB ☒

Use VLAN ☒

VLAN ID

802.1P

*For binding of local interfaces to STB service go to page "Local interfaces - Functional assignment".*

4. To apply the new configuration, click the «**Apply**» button.

To configure the STB in accordance with the example described in point 1, the following settings must be performed:

1. Set the flag in the «**Use VLAN**» field;
2. In the «**VLAN ID**» field set the value 13.

## Local interfaces configuration

To bind local interfaces to the STB service, go to the «**Local Interfaces**» menu on the «**Functional Assignment**» tab. Assign one of the device ports to the STB port. After that, the STB should only be connected to this port:

### Functional assignment

LAN 1

LAN 2

LAN 3

LAN 4

Wi-Fi 2.4 GHz

Wi-Fi 5 GHz

## VLAN management configuration

1. Go to the «**System**» menu on the «**Management Interface**» tab.
2. Set the flag «**Enable management interface**».
3. Select the management traffic type in the «**Access Type**» field:

- **Untagged** – management traffic to the device comes in untagged form. In this case, the VLAN must be configured for the Internet service;
- **Tagged** – a separate VLAN is used to control the device. If using the «Tagged» access type, in the «VLAN ID» field, specify the VLAN number that will be used to control the device.

The screenshot shows the 'Management interface' configuration page. The 'System' tab is selected. The 'Enable management interface' checkbox is checked. The 'Access type' dropdown is set to 'Untagged'. The 'Protocol' dropdown is set to 'DHCP'. The 'Alternative vendor ID (option 60)' checkbox is unchecked. There are empty input fields for '1st DNS-server' and '2nd DNS-server'. At the bottom, there are 'Apply' and 'Cancel' buttons.

4. In the «**Protocol**» field select the protocol for assigning the address to the VoIP service interface:

- **Static** – operation mode, when IP address and other necessary parameters of WAN interface are set statically;
- **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.

The screenshot shows the 'Management interface' configuration page. The 'Enable management interface' checkbox is checked. The 'Access type' dropdown is set to 'Tagged'. The 'VLAN ID' input field contains the value '20'. The '802.1P' dropdown is set to '0'. The 'Protocol' dropdown is set to 'Static'. There are empty input fields for 'IP address', 'Netmask', 'Default gateway', '1st DNS-server', and '2nd DNS-server'. At the bottom, there are 'Apply' and 'Cancel' buttons.

5. To apply the new configuration, click the «**Apply**» button.

To configure the management VLAN in accordance with the example described in point 1, the following settings must be performed:

- Set the flag in the «**Enable management interface**» field;
- In the «**Access Type**» field select «**Untagged**»;
- In the «**Protocol**» field, select «**Static**»;
- In the «**IP address**» field specify the IP address: 192.168.100.5;
- In the «**Subnet mask**» field: 255.255.255.0;
- In the «**Default gateway**» field: 192.168.100.1.



# Connection monitoring

When the session established successfully, the **Power** indicator on the device will light green. You can also track the uplift of a session in the «**Monitoring**» section of the «**Internet**» tab.

When the session is successfully established, the IP address received by the device should be displayed in the corresponding column (the figure below shows the state in which the address was not received).

Internet connection	
Network connection	Wired
Access protocol	PPPOE
IP address	address is not assigned
Provider inner IP address	78.0.0.17
<div>Refresh</div>	

If the device does not receive the address in the provider's internal network (fourth line), this means that either the device does not have access to the external network (check the WAN indicator - if it is not lit, it means there are problems with the cable), or in the network settings of the RG-4402-G VLAN was configured incorrectly.