Wireless access point

WOP-12ac-LR

Quick guide for FBWA configuration via web interface

Firmware version 1.22.2

IP address: 192.168.1.10

Username: admin

Password: password

Contents

1 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 softWLC controller.
The following scheme is given as an example.

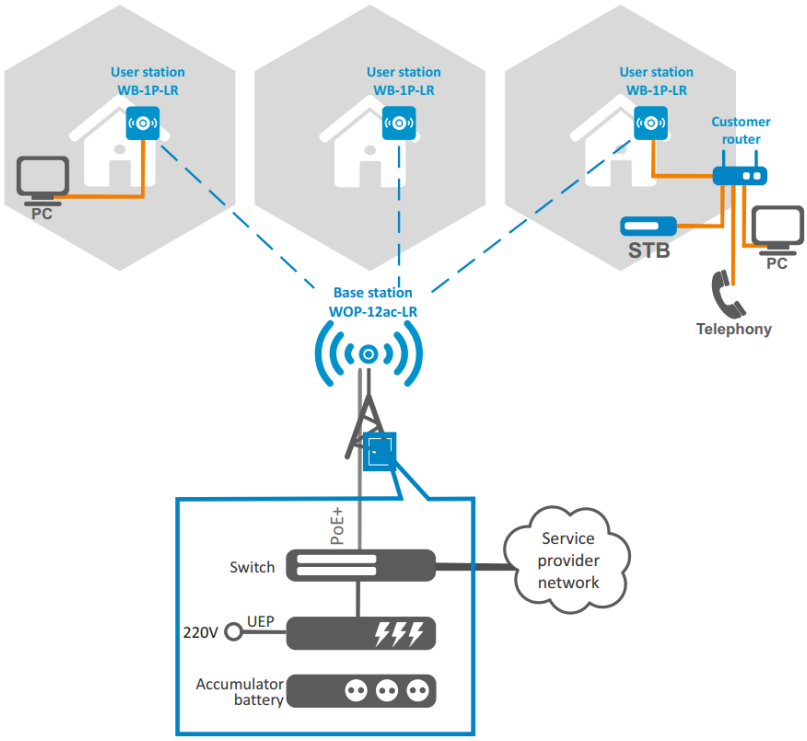


Figure 1 – Network structure

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. Configuration and management of 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.

2 WOP-12ac-LR configuration

2.1 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 for connection.
Connect the access point to the **Data & Power** connector of the injector, and the computer to the **Data** connector. Connect the injector to a 220 V power supply.

2.2 Configuring computer network interface settings

Set 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.

2.3 Connecting to the web interface

To connect to the web interface of the WOP-12ac-LR, perform the following:

1. Open a web browser, for example, Firefox, Opera, Chrome.
2. Enter the device IP address in the browser address bar.

   IP address by default: 192.168.1.10, subnet mask: 255.255.255.0.
   The device can obtain IP address via DHCP. Until then, it is available at the factory IP address.

   If the connection has been performed successfully, the authorization page will be displayed. Use the following data for authorization:

3. Enter username to “User Name” field and password to “Password” field.

   Factory default authorization settings: User Name – *admin*, Password – *password*.

4. Click the Logon button.

A starting page of the web interface will open in a browser window.

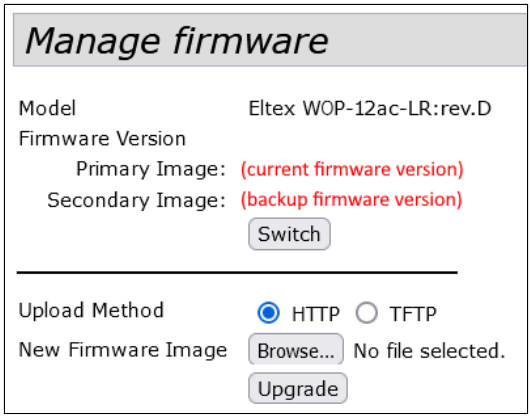
If after entering the IP address in the browser bar the authorization page does not appear, check the IP address on the PC/switch settings.
If the device factory configuration was changed, reset the current settings. To do this, press and hold the “F” button on the side panel of the device for 20 seconds. The color of the indicator should change to red – it means that the load is in progress.

2.4 WOP-12ac-LR firmware upgrade

For correct operation of WOP-12ac, it is recommended to upgrade the firmware to the latest version.

> The relevance of the version installed on the device can be clarified on the official website of the manufacturer in the Download Center section or by contacting the manufacturer directly. Contact details are given on the last page of this manual.

After obtaining the relevant firmware version, in the **Maintenance** menu, open **Upgrade** tab and perform the following:



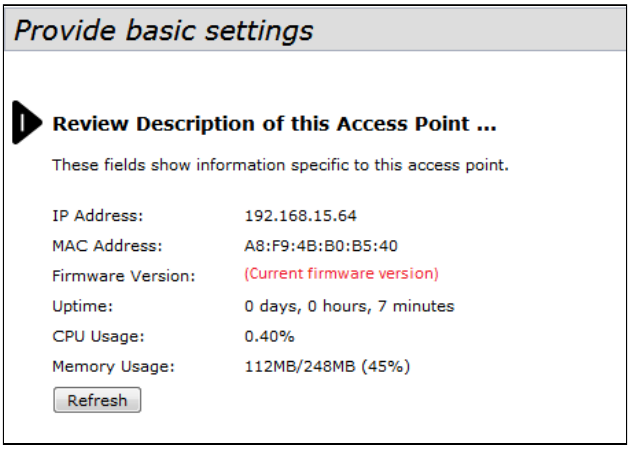
- *Upload Method* – check **HTTP**;
- *New Firmware Image* – click **Browse** button and select relevant firmware version in the window that opens.

Click **Switch** button to switch to an alternative firmware image set in **Secondary Image**.

To start the upgrade process, click **Upgrade**. 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 upgrade.

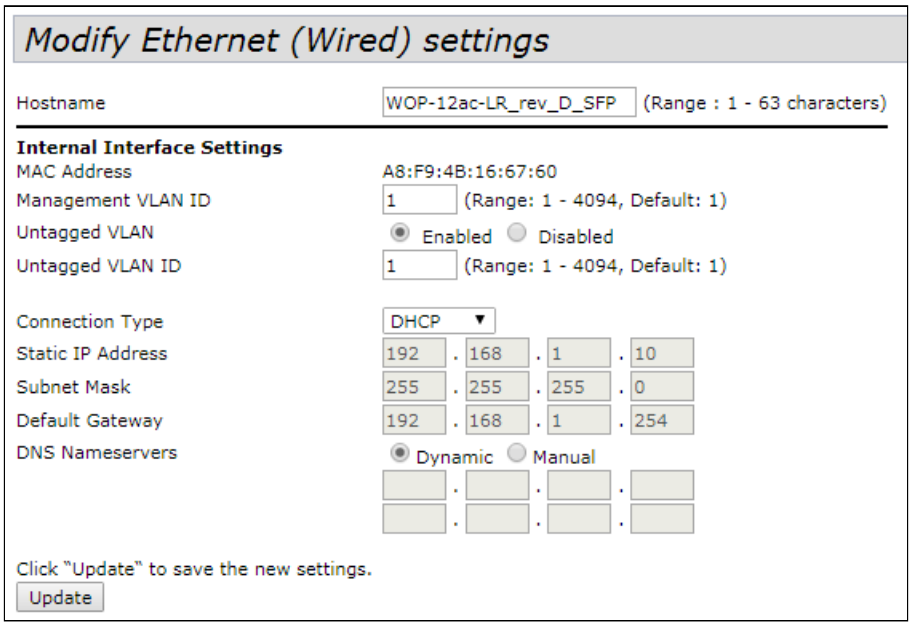
The current firmware version can be viewed in the **Basic Settings** menu. It is indicated in the **Firmware Version** field.



2.5 Network parameters

For remote management of WOP-12ac-LR, 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:



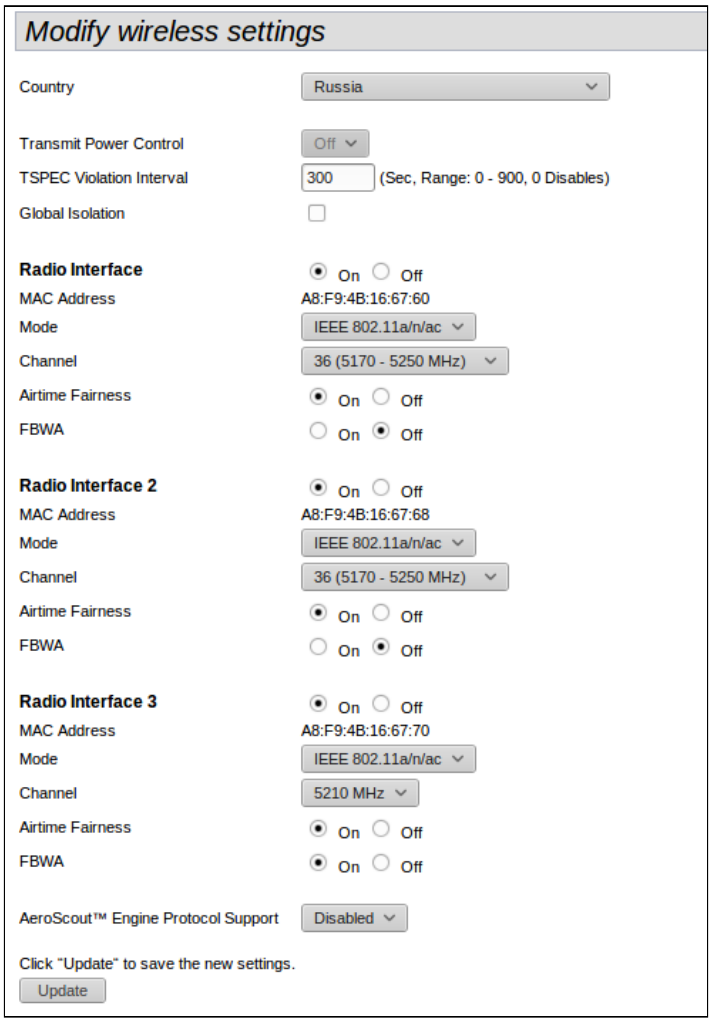
- *Management VLAN ID* – specify the VLAN number that will be used for access point management. VLAN 10 is used in the given example;
- *Connection Type* – selection of the method for setting the IP address on the control interface, through which the device's WAN interface will be connected to the provider's 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 this 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 making changes to the network settings of the access point, make sure that the host computer has access to the network where the access point will be located, based on the configured network settings. In case of entering and applying incorrect data while changing the settings, undo them by resetting the access point to factory settings. To do this, press and hold "F" button on the front panel of the device for 20 seconds until the LED indicator is blinking.

2.6 Radio interfaces 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:



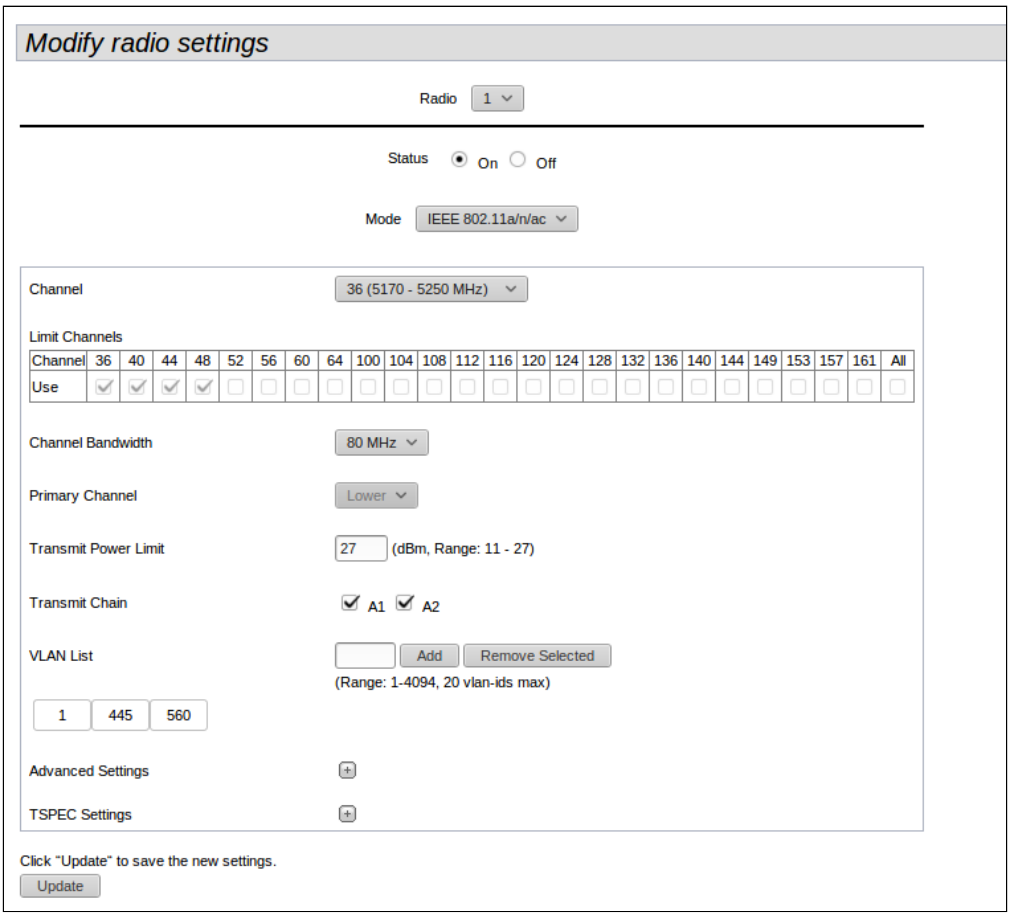
- *Country* – select settings according to the rules of selected country;
- *Radio Interface* – radio interface status:
  - *On* – when checked, the radio interface is enabled;
  - *Off* – when checked, the radio interface is disabled.
- *MAC Address* – MAC address of the radio interface;
- *Mode* – operating mode of the radio interface;
- *Channel* – channel number for operation of wireless network. If **Auto** is selected, 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:

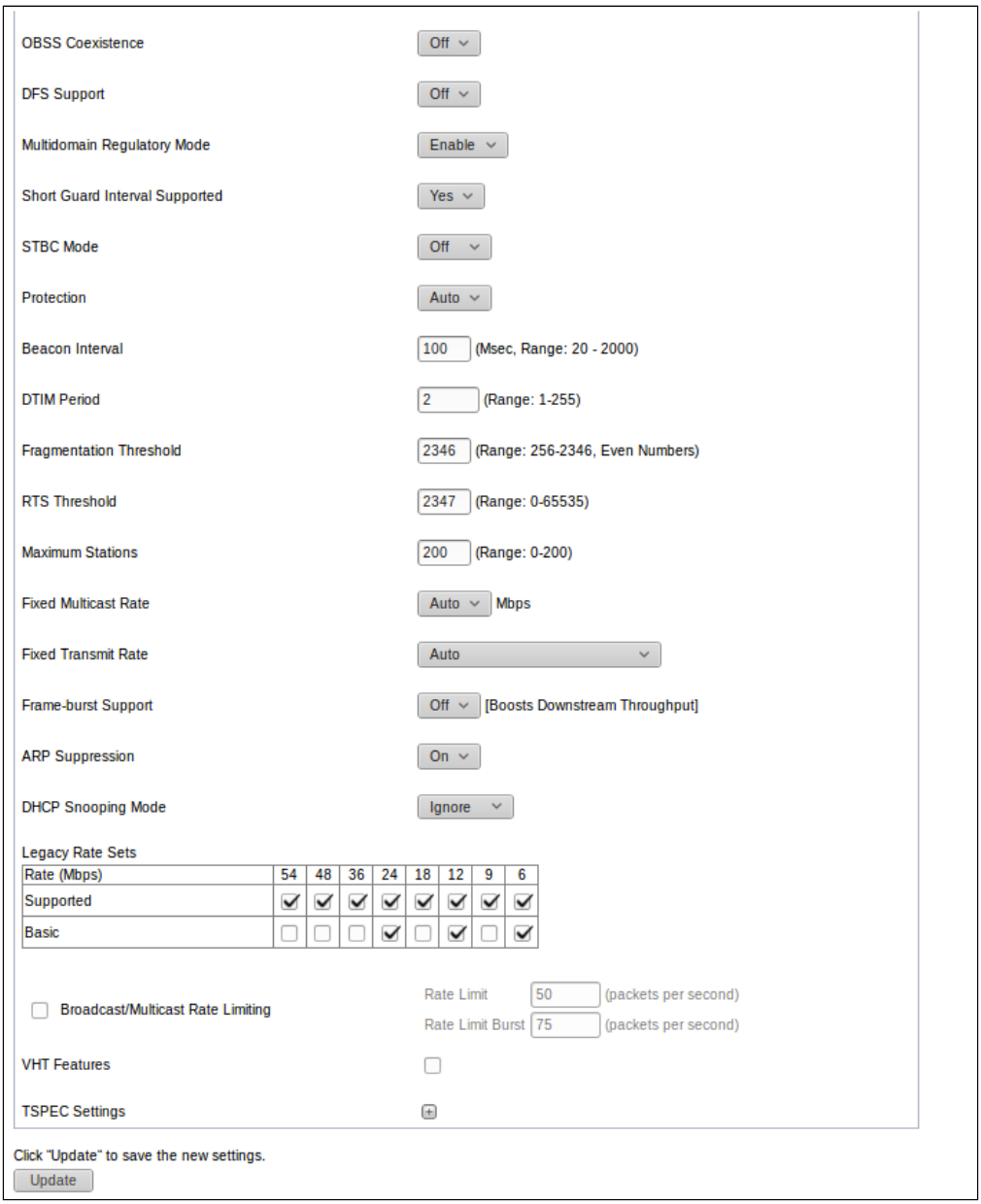
- *Radio Interface* – check the **On** box;
- *Mode* – select value **IEEE 802.11a/n/ac**.

To apply a new configuration and save setting to non-volatile memory of the access point, 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 operation of wireless network. If **Auto** is selected, 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.

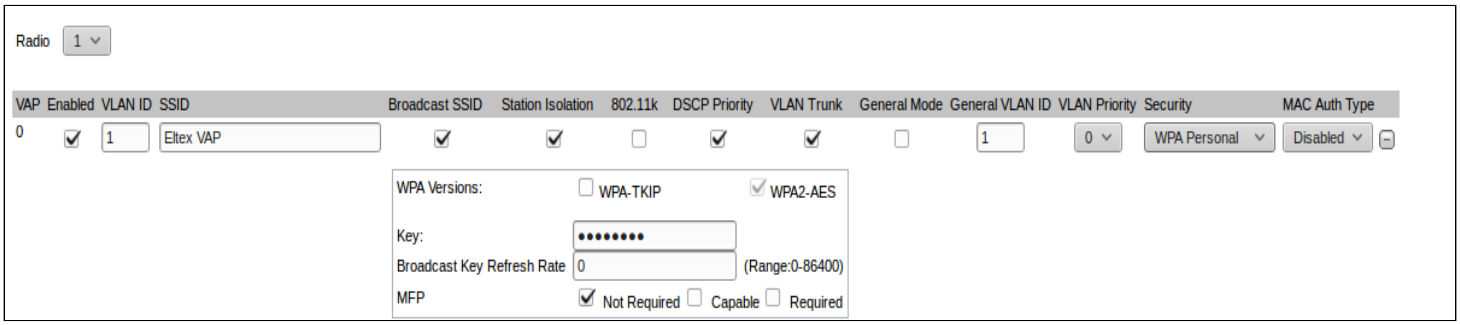
Radio1 configuration example:

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

To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

3 Virtual access points configuration

On each wireless interface, up to 8 virtual access points can be configured. 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.

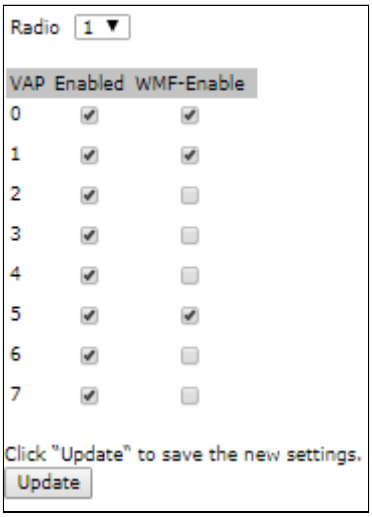
Radio1 VAP0 configuration example:

- *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 **Eltex123** password in the **Key** field.

To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

3.1 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-Enable* – 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 the same way.

3.2 Monitoring main parameters of wireless network

The list of connected users can be viewed in the **Client Association** tab of the **Status** menu:

View list of currently associated client stations

Click "Refresh" button to refresh the page.

Refresh

Total Number of Associated Clients 13

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capasity	Status
											Authorized
Eltex-Local (wlan0)	70:70:0d:d9:b0:2b	192.168.40.169	iPhoneViktoria2	00:00:00	-77	15 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	e0:b5:2d:7a:07:ff	192.168.40.205	iPhoneAleksandr	00:00:02	-79	13 dB	-92 dBm	69%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	dc:41:5f:64:1f:de	192.168.40.228	iPhone-Anuta	00:00:24	-70	22 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	b0:70:2d:bc:e1:39	192.168.40.200	iPhone-Anton	00:00:02	-77	15 dB	-92 dBm	94%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	2c:0e:3d:6b:29:48	192.168.40.81	Samsung-Galaxy-S7-edge	00:01:32	-53	39 dB	-92 dBm	96%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	38:a4:ed:18:e3:c7	192.168.40.227	MI5-MiPhone	00:02:13	-55	37 dB	-92 dBm	95%	Not supported	Not supported	Yes
Eltex-Local (wlan0)	44:00:10:b0:60:e6	192.168.40.239	iPhone-Olga	00:02:21	-47	45 dB	-92 dBm	97%	Not supported	Not supported	Yes
Eltex-Local (wlan1)	04:c2:3e:5e:f8:36	192.168.40.70	android-a55f042256a21ea	00:00:02	-72	20 dB	-92 dBm	75%	Not supported	Not supported	Yes
Eltex-Local (wlan1)	74:23:44:9e:50:c3			00:00:02	-43	49 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1)	d0:65:ca:6d:67:f2		android-f74c09ba39f7574e	00:00:05	-63	29 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1)	c8:aa:21:96:0e:a8	192.168.40.158	android-d772b762509129fa	00:00:06	-62	30 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1)	d0:5b:a8:b5:18:29	192.168.40.96	android-ab5a1351910958f9	00:00:13	-40	52 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Guest (wlan1vap1)	00:ec:0a:be:2a:a3	192.168.41.122	Redmi4X-Redmi	00:02:23	-35	57 dB	-92 dBm	95%	Not supported	Not supported	Yes

View list of currently associated client stations

Click "Refresh" button to refresh the page.

Refresh

Total Number of Associated Clients 13

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capasity	Status
											Authorized
Eltex-Local (wlan0)	70:70:0d:d9:b0:2b	192.168.40.169	iPhoneViktoria2	00:00:00	-77	15 dB	-92 dBm	100%	Not supported	Not supported	Yes

MAC:	70:70:0d:d9:b0:2b	Connection time:	00:00:00
AID:	8	Bandwidth:	20MHz
SSID:	Eltex-Local	PS Mode:	on
Mode:	802.11ac	Auth Mode:	WPA2
RSSI:	-77	Encryption:	AES-CCMP
VLAN:	148	Listen Interval:	20
Tx actual rate:	1	Rx actual rate:	0
Tx/Rx Packets:	203/176		
Tx/Rx Drop Packets:	0/0		
Tx/Rx Bytes:	83211/17792		
Tx/Rx Drop Bytes:	0/0		
Tx/Rx Rate:	130/86.7 Mbps		

Tx/Rx Statistics:

MCS	Rx Pkts	Tx Pkts	Tx Succ Pkts	Tx Retries	Tx Period Retries
1mbps	0	0	0	0.0%	0.0%
2mbps	0	0	0	0.0%	0.0%
5mbps5	0	0	0	0.0%	0.0%
6mbps	0	0	0	0.0%	0.0%
9mbps	0	0	0	0.0%	0.0%
11mbps	0	0	0	0.0%	0.0%

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 the **Status** menu, **Rogue AP Detection** tab:

View Rogue AP Detection

Click "Refresh" button to refresh the page.
Refresh

AP Detection for Radio 1 — Enabled / Disabled
AP Detection for Radio 2 — Enabled / Disabled
AP Detection for Radio 3 — Enabled / Disabled

Click "Update" to save the new settings.
Update

Detected Rogue AP List
Click "Delete old" to delete old entries from Detected Rogue AP List
Delete Old

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel [BandWidth]	Channel Blocks	Signal	Beacons	Last Beacon	Rates
Grant	a8:f9:4b:dc:f8:9a	wlan0	100	AP	ELTX-5GHz_WiFi_F898	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:dc:f7:62	wlan0	100	AP	ELTX-5GHz_WiFi_F760	On	On	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b4:8f:3f	wlan0	100	AP	(Non Broadcasting)	Off	Off	5	149 [80]	149 - 161		3	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:b4:8f:30	wlan0	100	AP	Eltex VAP	Off	Off	5	149 [80]	149 - 161		4	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:bd:0c:6d	wlan0	100	AP	ELTX-5GHz_WiFi_0C6B	On	On	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:e3:16:39	wlan0	100	AP	ELTX-5GHz_WiFi_1638	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:17:58:00	wlan0	100	AP	COUNTERS_5	Off	Off	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:dc:f8:39	wlan0	100	AP	ELTX-5GHz_WiFi_F838	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:17:57:e0	wlan0	100	AP	KRUTITSY	Off	Off	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:17:57:e1	wlan0	100	AP	Test_Ent1	On	On	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:e6:a7:70	wlan0	100	AP	tester9_5G	Off	Off	5	149 [80]	149 - 161		1	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:e3:16:81	wlan0	100	AP	ELTX-5GHz_WiFi_1680	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:dc:f6:b2	wlan0	100	AP	RT-5GHz_WiFi_F6B0	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54
Grant	a8:f9:4b:dc:f7:e1	wlan0	100	AP	ELTX-5GHz_WiFi_F7E0	On	On	5	149 [80]	149 - 161		2	Fri Oct 20 07:13:01 2017	**6**,9,**12**,18,**24**,36,48,54

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

View events generated by this access point

Options
Persistence — Enabled / Disabled
Severity — 7
Depth — 512 (Range : 1 - 512)
Click "Update" to save the new settings.
Update

Relay Options
Relay Log — Enabled / Disabled
Relay Host — (xxx.xxx.xxx.xxx/ xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/ Hostname max 253 Characters)
Relay Port — 514 (Range: 1 - 65535, Default: 514)
Click "Update" to save the new settings.
Update

Events

Click "Refresh" button to refresh the page.
Refresh

Time Settings (NTP)	Type	Service	Description
Oct 20 2017 07:17:28	info	hostapd[19729]	AP with MAC address a8:f9:4b:b0:43:72 and SSID Eltex-Guest is detected on channel 48
Oct 20 2017 07:16:22	info	hostapd[19729]	AP with MAC address a8:f9:4b:2a:00:00 and SSID EltexWiFi5G is detected on channel 46
Oct 20 2017 07:15:21	info	hostapd[19729]	AP with MAC address a8:f9:4b:b6:01:20 and SSID BRAS-Guest is detected on channel 40
Oct 20 2017 07:15:21	info	hostapd[19729]	AP with MAC address aa:f9:4b:0e:da:62 and SSID 5VI46000042 is detected on channel 42
Oct 20 2017 07:14:43	info	hostapd[19729]	AP with MAC address a8:f9:4b:b0:34:b2 and SSID Eltex-Guest is detected on channel 48
Oct 20 2017 07:14:42	info	hostapd[19729]	AP with MAC address a8:f9:4b:b0:34:b4 and SSID BRAS-Guest is detected on channel 48
Oct 20 2017 07:14:36	info	hostapd[19729]	AP with MAC address e0:d9:e3:70:98:80 and SSID TMSK_RTK_SBRF_WIFI is detected on channel 42
Oct 20 2017 07:14:32	info	hostapd[19729]	AP with MAC address e0:d9:e3:70:81:e1 and SSID OMSK_RTK_SBRF_0000-0000 is detected on channel 42
Oct 20 2017 07:14:30	info	hostapd[19729]	AP with MAC address a8:f9:4b:b0:34:b2 and SSID Eltex-Guest is detected on channel 48
Oct 20 2017 07:14:30	info	hostapd[19729]	AP with MAC address a8:f9:4b:b0:34:b1 and SSID Eltex-Local is detected on channel 48

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

4 WB-1P-LR configuration

4.1 Connecting the device to PC

PoE technology is used to power the WB-1P-LR, allowing it to transfer power through a UTP cable. A PoE injector is used for connection. 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.

4.2 Configuring computer network interface settings

Set 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

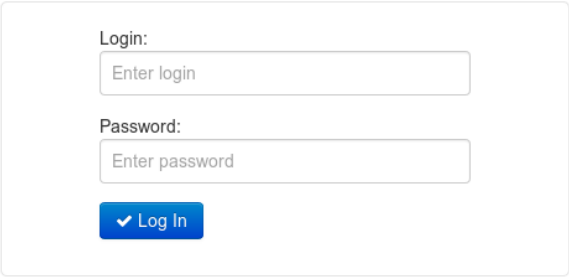
4.3 Connecting to the WB-1P-LR web interface

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

- **192.168.1.1**

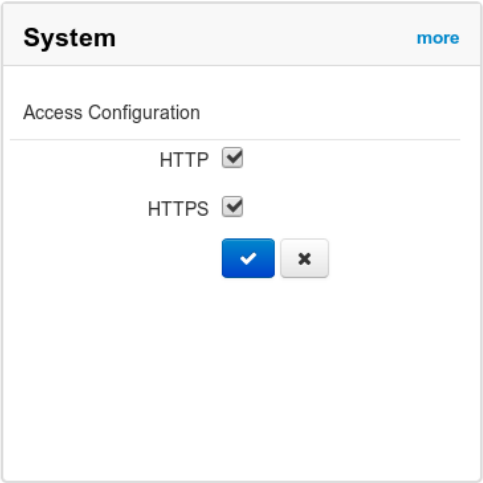
The authorization page will open, enter:

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

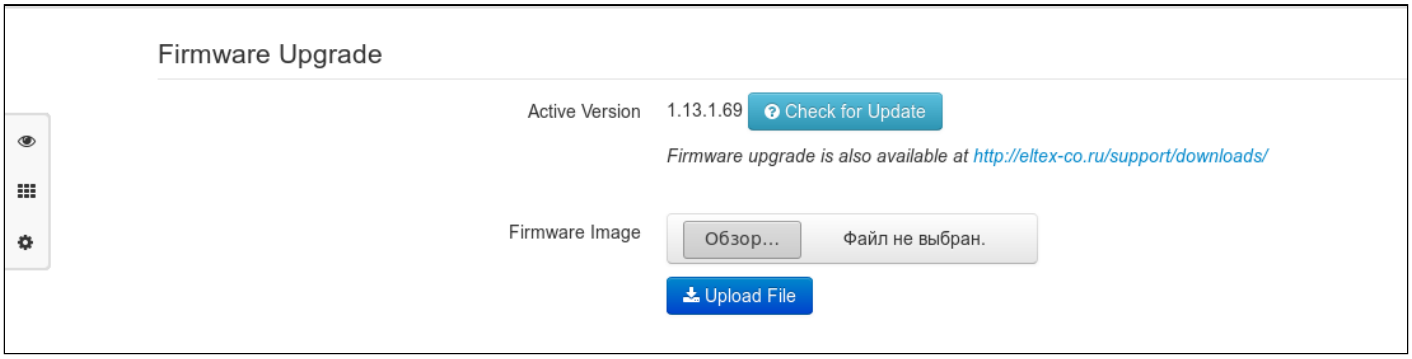


4.4 WB-1P-LR firmware upgrade

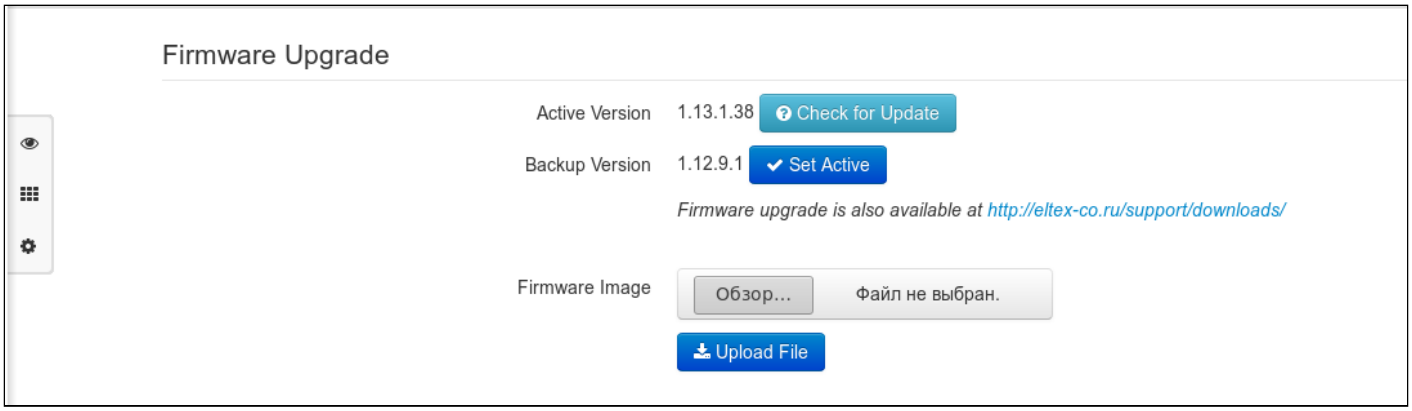
In the system settings, click the link **More**:



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



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



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* – 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 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 making 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 upgrade process, 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.

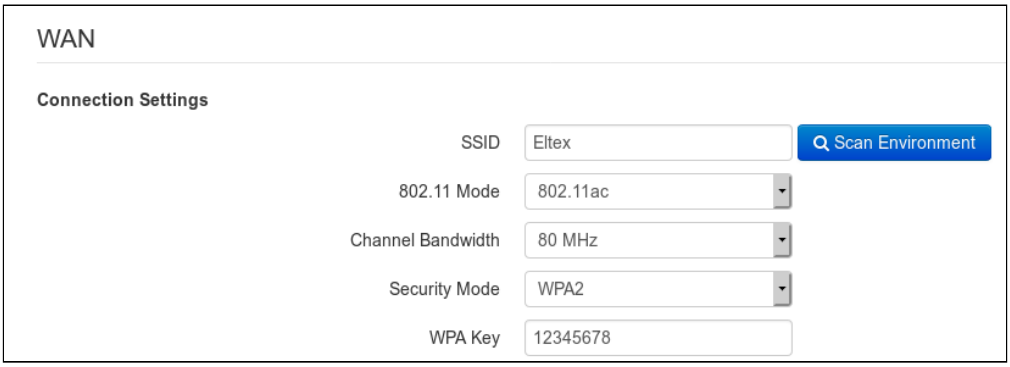
Do not switch off or reboot the device during the firmware update.

4.5 Configure Wi-Fi connection to the base station

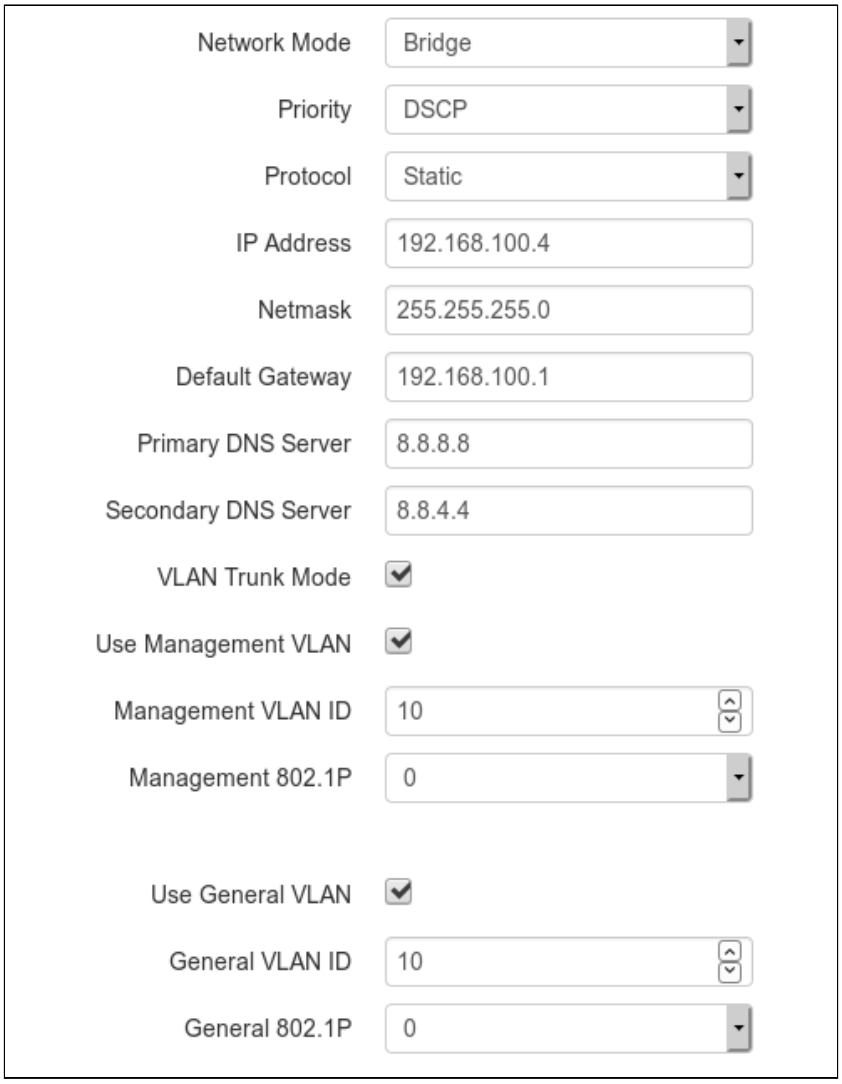
1. Connect to the web interface (see Section Connection to the WB-1P-LR web interface). In the Wi-Fi settings, click on the link **More**:

A page will open 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 using to connect Wi-Fi network without encryption, then select **Off** in the **Security mode** field. If using to connect Wi-Fi network with encryption, 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).



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.
4. Set the flags in the options **Use VLAN trunk**, **Use Management VLAN** and **Use General VLAN**.
5. 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:



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

For the example above, the following settings are used:

- In the *Network Identifier (SSID)*field 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 following 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.

4.6 Access the device from an external network

Go to the **Access tab** of the **System** submenu. 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:

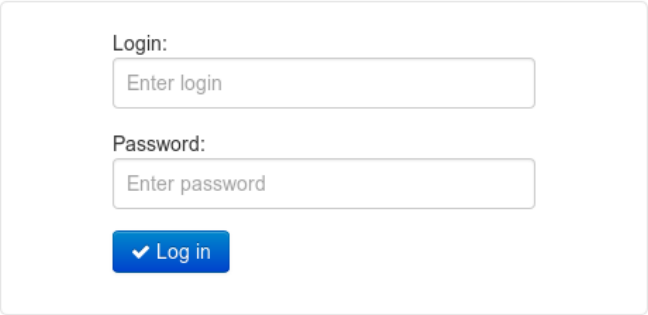
- SSH – when checked, SSH connection to the device through the WAN port is allowed.

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

5 RG-4402-G configuration

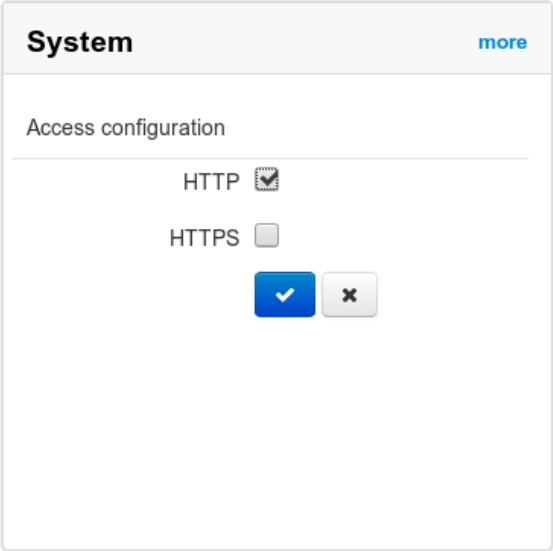
5.1 Connection to RG-4402-G web interface

1. Enable network settings obtaining via DHCP on the PC 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 browser URL bar:
   - **192.168.1.1**
3. In the window that appears, enter:
   - Login: **admin**
   - Password: **password**

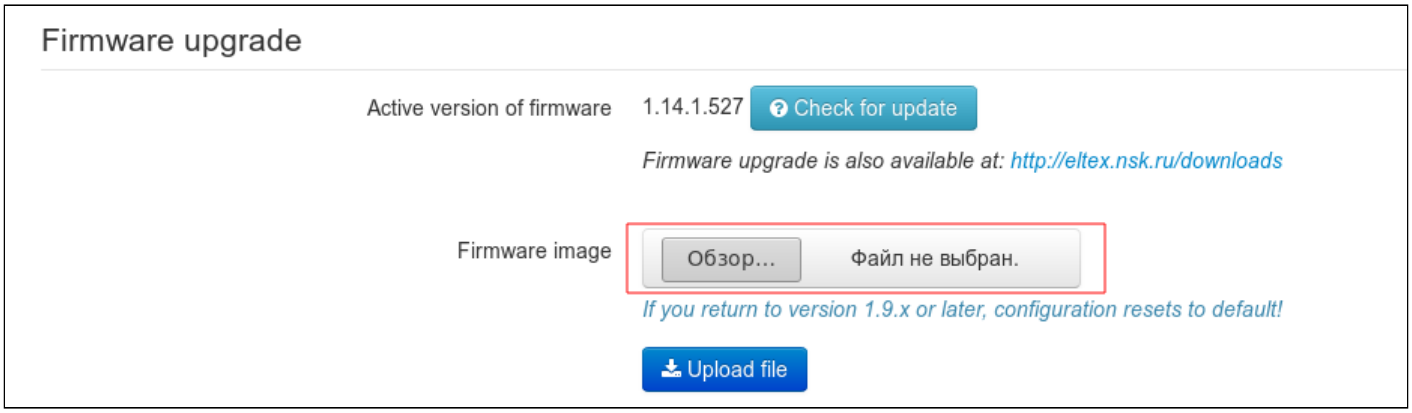


5.2 Firmware upgrade

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



2. Go to the **Firmware upgrade** 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.

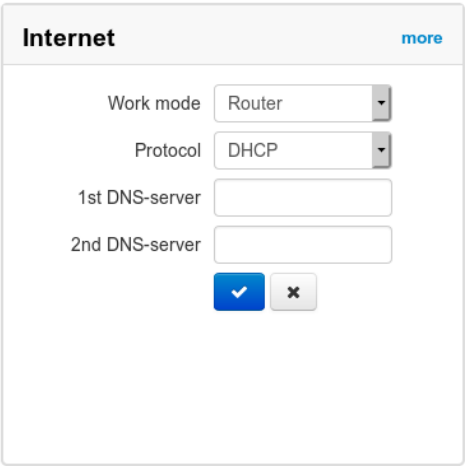


3. To start the upgrade process, click the **Upload file** button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the upgrade is completed.

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

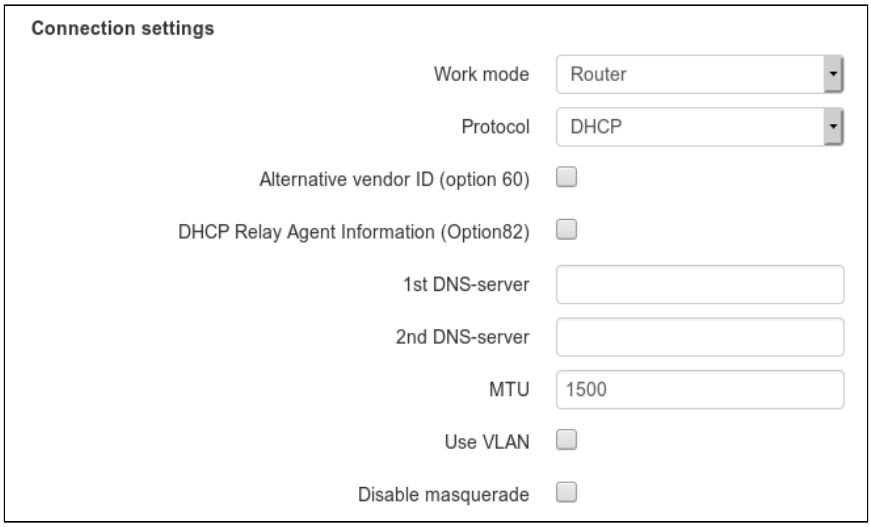
5.3 Internet service configuration

1. Connect to the web interface (see Section Connection to the RG-4402-G web interface).
2. In the **Internet** settings, click 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, defualt 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.

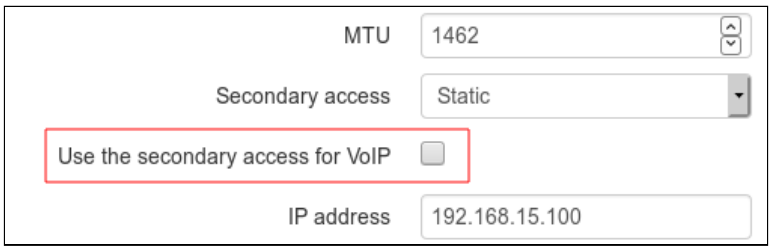
For the example above, the following settings are used:

- 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.

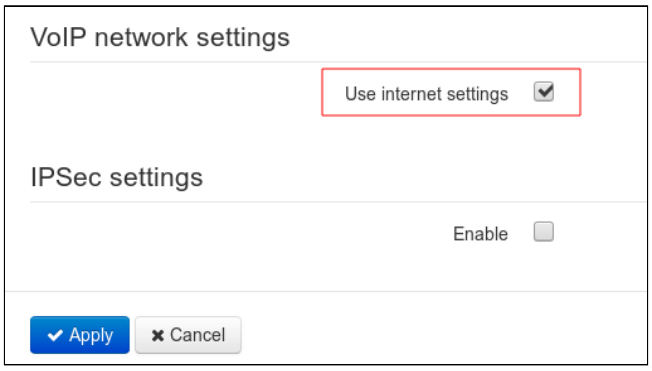
5.4 VoIP service configuration

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:



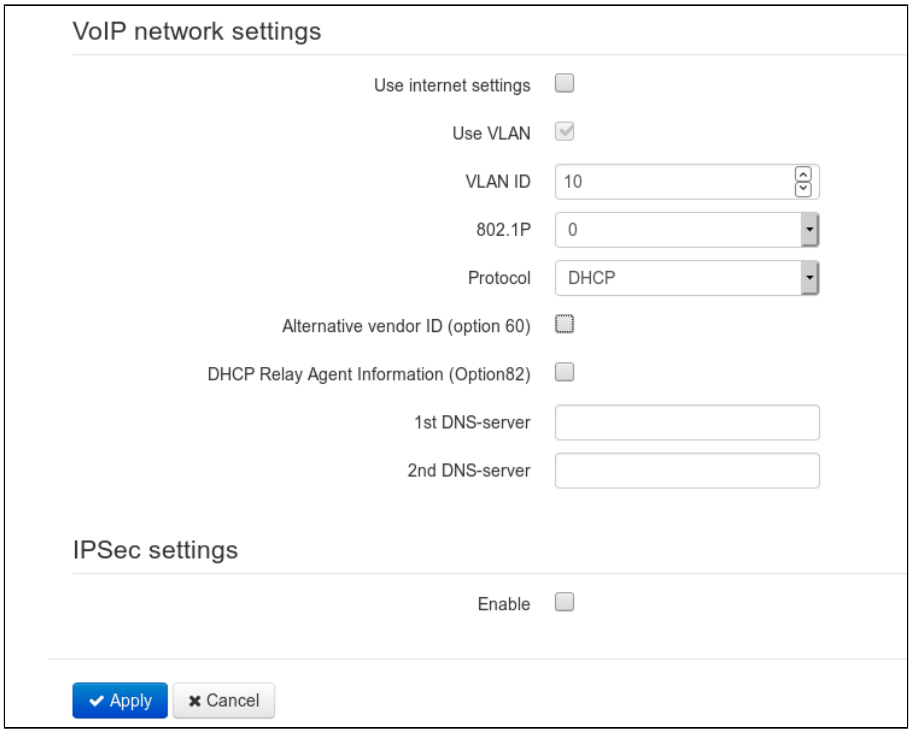
3. Go to the **VoIP** menu to the **Network settings** tab. Set the flag in the **Use Internet settings** field:



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:



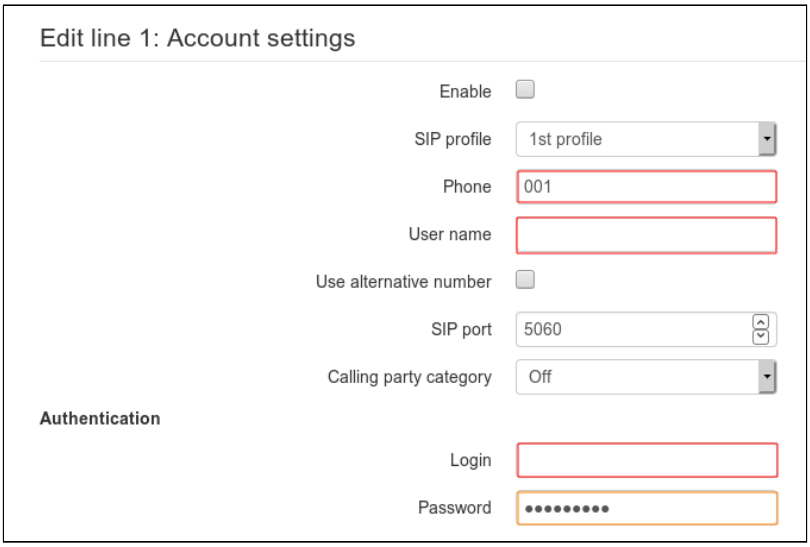
5. To apply the new configuration, click the **Apply** button.

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.

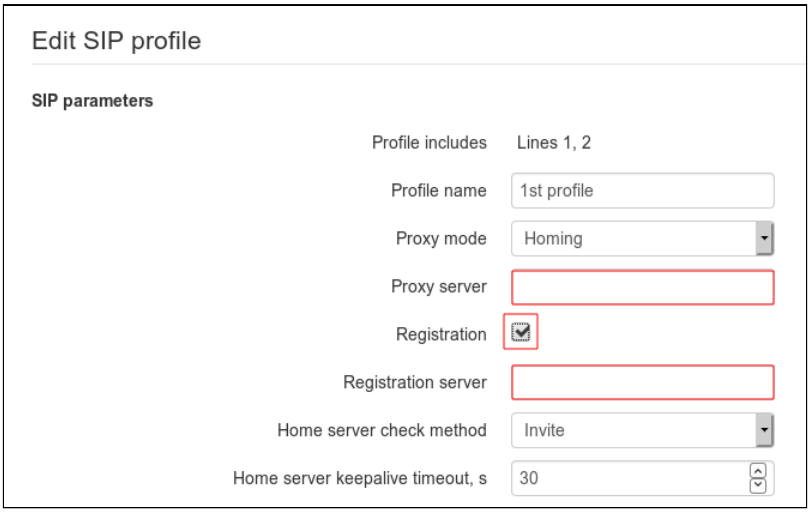
5.5 Line parameters configuration

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).



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



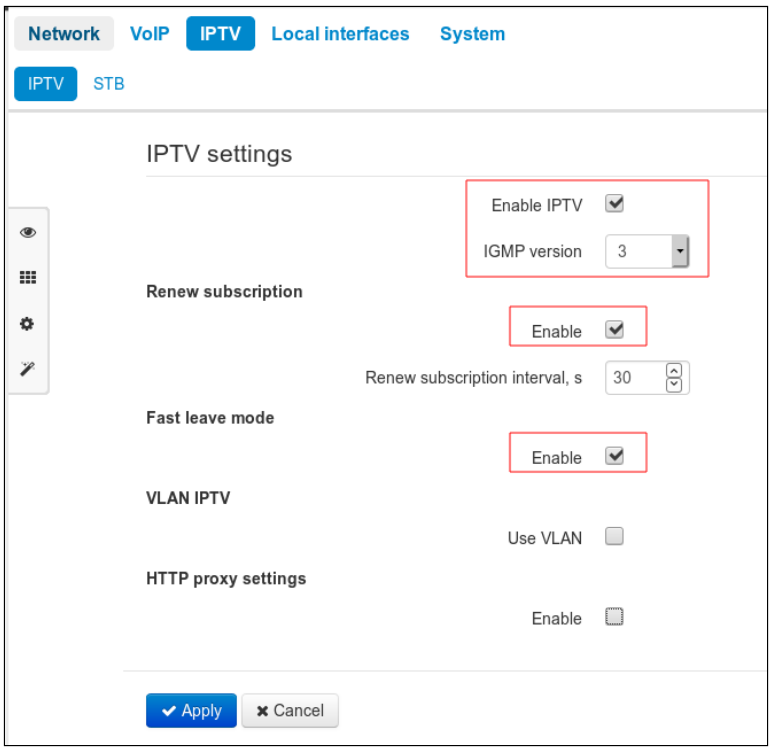
5.6 Profile configuration

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 **SIP proxy server** field. 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.

5.7 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**:



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.

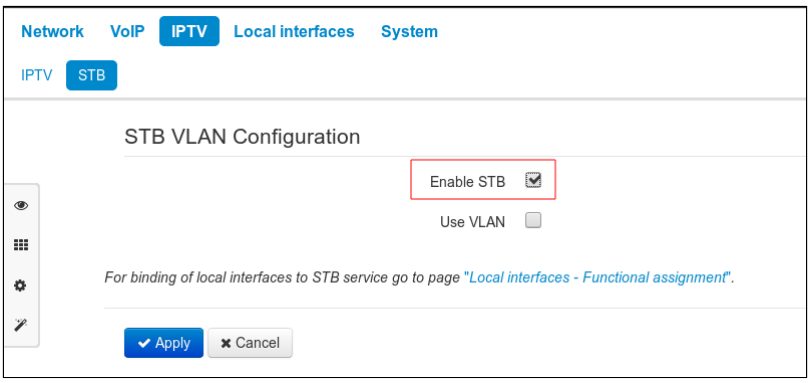
7. To apply the new configuration, click the **Apply** button.

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

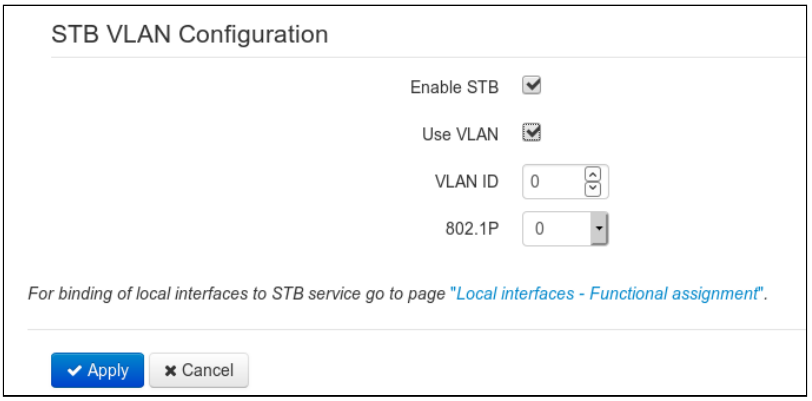
1. Set the flag in the **Use VLAN** field;
2. In the **VLAN ID** field set the value **13**.

STB configuration

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



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;



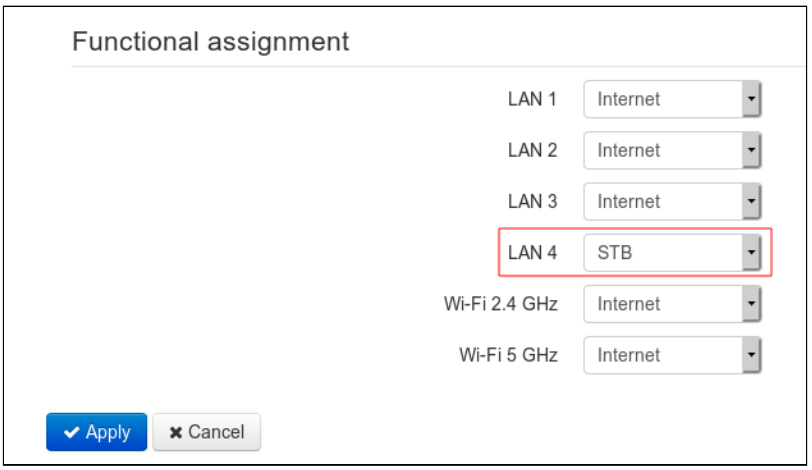
4. To apply the new configuration, click the **Apply** button.

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**.

5.8 Local interfaces configuration

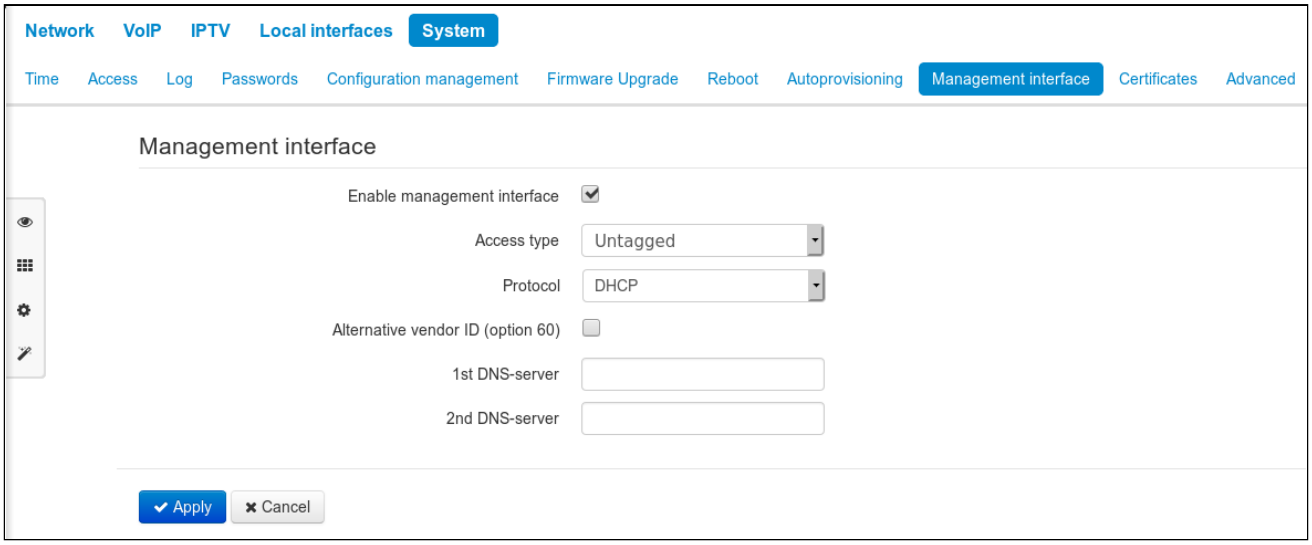
To bind local interfaces to the STB service, go to the **Local Interfaces** menu on the **Functional Assignment** tab. Assign one of the device ports to the STB port. After that, the STB should only be connected to this port:



5.9 VLAN management configuration

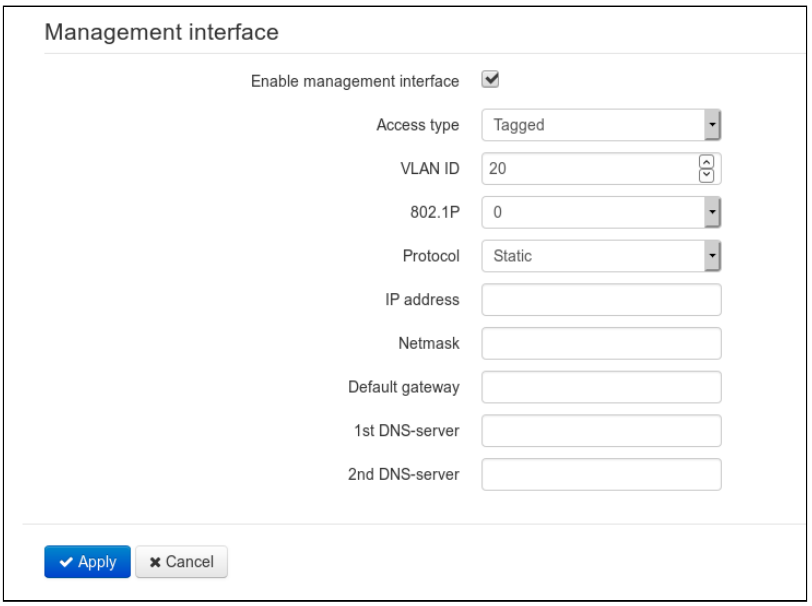
1. Go to the **System** menu on the **Management Interface** tab.
2. Set the flag **Enable management interface**.
3. Select the management traffic type in the **Access Type** field:

- **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.



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.



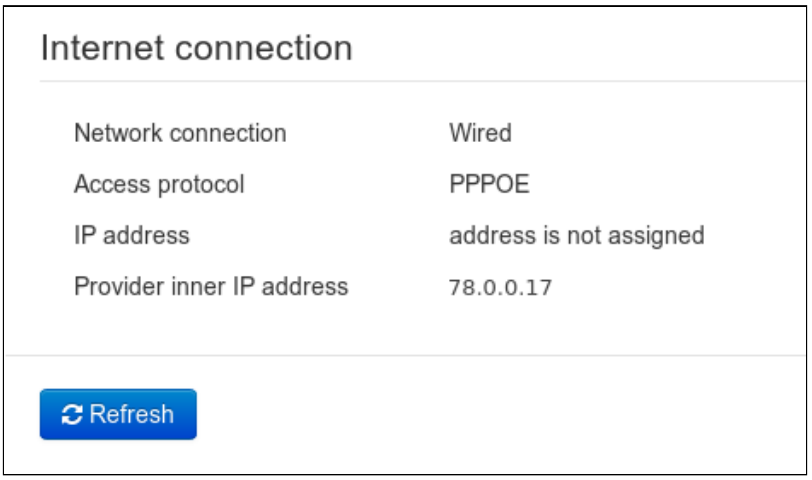
5. To apply the new configuration, click the **Apply** button.

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.

5.10 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).



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.

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

http://www.eltex-co.com/support

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist in our technical forum.

http://www.eltex-co.com/

http://www.eltex-co.com/support/downloads/