Wireless access point

WEP-2ac, WEP-2ac Smart

Quick manual
Firmware version 1.16.0

IP address: 192.168.1.10
Username: admin
Password: password

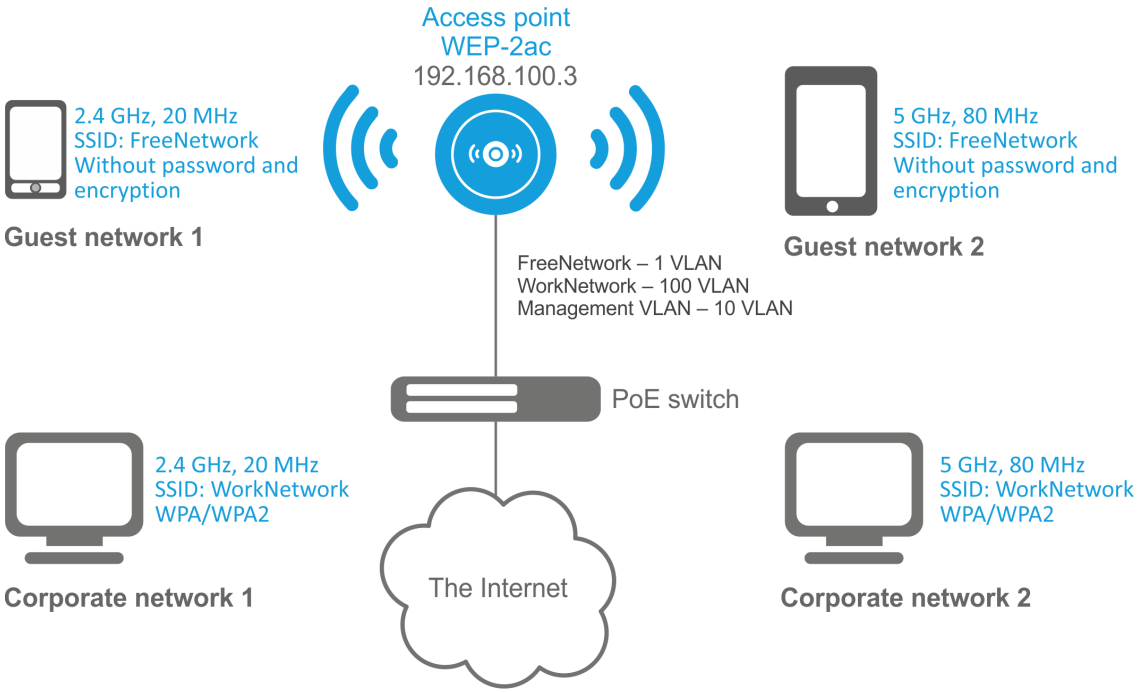
Contents

1 Annotation

This manual specifies the following:

- connection to WEP-2ac web interface;
- configuration of WEP-2ac network parameters;
- WEP-2ac firmware update;
- SNMP configuration;
- wireless interfaces configuration (operation mode, band);
- virtual access points configuration;
- monitoring of wireless network main parameters.

The manual gives an example of access point configuration without using a soft controller. The following scheme will be given as an example:



Type of the network	VLAN used	SSID used	Encryption/ authorization by password
Inner corporate wireless network using 2.4 and 5 GHz bands. The network is isolated from other guest networks. To connect to the network, password authorization is required. The network is dedicated to secure data exchange among company staff.	100	WorkNetwork	WPA/WPA2
Guest wireless network using 2.4 and 5 GHz bands. The network does not require password authorization. It is dedicated to connect users with standard wireless gadgets to a public network for Internet access, for instance.	1 (without VLAN)	FreeNetwork	No encryption and authorization

To perform the configuration, you need to have a PC with access to the device via Ethernet and any web browser (Internet Explorer, Firefox, Google Chrome, Opera, etc.)

2 Connecting the web interface

Connection of a PC to the device might be executed as follows:

- Connect network cable to PoE interface of WEP-2ac and to PoE injector (or switch). Then connect a PC to the PoE injector (or switch).

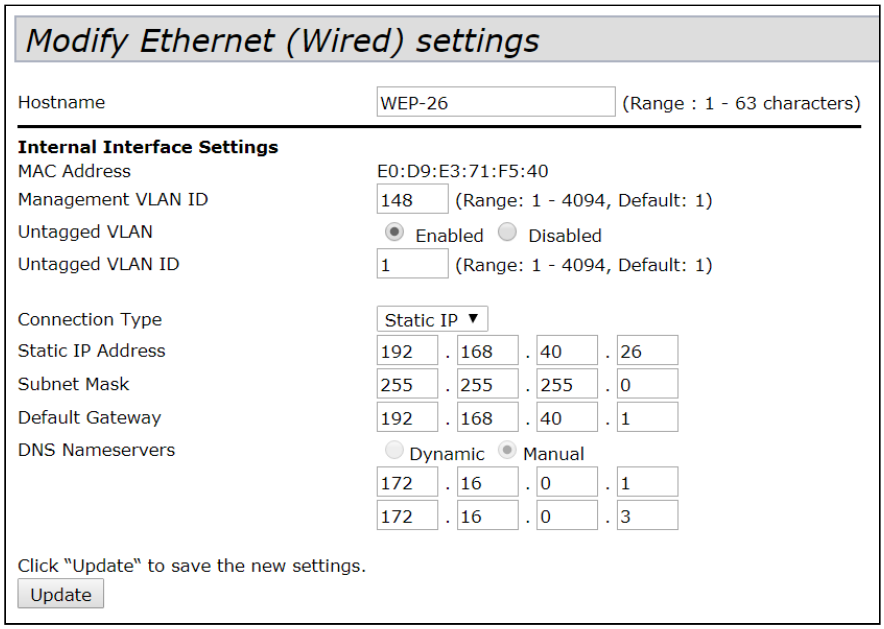
To connect to the web interface of the device, enter the following to the URL bar of your browser: **192.168.1.10.** If the connection has been performed successfully, the authorization page will be displayed. Use the following data for authorization:

- 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 perform this, press and hold the button «F» on the side panel of the device within 20 seconds. Wait for the indicator on the front panel to start blinking, and then release the button. The light of the indicator should be changed to red, it means that loading is in operation.

3 Network parameters configuration

For remote management of WEP-2ac, WEP-2ac Smart, you should set network parameters of the device according to the settings of the network that you intend to use. In **«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. 10 is used in the given example.
- **Connection Type** – select «Static IP» to set IP addresses for access points manually. Specify the IP address of WEP-2ac (in the example, it is 192.168.100.3) in «**Static IP Address**» field. Enter the address of the default gateway in «**Default Gateway**» field. 192.168.100.1. Changing the network mask is optional. If you want the access points to obtain IP addresses via DHCP, «Connection type» field should be set to «DHCP» value. If DHCP is selected, the network settings configuration is completed.

Click «**Update**». Since that, WEP-2ac is available in 10 VLAN via 192.168.100.3 address.

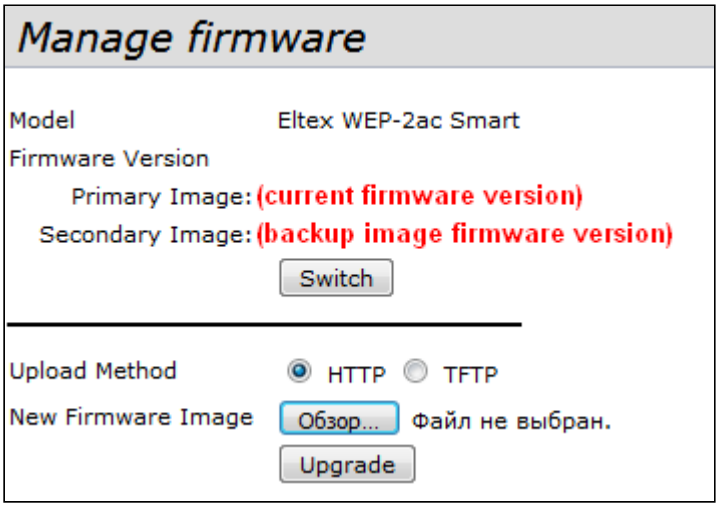
Before changing the settings, make sure that the managing computer has the access to the access point. If you make a mistake while changing the settings, you may undo them by resetting the access point to factory settings. To perform this, press and hold «F» button on the side panel of the device for 20 seconds until the indicator on the front panel is blinking.

4 Firmware update

For proper operation of WEP-2ac and WEP-2ac Smart, it is recommended to update the firmware. You may consult the vendor on the relevance of the firmware version:

Phone number: **+7(383) 272-83-31**
+7(383) 274-47-87
e-mail: **techsupp@eltex.nsk.ru**

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

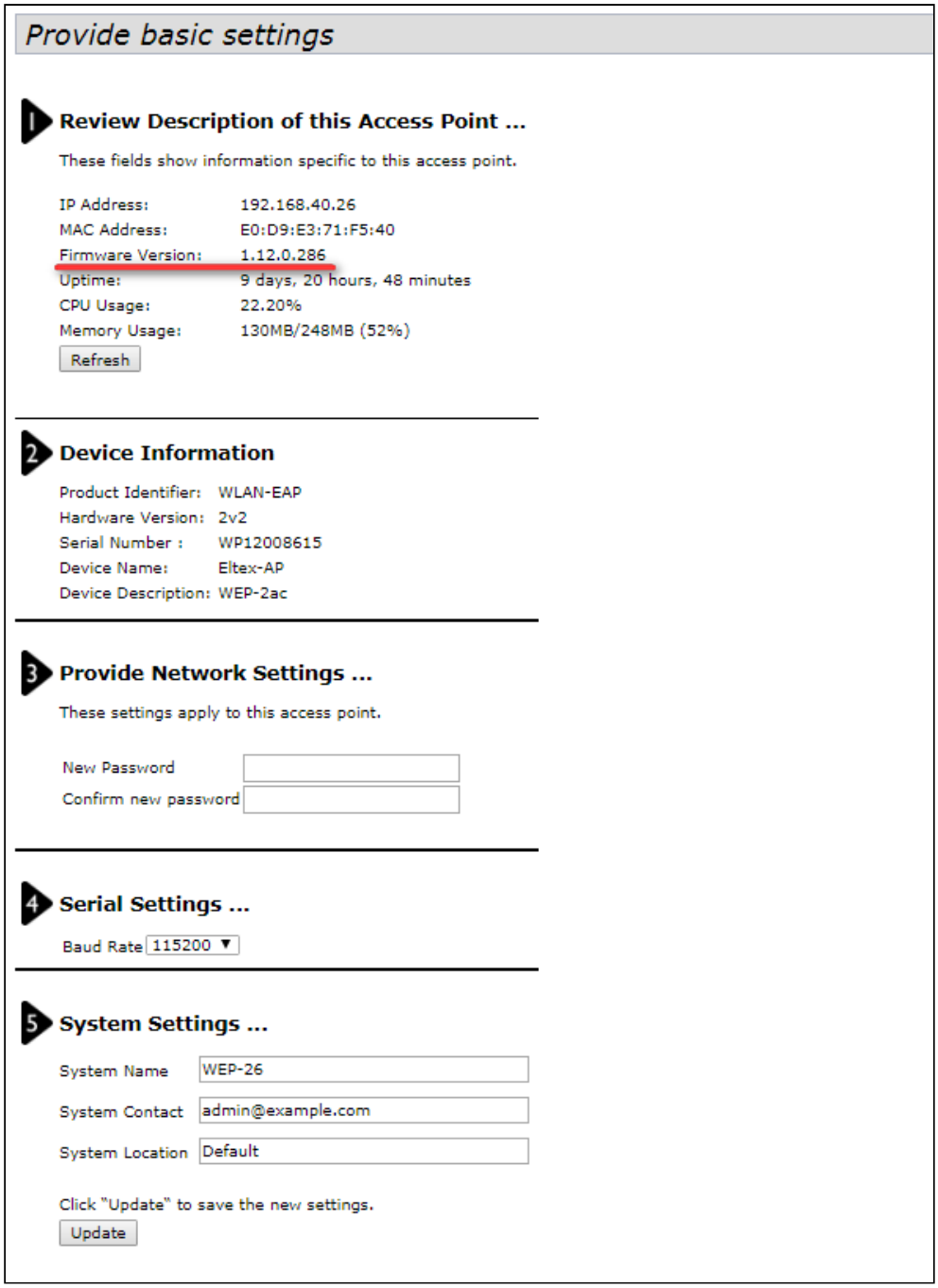


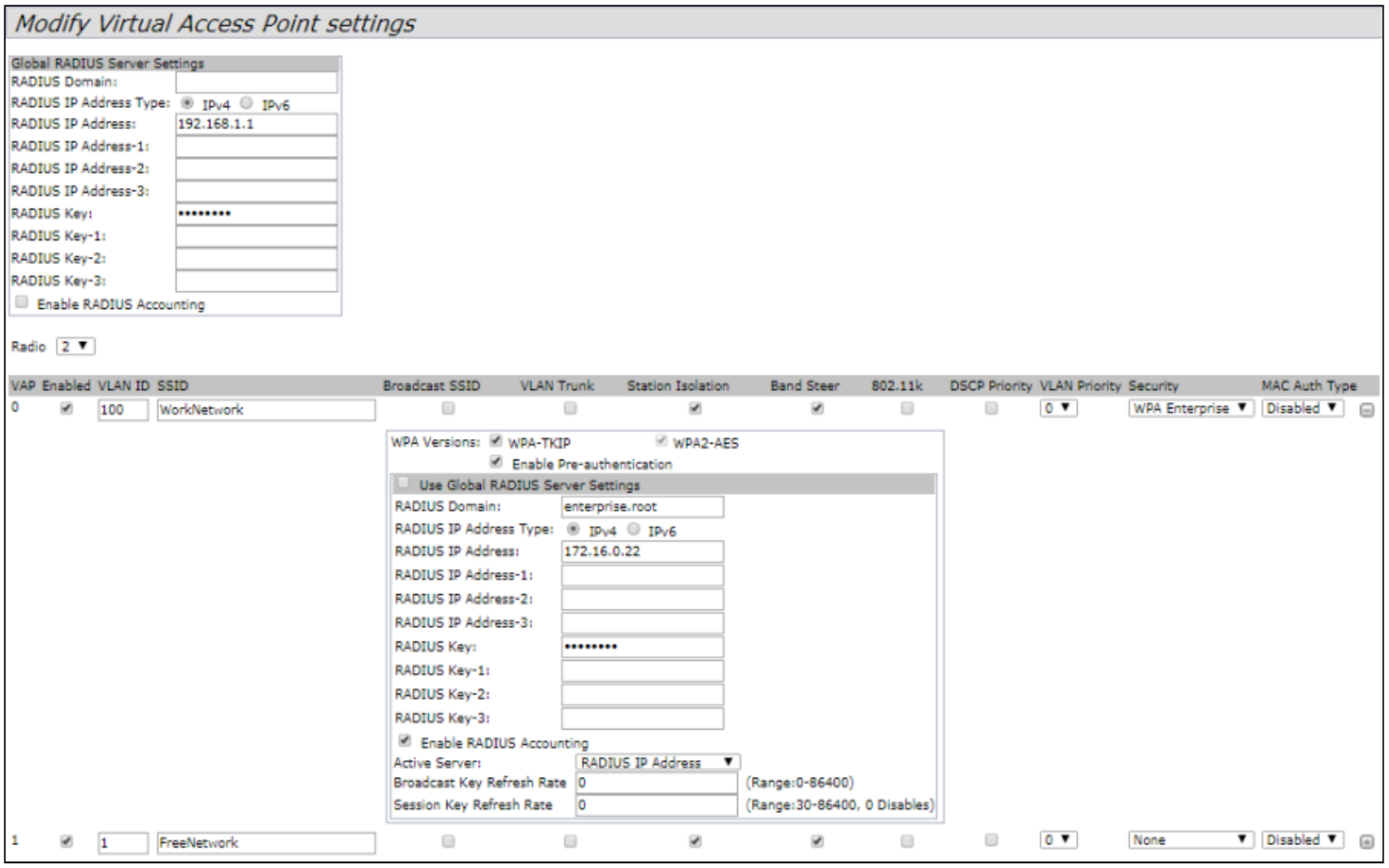
- Press «**Switch**» button if you want to switch to an Alternative firmware image set in «**SecondaryImage**» field.
- **Upload Method** – check **«HTTP»** box.
- **NewFirmwareImage** – click **«Browse»** button and select relevant firmware version, click **«Open»**.

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 update.

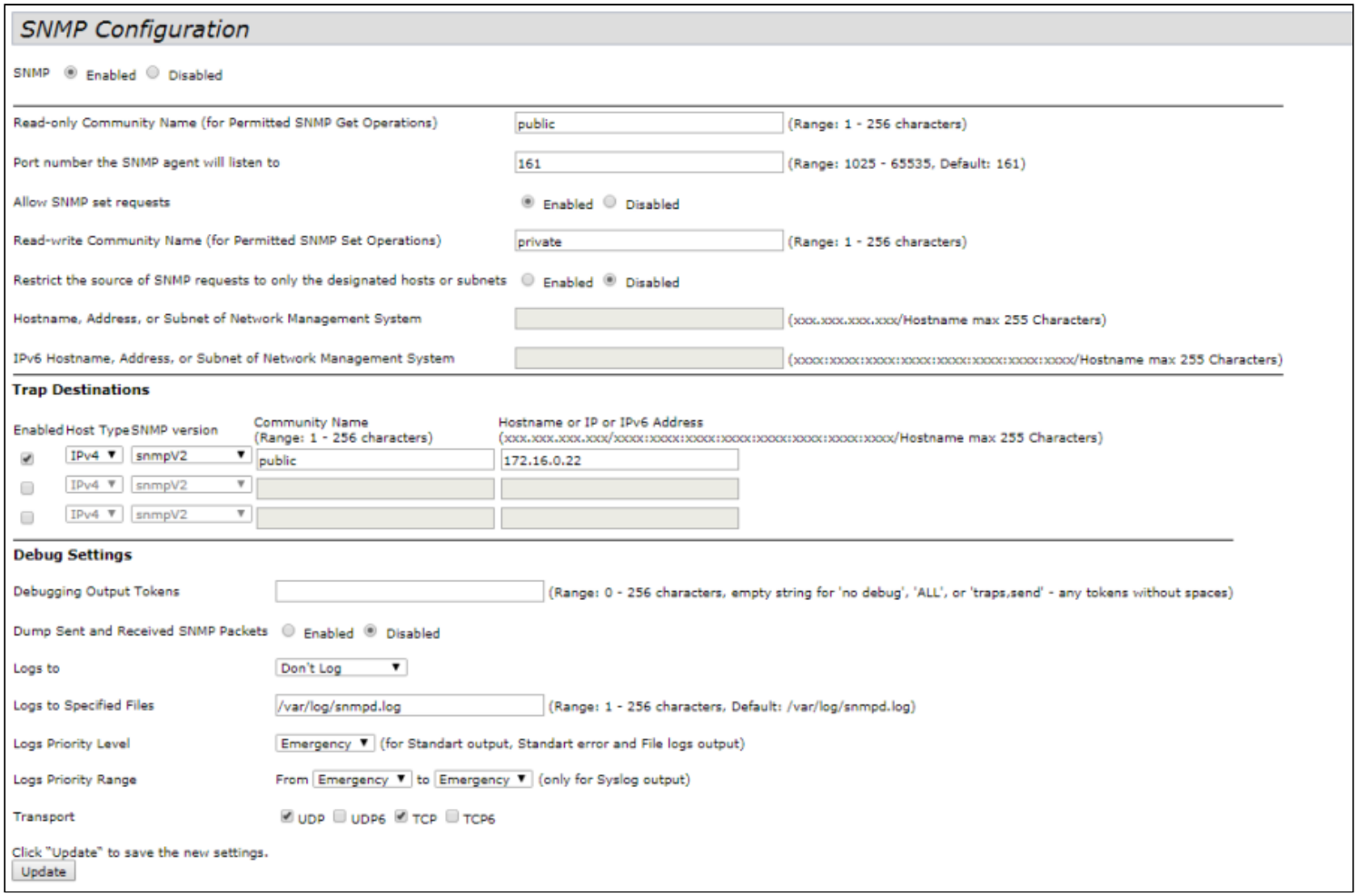
You may check the current firmware version in **«Basic Settings»** menu (Firmware Version).


Provide basic settings
1 Review Description of this Access Point ...
These fields show information specific to this access point.
IP Address: 192.168.40.26
MAC Address: E0:D9:E3:71:F5:40
Firmware Version: 1.12.0.286
Uptime: 9 days, 20 hours, 48 minutes
CPU Usage: 22.20%
Memory Usage: 130MB/248MB (52%)
Refresh
2 Device Information
Product Identifier: WLAN-EAP
Hardware Version: 2v2
Serial Number : WP12008615
Device Name: Eltex-AP
Device Description: WEP-2ac
3 Provide Network Settings ...
These settings apply to this access point.
New Password
Confirm new password
4 Serial Settings ...
Baud Rate 115200
5 System Settings ...
System Name WEP-26
System Contact admin@example.com
System Location Default
Click "Update" to save the new settings.
Update


Modify Virtual Access Point settings
Global RADIUS Server Settings
RADIUS Domain:
RADIUS IP Address Type: IPv4 IPv6
RADIUS IP Address: 192.168.1.1
RADIUS IP Address-1:
RADIUS IP Address-2:
RADIUS IP Address-3:
RADIUS Key:
RADIUS Key-1:
RADIUS Key-2:
RADIUS Key-3:
Enable RADIUS Accounting
Radio 2
VAP Enabled VLAN ID SSID Broadcast SSID VLAN Trunk Station Isolation Band Steer 802.11k DSCP Priority VLAN Priority Security MAC Auth Type
0 100 WorkNetwork 0 WPA Enterprise Disabled
WPA Versions: WPA-TKIP WPA2-AES
Enable Pre-authentication
Use Global RADIUS Server Settings
RADIUS Domain: enterprise.root
RADIUS IP Address Type: IPv4 IPv6
RADIUS IP Address: 172.16.0.22
RADIUS IP Address-1:
RADIUS IP Address-2:
RADIUS IP Address-3:
RADIUS Key:
RADIUS Key-1:
RADIUS Key-2:
RADIUS Key-3:
Enable RADIUS Accounting
Active Server: RADIUS IP Address
Broadcast Key Refresh Rate 0 (Range:0-86400)
Session Key Refresh Rate 0 (Range:30-86400, 0 Disables)
1 1 FreeNetwork 0 None Disabled

5 SNMP service configuration

SNMP service configuration is performed in **«Services»** menu, **«SNMP»** section.



- **Restrict the source of SNMP requests to only the designated hosts or subnets** – check **«Enabled»** box.
- **Hostname, address, or subnet of Network Management System** – specify an IP-address of SNMP server, from which SNMP commands will be transmitted.
- **Community name for traps** – set **«public»**.
- **Enabled / HostType / Host nameorIP orIPv6 Address** – check one of the fields for specifying traps receiver address and enter an IP address of the device to which WEP-2ac will send traps.

Click «**Update**».

6 Wireless interfaces configuration

WEP-2ac and WEP-2ac Smart have 2 radio interfaces (Radio1 and Radio 2) that capable to operate simultaneously. Radio 1 operates at 5 GHz band, Radio 2 – at 2.4 GHz. The example of configuration of a network with the following characteristics is given below:

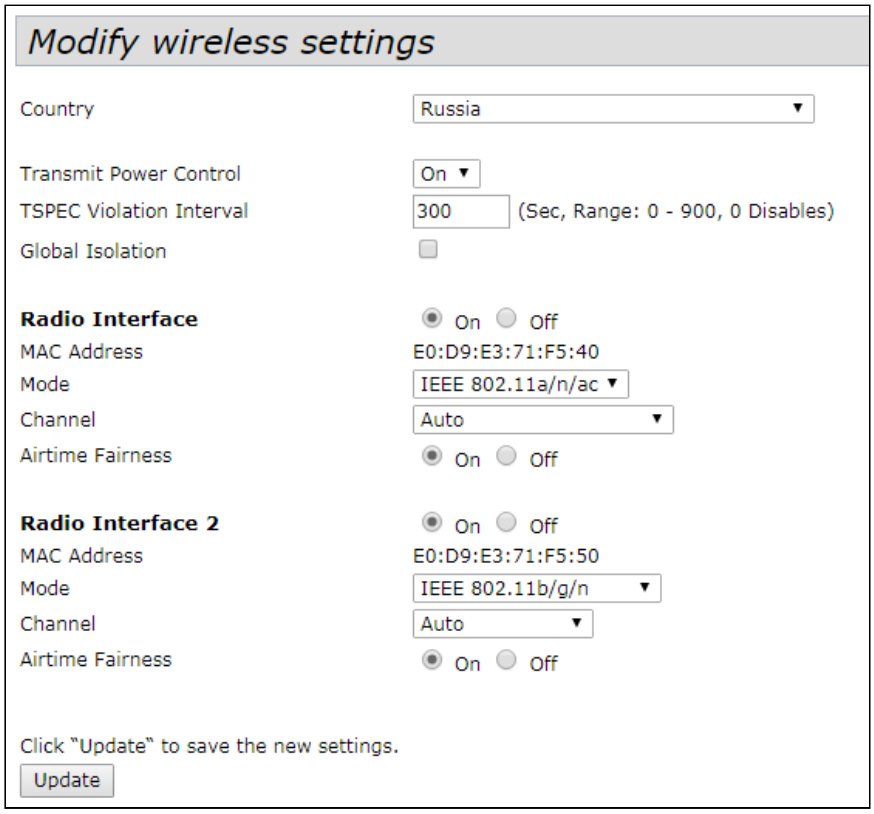
Radio1:

- Frequency range: 5 GHz;
- Standards: 802.11a/n/ac;
- Bandwidth: 80 MHz.

Radio2:

- Frequency range: 2.4 GHz;
- Standards: 802.11b/g/n;
- Bandwidth: 20 MHz.

In **«Manage»** menu, open **«Wireless Settings»** tab and perform the following:



- **Country** – select settings according to the rules of selected country. Select **«Russia»** in the list.
- **Transmit Power Control** – configuring *Transmit Power Limit* parameter restrictions. Select **«On»** in the list.

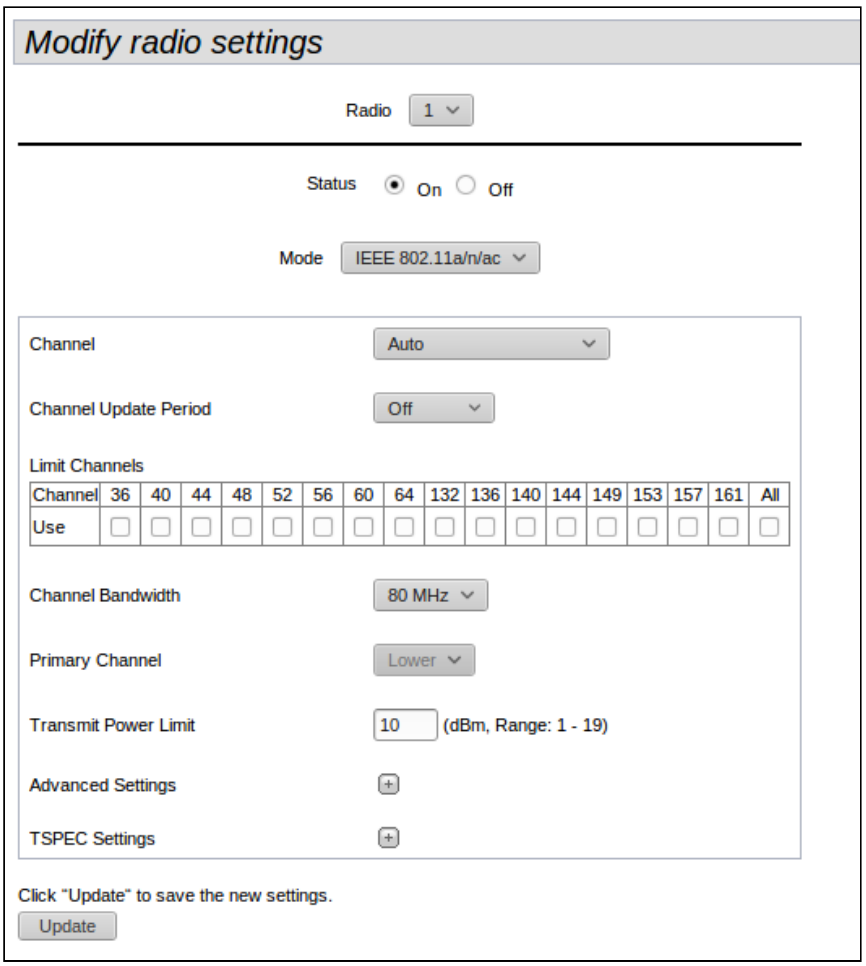
Configuring Radio 1:

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

Configuring Radio 2:

- **Radio Interface 2** – check **«On»** box;
- **Mode** – select value «**IEEE 802.11 b/g/n**».
- Click «**Update**».

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



Configuring Radio 1:

- **Radio** – select value **«1»;**
- **Channel Bandwidth** – set value **«80MHz»**;
- Click «**Update**».

Configuring Radio 2:

- **Radio** – select value **«2»;**
- **Channel Bandwidth** – set value **«20MHz»**;
- Click «**Update**».

7 Virtual access points configuration

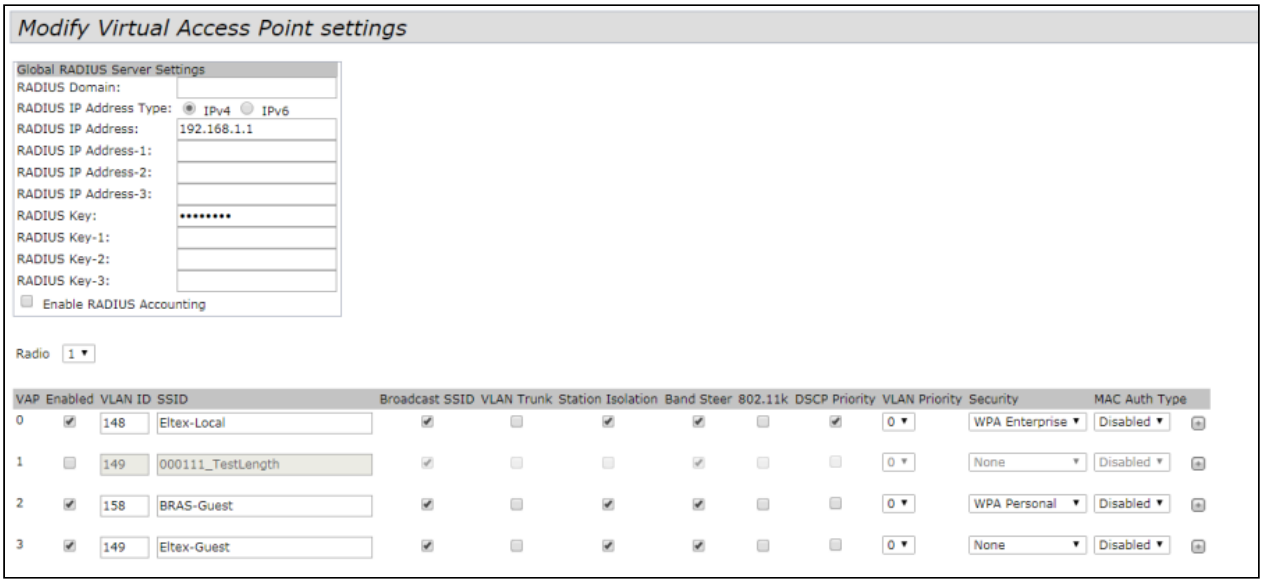
On each wireless interface, you may configure up to 16 virtual access points. Each access point may have individual name of wireless network (SSID) and type of authentication/authorization. According to the network scheme given in the figure 1, it is necessary to configure 2 virtual access points on Radio 1 and Radio 2.

Band Steer feature allows clients having opportunity of operation at 2.4 GHz and 5 GHz to set priority of connection to 5 GHz band.

The followings are necessary for Band Steer feature operation:

- configure radio interfaces for operation at different frequency ranges;
- create virtual access points (VAP) on each frequency range with the same SSID;
- when using encryption, make sure the passwords of the VAPs are the same;
- activate Band Steer feature on the access points.

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



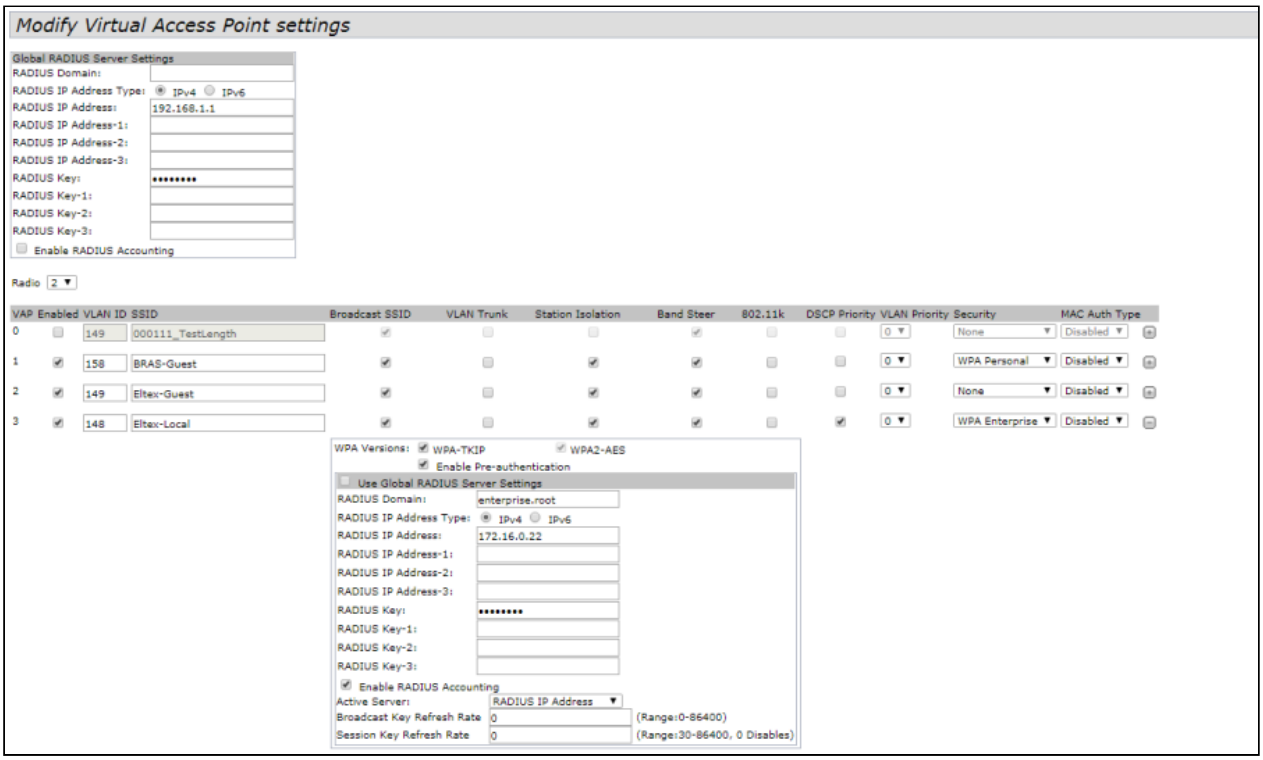
Configuring Radio 1:

- **Radio** – select value **«1»;**
- **Enabled** – check the boxes for VAP 0 and VAP1.
- **VLAN ID** – VLAN number:
  - set value **«100»** for VAP 0;
  - set value **«1»** for VAP 1;
- **SSID** – wireless network name:
  - set value **«Work Network»** for VAP 0;
  - set value **«Free Network»** for VAP 1;
- **Station Isolation** – forbid packet transmission among access point's clients. Check the box.
- **Band Steer** – set a priority of users connection to SSID configured at 5 GHz. Check the box.
- **Security** – secure network mode:
  - set **«WPA Personal»** value for VAP 0 and set a password for this network connection in **«Key»** field;
  - set value **«None»** for VAP 1.
- Click «**Update**».

Configuration of Radio 2 is performed in the same way. Select **«2»** value in **Radio** and perform the configuration as for the Radio 1 (given above). The password for «WorkNetwork» should be the same. Click «**Update**».

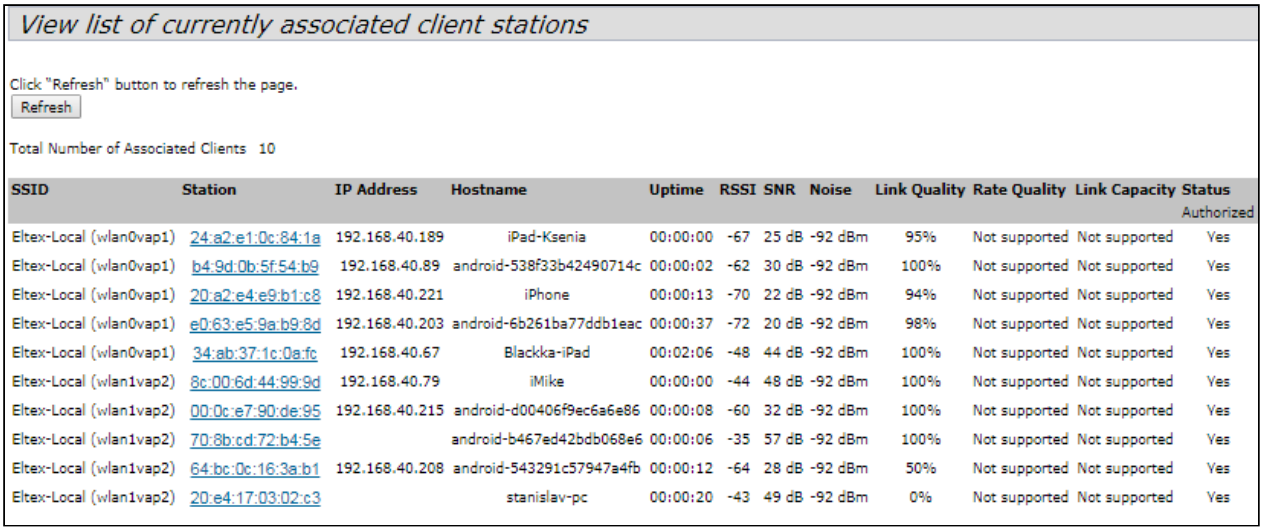
When using WPA Enterprise mode, the authorization is implemented through a RADIUS server. The request on user connection to SSID is sent to a RADIUS server. The table *Global RADIUS server settings* specifies the followings:

- RADIUS IP Address – an IP address of a RADIUS server;
- RADIUS Key – a password to access the RADIUS server.



8 Monitoring main parameters of wireless network

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



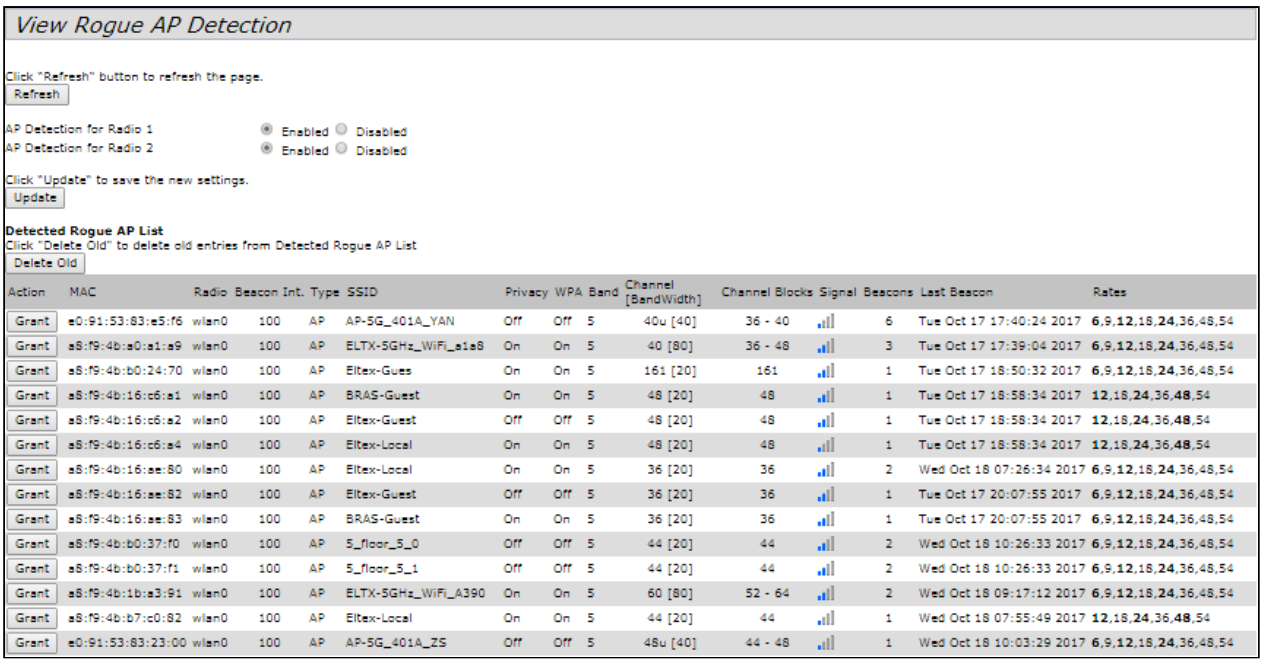
View list of currently associated client stations

Click "Refresh" button to refresh the page.
Refresh

Total Number of Associated Clients 10

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capacity	Status
											Authorized
Eltex-Local (wlan0vap1)	24:a2:e1:0c:84:1a	192.168.40.189	iPad-Ksenia	00:00:00	-67	25 dB	-92 dBm	95%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	b4:9d:0b:5f:54:b9	192.168.40.89	android-538f33b42490714c	00:00:02	-62	30 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	20:a2:e4:e9:b1:c8	192.168.40.221	iPhone	00:00:13	-70	22 dB	-92 dBm	94%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	e0:63:e5:9a:b9:8d	192.168.40.203	android-6b261ba77ddb1eac	00:00:37	-72	20 dB	-92 dBm	98%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	34:ab:37:1c:0a:fc	192.168.40.67	Blackka-iPad	00:02:06	-48	44 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	8c:00:6d:44:99:9d	192.168.40.79	iMike	00:00:00	-44	48 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	00:0c:e7:90:de:95	192.168.40.215	android-d00406f9ec6a6e86	00:00:08	-60	32 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	70:8b:cd:72:b4:5e		android-b467ed42bdb068e6	00:00:06	-35	57 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	64:bc:0c:16:3a:b1	192.168.40.208	android-543291c57947a4fb	00:00:12	-64	28 dB	-92 dBm	50%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	20:e4:17:03:02:c3		stanislav-pc	00:00:20	-43	49 dB	-92 dBm	0%	Not supported	Not supported	Yes

The list of third-party access points in WEP-2ac area with data on wireless channel used and transmitted signal level is presented in **«Status»** menu, **«Rogue AP Detection»** tab.



View Rogue AP Detection

Click "Refresh" button to refresh the page.
Refresh

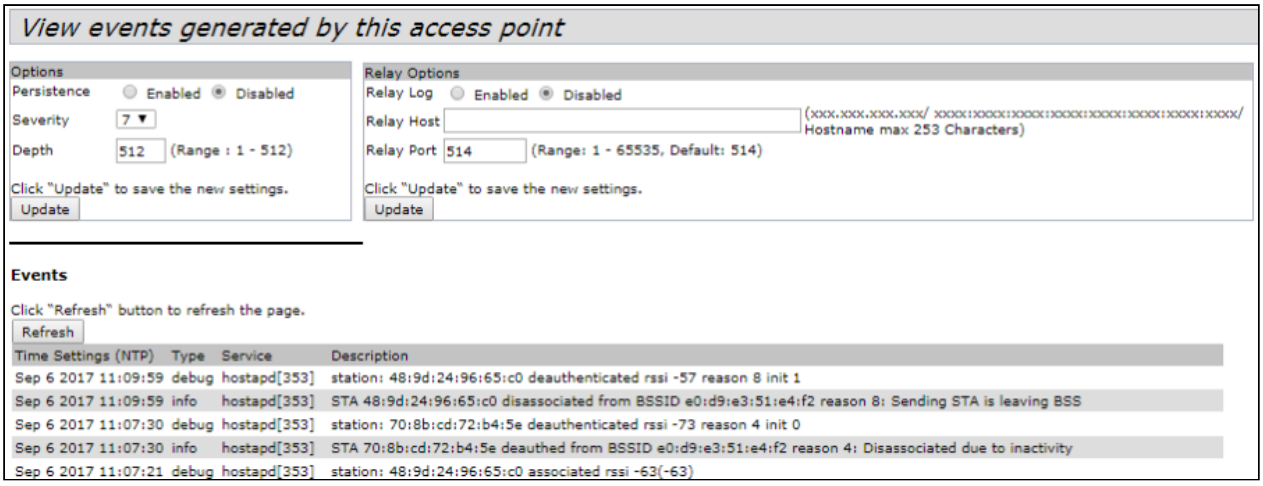
AP Detection for Radio 1 Enabled Disabled
AP Detection for Radio 2 Enabled Disabled

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	e0:91:53:83:e5:f6	wlan0	100	AP	AP-5G_401A_YAN	Off	Off	5	40u [40]	36 - 40		6	Tue Oct 17 17:40:24 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:a0:a1:a9	wlan0	100	AP	ELTX-5GHz_WiFi_a1a8	On	On	5	40 [80]	36 - 48		3	Tue Oct 17 17:39:04 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:b0:24:70	wlan0	100	AP	Eltex-Gues	On	On	5	161 [20]	161		1	Tue Oct 17 18:50:32 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:16:c6:a1	wlan0	100	AP	BRAS-Guest	On	On	5	48 [20]	48		1	Tue Oct 17 18:58:34 2017	12,18,24,36,48,54
Grant	a8:f9:4b:16:c6:a2	wlan0	100	AP	Eltex-Guest	Off	Off	5	48 [20]	48		1	Tue Oct 17 18:58:34 2017	12,18,24,36,48,54
Grant	a8:f9:4b:16:c6:a4	wlan0	100	AP	Eltex-Local	On	On	5	48 [20]	48		1	Tue Oct 17 18:58:34 2017	12,18,24,36,48,54
Grant	a8:f9:4b:16:ae:80	wlan0	100	AP	Eltex-Local	On	On	5	36 [20]	36		2	Wed Oct 18 07:26:34 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:16:ae:82	wlan0	100	AP	Eltex-Guest	Off	Off	5	36 [20]	36		1	Tue Oct 17 20:07:55 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:16:ae:83	wlan0	100	AP	BRAS-Guest	On	On	5	36 [20]	36		1	Tue Oct 17 20:07:55 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:b0:37:f0	wlan0	100	AP	5_floor_5_0	Off	Off	5	44 [20]	44		2	Wed Oct 18 10:26:33 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:b0:37:f1	wlan0	100	AP	5_floor_5_1	Off	Off	5	44 [20]	44		2	Wed Oct 18 10:26:33 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:1b:a3:91	wlan0	100	AP	ELTX-5GHz_WiFi_A390	On	On	5	60 [80]	52 - 64		2	Wed Oct 18 09:17:12 2017	6,9,12,18,24,36,48,54
Grant	a8:f9:4b:b7:c0:82	wlan0	100	AP	Eltex-Local	On	On	5	44 [20]	44		1	Wed Oct 18 07:55:49 2017	12,18,24,36,48,54
Grant	e0:91:53:83:23:00	wlan0	100	AP	AP-5G_401A_ZS	Off	Off	5	48u [40]	44 - 48		1	Wed Oct 18 10:03:29 2017	6,9,12,18,24,36,48,54

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



To obtain more detailed information, read the full user manual (WEP-2ac, WEP-2ac Smart user manual).

9 Cluster operation mode

9.1 Description

The cluster is a group of devices allocated in a single broadcast domain with synchronized configuration and firmware. Cluster mode is enabled by default. The defining parameter of the mode is the name of a cluster by which the identification of device attachment to this cluster is performed.

The cluster operation mode allows to manage devices in a cluster simultaneously, that sufficiently improves operation efficiency while deploying, configuring or exploiting a wireless network.

When operating in Cluster mode, it is sufficiently that you configure only one access point. The rest of the access points will copy the configuration of the device with set parameters. If the configuration of one access point in a cluster has been changed, the other access points will apply the same changes. The solution is valid while firmware update. Operation in Cluster mode allows to perform manageable consistent firmware update of devices in a cluster.

The default name of a cluster is *«default»*. After loading, WEP-2ac defines if there are devices located on the network with the same name as in its configuration. If the devices with these parameters are not found, WEP-2ac becomes a master of the cluster. If the devices belonging to the cluster are found, WEP-2ac starts copying the configuration of a master. Thus, the first device with enabled Cluster mode occurred on the network becomes a master of its cluster. Other devices occurred on the network later and having the same cluster name start duplicating the master configuration. Several clusters with different names might be located in the same network simultaneously. One access point should be included to only one cluster.

WEP-2ac announces its affiliation to a cluster through a special protocol. The device sends broadcast UDP packets to LAN with data on affiliation to a particular cluster. Thus, all the access points included to a cluster exchange data among them, identify a master of the cluster and its configuration. The master carries out an inventory of the devices in the cluster and always controls the quantity of the access points in the cluster and their addresses.

9.2 Installation

It is sufficient that only one access point be configured when deploying a network. For providing data exchange among devices in a cluster, you should install a DHCP server for network addresses distribution. Network installation algorithm:

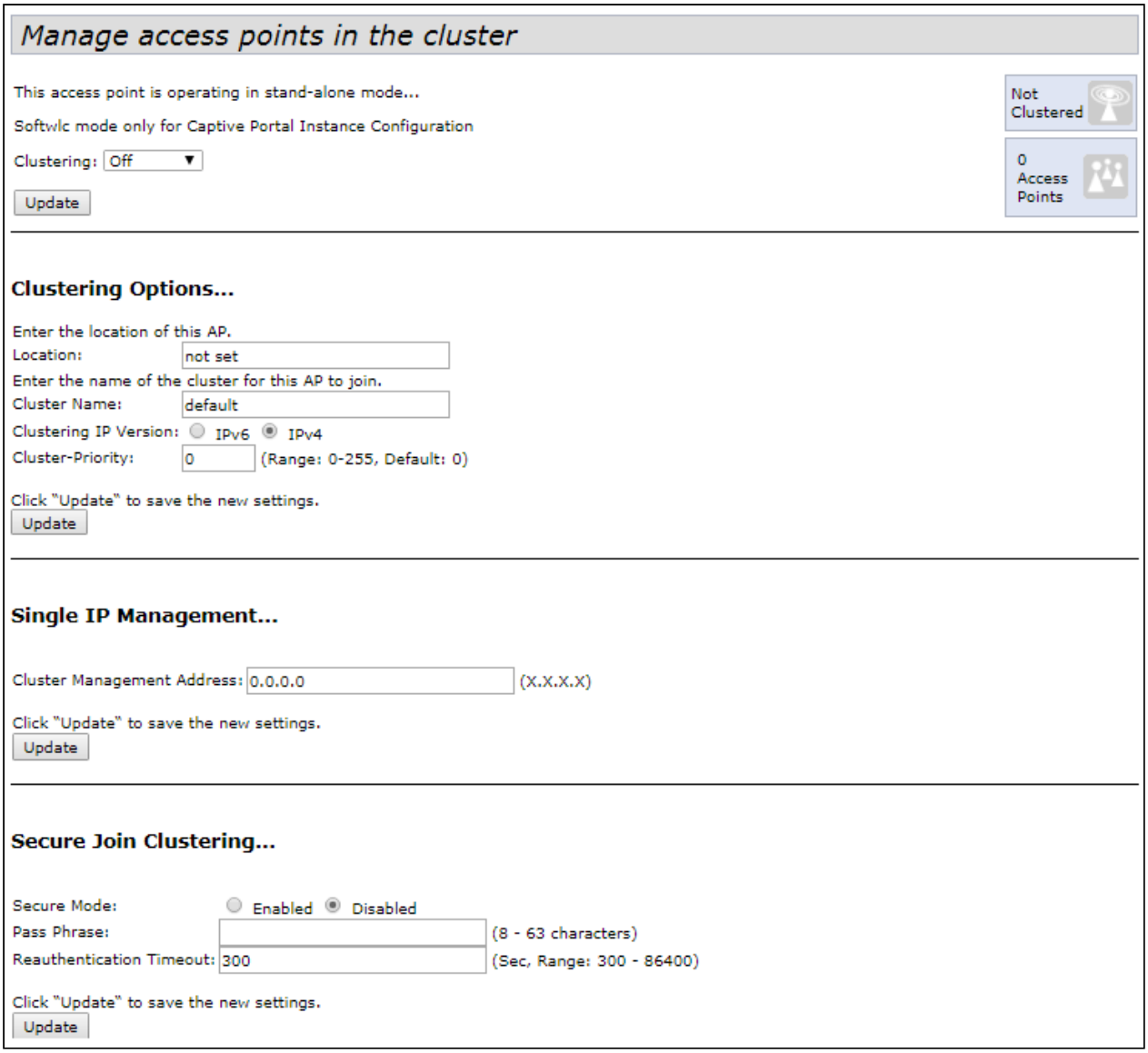
1. DHCP server installation.
2. Configuration and physical connection of an access point.
3. Physical connection of other access points in the cluster.

After installing the first access point, you do not need to configure the rest, it is sufficient to connect them physically to the network. The devices will obtain network addresses, define the master of the «default» cluster and will be automatically configured according to the master configuration.

9.3 Cluster configuration

1. The device may operate in a cluster only if WDS (Wireless Distribution System) and WGB (Work Group Bridge) features are disabled.
2. For operation in a cluster Management Ethernet interfaces of all access points should be located in one network.
3. Cluster operation mode is disabled by default.

In **«Cluster»** menu, open **«Access Points»** tab and perform the following:



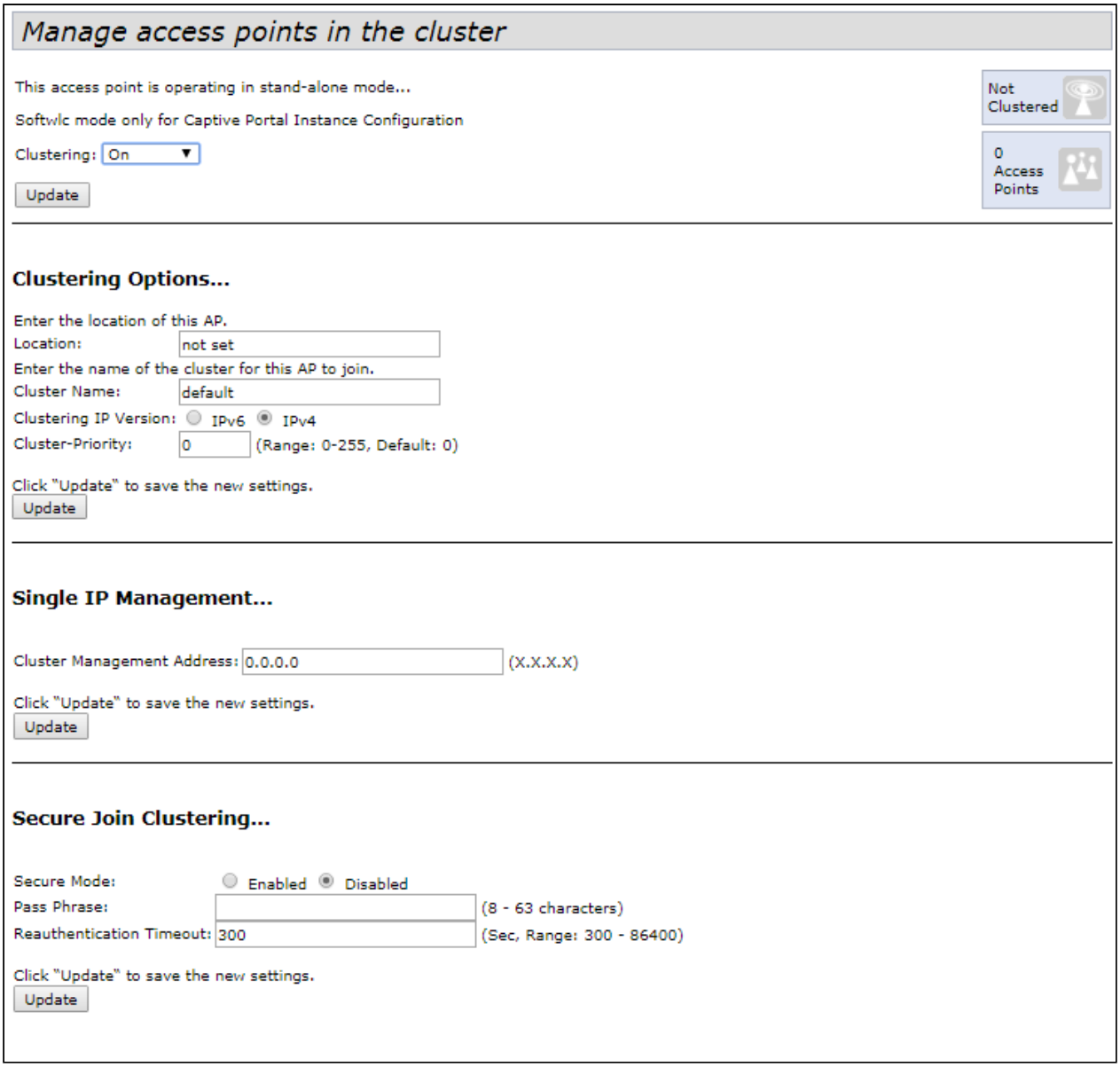
To edit the settings in **«Clustering Options»** section, switch cluster mode to **«Off»** state. In **«Clustering Options»** menu, perform the following configuration:

- **Location** – specify physical location of the access point. The option is used to analyse and control the network in different monitoring tables. *«Eltex»* is used in the example;
- **Cluster Name** – set name cluster. The access point will be connected only to a cluster, which name is specified in *«Cluster Name»*. *«default»* is used in the example;
- **Clustering IP Version** – select used IP version for management data exchange among access points in the cluster. *«IPv4»* is used in the example;
- **Cluster-Priority** – set the priority of the device in the cluster.

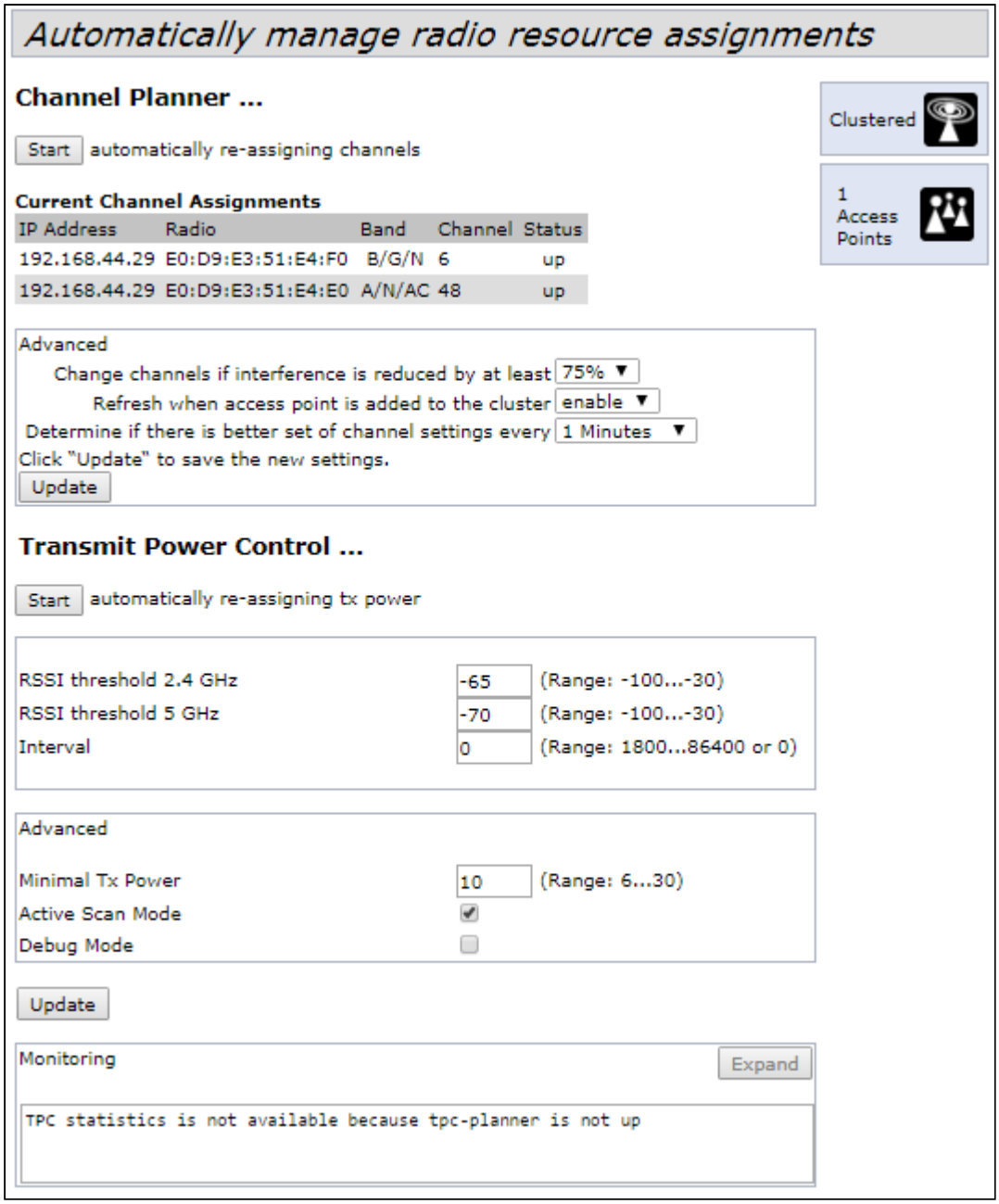
Click **«Update»** to save changes. In **«Single IP Management»** menu, perform the following configuration:

- **Cluster Management Address** – specify an address via which the device may access the master cluster. The master should be located in the same subnet with the cluster. *«192.168.10.10»* is used in the example.

Click **«Update»** to save changes. To enable cluster mode, select **«On»** in **«Clustering»** field.



To enable automatic channel selection according to the data on channels used by neighbouring access points and spectral analysis of environment on third-party access points noise, switch to **«Radio Resource Management»** tab and click **«Start»** in «**Channel Planner»** section. To enable automatic output power distribution of the access point according to influence of neighbouring access points which operate in the same cluster, switch to **«Radio Resource Management»** tab and click **«Start»** in **«Transmit Power Control»** section.



In **«Advanced»** menu, perform the following configuration:

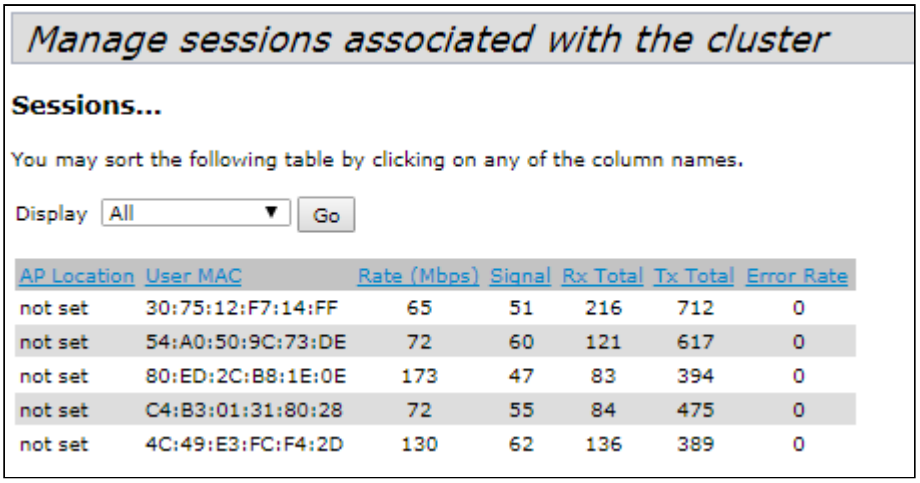
- **Change channels if interference is reduced by at least** – select a percentage that the interference must be reduced by for the access point to change channels. *«75%»* is used in the example.
- **Refresh when access point is added to the cluster** – enable re-counting of common spectral structure of environment and selection of optimal channel for the access point (**«enable»** value) when new access point is being connected to the cluster.
- **Determine if there is better set of channel settings every** – set a time interval to schedule updates of environment spectral structure determination and selection of better channel for the access points. *«1Day»* is used in the example.

Click **«Update»** to save changes.

9.4 Monitoring

To view sessions parameters of clients connected to the access points of given cluster, switch to **«Sessions»** tab. Clients are defined through MAC addresses and an access points which they are connected to. To view the statistics, select necessary value and click **«Go»** in **«Display»** section.

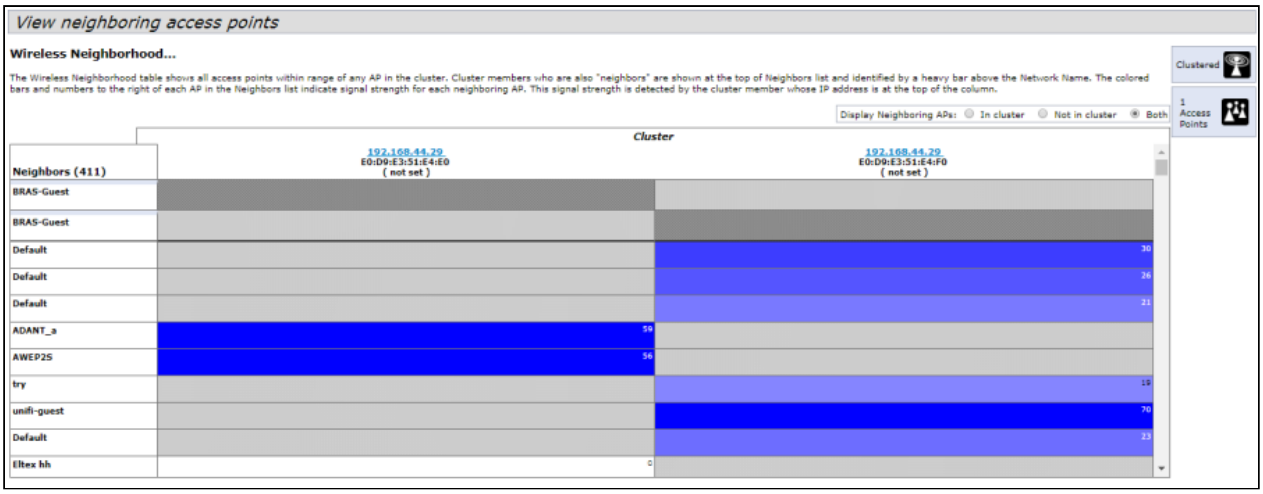
The following parameters might be viewed:



AP Location	User MAC	Rate (Mbps)	Signal	Rx Total	Tx Total	Error Rate
not set	30:75:12:F7:14:FF	65	51	216	712	0
not set	54:A0:50:9C:73:DE	72	60	121	617	0
not set	80:ED:2C:B8:1E:0E	173	47	83	394	0
not set	C4:B3:01:31:80:28	72	55	84	475	0
not set	4C:49:E3:FC:F4:2D	130	62	136	389	0

- **AP Location** – access point's location. The value is obtained from location description on **«Basic Settings»** tab;
- **User MAC** – MAC address of client's wireless device;
- **Idle** – average time that the device has been in stand-by mode (when the device does not receive or transmit data).
- **Rate** – transmit data rate between an access point and a particular client, in Mbps;
- **Signal** – a level of signal received from an access point;
- **Rx Total** – total number of packets received by a client within current session;
- **Transmit Total** – total number of packets transmitted by a client within current session;
- **Error Rate** – total number of packets dropped by an access point within current session.

To view correspondence of access points in a cluster and wireless networks detected by these devices, switch to **«Wireless Neighborhood»** tab. There is a table, on **«Wireless Neighborhood»** tab, that shows which wireless networks are detected by each access point and what signal level each access point accept.



According to this table, spectral analysis of the whole network might be carried out and there is an opportunity to estimate interference influence to each access point. It will help you to estimate better location of access points among coverage area and to define locations with exceeding level of noise. The top string of the table contains

data on each radio interface of access points included in a particular cluster. The left column contains data on wireless networks which are defined by the devices in the cluster. A value of signal level of each access point is displayed in the top-right cell of the table.

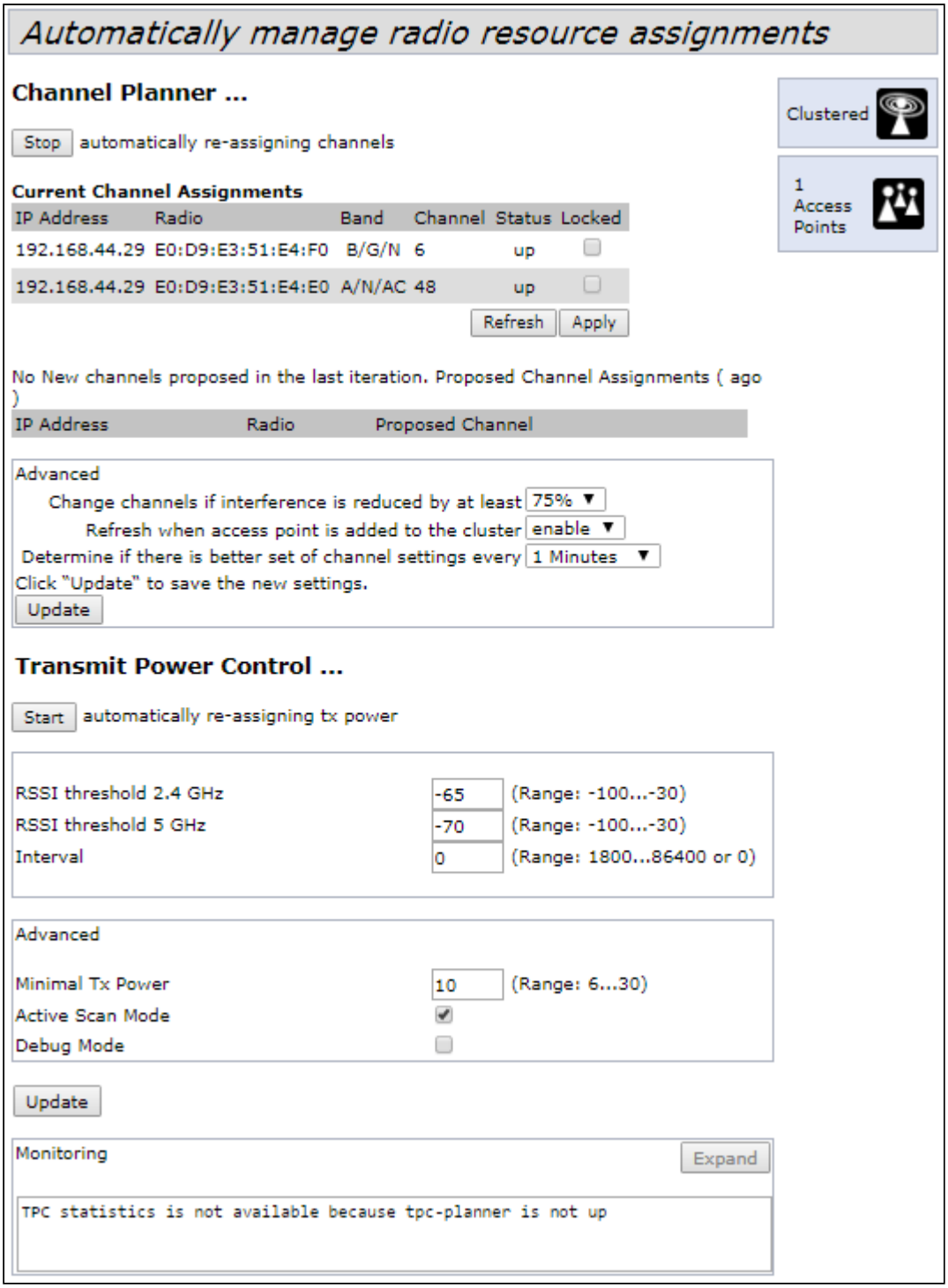
The table is formed in the way that wireless networks organized by a cluster are displayed first, the third-party networks follow after them. The table might be displayed in 3 modes:

- **In cluster** – when checked, the table consists data only on wireless networks organized by the cluster;
- **Not in cluster** – when checked, the table consists data only on third-party wireless networks;
- **Both** – when checked, the table consists data on all wireless networks.

To view current list of the access points in the cluster and their parameters, switch to **«Radio Resource Management»** tab. The table **«Current Channel Assignments»** consists the following parameters:

- **IP Address** – IP address of the access point in the cluster;
- **Radio** – MAC address of a radio interface of the access point in the cluster;
- **Band** – standards supported by the radio interface of the access point in the cluster at the moment;
- **Channel** – number of a channel on which the access point operates;
- **Status** – operation state of the access point's radio interface in the cluster;
- **Locked** – block channel change. When checked, the radio interface will always use the same channel even when another channel is selected as optimal for all the access points in the cluster.

Click **«Refresh»** to update the table **«Current Channel Assignments»**.



The table **«Proposed Channel Assignments»** contains data on available channel values, which the radio interface will switch to if optimal channel selection has been launched:

- **IP Address** – an IP address of the access point in the cluster;
- **Radio** – a MAC address of the radio interface of the access point in the cluster;
- **Proposed Channel** – a channel number to which the radio interface will switch when optimal channel selection is launched.

9.5 Firmware update

The operation in the cluster mode allows to perform automatic firmware update for all the access points in the cluster without using external systems or controllers.

Firmware update might be performed:

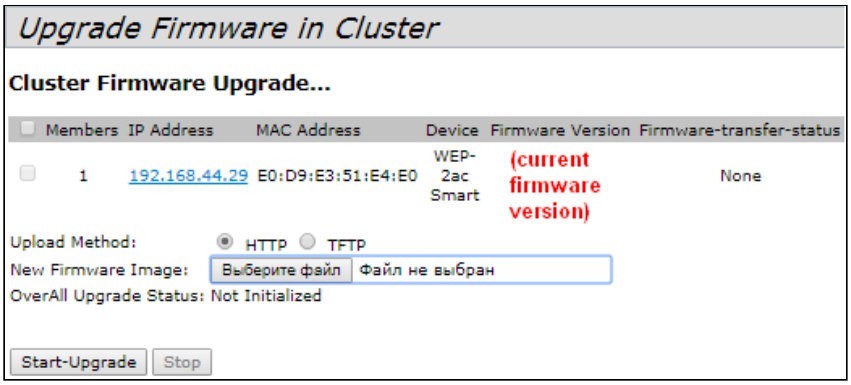
- through the web interface;
- through DHCP Autoprovisioning (opt 66, opt 67).

9.5.1 Firmware update via web interface

To update firmware on devices in a cluster through web interface, open **«Cluster Firmware Upgrade»** tab of an access point.

When updating firmware of devices in a cluster, the firmware file will be loaded to each access point and set to *«Primary Image»*. Reloading of the devices with new firmware version loading is performed automatically. The previous firmware version will be saved as *«Secondary Image»* (backup firmware version).

Perform the following in **«Cluster Firmware Upgrade»** tab:



- **Upload Method** – select the firmware loading method for the devices. The loading through TFTP is used in the example.
- **New Filename Image** – enter a file name of firmware image which will be loaded to the device.

Click **«Start-Upgrade»** to start updating. While firmware updating, do not switch off the devices and do not update or change the web page with progress bar.

9.5.2 Firmware updating through DHCP Autoprovisioning

To update firmware, you need a TFTP server and a DHCP server with particular configuration. The updating process is as follows:

1. An access point is loaded and obtains address via DHCP. The access point obtains 2 parameters from the server while DHCP session: tftp-server and file name, where tftp-server – an IP address of TFTP server, and filename is a name of the file with .manifest extension which contains data on the firmware.
2. A master of the cluster, according to received data, starts make attempts to download manifest-file from TFTP server. After downloading the file, the master compares firmware version specified in a file with its own. If firmware versions are different, the master downloads firmware file from the TFTP server (file name of the firmware is specified in manifest-file) and updates automatically.
3. The other devices in the cluster define that the master is not in operation. Then, new master is selected in the cluster. The device with bigger «uptime» value becomes a master. New master also repeat the second step: downloads manifest-file, compares firmware versions and updates.
4. The cycle is repeated until all the devices in the cluster are updated.

Update configuration algorithm:

1) Place **"wep2.manifest"** file on TFTP server, the file should contain the following string:

VERSION= "1.16.0.X" WEP-2ac-1.16.0.X.tar.gz,
where WEP-2ac-1.16.0.X.tar.gz – name of the archive containing firmware for WEP-2ac;1.16.0.X – a firmware version included to the archive. The firmware version might be viewed in «version» file in firmware archive.

2) Place archive with firmware for WEP-2ac on TFTP server.

3) Correct DHCP server settings (dhcpd.conf) as follows:

option tftp-server-name "100.0.0.1";option bootfile-name "wep2.manifest";
where 100.0.0.1 – an address of TFTP server;wep2.manifest – manifest-name of the file.

TECHNICAL SUPPORT

For technical assistance in issues related to handling of ELTEXALATAU Ltd. equipment please address to Service Centre of the company:

Republic of Kazakhstan, 050032, Medeu district, microdistrict Alatau, 9 st. Ibragimova, 9
Phone:
+7(727) 220-76-10
+7(727) 220-76-07
E-mail: post@eltexalatau.kz

In official website of the ELTEXALATAU Ltd. you can find technical documentation and software for products, refer to knowledge base, consult with engineers of Service center in our technical forum:

http://www.eltexalatau.kz/en/