Integrated Networking Solutions

Wireless access point

# WOP-2ac

Quick guide

Firmware version 1.22.2

IP address: 192.168.1.10

Username: admin

Password: password

Contents

# 1 Annotation

This manual contains the following information:

- connection to WOP-2ac web interface;
- configuration of WOP-2ac network parameters;
- WOP-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 softWLC controller.

The following scheme is given as an example:

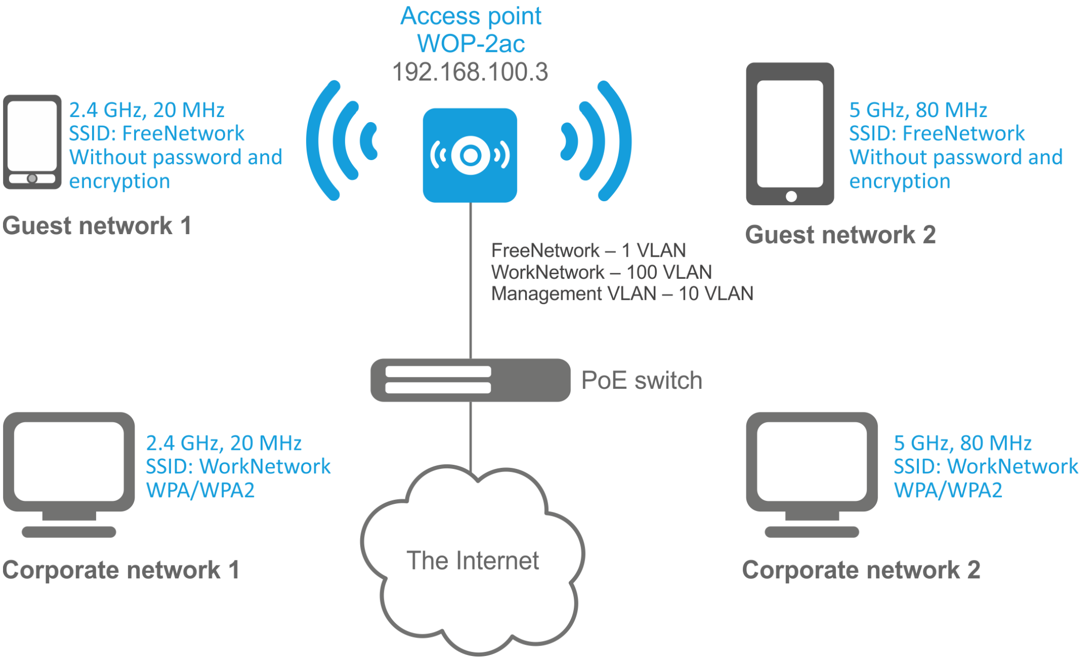


Figure 1 – Example of network configuration

| 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, a PC with access to the device via Ethernet and any web browser (Internet Explorer, Firefox, Google Chrome, Opera, etc.) are required.

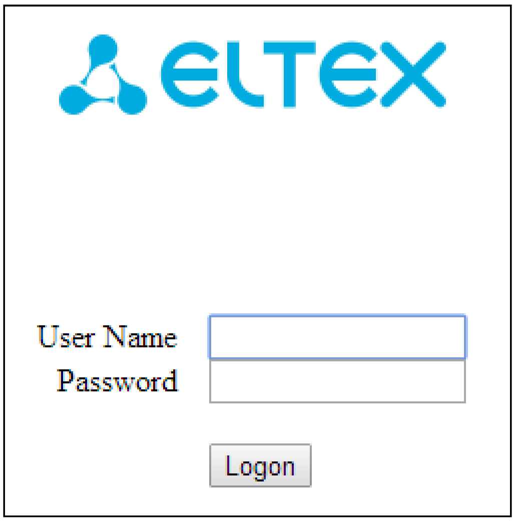
## 2 Connecting the web interface

Connect network cable to the PoE interface of the access point and to the PoE switch/injector. Next, connect a PC to the injector or switch.

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.

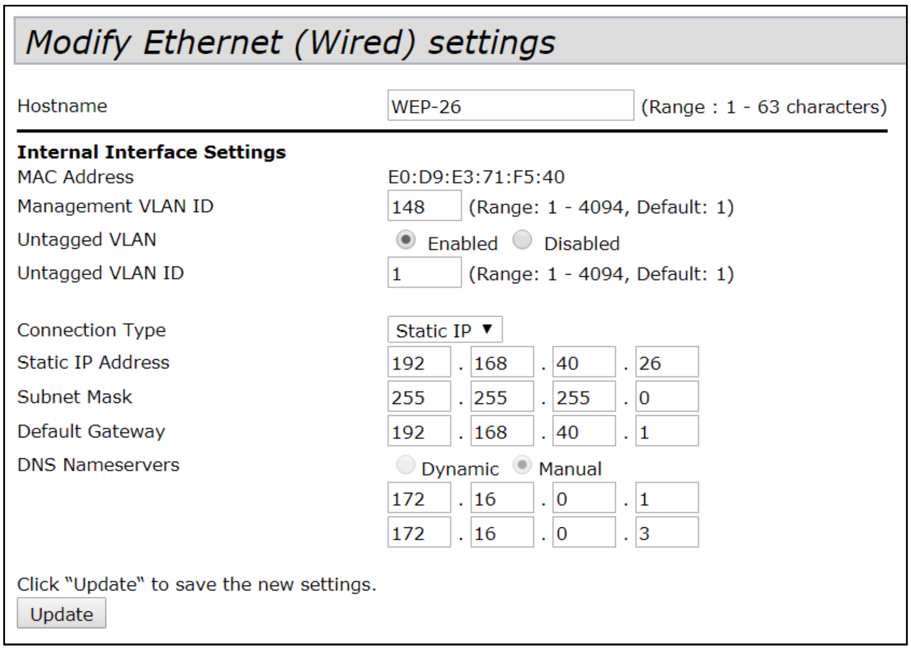
A menu for monitoring the status of the device will open in a browser window.

> ! 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.

# 3 WOP-2ac network parameters configuration

For remote management of WOP-2ac, 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:



Modify Ethernet (Wired) settings

Hostname: WEP-26 (Range : 1 - 63 characters)

**Internal Interface Settings**

MAC Address: E0:D9:E3:71:F5:40

Management VLAN ID: 148 (Range: 1 - 4094, Default: 1)

Untagged VLAN: ● Enabled ○ Disabled

Untagged VLAN ID: 1 (Range: 1 - 4094, Default: 1)

Connection Type: Static IP ▼

Static IP Address: 192 . 168 . 40 . 26

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 192 . 168 . 40 . 1

DNS Nameservers: ○ Dynamic ● Manual

172 . 16 . 0 . 1

172 . 16 . 0 . 3

Click "Update" to save the new settings.

- *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* – select **Static IP** to set IP addresses for access points manually. If it is necessary to distribute IP addresses and other network parameters to access points via the DHCP protocol, set the **Connection Type** field to **DHCP** and this will complete the configuration of the network part;
- *Static IP Address* – specify the IP address of WOP-2ac. In the given example, VLAN 10 address is **192.168.100.3**.
- *Subnet Mask* – specify the subnet mask. In the given example, subnet mask is **255.255.255.0**.
- *Default Gateway* – enter the IP address of the default gateway field. In the given example, IP address of the default gateway is **192.168.100.1**.

For the new configuration to take effect and the settings to be stored in the non-volatile memory of the access point, click the **Update** button.

After the configuration, WOP-2ac will be available in 10 VLAN via 192.168.100.3 address.

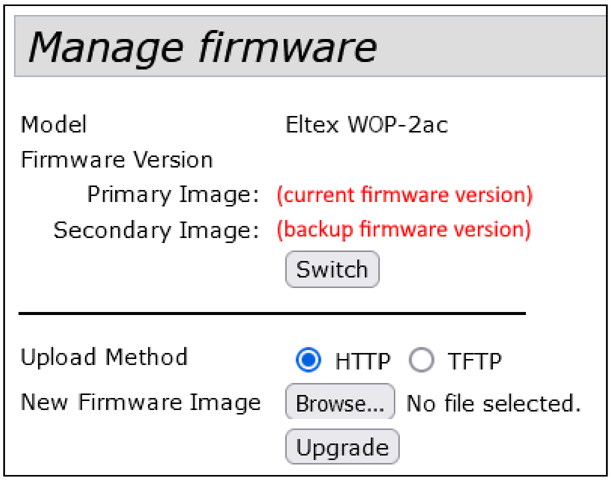
Before making changes to the network settings of the access point, make sure that the host computer has access to the network where the access point will be located, based on the configured network settings. In case of entering and applying incorrect data while changing the settings, undo them by resetting 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.

## 4 WOP-2ac firmware upgrade

For correct operation of WOP-2ac, 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:



*Manage firmware*

Model Eltex WOP-2ac

Firmware Version

Primary Image: (current firmware version)

Secondary Image: (backup firmware version)

Upload Method ● HTTP ○ TFTP

New Firmware Image No file selected.

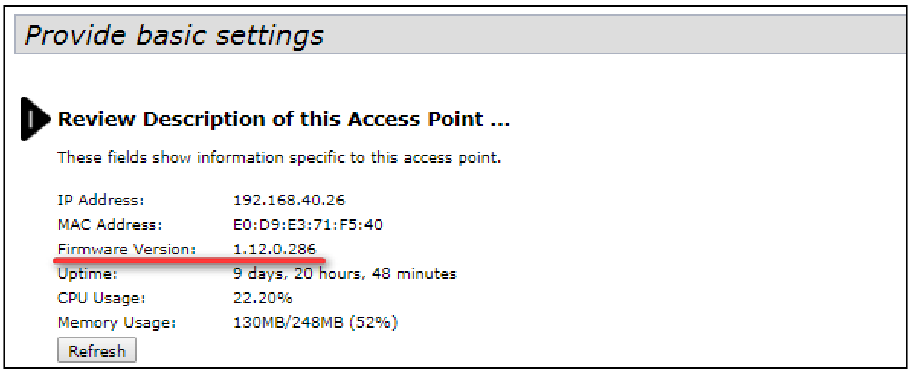
- *Upload Method* – check **HTTP**;
- *New Firmware Image* – click **Browse** button and select relevant firmware version in the window that opens.

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.



*Provide basic settings*

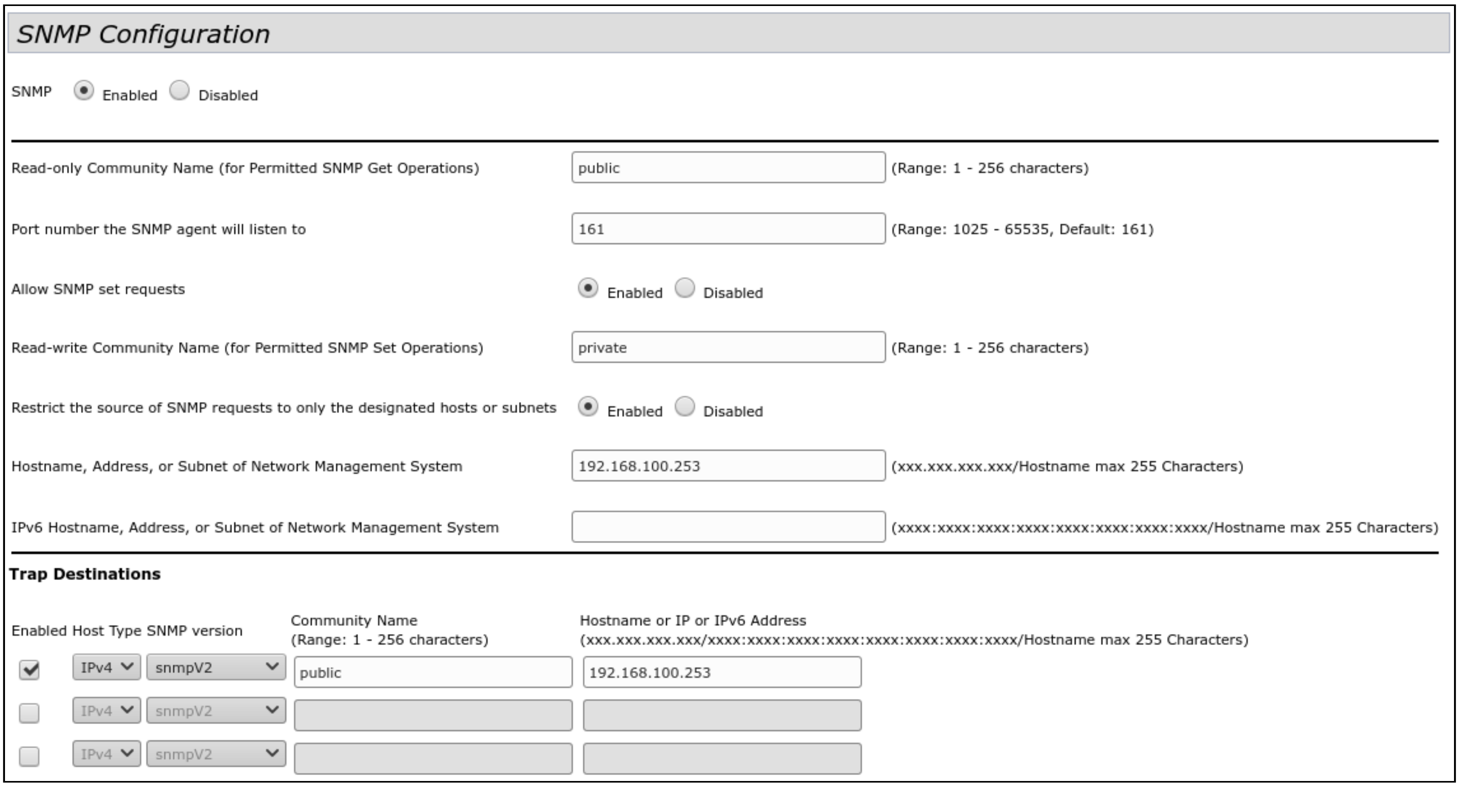
**Review Description of this Access Point ...**

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%) |

# 5 SNMP service configuration

SNMP service configuration is performed in the **SNMP** section of the **Services** menu.



*SNMP Configuration*

SNMP ● Enabled ○ Disabled

| | | |
|---|---|---|
| Read-only Community Name (for Permitted SNMP Get Operations) | public | (Range: 1 - 256 characters) |
| Port number the SNMP agent will listen to | 161 | (Range: 1025 - 65535, Default: 161) |
| Allow SNMP set requests | ● Enabled ○ Disabled | |
| Read-write Community Name (for Permitted SNMP Set Operations) | private | (Range: 1 - 256 characters) |
| Restrict the source of SNMP requests to only the designated hosts or subnets | ● Enabled ○ Disabled | |
| Hostname, Address, or Subnet of Network Management System | 192.168.100.253 | (xxx.xxx.xxx.xxx/Hostname max 255 Characters) |
| IPv6 Hostname, Address, or Subnet of Network Management System | | (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters) |

**Trap Destinations**

| Enabled | Host Type | SNMP version | Community Name (Range: 1 - 256 characters) | Hostname or IP or IPv6 Address (xxx.xxx.xxx.xxx/xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters) |
|---|---|---|---|---|
| ☑ | IPv4 | snmpV2 | public | 192.168.100.253 |
| ☐ | IPv4 | snmpV2 | | |
| ☐ | IPv4 | snmpV2 | | |

- *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. In the given example, IP address is **192.168.100.253**.

In the **Trap Destinations** section, perform the following settings:

- Set the flag in the column with the **Enabled** heading;
- *Host Type* – specify whether the enabled host is an IPv4 host or an IPv6 host. In this example, IPv4 is selected;
- *SNMP version* – select the version of the SNMP protocol. In this example, the **snmpV2** protocol is selected;
- *Community name for traps* – set community name **public**.
- *Host name or IP or IPv6 Address* – check one of the fields for specifying traps receiver address and enter an IP address of the device to which WOP-2ac will send traps. In the given example, IP address to receive SNMP traps is **192.168.100.253**.

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

# 6 Wireless interfaces configuration

WOP-2ac has 2 radio interfaces (Radio 1 and Radio 2) which are capable to operate simultaneously. Each interface is capable to operate on its frequency band in different wireless network modes. 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:

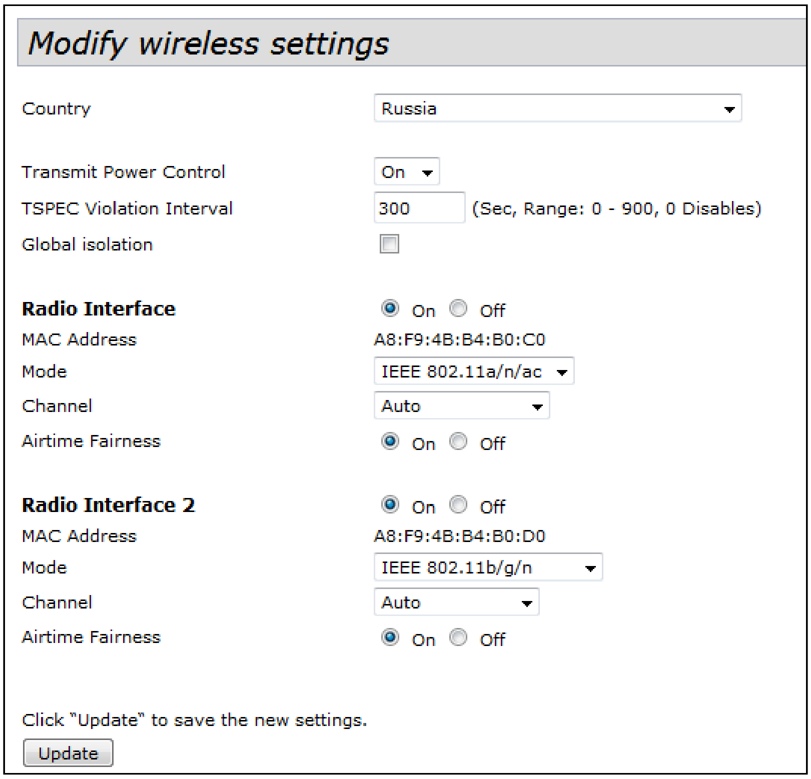
Radio1:

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

Radio2:

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

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



*Modify wireless settings*

| | |
|---|---|
| Country | Russia |
| Transmit Power Control | On |
| TSPEC Violation Interval | 300 (Sec, Range: 0 - 900, 0 Disables) |
| Global isolation | □ |
| **Radio Interface** | ● On ○ Off |
| MAC Address | A8:F9:4B:B4:B0:C0 |
| Mode | IEEE 802.11a/n/ac |
| Channel | Auto |
| Airtime Fairness | ● On ○ Off |
| **Radio Interface 2** | ● On ○ Off |
| MAC Address | A8:F9:4B:B4:B0:D0 |
| Mode | IEEE 802.11b/g/n |
| Channel | Auto |
| Airtime Fairness | ● On ○ Off |

Click "Update" to save the new settings.

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

Configuring Radio 1:

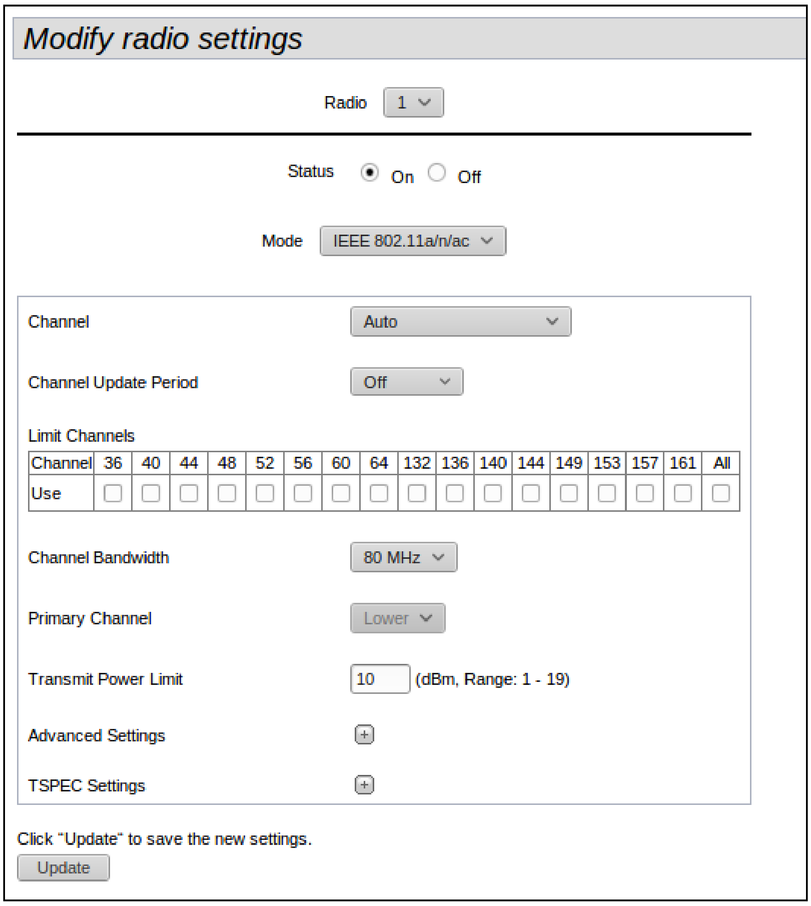
- *Radio Interface* – enable radio interface. Set **On**;
- *Mode* – radio interface operation mode. Select the **IEEE 802.11a/n/ac** value.

Configuring Radio 2:

- *Radio Interface* – enable radio interface. Set **On**;
- *Mode* – radio interface operation mode. Select the **IEEE 802.11b/g/n**

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:



Modify radio settings

Radio: 1

Status: ● On ○ Off

Mode: IEEE 802.11a/n/ac

Channel: Auto

Channel Update Period: Off

Limit Channels

| Channel | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 | 132 | 136 | 140 | 144 | 149 | 153 | 157 | 161 | All |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Use | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ | □ |

Channel Bandwidth: 80 MHz

Primary Channel: Lower

Transmit Power Limit: 10 (dBm, Range: 1 - 19)

Advanced Settings ⊞

TSPEC Settings ⊞

Click "Update" to save the new settings.

Configuring Radio 1:

- *Radio* – select the configured interface. Select **1**;
- *Channel Bandwidth* – set **80 MHz.**

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

Configuring Radio 2:

- *Radio* – select the configured interface. Select **2**;
- *Channel Bandwidth* – set **20 MHz**.

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

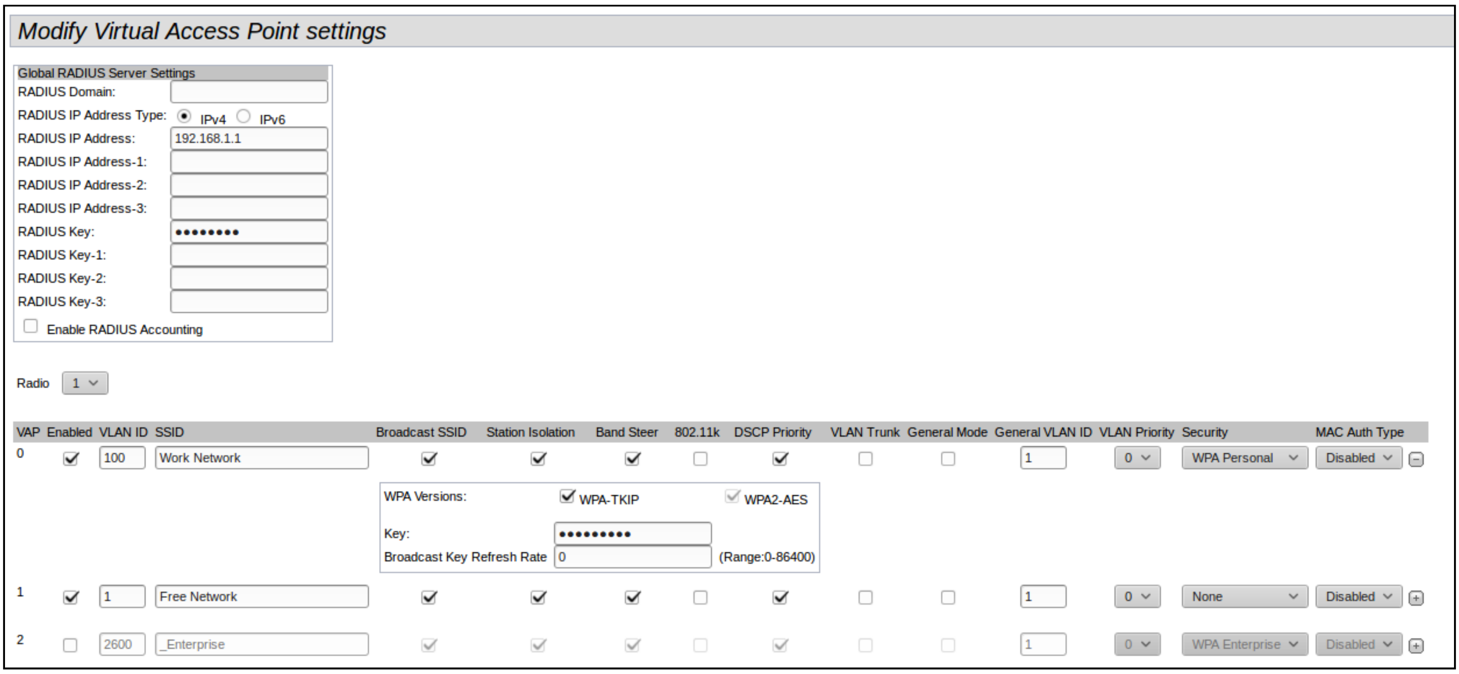
# 7 Virtual access points configuration

On each wireless interface, up to 16 virtual access points can be configured. 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  virtual access points operating at 5 GHz.
The following is necessary for Band Steer feature operation:

- create virtual access points (VAP) with the same SSID on each radio interface;
- when using encryption, make sure that the passwords on the created VAPs match;
- activate Band Steer parameter on VAP.

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



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 1

| VAP | Enabled | VLAN ID | SSID | Broadcast SSID | Station Isolation | Band Steer | 802.11k | DSCP Priority | VLAN Trunk | General Mode | General VLAN ID | VLAN Priority | Security | MAC Auth Type |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | ☑ | 100 | Work Network | ☑ | ☑ | ☑ | □ | ☑ | □ | □ | 1 | 0 | WPA Personal | Disabled |
| 1 | ☑ | 1 | Free Network | ☑ | ☑ | ☑ | □ | ☑ | □ | □ | 1 | 0 | None | Disabled |
| 2 | □ | 2600 | _Enterprise | ☑ | ☑ | ☑ | □ | ☑ | □ | □ | 1 | 0 | WPA Enterprise | Disabled |

WPA Versions: ☑ WPA-TKIP ☑ WPA2-AES
Key: •••••••••
Broadcast Key Refresh Rate 0 (Range:0-86400)

Configuring Radio 1:

- *Radio* – select radio interface on which VAP will be configured. Select **1**;
- *Enabled* – enable VAP. Check the boxes for VAP 0 and VAP1;
- *VLAN ID* – VLAN number from which the tag will be removed when transmitting Wi-Fi traffic to clients connected to this VAP. When traffic flows in the opposite direction, untagged traffic from clients will be tagged with VLAN ID (when VLAN Trunk mode is disabled):
  - set VLAN ID value **100** for VAP 0;
  - set VLAN ID value **1** for VAP 1.
- *SSID* – wireless network name:
  - set SSID value **Work Network** for VAP 0;
  - set SSID 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.
- *VLAN Priority* – the 2nd priority level which will be assigned to packets transmitted through the given VAP from radio environment to wired network.
- *Security* – secure network mode:
  - set **WPA Personal** value for VAP 0;
    - set a password for this network connection in the **Key** field;
- set value **None** for VAP 1.

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

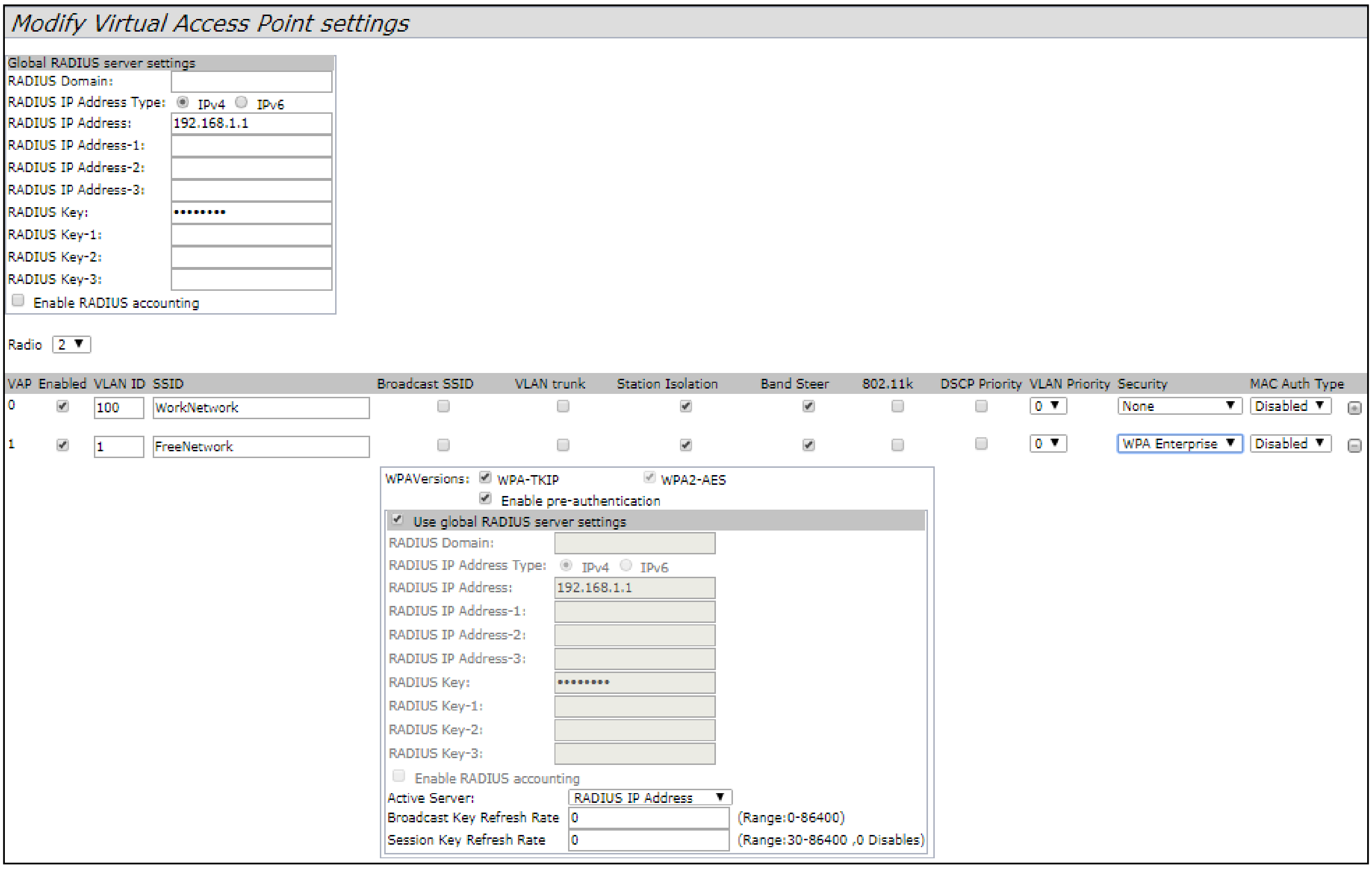
Configuration of VAP on Radio 2 is performed the same way. Select value **2** in **Radio** and perform the configuration as for the Radio 1 (given above). The password for “Work Network” SSID should be the same for both VAP Radio 1 and VAP Radio 2.

After configuring VAP on Radio 2, click **Update**.

When using WPA Enterprise security mode, the authorization is implemented through a RADIUS server. The request on user connection to SSID with **WPA Enterprise** security mode is sent to a RADIUS server. To connect to the RADIUS server, specify the following parameters in the *Global RADIUS server settings* table:

- *RADIUS Domain* – user domain;
- *RADIUS IP Address* – IP address of the RADIUS server;
- *RADIUS Key* – password to access the RADIUS server;
- *Enable RADIUS Accounting* – when checked, the Accounting messages will be sent to RADIUS server.

In the VAP settings, in the Security field, select **WPA Enterprise**, then check the box next to the **Use Global RADIUS Server Settings** in the window that opens (if the window does not appear, click the "+" sign on the left in the VAP settings line).
If it is necessary to use a different RADIUS server for each VAP, then uncheck the box next to the **Use Global RADIUS Server Settings** and set the parameters for the RADIUS server listed above in the VAP settings window.



*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 ▼ | None ▼ | Disabled ▼ | ⊕ |
| 1 | ☑ | 1 | FreeNetwork | □ | □ | ☑ | ☑ | □ | □ | 0 ▼ | WPA Enterprise ▼ | Disabled ▼ | ⊖ |

WPAVersions: ☑ WPA-TKIP ☑ WPA2-AES
☑ Enable pre-authentication

☑ Use 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

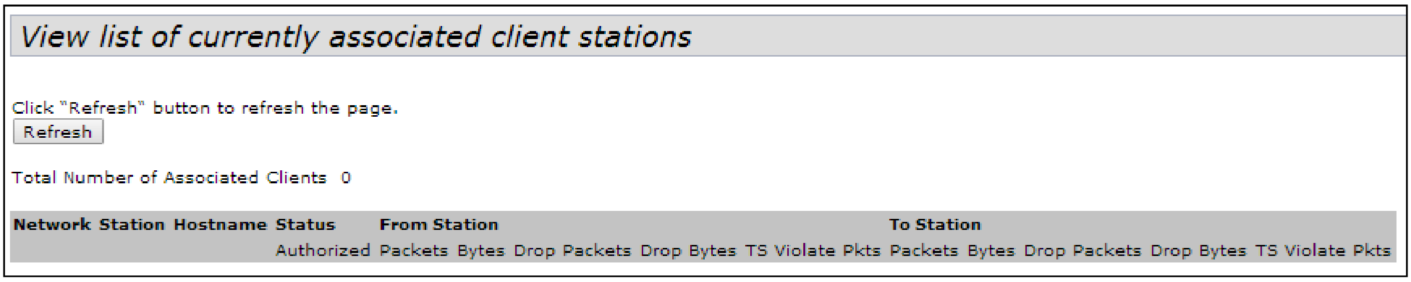
| | | |
|---|---|---|
| Active Server: | RADIUS IP Address ▼ | |
| Broadcast Key Refresh Rate | 0 | (Range:0-86400) |
| Session Key Refresh Rate | 0 | (Range:30-86400 ,0 Disables) |

# 8 Monitoring main parameters of wireless network

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

Clicking on the client's MAC address reveals detailed information about the client operation and statistics on packet transmission.

To update information on the page, click **Refresh**.



*View list of currently associated client stations*

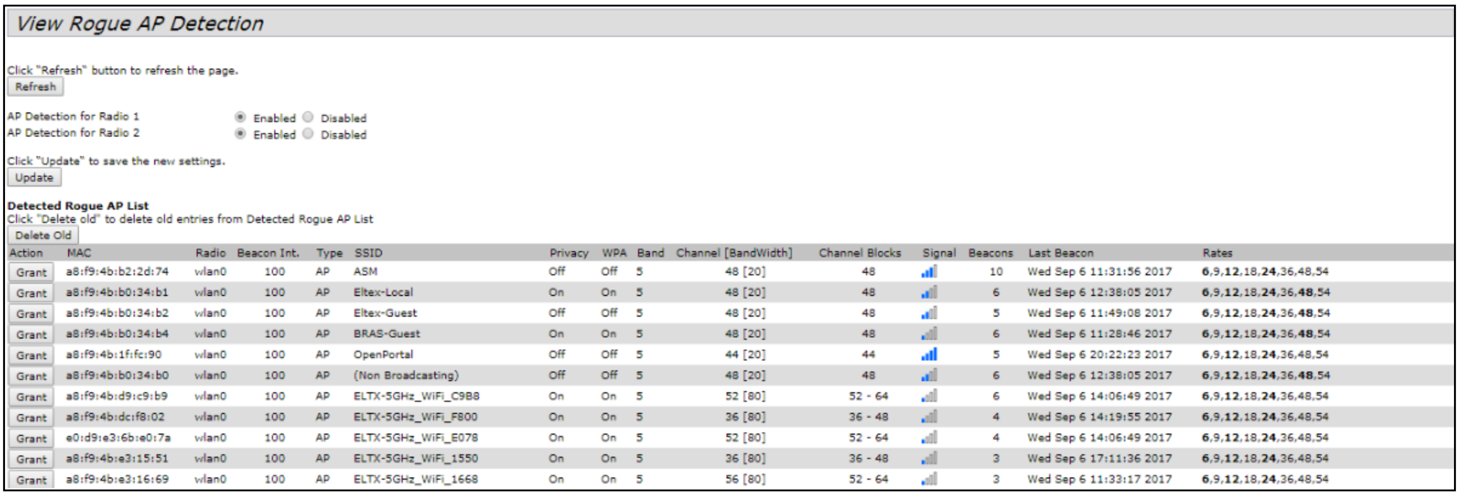
Click "Refresh" button to refresh the page.

Refresh

Total Number of Associated Clients 0

| Network | Station | Hostname | Status | From Station | | | | | To Station | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Authorized | Packets | Bytes | Drop Packets | Drop Bytes | TS Violate Pkts | Packets | Bytes | Drop Packets | Drop Bytes | TS Violate Pkts |

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



*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.

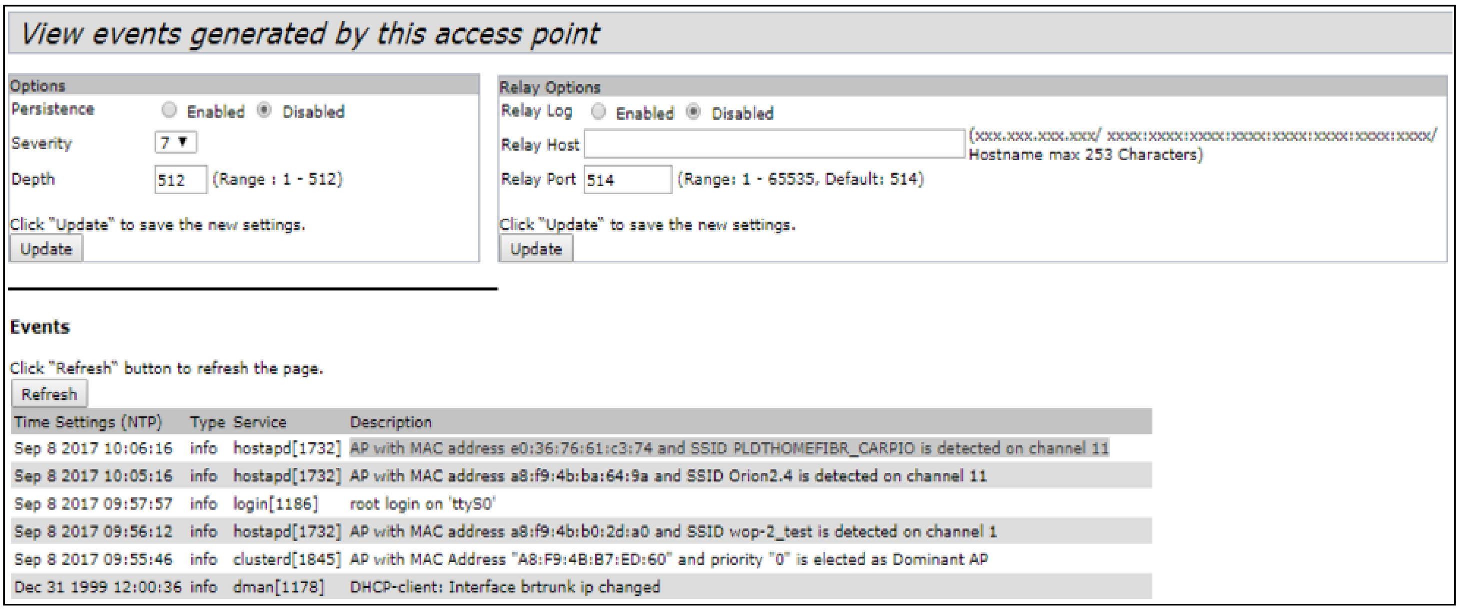
Update

**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 | a8:f9:4b:b2:2d:74 | wlan0 | 100 | AP | ASM | Off | Off | 5 | 48 [20] | 48 | | 10 | Wed Sep 6 11:31:56 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b1 | wlan0 | 100 | AP | Eltex-Local | On | On | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 12:38:05 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b2 | wlan0 | 100 | AP | Eltex-Guest | Off | Off | 5 | 48 [20] | 48 | | 5 | Wed Sep 6 11:49:08 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b4 | wlan0 | 100 | AP | BRAS-Guest | On | On | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 11:28:46 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:1f:fc:90 | wlan0 | 100 | AP | OpenPortal | Off | Off | 5 | 44 [20] | 44 | | 5 | Wed Sep 6 20:22:23 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:b0:34:b0 | wlan0 | 100 | AP | (Non Broadcasting) | Off | Off | 5 | 48 [20] | 48 | | 6 | Wed Sep 6 12:38:05 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:d9:c9:b9 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_C9B8 | On | On | 5 | 52 [80] | 52 - 64 | | 6 | Wed Sep 6 14:06:49 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:dc:f8:02 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_F800 | On | On | 5 | 36 [80] | 36 - 48 | | 4 | Wed Sep 6 14:19:55 2017 | 6,9,12,18,24,36,48,54 |
| Grant | e0:d9:e3:6b:e0:7a | wlan0 | 100 | AP | ELTX-5GHz_WiFi_E078 | On | On | 5 | 52 [80] | 52 - 64 | | 4 | Wed Sep 6 14:06:49 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:e3:15:51 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_1550 | On | On | 5 | 36 [80] | 36 - 48 | | 3 | Wed Sep 6 17:11:36 2017 | 6,9,12,18,24,36,48,54 |
| Grant | a8:f9:4b:e3:16:69 | wlan0 | 100 | AP | ELTX-5GHz_WiFi_1668 | On | On | 5 | 56 [80] | 52 - 64 | | 3 | Wed Sep 6 11:33:17 2017 | 6,9,12,18,24,36,48,54 |

The list of events is given in the **Events** tab of the **Status** menu. Redirection of events to a third-party SYSLOG server can be configured here as well.



*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 |
|---|---|---|---|
| Sep 8 2017 10:06:16 | info | hostapd[1732] | AP with MAC address e0:36:76:61:c3:74 and SSID PLDTHOMEFIBR_CARPIO is detected on channel 11 |
| Sep 8 2017 10:05:16 | info | hostapd[1732] | AP with MAC address a8:f9:4b:ba:64:9a and SSID Orion2.4 is detected on channel 11 |
| Sep 8 2017 09:57:57 | info | login[1186] | root login on 'ttyS0' |
| Sep 8 2017 09:56:12 | info | hostapd[1732] | AP with MAC address a8:f9:4b:b0:2d:a0 and SSID wop-2_test is detected on channel 1 |
| Sep 8 2017 09:55:46 | info | clusterd[1845] | AP with MAC Address "A8:F9:4B:B7:ED:60" and priority "0" is elected as Dominant AP |
| Dec 31 1999 12:00:36 | info | dman[1178] | DHCP-client: Interface brtrunk ip changed |

# 9 Cluster operation mode

## 9.1 Description

The Cluster operation mode allows managing 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 enough to 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 performing manageable consistent firmware update of devices in a cluster.

The cluster is a group of devices allocated in a single broadcast domain with synchronized configuration and firmware. Cluster mode on the access point 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 default name of a cluster is *"default"*.

Multiple clusters with different names can be present on the network at the same time. One access point can only belong to one of the clusters.

After loading, the device 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, WOP-2ac becomes a master of the cluster. If the devices belonging to the cluster are found, WOP-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.

The device 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.

Only access points from the same group can be combined into a cluster:

| | | | | | |
|---|---|---|---|---|---|
| 1 group | WEP-12ac | WOP-12ac | | | |
| 2 group | WEP-2ac | WEP-2ac Smart | WOP-2ac | WOP-2ac SFP | WOP-2ac GPON |

## 9.2 Installation

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

Network installation algorithm:

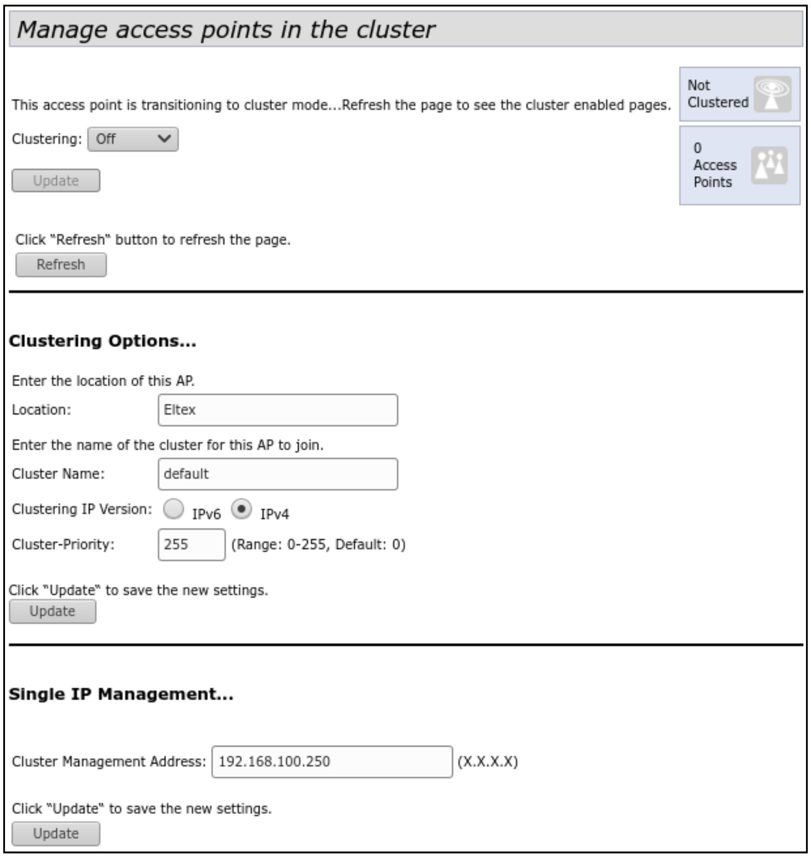
1. DHCP server installation.
2. Configuration and physical connection of an access point.
3. Physical connection of other access points in the cluster.

After installing the first access point, there is no 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.

# 10 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 the **Cluster** menu, open **Access Points** tab and perform the following:



Manage access points in the cluster

This access point is transitioning to cluster mode...Refresh the page to see the cluster enabled pages.

Clustering: Off

Click "Refresh" button to refresh the page.

**Clustering Options...**

Enter the location of this AP.

Location: Eltex

Enter the name of the cluster for this AP to join.

Cluster Name: default

Clustering IP Version: ○ IPv6 ● IPv4

Cluster-Priority: 255 (Range: 0-255, Default: 0)

Click "Update" to save the new settings.

**Single IP Management...**

Cluster Management Address: 192.168.100.250 (X.X.X.X)

Click "Update" to save the new settings.

To edit the settings in the **Clustering Options** section, switch cluster mode to **Off** state.

In the **Clustering Options** section, perform the following configuration:

- *Location* – specify physical location of the access point. The option is used to analyze and control the network in different monitoring tables. *"***Eltex***"* is used in the example;
- *Cluster Name* – set cluster name. 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. The access point with the maximum value of this parameter becomes the Master point. If the parameter is not set, the access point with the lowest MAC address becomes the master point in the cluster. To avoid a situation in which the master point of the cluster will be re-elected, since an access point with a lower MAC address than that of the configured point was included in the network, set the value of the parameter to **255**.

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

In the **Single IP Management** menu, perform the following configuration:

- *Cluster Management Address* – specify unique IPv4 address via which the device may access the master cluster. The master should be located in the same subnet with the cluster and not match IP address of other devices. **192.168.100.250** is used in the example.

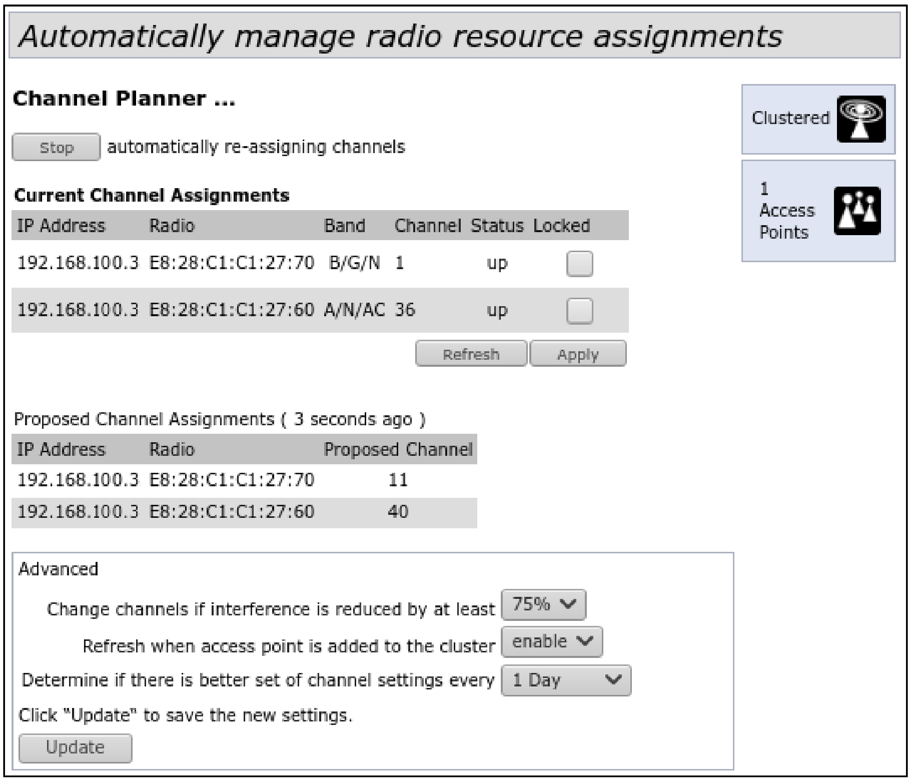
To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

To enable cluster mode, select **On** in the **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 the **Radio Resource Management** tab and click **Start** in the **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 the **Radio Resource Management** tab and click **Start** in the **Transmit Power Control** section.

In the **Locked** field, channel change for the radio interface of the access point can be locked. If the flag is set, when the optimal channel is selected by all access points, this radio interface will use the previous channel for any outcome of the optimal channel selection.



Automatically manage radio resource assignments

Channel Planner ...

Stop automatically re-assigning channels

Current Channel Assignments

| IP Address | Radio | Band | Channel | Status | Locked |
|---|---|---|---|---|---|
| 192.168.100.3 | E8:28:C1:C1:27:70 | B/G/N | 1 | up | □ |
| 192.168.100.3 | E8:28:C1:C1:27:60 | A/N/AC | 36 | up | □ |

Proposed Channel Assignments ( 3 seconds ago )

| IP Address | Radio | Proposed Channel |
|---|---|---|
| 192.168.100.3 | E8:28:C1:C1:27:70 | 11 |
| 192.168.100.3 | E8:28:C1:C1:27:60 | 40 |

Advanced

Change channels if interference is reduced by at least: 75%

Refresh when access point is added to the cluster: enable

Determine if there is better set of channel settings every: 1 Day

Click "Update" to save the new settings.

In the **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.

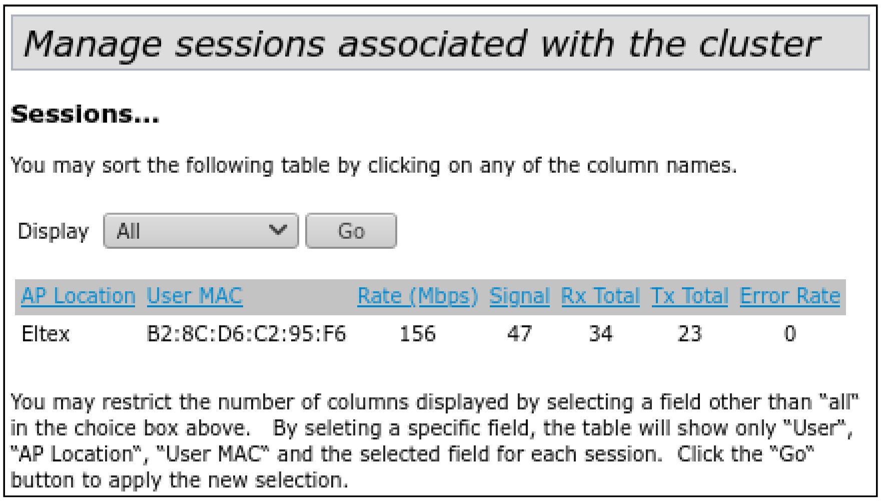
To apply a new configuration and save setting to non-volatile memory of the access point, click **Update**.

## 10.1 Monitoring

To view sessions parameters of clients connected to the access points of given cluster, switch to the **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 the **Display** section. The following parameters might be viewed:



Manage sessions associated with the cluster

**Sessions...**

You may sort the following table by clicking on any of the column names.

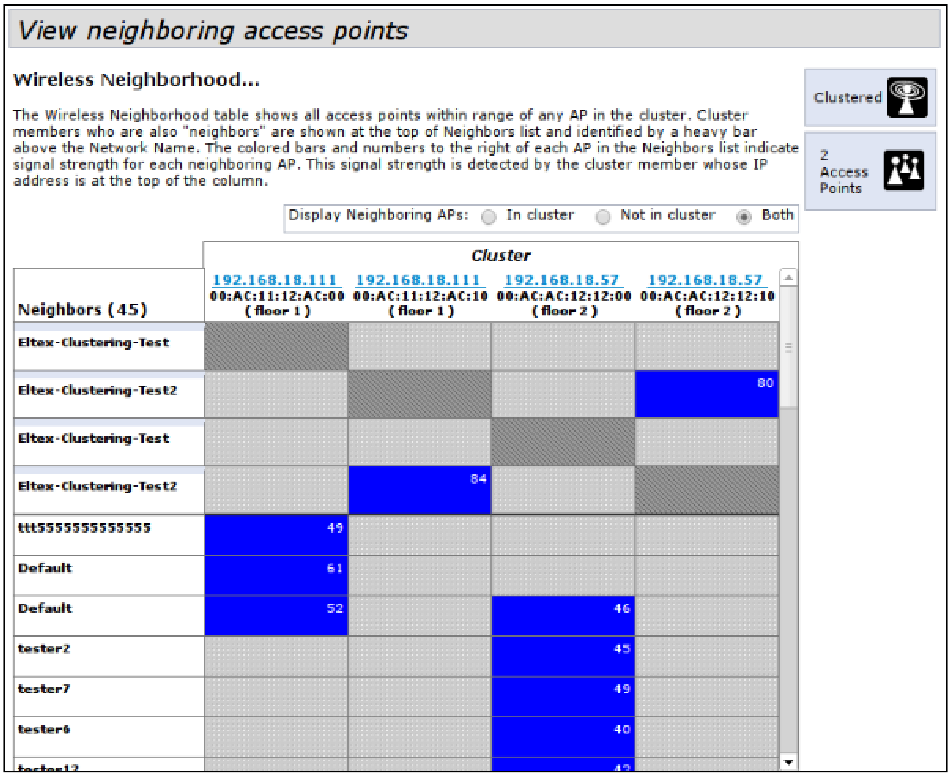
Display All Go

| AP Location | User MAC | Rate (Mbps) | Signal | Rx Total | Tx Total | Error Rate |
|---|---|---|---|---|---|---|
| Eltex | B2:8C:D6:C2:95:F6 | 156 | 47 | 34 | 23 | 0 |

You may restrict the number of columns displayed by selecting a field other than "all" in the choice box above. By seleting a specific field, the table will show only "User", "AP Location", "User MAC" and the selected field for each session. Click the "Go" button to apply the new selection.

- AP Location – access point physical location. The value is obtained from location description on the **Access Points** tab;
- *User MAC* – MAC address of client wireless device;
- *Rate* – transmit data rate between an access point and a particular client, in Mbps;
- *Signal* – level of signal received from an access point, dBm;
- *Rx Total* – total number of packets received by a client within current session;
- *Tx 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 the **Wireless Neighborhood** tab.



View neighboring access points

Wireless Neighborhood...

The Wireless Neighborhood table shows all access points within range of any AP in the cluster. Cluster members who are also "neighbors" are shown at the top of Neighbors list and identified by a heavy bar above the Network Name. The colored bars and numbers to the right of each AP in the Neighbors list indicate signal strength for each neighboring AP. This signal strength is detected by the cluster member whose IP address is at the top of the column.

Display Neighboring APs: ○ In cluster ○ Not in cluster ● Both

| | Cluster | | | |
|---|---|---|---|---|
| Neighbors (45) | 192.168.18.111<br>00:AC:11:12:AC:00<br>( floor 1 ) | 192.168.18.111<br>00:AC:11:12:AC:10<br>( floor 1 ) | 192.168.18.57<br>00:AC:AC:12:12:00<br>( floor 2 ) | 192.168.18.57<br>00:AC:AC:12:12:10<br>( floor 2 ) |
| Eltex-Clustering-Test | ▨ | | | |
| Eltex-Clustering-Test2 | | ▨ | | 80 |
| Eltex-Clustering-Test | | | ▨ | |
| Eltex-Clustering-Test2 | | 84 | | ▨ |
| ttt5555555555555 | 49 | | | |
| Default | 61 | | | |
| Default | 52 | | 46 | |
| tester2 | | | 45 | |
| tester7 | | | 49 | |
| tester6 | | | 40 | |
| tester12 | | | 42 | |

This table 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.  This will allow assessing the correct location of access points across the coverage area and indicating problem areas in which the level of interference may interfere with the quality of services.

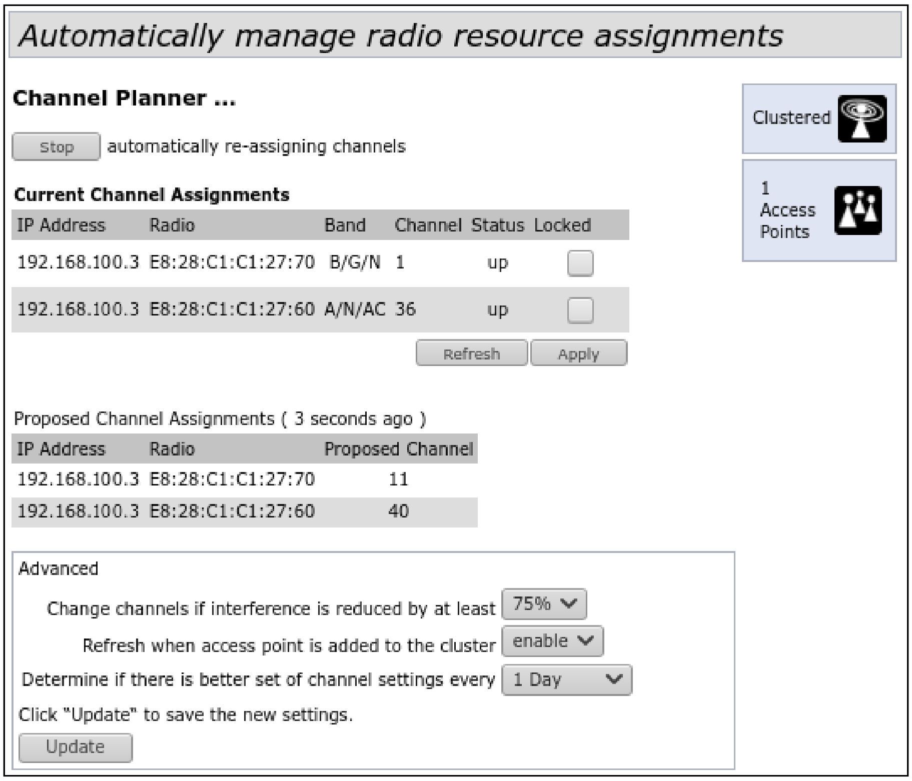
The top line of the table contains data on each radio interface of access points included in a particular cluster. The left column contains data on wireless networks which are defined by the devices in the cluster. A value of signal level of each access point is displayed in the top-right cell of the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

To view current list of the access points in the cluster and their parameters, switch to the **Radio Resource Management** tab. The **Current Channel Assignments** table consists of 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 operate;
- *Status* – operation state of the access point radio interface in the cluster.

To update information on the page, click **Refresh.**



Automatically manage radio resource assignments

**Channel Planner ...**

Stop automatically re-assigning channels

**Current Channel Assignments**

| IP Address | Radio | Band | Channel | Status | Locked |
|---|---|---|---|---|---|
| 192.168.100.3 | E8:28:C1:C1:27:70 | B/G/N | 1 | up | □ |
| 192.168.100.3 | E8:28:C1:C1:27:60 | A/N/AC | 36 | up | □ |

Refresh Apply

Proposed Channel Assignments ( 3 seconds ago )

| IP Address | Radio | Proposed Channel |
|---|---|---|
| 192.168.100.3 | E8:28:C1:C1:27:70 | 11 |
| 192.168.100.3 | E8:28:C1:C1:27:60 | 40 |

Advanced

Change channels if interference is reduced by at least 75%

Refresh when access point is added to the cluster enable

Determine if there is better set of channel settings every 1 Day

Click "Update" to save the new settings.

Update

Clustered

1 Access Points

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

- *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;
- *Proposed Channel* – channel number to which the radio interface will switch when optimal channel selection is launched.

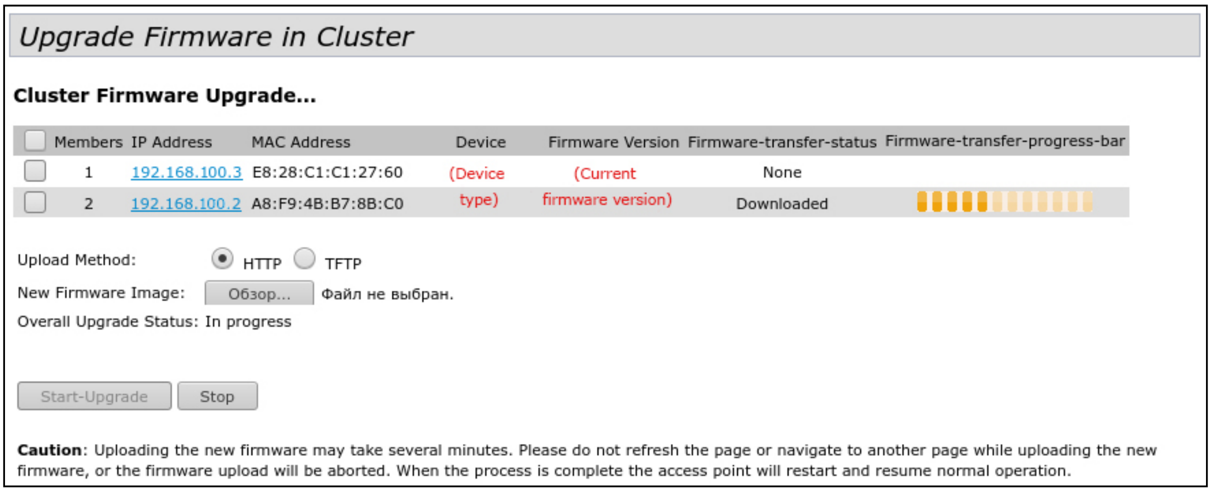
## 10.2 Firmware upgrade

The operation in the cluster mode allows performing automatic firmware update for all the access points in the cluster without using external systems or controllers.
Firmware update might be performed:

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

### 10.2.1 Firmware upgrade via web interface

To upgrade firmware on devices in a cluster through web interface, open the **Cluster Firmware Upgrade** tab of an access point.
When upgrading 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).
Download the file with the current firmware version on PC.



Upgrade Firmware in Cluster

**Cluster Firmware Upgrade...**

| □ | Members | IP Address | MAC Address | Device | Firmware Version | Firmware-transfer-status | Firmware-transfer-progress-bar |
|---|---|---|---|---|---|---|---|
| □ | 1 | 192.168.100.3 | E8:28:C1:C1:27:60 | (Device type) | (Current firmware version) | None | |
| □ | 2 | 192.168.100.2 | A8:F9:4B:B7:8B:C0 | | | Downloaded | |

Upload Method: ● HTTP ○ TFTP

New Firmware Image: Обзор... Файл не выбран.

Overall Upgrade Status: In progress

**Caution**: Uploading the new firmware may take several minutes. Please do not refresh the page or navigate to another page while uploading the new firmware, or the firmware upload will be aborted. When the process is complete the access point will restart and resume normal operation.

The firmware file can be uploaded to the device via HTTP or TFTP protocols:

**Upload via HTTP.** Set **Upload Method** flag to HTTP. Click **Browse**. In the window that opens select a path to the firmware file on the PC. In the leftmost column of the table, set flags for access points for which firmware will be updated. Click **Start-Upgrade** to start upgrading.

**Upload via TFTP.** Set **Upload Method** flag to TFTP. In the **Image Filename** field specify the name of the firmware file that will be uploaded to the device. File name must contain .tar extension. In the **Server IP** field specify the IP address for the TFTP server on which the firmware file will be stored.

Click **Stop** to abort device upgrade process.

In the **Overall Upgrade Status** field, a summary status of the software upgrade process on access points is displayed.

While firmware upgrade, do not switch off the devices and do not update or change the web page with progress bar.

### 10.2.2 Firmware upgrade through DHCP Autoprovisioning

To update firmware, a TFTP server and a DHCP server with particular configuration are required. The upgrade 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 upgraded.

**Firmware upgrade algorithm via DHCP Autoprovisioning:**

1. Place the "wop2.manifest" file on TFTP server, the file should contain the following string:

```
VERSION= "1.22.X.X" WOP-2ac-1.22.X.X.tar.gz,
```

where WOP-2ac-1.22.X.X.tar.gz is a name of the archive containing firmware for WOP-2ac;
1.22.X.X is a firmware version included to the archive. The firmware version can be viewed in "version" file in firmware archive.

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

3. Add the following strings to the DHCP server configuration file (dhcpd.conf):

```
option tftp-server-name "192.168.100.253";
option bootfile-name "wop2.manifest";
```

where 192.168.100.253 is an address of the TFTP server;
wop2.manifest is a manifest file name.

# 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/