Беспроводная точка доступа

WOP-2ac

Управление устройством через web-конфигуратор

Версия ПО 1.20.0

IP-адрес: 192.168.1.10

Username: admin

Password: password

Содержание

1 Введение 5

1.1 Аннотация 5

1.2 Целевая аудитория 5

1.3 Условные обозначения 5

2 Описание web-интерфейса 6

2.1 Начало работы 6

2.2 Смена пароля 6

2.3 Элементы web-конфигуратора 7

3 Меню «Basic Settings» 9

4 Меню «Status» 11

4.1 Подменю «Interfaces» 11

4.2 Подменю «Events» 13

4.3 Подменю «Transmit/Receive» 15

4.4 Подменю «Passpoint» 18

4.5 Подменю «Wireless Multicast Forwarding Statistic» 25

4.6 Подменю «Client Associations» 27

4.7 Подменю «TSPEC Client Associations» 29

4.8 Подменю «Rogue AP Detection» 29

4.9 Подменю «TSPEC Status and Statistics» 32

4.10 Подменю «TSPEC AP Statistics» 33

4.11 Подменю «Radio Statistics» 34

4.12 Подменю «Email Alert Status» 35

5 Меню «Manage» 36

5.1 Подменю «Ethernet Settings» 36

5.2 Подменю «Management IPv6» 37

5.3 Подменю «IPv6 Tunnel» 38

5.4 Подменю «Wireless Settings» 38

5.5 Подменю «Radio» 40

5.6 Подменю «Scheduler» 45

5.7 Подменю «Scheduler Association» 47

5.8 Подменю «VAP» 48

5.9 Подменю «VAP Minimal Signal» 50

5.10 Подменю «Fast Bss Transition» 51

5.11 Подменю «Wireless Multicast Forwarding» 53

5.12 Подменю «WDS» 54
5.13 Подменю «MAC Authentication» 56
5.14 Подменю «Load Balancing» 57
5.15 Подменю «Authentication» 58
5.16 Подменю «Management ACL» 58
5.17 Подменю «OTT Settings» 59
5.18 Подменю «Mesh»* 62
5.19 Подменю «Mesh Monitoring»* 63
6 Меню «Services» 66
6.1 Подменю «Bonjour» 66
6.2 Подменю «Web Server» 67
6.3 Подменю «SSH» 69
6.4 Подменю «Telnet» 69
6.5 Подменю «QoS» 69
6.6 Подменю «Email Alert» 72
6.7 Подменю «LLDP» 73
6.8 Подменю «SNMP» 74
6.9 Подменю «Time Settings (NTP)» 75
7 Меню «SNMPv3» 77
7.1 Подменю «SNMPv3 Views» 77
7.2 Подменю «SNMPv3 Groups» 77
7.3 Подменю «SNMPv3 Users» 79
7.4 Подменю «SNMPv3 Targets» 80
8 Меню «Maintenance» 81
8.1 Подменю «Configuration» 81
8.2 Подменю «Upgrade» 82
8.3 Подменю «Packet Capture» 83
8.4 Подменю «Support Information» 85
9 Меню «Cluster» 86
9.1 Подменю «Access Points» 87
9.2 Подменю «Sessions» 89
9.3 Подменю «Radio Resource Management» 89
9.4 Подменю «Wireless Neighborhood» 92
9.5 Подменю «Cluster Firmware Upgrade» 92
10 Меню «Captive Portal» 94

10.1 Подменю «Global Configuration» 94
10.2 Подменю «Instance Configuration» 95
10.3 Подменю «VAP Configuration» 98
10.4 Подменю «Authenticated Clients» 98
10.5 Подменю «Failed Authentication Clients» 99
11 Меню «Client QoS» 100
11.1 Подменю «VAP QoS Parameters» 100
11.2 Подменю «Class Map» 101
11.3 Подменю «Policy Map» 102
11.4 Подменю «Client Configuration» 104
12 Меню «Work Group Bridge» 105
12.1 Подменю «Work group bridge» 105
12.2 Подменю «Workgroup Bridge Transmit/Receive» 107
13 Список изменений 108

1 Введение

1.1 Аннотация

В настоящем приложении к руководству по эксплуатации приведена информация о составе web-интерфейса устройства, об основных навыках навигации по страницам интерфейса, правилах конфигурирования, мониторинга и смене программного обеспечения беспроводной точки доступа (в дальнейшем именуемого устройством).

Web-интерфейс позволяет сделать управление устройством более наглядным и комфортным. С помощью Web-интерфейса выполняется конфигурирование, мониторинг, отладка устройства с удаленного рабочего места, используя Web-браузер.

1.2 Целевая аудитория

Web-интерфейс предназначен для технического персонала, выполняющего настройку и мониторинг устройства посредством Web-интерфейса. Квалификация технического персонала предполагает знание основ работы стеков протоколов TCP/IP, UDP/IP, принципов построения проводных и беспроводных сетей.

1.3 Условные обозначения

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред программно-аппаратному комплексу, привести к некорректной работе системы или потере данных.

2 Описание web-интерфейса

2.1 Начало работы

Для начала работы нужно подключиться к устройству через Web-браузер:

1. Откройте Web-браузер (программу-просмотрщик web -страниц), например, Firefox, Opera, Chrome.

2. Введите в адресной строке браузера IP-адрес устройства.

   Заводской IP-адрес устройства: 192.168.1.10, маска подсети: 255.255.255.0
   В дефолтной конфигурации устройство получает адрес по DHCP. До этого оно доступно по заводскому IP-адресу.

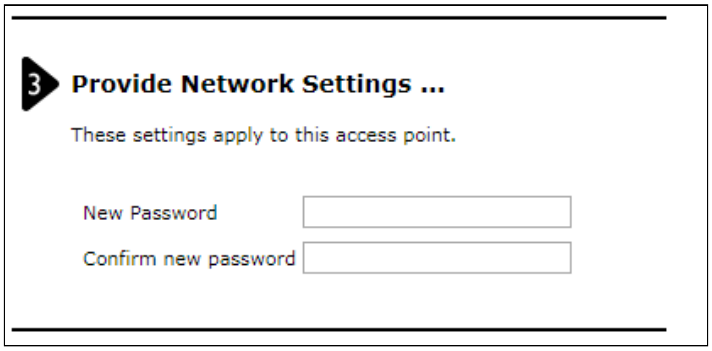
   При успешном подключении в окне браузера отобразится страница с запросом имени пользователя и пароля.

   Заводские установки: User Name – *admin*, Password – *password*.

3. Введите имя пользователя в строке «User Name» и пароль в строке «Password».
4. Нажмите кнопку «Logon». В окне браузера откроется начальная страница web-конфигуратора устройства.

2.2 Смена пароля

Для смены пароля для подключения к web-конфигуратору устройства в разделе *Basic Settings,* пункт «Provide Network Settings», в полях «*New Password*» и «*Confirm new password*» введите новый пароль.



2.3 Элементы web-конфигуратора

На рисунке 1 представлены элементы навигации web-конфигуратора.

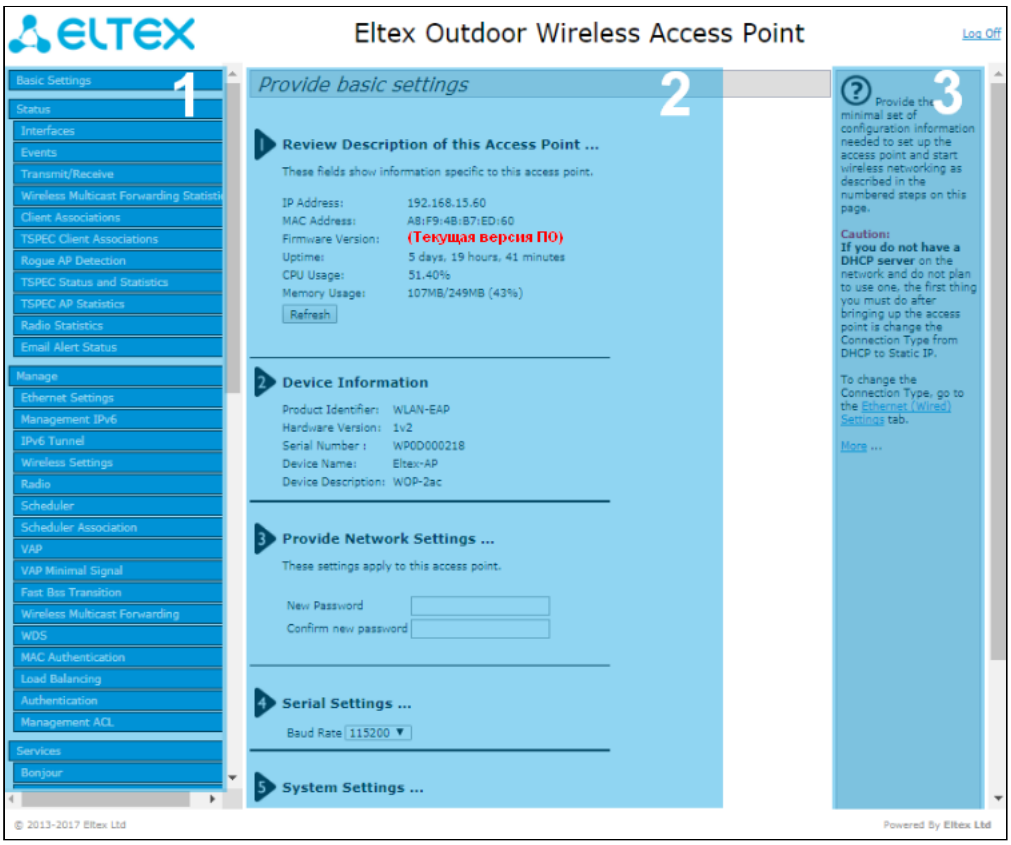
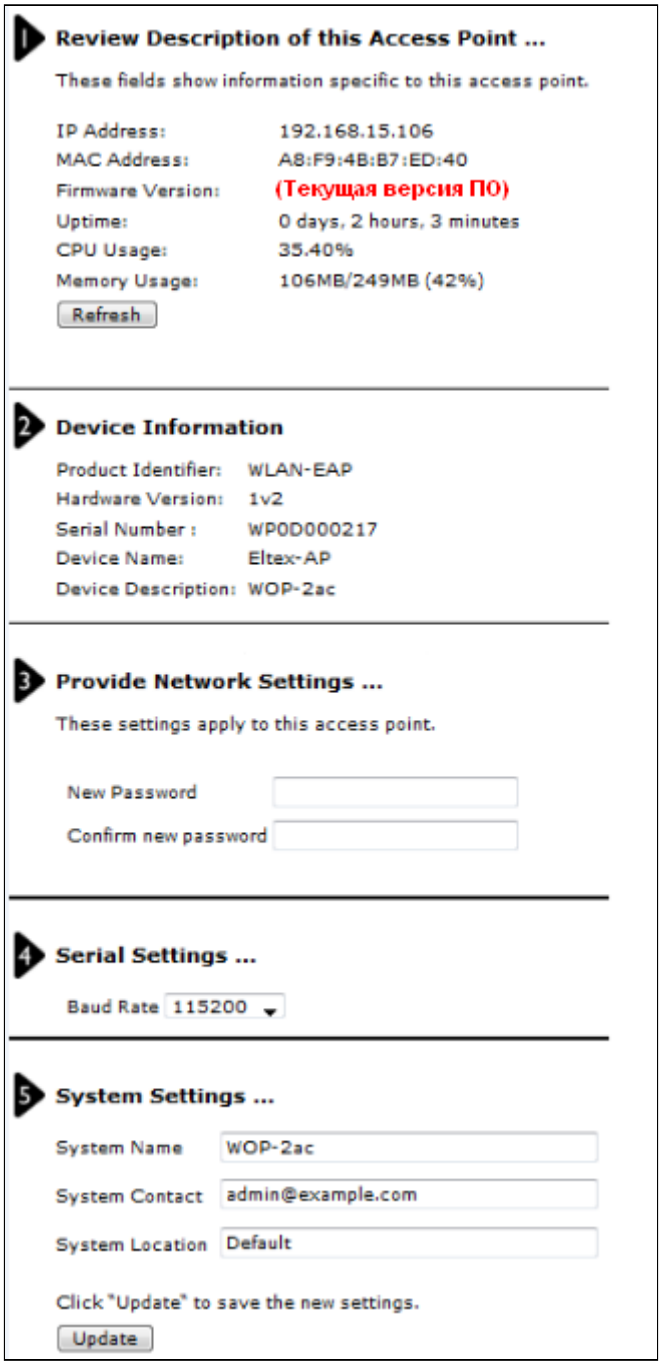


Рисунок 1 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса можно условно разделить на 3 части:

1. Разделы меню настроек устройства.
2. Основное окно настроек выбранного раздела.
3. Справочная информация по выбранному разделу меню.

3 Меню «Basic Settings»



В меню «Basic Settings» отображается основная информация об устройстве, сетевые настройки, версия программного обеспечения, системная информация. Выполняется смена пароля и установка скорости порта Console.

Review Description of this Access Point – в данном разделе приводится информация о сетевых настройках устройства и версии ПО.

- *IP Address* – IP-адрес устройства;
- *MAC Address* – MAC-адрес устройства;
- *Firmware Version* – версия программного обеспечения;
- *Uptime* – время работы;
- CPU Usage – средний % загрузки процессора за последние 10 секунд;
- Memory Usage – % использования физической памяти устройства

Device Information – основная информация об устройстве.

- *Product Identifier* – идентификатор устройства;
- *Hardware Version* – версия аппаратного обеспечения;
- *Serial Number* – серийный номер устройства;
- *Device Name* – системное имя устройства;
- *Device Description* – описание устройства.

Provide Network Settings – в данном разделе выполняется смена пароля для доступа к Web/ CLI-конфигуратору устройства.

- *New Password* – новый пароль;
- *Confirm new password* – подтверждение нового пароля.

Serial Settings – настройки интерфейса Console.

- *Baud Rate* – скорость передачи данных по интерфейсу Console, бит/с, принимает значения: 9600; 19200; 38400; 57600; 115200.

System Settings – в разделе можно выполнить системные настройки устройства.

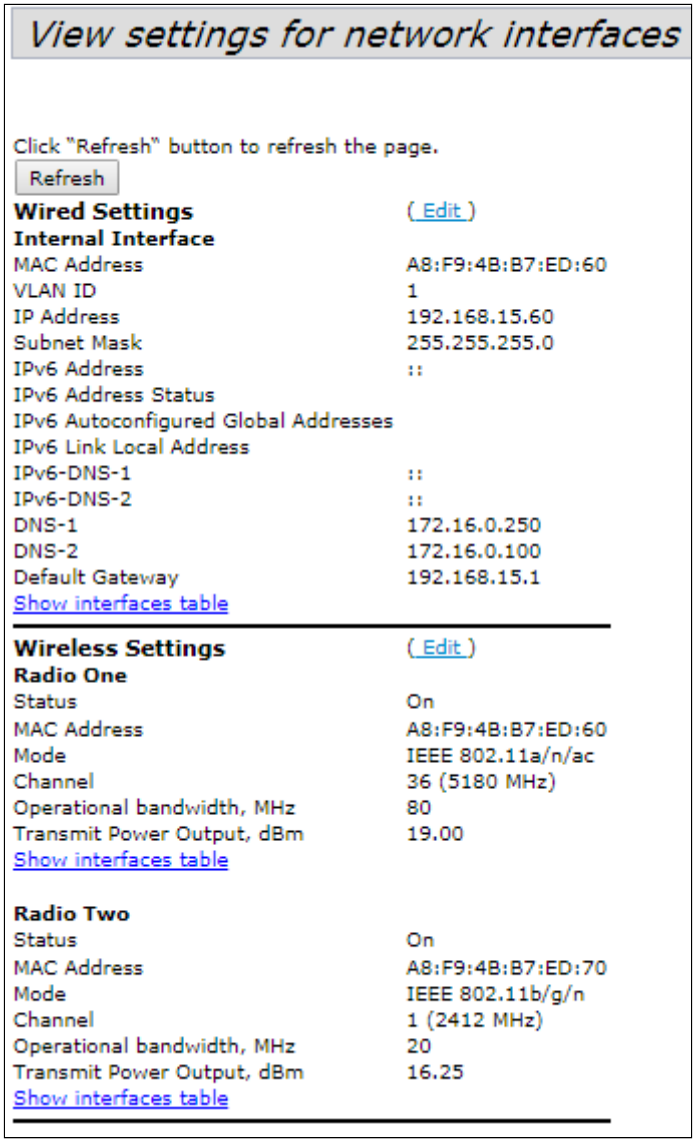
- *System Name* – системное имя устройства;
- *System Contact* – контактная информация для связи с администратором;
- *System Location* – информация по размещению устройства.

Для сохранения настроек и обновления информации нажмите кнопку «Update».

4 Меню «Status»

В меню «Status» приводится информация о состоянии интерфейсов устройства, регистрируемых на устройстве событиях, радиоокружении и радиостатистике устройства.

4.1 Подменю «Interfaces»



В данном разделе можно узнать подробную информацию о текущем состоянии проводных интерфейсов и настройках беспроводной сети. Настройка проводных интерфейсов выполняется в меню «*Manage – Ethernet Settings*». Настройка беспроводного интерфейса выполняется в «*Manage – Wireless Settings*». Для перехода в меню настроек можно нажать ссылку «Edit» в соответствующем разделе.

Wired Settings – приводится информация о текущем состоянии проводных интерфейсов:

- *MAC Address* – MAC-адрес устройства на интерфейсах Ethernet;
- *VLAN ID* – номер VLAN для управления устройством;
- *IP Address* – IP-адрес управления устройством;
- *Subnet Mask* – маска IPv4-сети управления;
- *IPv6 Address* – IPv6-адрес управления устройством;
- *IPv6 Autoconfigured Global Addresses* – список сконфигурированных автоматически IPv6-адресов;
- *IPv6 Link Local Address* – автоматически сконфигурированный локальный IPv6-адрес;
- *IPv6-DNS-1* – адрес первого сервера DNS в IPv6-сети;
- *IPv6-DNS-2* – адрес второго сервера DNS в IPv6-сети;
- *DNS-1* – адрес первого сервера DNS в IPv4-сети;
- *DNS-2* – адрес второго сервера DNS в IPv4-сети;
- *Default Gateway* – шлюз по умолчанию в IPv4-сети.

Show interfaces table – приводится таблица интерфейсов:

- *Interface* – название интерфейса ТД;
- *Status* – статус интерфейса;
- *MAC Address* – MAC-адрес интерфейса;
- *VLAN ID* – идентификатор VLAN, используемый на интерфейсе;
- *Name (SSID)* – имя беспроводной сети.

Wireless Settings – приводится информация о текущем состоянии беспроводных интерфейсов:

- *Radio One Status* – состояние работы первого радиоинтерфейса;
- *Radio Two Status* – состояние работы второго радиоинтерфейса;
- *MAC Address* – MAC-адрес радиоинтерфейса;
- *Mode* – режим работы радиоинтерфейса;
- *Channel* – номер беспроводного канала согласно 802.11, на котором работает радиоинтерфейс;
- *Operational bandwidth* – ширина полосы, занимаемой спектром радиоинтерфейса;
- *Transmit Power Output* – фактическая излучаемая мощность передатчика.

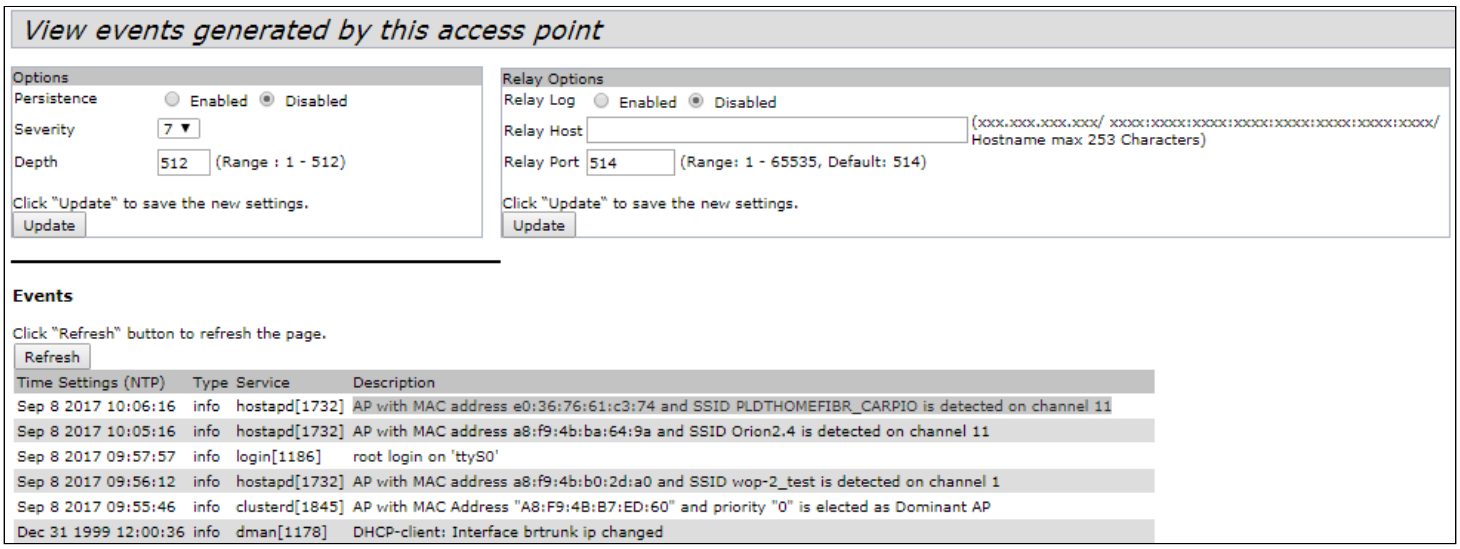
SFP Settings опционально только для WOP-2ac SFP и WOP-2ac GPON - приводится информация о текущем состоянии оптического интерфейса:

- *Link Status* – состояние работы оптического интерфейса;
- *SFP-module Status* – отображает наличие/отсутствие SFP-модуля;
- *Temperature* – текущая температура SFP-модуля;
- *Transceiver Supply Voltage* – напряжение питания SFP-модуля;
- *Laser Bias Current* – ток смещения лазера SFP-модуля;
- *Transmit Power* – мощность излучения;
- *Receive Power* – мощность на входе приемника;
- *Speed* – скорость передачи данных.

Для обновления информации на странице нажмите кнопку «Refresh».

4.2 Подменю «Events»

В разделе «Events» вы можете посмотреть журнал событий, происходящих с устройством, а также перенаправить информацию о событиях на сторонний SYSLOG-сервер.



Options – в разделе выполняется настройка параметров журнала сообщений: уровень важности и количество сообщений, сохраняемых в энергонезависимой памяти устройства.

- *Persistence* – выбор способа сохранения информационных сообщений:
  - *Enabled* – при установке данного флага события журнала будут сохраняться в энергонезависимой памяти;
  - *Disabled* – при установке данного флага события будут сохраняться в энергозависимой памяти. Сообщения в энергозависимой памяти будут удалены при перезагрузке системы.
- *Severity* – уровень важности сообщения, которое нужно сохранить в энергонезависимой памяти, описание приведено в таблице 1.

Таблица 1 – Уровни важности сообщений

Уровень	Тип важности сообщений	Описание
0	Чрезвычайные (emergency)	В системе произошла критическая ошибка, система может работать неправильно.
1	Сигналы тревоги (alert)	Необходимо немедленное вмешательство в систему.
2	Критические (critical)	В системе произошла критическая ошибка.
3	Ошибочные (error)	В системе произошла ошибка.
4	Предупреждения (warning)	Предупреждение, неаварийное сообщение.
5	Уведомления (notice)	Уведомление системы, неаварийное сообщение.
6	Информационные (informational)	Информационные сообщения системы.
7	Отладочные (debug)	Отладочные сообщения предоставляют пользователю информацию для корректной настройки системы.

- *Depth* – максимальное количество сообщений, которое может быть сохранено в энергозависимой памяти, по умолчанию до 512 сообщений, принимает значения 1-512. При превышении данного порога происходит перезапись сообщения, которое хранится в системе дольше всех, новым.

Кнопка «Update» используется для сохранения настроек.

Relay Options – в данном разделе выполняются настройки отправки информационных сообщений устройства на сторонний сервер.

- *Relay Log* – включение/выключение отправки информационных сообщений устройства на сторонний сервер:
    - *Enabled* – при установленном флаге отправка включена;
    - *Disabled* – при установленном флаге отправка отключена.
- *Relay Host* – адрес сервера, на который перенаправляются сообщения;
- *Relay Port* – номер порта (layer 4), на который перенаправляются сообщения, принимает значения 1-65535, по умолчанию – 514.

Кнопка «Update» используется для сохранения настроек.

Events – в данном разделе можно просмотреть список информационных сообщений в реальном времени и следующую информацию:

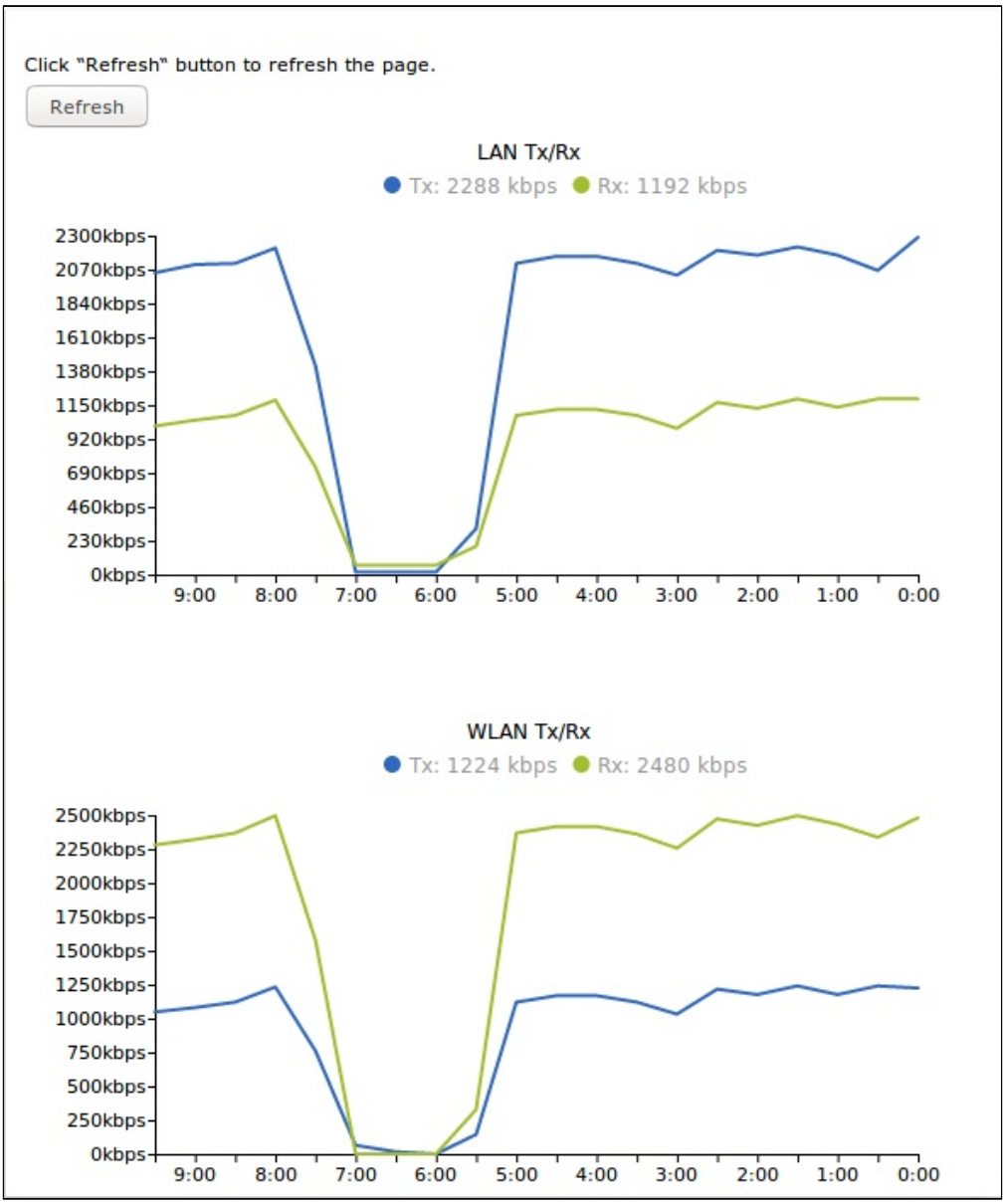
- *Time Setting (NTP)* – время, когда событие было сгенерировано;
- *Type* – уровень важности события, таблица 1;
- *Service* – имя процесса, сгенерировавшего сообщение;
- *Description* – описание сообщения.

Для обновления информации в разделе «Events» нажмите кнопку «Refresh».

Для удаления всех сообщений нажмите кнопку «Clear All».

4.3 Подменю «Transmit/Receive»

В разделе «Transmit/Receive» отображаются графики со скоростью переданного/полученного трафика за последние 10 минут, а так же статистика о количестве переданного/полученного трафика с момента включения точки доступа.



Transmit

Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	344198	55688199	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	821518	84259196	0	0	0
wlan0:vap2	267212	29245013	0	0	0
wlan0:vap3	60086	8876470	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	912965	278556503	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	0	0	0	0	0
wlan1:vap1	196157	24831353	0	0	0
wlan1:vap2	220171	38905459	0	0	0
wlan1:vap3	50371	8291922	0	0	0
wlan1:vap4	0	0	0	0	0

Receive

Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	1582810	412950884	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	0	0	0	0	0
wlan0:vap1	420	106293	0	0	0
wlan0:vap2	12	1092	0	0	0
wlan0:vap3	0	0	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	91066	12027947	0	0	0
wlan0:vap6	0	0	0	0	0
wlan0:vap7	0	0	0	0	0
wlan0:vap8	0	0	0	0	0
wlan0:vap9	0	0	0	0	0
wlan0:vap10	0	0	0	0	0
wlan0:vap11	0	0	0	0	0
wlan0:vap12	0	0	0	0	0
wlan0:vap13	0	0	0	0	0
wlan0:vap14	0	0	0	0	0
wlan0:vap15	0	0	0	0	0
wlan1:vap0	0	0	0	0	0
wlan1:vap1	215	25160	0	0	0
wlan1:vap2	0	0	0	0	0
wlan1:vap3	0	0	0	0	0
wlan1:vap4	0	0	0	0	0

Для обновления информации нажмите кнопку «Refresh».

Описание графиков "Transmit/Receive":

График LAN Tx/Rx показывает скорость переданного/полученного трафика через Ethernet интерфейс точки доступа за последние 10 минут. График автоматически обновляется каждые 30 секунд.

График WLAN Tx/Rx показывает скорость переданного/полученного трафика через Radio интерфейсы точки доступа за последние 10 минут. График автоматически обновляется каждые 30 секунд.

- *Interface* – имя интерфейса;
- *Status* – состояние интерфейса:
    - *Up* – интерфейс включен;
    - *Down* – интерфейс выключен.
- *MAC Address* – MAC-адрес интерфейса;
- *VLAN ID* – идентификационный номер VLAN;
- *Name (SSID)* – имя беспроводной сети

Описание таблицы «Transmit»:

- *Interface* – имя интерфейса;
- *Total packets* – количество успешно отправленных пакетов;
- *Total bytes* – количество успешно отправленных байт;
- *Total drop packets* – количество отброшенных при отправке пакетов;
- *Total drop bytes* – количество отброшенных при отправке байт;
- *Errors* – количество ошибок.

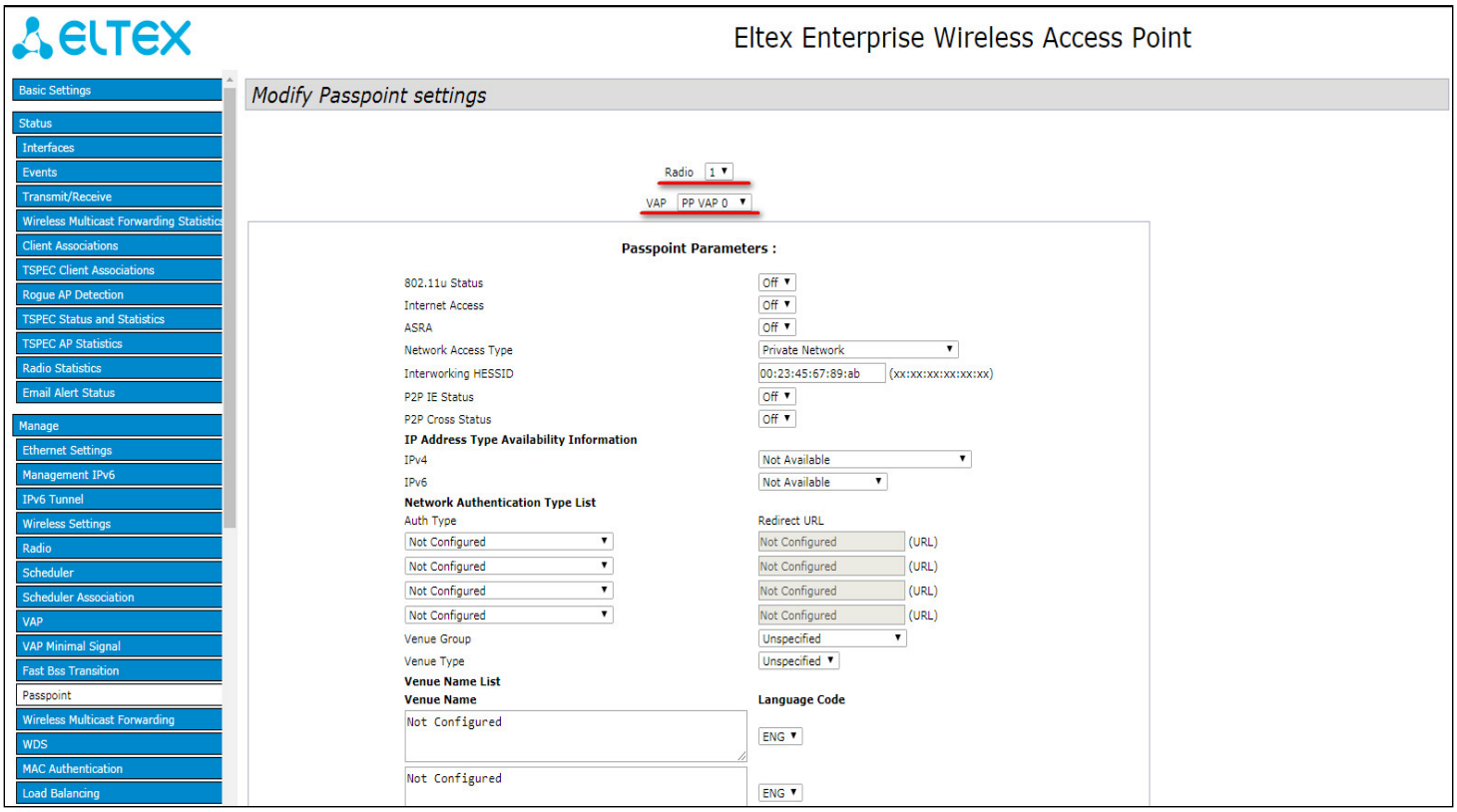
Описание таблицы «Receive»:

- *Interface* – имя интерфейса;
- *Total packets* – количество успешно полученных пакетов;
- *Total bytes* – количество успешно полученных байт;
- *Total drop packets* – количество отброшенных при получении пакетов;
- *Total drop bytes* – количество отброшенных при получении байт;
- *Errors* – количество ошибок.

4.4 Подменю «Passpoint»

Passpoint – это функция, позволяющая пользователям бесшовно переходить с 3G/4G-сетей на Wi-Fi сети. Passpoint поддерживает следующие типы аутентификации: EAP-TLS (идентификация на основе сертификата), EAP-SIM (идентификация на основе данных GSM SIM-карты), EAP-AKA (идентификация на основе данных UMTS USIM) или EAP-TTLS с MS-CHAPv2 (запрос имени пользователя и пароля, сертификат для сервера).

Выберите радиоинтерфейс и виртуальную точку доступа, на которой будет работать Passpoint и заполните поля ниже (по необходимости).



- *Radio* – радиоинтерфейс, на котором необходимо активировать функцию Passpoint;
- *VAP* – виртуальная точка доступа (SSID), на которой необходимо активировать функцию Passpoint.

Межсетевые параметры 802.11u (Passpoint parameters)

Passpoint Parameters :

802.11u Status: Off
Internet Access: Off
ASRA: Off
Network Access Type: Private Network
Interworking HESSID: 00:23:45:67:89:ab (xx:xx:xx:xx:xx:xx)
P2P IE Status: Off
P2P Cross Status: Off

IP Address Type Availability Information

IPv4: Not Available
IPv6: Not Available

Network Authentication Type List

Auth Type	Redirect URL
Not Configured	Not Configured (URL)
Not Configured	Not Configured (URL)
Not Configured	Not Configured (URL)
Not Configured	Not Configured (URL)

Venue Group: Unspecified
Venue Type: Unspecified

Venue Name List

Venue Name	Language Code
Not Configured	ENG
Not Configured	ENG

Roaming Consortium List

OUI Name	Is Beacon
Not Configured	No
Not Configured	No

3GPP Cellular Network Information List

Country Code	Network Code
Not Configured	Not Configured
Not Configured	Not Configured
Not Configured	Not Configured
Not Configured	Not Configured
Not Configured	Not Configured
Not Configured	Not Configured

Domain List

1 Not Configured
2 Not Configured
3 Not Configured
4 Not Configured

- *802.11u status* – включить/выключить функцию Passpoint;
- *Internet Access* – включить/выключить доступ к Интернету;
- *ASRA* – (Additional Step Required for Access) – добавить/убрать дополнительный шаг авторизации при получении доступа;
- *Network Access Type* – тип взаимодействия с сетью доступа:
  - *Private Network* – частная сеть;
  - *Private Network with Guest Access* – частная сеть с гостевым доступом;
  - *Chargable public network* – тарифицируемая публичная сеть;
  - *Free public network* – бесплатная публичная сеть;
  - *Emergency Services only Network* – сеть для аварийных служб и служб скорой помощи;

    - *Personal Device Network* – личная сеть устройства;
    - *Test or Experimental* – тестовая сеть;
    - *Wildcard* – взаимодействие через ваучеры (wildcard-сертификат);
- *Interworking HESSID* – MAC-адрес, единый для всех точек доступа одной сети.

Информация о типе доступа (IP Address Type Availability Information)

- IPv4 – настройка доступа используя протокол IPv4;
- IPv6 – настройка доступа используя протокол IPv6.

Типы аутентификации в сети (Network Authentication Type List)

- *Auth Type* – выберите в поле тип аутентификации:
    - *Not Configured* – тип аутентификации не установлен;
    - *Acceptance of term and Conditions* – аутентификация с принятием пользовательского соглашения;
    - *Online Enrollment* – регистрация онлайн;
    - *HTTP/HTTPS Redirection* – переадресация по HTTP/HTTPS;
    - *DNS Redirection* – переадресация по DNS.
- *Redirect URL* – поле для ввода URL-адреса, на который будет выполнена переадресация.

Информация о месте установки (Venue Details)

- *Venue Group* – категория места установки, определенная стандартом IEEE 802.11u:
    - *Unspecified* – не выбрано;
    - *Assembly* – места большого скопления людей (стадионы, театры, рестораны, вокзалы, аэропорты и т.п.).
    - *Business* – банки, офисы, научные центры и т.п.
    - *Educational* – учебные центры;
    - *Factory and Industrial* – промышленные здания;
    - *Institutional* – государственные учреждения;
    - *Mercantile* – коммерческие (торговые) организации;
    - *Residential* – жилые комплексы;
    - *Storage* – хранилища/склады;
    - *Utility and Miscellaneous* – коммунальные службы и т.п.;
    - *Vehicular* – транспорт;
    - *Outdoor* – размещение на улице (городские парки, зоны отдыха, остановки, киоски)
    - *Reserved* – частные территории.
- *Venue Type* – тип местоположения. Доступные варианты зависят от выбранной выше категории расположения.

Список местоположений точек доступа (Venue Name List)

- *Venue Name* – наименования места установки точки доступа;
- *Language Code* – язык.

Список организаций (Roaming Consortium List)

- *OUI Name* – уникальный идентификатор организации (OUI);
- *Is Beacon* – добавить OUI в beacon (yes), не добавлять OUI в beacon (No).

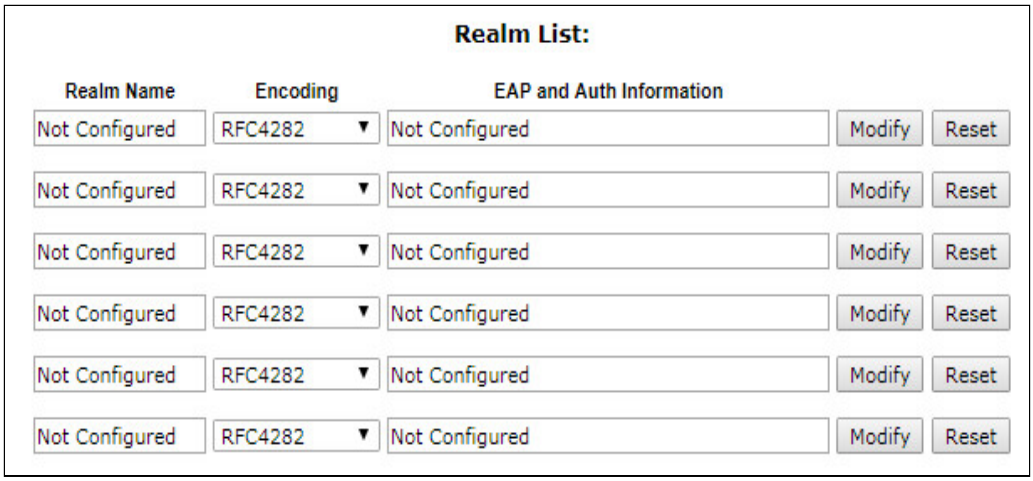
Информация о 3GPP сетях сотовой связи (3GPP Cellular Network Information List)

- *Country Code* – код страны;
- *Network Code* – код сети.

Список доменов (Domain List)

Впишите домены в свободные поля.

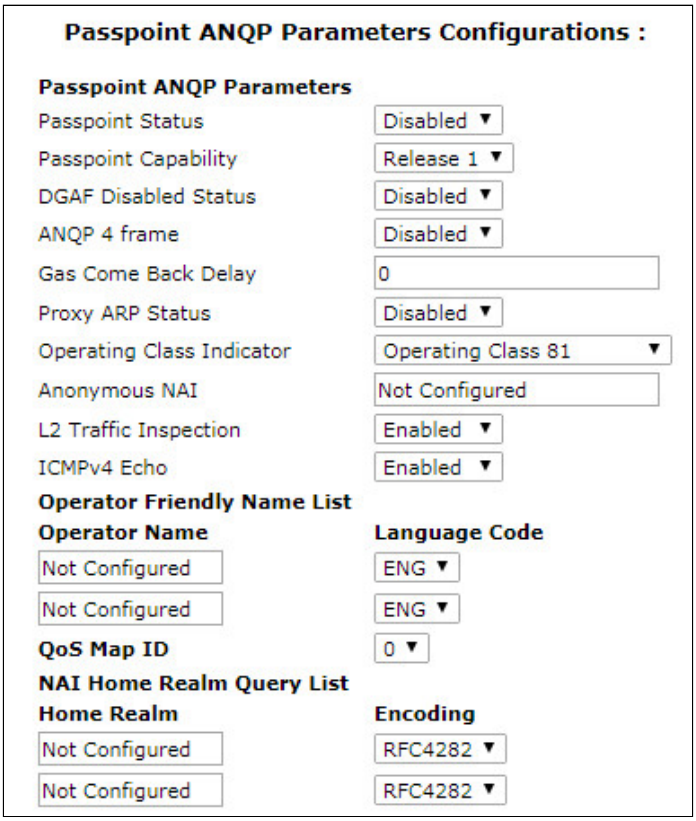
Список областей (Realm list)



- *Realm Name* – название области;
- *Encoding* – кодировка (RFC4282, UTF8);
- *EAP and Auth Information* – информация о протоколе и аутентификации.

- *Modify* – настроить тип и параметры аутентификации;
- *Reset* – сбросить настройки.

Настройка параметров работы ANQP протокола (Passpoint ANQP Parameters Configurations)



- *Passpoint Status* – включить (enable) / отключить (disable) функцию Passpoint;
- *Passpoint Capability* – определить поддерживает ли устройство функцию Passpoint;
- *DGAF Disabled Status* – включить (enable) / выключить (disable) переадресацию нисходящих групповых адресных кадров(для мультикаста). Когда ТД передает кадры, содержащие элемент индикации HS2.0, в котором значение DGAF Disable установлено равным disable, мобильное устройство должно отбросить все принятые юникаст IP-пакеты, которые были расшифрованы с помощью ключа группы;
- *ANQP 4 frame* – включить (enable) / выключить (disable) обмен 4 GAS-фреймами;
- *Gas Come Back Delay* – задержка возврата GAS (GAS Comeback Delay) в TU зависит от настройки ANQP 4 frame;
- *Proxy ARP Status* – активировать (enable) / деактивировать (disable) ARP-прокси (Proxy ARP);
- *Operating Class Indicator:*
    - *Operating Class 81* – работа в диапазоне 2.4 ГГц;
    - *Operating Class 115* – работа в диапазоне 5 ГГц;
    - *Operating Class 81&115* – одновременная работа в диапазонах 2.4 и 5 ГГц.
- *Anonymous NAI* – установить анонимный ID доступа к сети (NAI – Network Access Identifier);
- *L2 Traffic Inspection* – включить (enable) / выключить (disable) контроль и фильтрацию L2-трафика (доступно для точек доступа, которые имеют встроенную функцию контроля и фильтрации трафика);
- *ICMPv4 Echo* – функция фильтрации для ICMPv4 Echo запросов.

Операторы, которым доступно подключение Passpoint на данной точке доступа (Operator Friendly Name List)

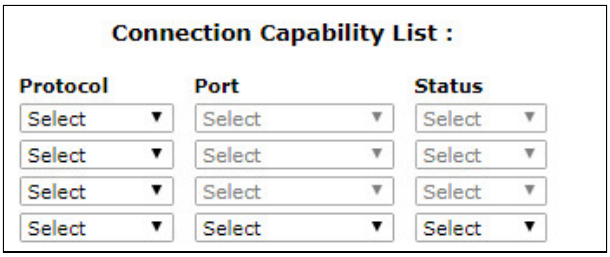
- *Operator Name* – имя оператора;
- *Language Code* – язык;
- *QoS Map ID* – идентификатор QoS Map.

Список домашних областей (NAI Home Realm Query List)

- *Home Realm* – домашняя область;

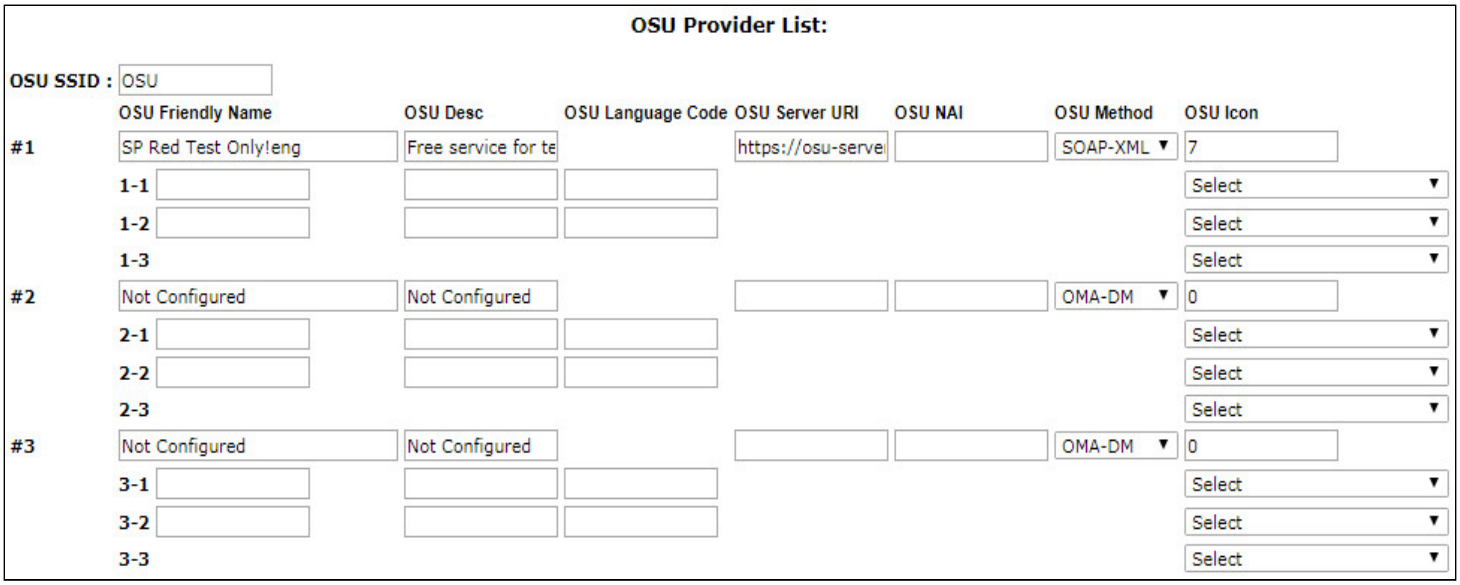
- *Encoding* – кодировка (RFC4282 или UTF8).

Список возможных подключений (Connection Capability List)



- *Protocol* – протокол, по которому возможно подключение:
  - *ICMP (0x1)* – ICMP протокол;
  - *TCP (0x6)* – TCP протокол;
  - *UDP (0x11)* – UDP протокол;
  - *ESP (0x32)* – протокол ESP.
- *Port* – порт, по которому возможно подключение;
- *Status* – статус подключения:
  - *Closed* – подключение по данным параметрам закрыто;
  - *Open* – подключение по данным параметрам доступно;
  - *Unknown* – статус подключения неизвестен.

Список провайдеров, которым доступна онлайн-регистрация (OSU Provider List)



- *OSU SSID* – идентификатор сети для онлайн-регистрации;
- *OSU Friendly Name* – имя интернет провайдера;
- *OSU Desc* – описание сервера онлайн-регистрации;
- *OSU Language Code* – код языка онлайн-регистрации;
- *OSU Server URI* – URL сервера онлайн-регистрации;
- *OSU NAI* – ID доступа к сети для онлайн-регистрации;
- *OSU Method* – метода онлайн-регистрации;
- *OSU Icon* – Логотип провайдера.

Информация о метрике WAN (WAN Metrics Information)

WAN Metrics Information :

Link Status		Symmetric Link		At Capacity		Down Link Speed		Up Link Speed		Down Link Load		Up Link Load		Lmd
▼	:	▼	:	▼	=		>		=		>		=	

- *Link Status* – состояние соединения:
  - *Link Up* – соединение активно;
  - *Link Down* – соединение неактивно;
  - *Link Test* – соединение работает в тестовом режиме.
- *Symmetric Link* – соединение симметрично (Symetric Link) или не симметрично (Not Symmetric Link);
- *At Capacity* – пропускная способность;
- *Down Link speed* – скорость нисходящего потока;
- *Up Link speed* – скорость восходящего потока;
- *Down Link Load* – нагрузка на нисходящий поток;
- *Up Link Load* – нагрузка на восходящий поток;
- *Lmd* – длительность измерения нагрузки (Load Measurement Duration).

4.5 Подменю «Wireless Multicast Forwarding Statistic»

В разделе «Wireless Multicast Forwarding Statistic» отображается статистика по работе Wireless Multicast Forwarding.

View WMF transmit and receive statistics for this access point

Click "Refresh" button to refresh the page.

Refresh

Transmit/Receive Statistics

Interface	Mcast-Data-Frames	Mcast-Data-Fwd	Mcast-Data-Flooded	Mcast-Data-Sentup	Mcast-Data-Dropped
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	149602	0	0	0	115795
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

IGMP Statistics

Interface	Igmp-Frames	Igmp-Frames-Fwd	Igmp-Frames-Sentup	Mfdb-Cache-Hits	Mfdb-Cache-Misses
wlan0:vap0					
wlan0:vap1					
wlan0:vap2					
wlan0:vap3					
wlan0:vap4					
wlan0:vap5					
wlan0:vap6					
wlan0:vap7					
wlan0:vap8					
wlan0:vap9					
wlan0:vap10					
wlan0:vap11					
wlan0:vap12					
wlan0:vap13					
wlan0:vap14					
wlan0:vap15					
wlan1:vap0					
wlan1:vap1	9	9	0	0	143697
wlan1:vap2					
wlan1:vap3					
wlan1:vap4					
wlan1:vap5					
wlan1:vap6					
wlan1:vap7					
wlan1:vap8					
wlan1:vap9					
wlan1:vap10					
wlan1:vap11					
wlan1:vap12					
wlan1:vap13					
wlan1:vap14					
wlan1:vap15					

Multicast-Group

Interface	Multicast-Group	Stations	Packets

Описание таблицы «Transmit/Receive Statistics»:

- *Interface* – имя интерфейса.
- *Mcast-Data-Frames* – количество multicast-кадров, полученных точкой доступа;
- *Mcast-Data-Fwd* – количество multicast-кадров, принятых клиентами;
- *Mcast-Data-Flooded* – количество multicast-кадров, отправленных на все порты;
- *Mcast-Data-Sentup* – количество отправленных multicast-кадров;
- *Mcast-Data-Dropped* – количество отброшенных multicast-кадров.

Описание таблицы «IGMP Statictics»:

- *Interface* – имя интерфейса;
- *Igmp-Frames* – количество IGMP-кадров, полученных точкой доступа;
- *Igmp-Frames-Fwd* – количество IGMP-кадров, принятых клиентами;
- *Igmp-Frames-Sentup* – количество IGMP-кадров, отправленных на все порты;
- *Mfdb-Cache-Hits* – количество пакетов, отправленных на известный multicast-адрес;
- *Mfdb-Cache-Misses* – количество пакетов, отправленных на неизвестный multicast-адрес.

Описание таблицы «Multicast-Group»:

- *Interface* – имя интерфейса;
- *Multicast-Group* – IP-адрес multicast-группы;
- *Stations* – MAC-адрес клиента multicast-группы;
- *Packets* – количество принятых пакетов клиентов multicast-группы.

4.6 Подменю «Client Associations»

В разделе «Client Associations» отображается информация о подключенных клиентах к точке доступа и статистика переданного/полученного трафика по каждому клиенту.

View list of currently associated client stations

Click "Refresh" button to refresh the page.

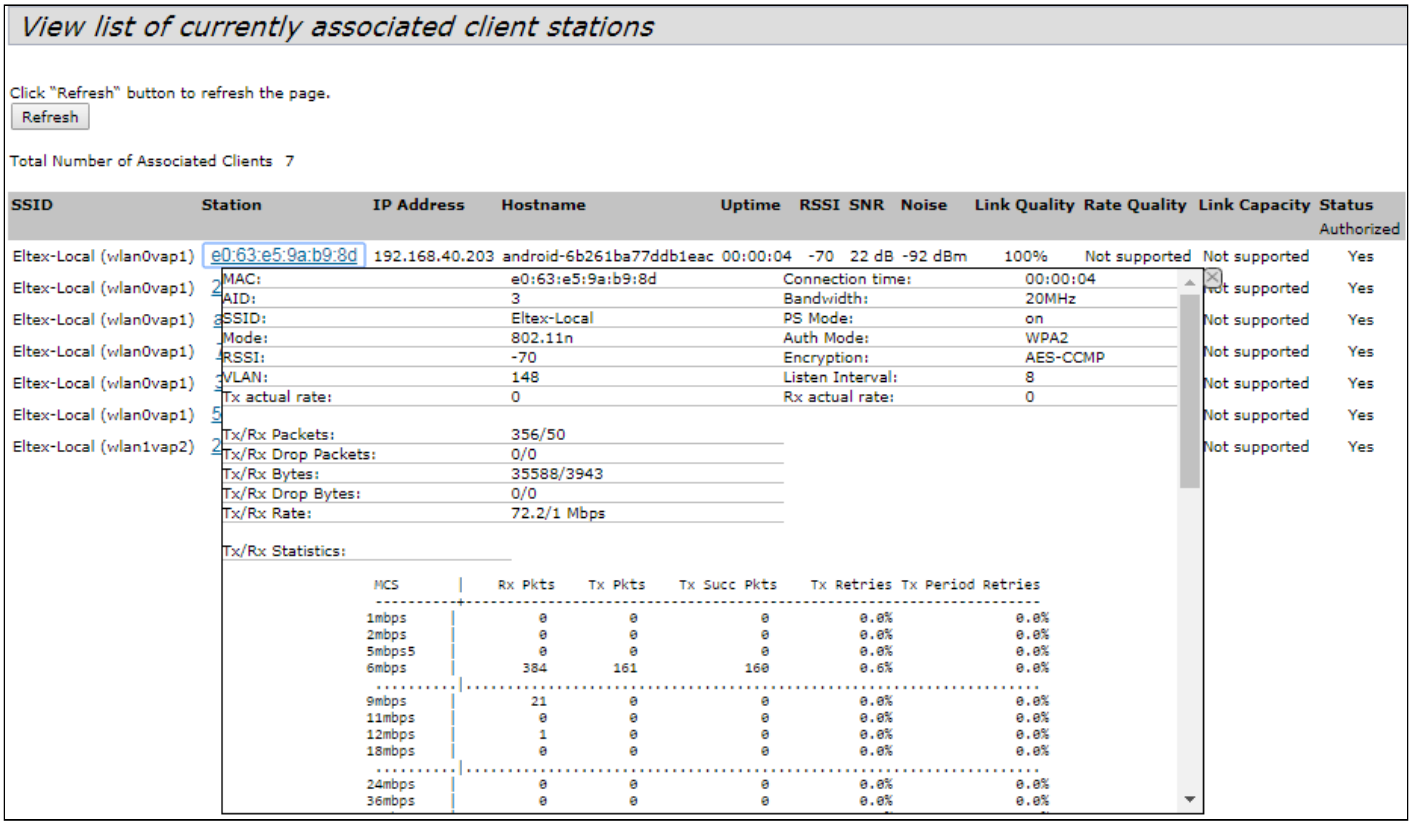
Refresh

Total Number of Associated Clients 7

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capacity	Status Authorized
Eltex-Local (wlan0vap1)	e0:63:e5:9a:b9:8d	192.168.40.203	android-6b261ba77ddb1eac	00:00:04	-70	22 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	20:a2:e4:e9:b1:c8	192.168.40.221	iPhone	00:00:25	-72	20 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	a4:e9:75:1f:84:ba	192.168.40.80		00:00:46	-64	28 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	78:02:f8:f4:73:7e	192.168.40.153	RedmiNote4-Redmi	00:02:29	-52	40 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	34:ab:37:1c:0a:fc	192.168.40.67	Blackka-iPad	00:04:43	-43	49 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan0vap1)	54:a0:50:9c:73:de	192.168.40.82	android-f83b3403e7582a0c	00:06:37	-56	36 dB	-92 dBm	100%	Not supported	Not supported	Yes
Eltex-Local (wlan1vap2)	20:e4:17:03:02:c3			00:00:10	-50	42 dB	-92 dBm	100%	Not supported	Not supported	Yes

- *SSID* – имя беспроводного интерфейса и имя виртуальной точки доступа на интерфейсе, к которой подключен клиент. Например, запись wlan0vap2 означает, что клиент связан с Radio 1 виртуальной точкой доступа VAP2; запись wlan1 означает, что клиент связан с VAP0 на Radio2;
- *Station* – MAC-адрес клиента;
- *IP Address* – IP-адрес клиента;
- *Hostname* – сетевое имя устройства, задается строка 1-63 символов: латинские заглавные и сточные буквы, цифры, знак дефис «-» (дефис не может быть последним символом в имени);
- *Uptime* – продолжительность сессии клиента;
- *RSSI* – уровень сигнала от клиента;
- *SNR* – уровень отношения сигнал/шум от клиента;
- *Noise* – уровень шума;
- *Link Quality* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества ретрансмитов пакетов, отправленных клиенту. Максимальное значение – 100% (все переданные пакеты отправились с первой попытки), минимальное значение- 0% (ни один пакет до клиента не был успешно отправлен);
- *Rate Quality* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества ретрансмитов пакетов, отправленных клиенту, для модуляции, которая используется в данный момент. Максимальное значение – 100% (все переданные пакеты на данной модуляции отправились с первой попытки), минимальное значение- 0% (ни один пакет на данной модуляции до клиента не был успешно отправлен);
- *Link Capacity* – параметр, который отображает эффективность использования точкой доступа модуляции на передачу. Рассчитывается исходя из количества пакетов, переданных на каждой модуляции до клиента,и понижающих коэффициентов. Максимальное значение- 100% (означает, что все пакеты передаются до клиента на максимальной модуляции для максимального типа nss, поддерживаемого клиентом). Минимальное значение- 2% (в случае, когда пакеты передаются на модуляции nss1mcs0 для клиента с поддержкой MIMO 3x3). Для клиентов, подключенных без использования AMPDU, параметр не поддерживается;
- *Status* – статус авторизации.

При нажатии на MAC-адрес клиента раскрывается подробная информация о работе клиента и статистика по передачи пакетов (STA_info).

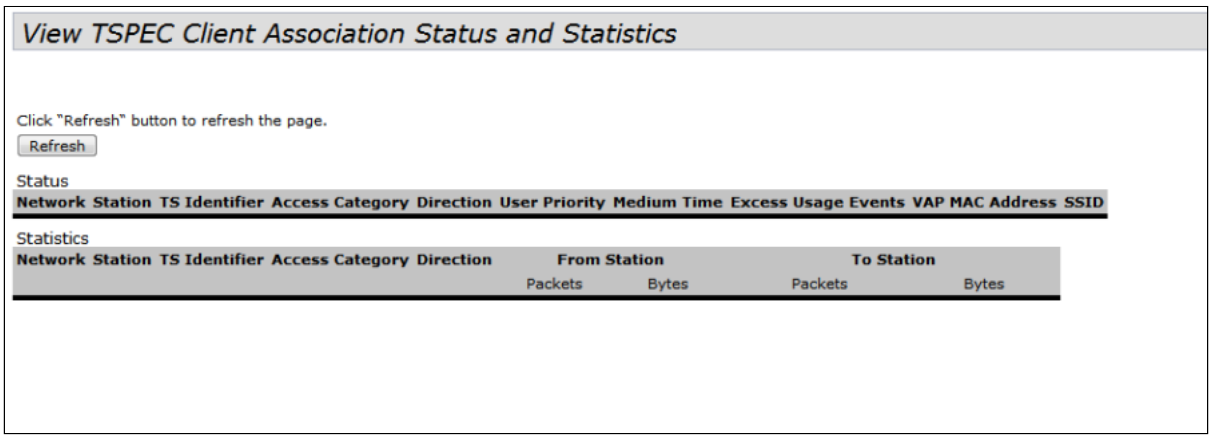


- *MAC* – MAC-адрес клиента;
- *AID* – уникальный идентификатор подключения;
- *SSID* – имя сети к которой подключен клиент;
- *Mode* – стандарт IEEE 802.11 в котором работает клиент;
- *RSSI* – уровень сигнала от клиента;
- *VLAN* – номер VLAN виртуальной точки доступа;
- *Tx actual rate* – текущая скорость передачи данных в сторону клиента, в кбит/с;
- *Tx/Rx Packets* – количество переданных и принятых пакетов от клиента;
- *Tx/Rx Drop Packets* – количество отброшенных пакетов в двух направлениях (на передачу и прием соответственно);
- *Tx/Rx Bytes* – количество переданной и принятой информации от клиента (в байтах);
- *Tx/Rx Drop Packets* – количество отброшенной информации в двух направлениях (на передачу и прием соответственно, в байтах);
- *Tx/Rx Rate* – канальная скорость в двух направлениях, в Мбит/с;
- *Connection time* – продолжительность сессии;
- *Bandwidth* – ширина полосы, в которой работает клиент, Мгц;
- *PS Mode* – режим "сна": 0 – клиент активен, 1 – клиент находится в "спящем" режиме;
- *Auth Mode* – тип безопасности;
- *Encryption* – тип шифрования;
- *Listen Interval* – количество beacon frame-ов спустя которые клиент должен проверить наличие для него трафика траффика (в случае сна);
- *Rx actual rate* – текущая скорость передачи данных в сторону точки доступа, в кбит/с;
- *MCS* – модуляция;
- *Rx Pkts* – количество принятых от клиента пакетов на каждой модуляции;
- *Tx Pkts* – количество переданных клиенту пакетов на каждой модуляции;
- *Tx Succ Pkts* – количество успешно переданных клиенту пакетов;
- *Tx Retries* – % дублированных пакетов в сторону клиента;
- *Tx Period Retries* – % повторно отправленных пакетов за последний период (10 секунд).

Для обновления информации на странице нажмите кнопку «Refresh».

4.7 Подменю «TSPEC Client Associations»

В разделе «TSPEC Client Associations» отображается информация о клиентских данных Tspec переданных и полученных с помощью этой точки доступа.



- *Network* – имя беспроводного интерфейса и имя виртуальной точки доступа на интерфейсе, к которой подключен клиент. Например, запись wlan0vap2 означает, что клиент связан с Radio 1 виртуальной точкой доступа VAP2; запись wlan1 означает, что клиент связан с VAP0 на Radio2;
- *Station* – MAC-адрес клиента;
- *TS Identifier* – TSPEC идентификатор потока трафика (range 0-7);
- *Access Category* – категория доступа (voice или video);
- *Direction* – направление трафика (uplink/downlink);
- *User Priority* – приоритет пользователя;
- *Medium Time* – среднее время, которое поток трафика занимает среду передачи;
- *Excess Usage Events* – количество времени, когда клиент превысил средний срок передачи;
- *Vap* – номер виртуальной точки доступа;
- *Mac Address* – MAC-адрес точки доступа;
- *SSID* – имя беспроводной сети;
- *From Station* – информация о трафике, который передается от беспроводного клиента к точке доступа;
- *To Station* – информация о трафике, который передается от точки доступа к клиенту:
    - *Packets* – количество переданных пакетов;
    - *Bytes* – количество переданных байт;
    - *Drop Packets* – количество отброшенных пакетов;
    - *Drop Bytes* – количество отброшенных байт.

Для обновления информации на странице нажмите кнопку «Refresh».

4.8 Подменю «Rogue AP Detection»

В данном подменю отображается информация обо всех беспроводных точках доступа, которые устройство детектирует вокруг себя.

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

Known AP List

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel	Rate	Signal	Beacons	Last Beacon	Rates

Save Known AP List to a file
Save

Import Known AP List from a file
◉ Replace ○ Merge
Выберите файл Файл не выбран Import

Для обновления информации нажмите кнопку «Refresh».

- *AP Detection for Radio 1/ AP Detection for Radio 2* – включение детектирования сторонних точек доступа в фоне для Radio1 и Radio2.

Кнопка «Update» используется для сохранения настроек.

Detected Rogue AP List – в разделе приводится информация обо всех беспроводных точках доступа, которые устройство детектирует вокруг себя.

Кнопка «Delete Old» используется для удаления записей о неактивных устройствах в радиоокружении.

- *Action* – если точка доступа находится в списке обнаруженных, то нажатие кнопки «Grant» перенесет ее в список доверенных точек доступа. Если точка доступа находится в списке доверенных, то нажатие кнопки «Delete» переведет ее в список обнаруженных точек доступа;
- *MAC* – MAC-адрес точки доступа;
- *Radio* – используемый радиоинтерфейс;
- *Beacon Int.* – интервал посылки Beacon-пакета точкой доступа;
- *Type* – тип обнаруженного устройства:
  - *AP* – точка доступа;
  - *Ad hoc* – децентрализованное клиентское устройство;
- *SSID* – имя беспроводной сети;
- *Privacy* – статус работы режима безопасности точки доступа:
  - *On* – режим безопасности выключен;
  - *Off* – режим безопасности включен;
- *WPA* – состояние шифрования WPA: выключено ☐, включено ☐;
- *Band* – частотный спектр работы точки доступа: 2.4 ГГц или 5 ГГц;
- *Channel [BandWidth]* – используемый частотный канал и ширина полосы;
- *Channel Blocks* – диапазон каналов, которые занимает ТД;
- *Signal* – уровень сигнала, принимаемый от точки доступа. При наведении указателя на графическое изображение сигнала всплывают численные показатели этого сигнала;
- *Beacons* – общее число Beacon-пакетов, принятых от точки доступа с момента ее обнаружения;

- *Last Beacon* – дата и время приема последнего Beacon-пакета от точки доступа;
- *Rates* – список канальных скоростей, поддерживаемых данной точкой доступа.

Known AP List – в таблице приводится список доверенных точек доступа.

Save Known AP List to a file – в данном разделе выполняется сохранение списка «Known AP List» в файл. Для сохранения нажмите кнопку «Save».

Import Known AP List from a file – в данном разделе выполняется загрузка списка «Known AP List» из файла.

- *Replace* – при импорте списка доверенных точек доступа импортируемый список полностью заменит текущий список доверенных точек доступа;
- Merge – при импорте списка доверенных точек доступа доверенные точки доступа из импортируемого списка будут добавлены к точкам доступа, находящимся в импортируемом списке в данный момент времени.

Для загрузки файла нажмите кнопку «Выберите файл», укажите файл, который нужно загрузить и нажмите кнопку «Import».

4.9 Подменю «TSPEC Status and Statistics»

В данном подменю отображается информация о Tspec сессиях на радио интерфейсах.

View TSPEC Status and Statistics

Click "Refresh" button to refresh the page.

Refresh

AP Status

Interface	Access Category	Status	Active TS	TS Clients	Med. Time Admitted	Med. Time Unallocated
wlan0	Best Effort	down	0	0	0	0
wlan0	Background	down	0	0	0	0
wlan0	Voice	down	0	0	0	0
wlan0	Video	down	0	0	0	0
wlan1	Best Effort	down	0	0	0	0
wlan1	Background	down	0	0	0	0
wlan1	Voice	down	0	0	0	0
wlan1	Video	down	0	0	0	0

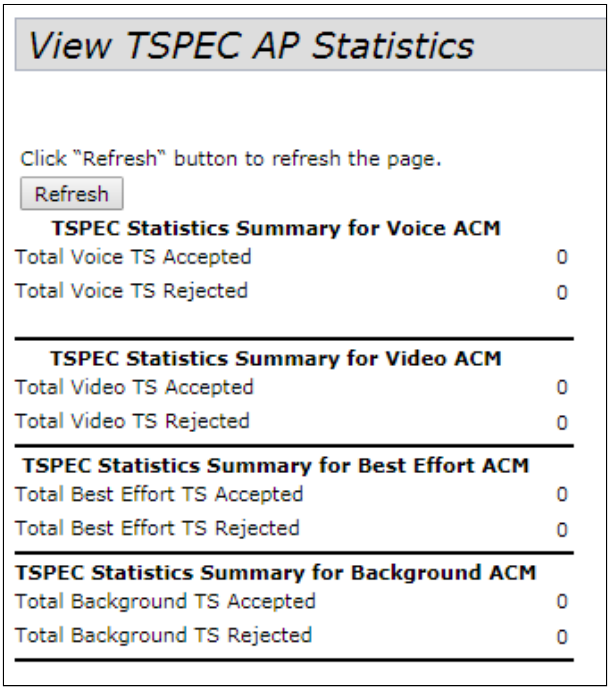
VAP Status

wlan0:vap0	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0
wlan0:vap1	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0
wlan0:vap2	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0
	Video	down	0	0	0	0
wlan0:vap3	Best Effort	down	0	0	0	0
	Background	down	0	0	0	0
	Voice	down	0	0	0	0

- *Interface* – имя интерфейса;
- *Access Category* – категория доступа (voice, video, BE, BK);
- *Status* – состояние сессии;
- *Active TS* – количество текущих активных потоков трафика;
- *TS Clients* – количество клиентов;
- *Medium Time Admitted* – среднее время, которое поток трафика занимает среду передачи;
- *Medium Time Unallocated* – время простоя полосы в данной категории.

4.10 Подменю «TSPEC AP Statistics»

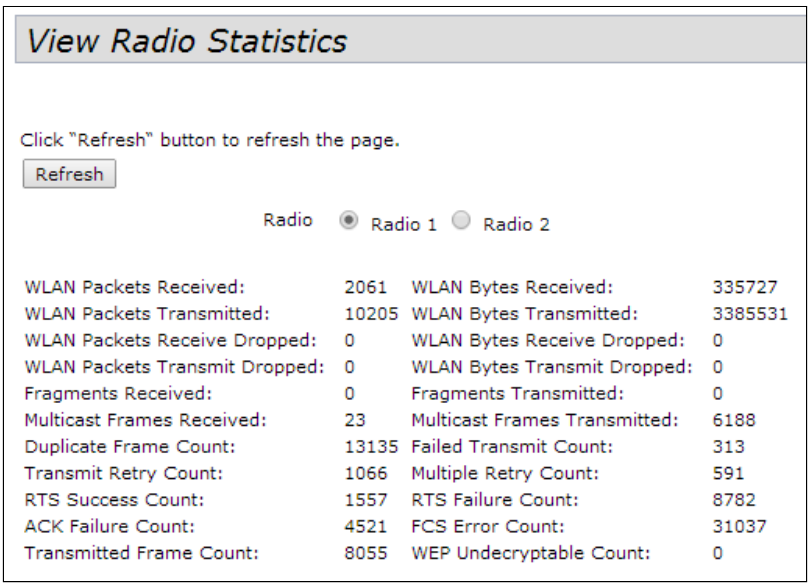
В разделе «TSPEC AP Statistics» отображается статистика по количеству переданного/полученного потоков трафика (Voice, Video, BE, BK).



- *TSPEC Statistics Summary for Voice ACM* – общее количество принятых и отклоненных потоков трафика категории Voise;
- *TSPEC Statistics Summary for Video ACM* – общее количество принятых и отклоненных потоков трафика категории Video;
- *TSPEC Statistics Summary for Best effort ACM* – общее количество принятых и отклоненных потоков трафика категории BE;
- *TSPEC Statistics Summary for Background ACM* – общее количество принятых и отклоненных потоков трафика категории BK.

4.11 Подменю «Radio Statistics»

В разделе «Radio Statistics» отображается подробная статистика по количеству переданного/полученного трафика, пакетов, кадров и другого для каждого радиоинтерфейса.

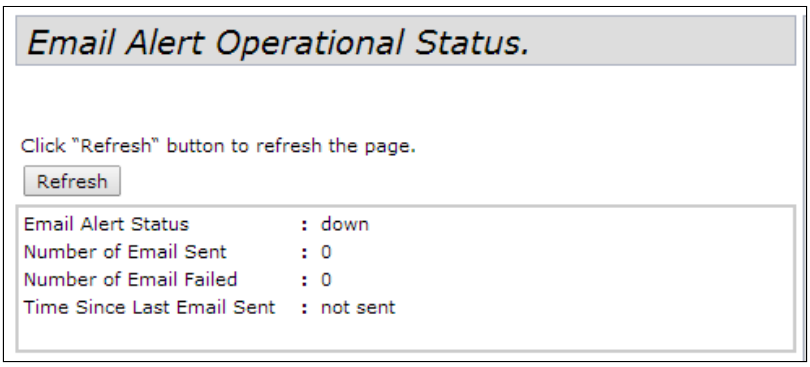


- *WLAN Packets Received* – количество информации (пакетов) полученных через радио интерфейс;
- *WLAN Bytes Received* – количество информации (в байтах) полученных через радио интерфейс;
- *WLAN Packets Transmitted* – количество информации (пакетов) переданных через радио интерфейс;
- *WLAN Bytes Transmitted* – количество информации (в байтах) переданных через радио интерфейс;
- *WLAN Packets Receive Dropped* – количество информации (пакетов) отброшенных при получении через радио интерфейс;
- *WLAN Bytes Receive Dropped* – количество информации (в байтах) отброшенных при получении через радио интерфейс;
- *WLAN Packets Transmit Dropped* – количество информации (пакетов) отброшенных при попытке передачи через радио интерфейс;
- *WLAN Bytes Transmit Dropped* – количество информации (в байтах) отброшенных при попытке передачи через радио интерфейс;
- *Fragments Received* – количество полученных фрагментов пакетов;
- *Fragments Transmitted* – количество переданных фрагментов пакетов;
- *Multicast Frames Received* – количество полученных кадров мультикаст;
- *Multicast Frames Transmitted* – количество переданных кадров мультикаст;
- *Duplicate Frame Count* – количество дублирующих кадров;
- *Failed Transmit Count* – количество не переданных пакетов из-за ошибки;
- *Transmit Retry Count* – количество повторно отправленных пакетов;
- *Multiple Retry Count* – количество пакетов переотправляемых несколько раз;
- *RTS Success Count* – количество пакетов подтверждения о готовности принимать трафик(CTS);
- *RTS Failure Count* – количество пакетов на которые не пришли подтверждения о готовности на прием(CTS);
- *ACK Failure Count* – количество пакетов на которые не пришли подтверждения о успешном приеме(ACK);
- *FCS Error Count* – количество кадров не прошедших проверку контрольной суммы;
- *Transmitted Frame Count* – количество успешно переданных кадров;
- *WEP Undecryptable Count* – количество пакетов, которые не удалось расшифровать (WEP).

Для обновления информации нажмите кнопку «Refresh».

4.12 Подменю «Email Alert Status»

В разделе «Email Alert Status» отображается информация об отправке сообщений о работе устройства на электронную почту.



- *Email Alert Status* – статус работы оповещения по электронной почте о работе устройства:
  - *Up* – оповещение включено;
  - *Down* – оповещение выключено;
- *Number of Email Sent* – количество сообщений, которое было отправлено;
- *Number of Email Failed* – количество потерянных сообщений;
- *Time Since Last Email Sent* – период времени, который прошел с последней передачи сообщения на электронную почту.

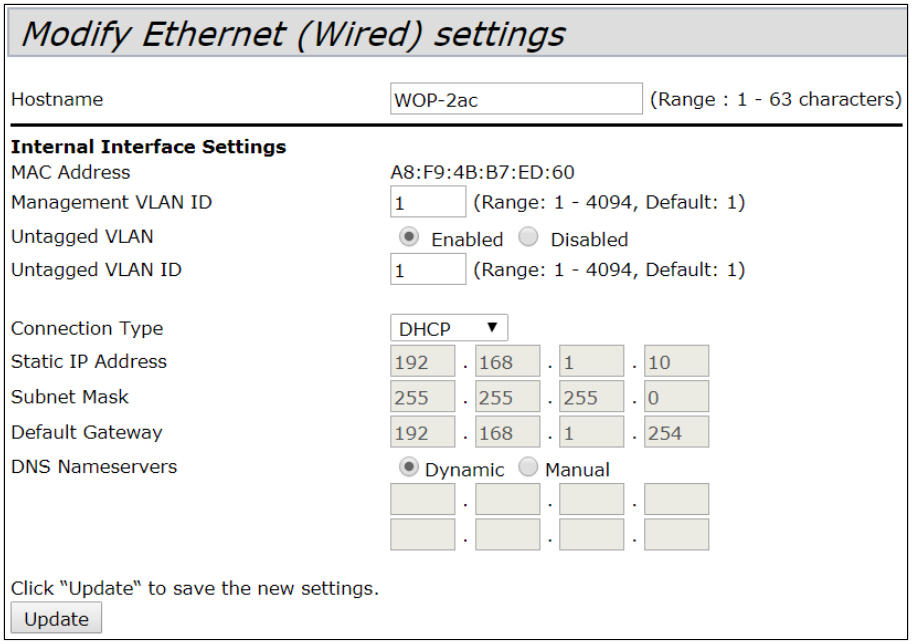
Для обновления информации нажмите кнопку «Refresh».

5 Меню «Manage»

В меню «Manage» выполняются сетевые настройки устройства.

5.1 Подменю «Ethernet Settings»

В текущем разделе выполняются сетевые настройки устройства.



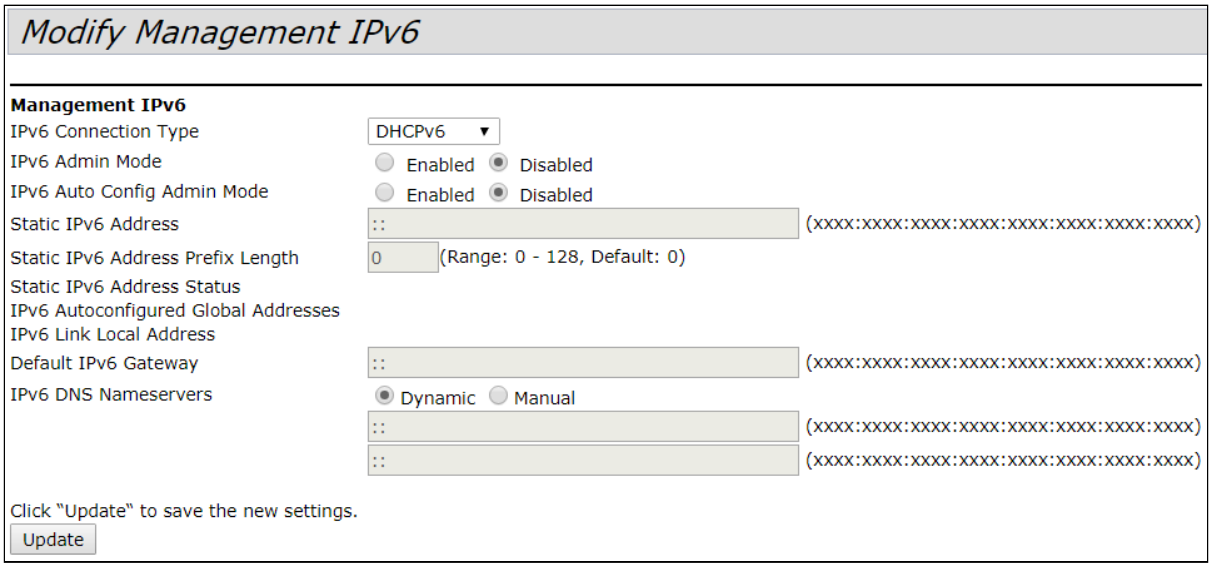
- *Hostname* – сетевое имя устройства, задается строка 1-63 символов: латинские заглавные и сточные буквы, цифры, знак дефис «-» (дефис не может быть последним символом в имени);
- *MAC Address* – MAC-адрес устройства на интерфейсах Ethernet;
- *Management VLAN ID* – идентификатор VLAN, используемый для доступа к устройству, принимает значения 1-4094, по умолчанию – 1;
- *Untagged VLAN* – перевести LAN-порты в access-режим, в котором добавляется VLAN-тег для входящего нетегированного трафика и снимается установленный VLAN-тег с исходящего:
  - *Enabled* – включить access-режим LAN-портов;
  - *Disabled* – выключить access-режим LAN-портов;
- *Untagged VLAN ID* – идентификатор VLAN, который будет назначен нетегированному трафику, поступающему на устройство, и снят с исходящего трафика. Принимает значения 1-4094, по умолчанию – 1;
- *Connection Type* – выбор способа установки IP-адреса на управляющем интерфейсе, по которому будет осуществляться подключение WAN-интерфейса устройства к сети предоставления услуг провайдера:
  - *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от DHCP-сервера автоматически;
  - *Static IP* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *Static IP Address* – IP-адрес устройства в сети провайдера;
    - *Subnet Mask* – маска внешней подсети;
    - *Default Gateway* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
    - *DNS Nameservers* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). При установке флага «Dynamic» будут

использованы DNS-сервера, полученные по DHCP; при установке флага «Manual» необходимо указать DNS-сервера вручную.

Кнопка «Update» используется для сохранения настроек.

5.2 Подменю «Management IPv6»

В разделе «Management IPv6» выполняется настройка конфигурации IPv6-адреса для доступа к управлению устройством.

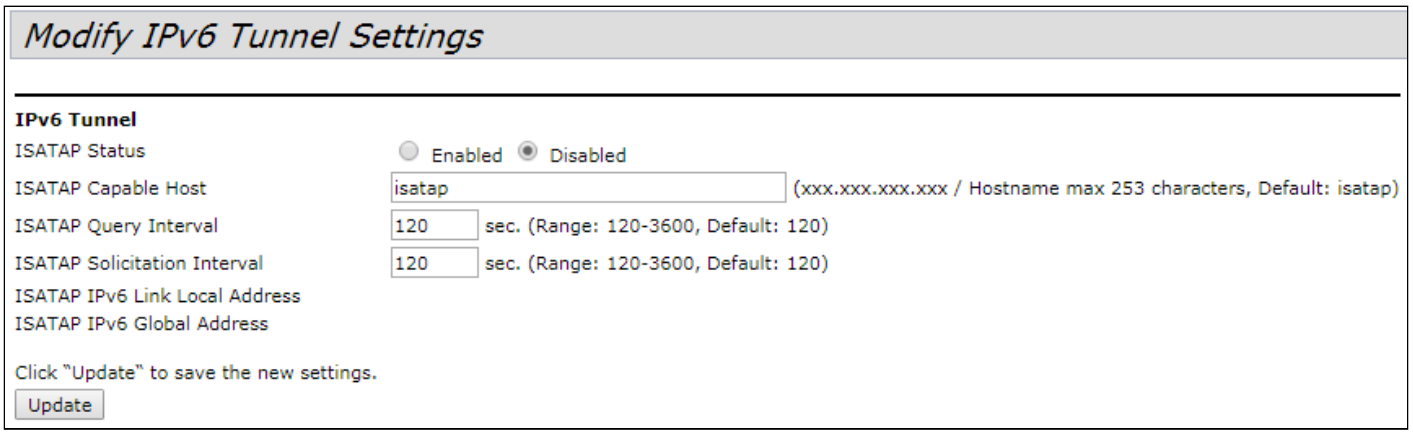


- *IPv6 Cinnection Type* – выбор использования статического IPv6-адреса устройства (*Static IPv6*) или динамического (DHCPv6);
- *IPv6 admin Mode* – доступ к устройству по протоколу IPv6:
  - *Enable* – доступ разрешен;
  - *Disable* – доступ запрещен;
- *IPv6 Auto Config Admin Mode* – режим автоконфигурирования IPv6-адреса:
  - *Enable* – используется;
  - *Disable* – не используется;
- *Static IPv6 Address* – IPv6-адрес устройства при использовании статического IPv6. Точка доступа может иметь установленный статический IPv6-адрес и в случае, если был сконфигурирован адрес(а) через «Auto Config»;
- *Static IPv6 Address Prefix Length* – префикс статического IPv6-адреса, принимает значение 0-128, по умолчанию – 0;
- *Static IPv6 Address Status* – просмотр рабочего статуса статически сконфигурированного IPv6-адреса, принимает значения:
  - *Operational* – текущий действующий;
  - *Tentative* – резервный.
- *IPv6 Autoconfigured global Addresses* – список действующих IPv6-адресов на устройстве;
- *IPv6 Link Local Address* – локальный IPv6-адрес, установленный на LAN-интерфейсе. Данный адрес не конфигурируется и назначается автоматически;
- *Default IPv6 Gateway* – шлюз по умолчанию для IPv6;
- *IPV6 DNS Nameservers* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). При установке флага «*Dynamin*» будут использованы DNS-сервера, полученные по DHCPv6; при установке флага «*Manual*» необходимо указать DNS-сервера вручную.

Кнопка «Update» используется для сохранения настроек.

5.3 Подменю «IPv6 Tunnel»

В разделе «IPv6 Tunnel» выполняется настройка туннелирования IPv6 внутри IPv4. Используется протокол ISATAP (Intra-Site Automatic Tunnel Addressing Protocol – протокол внутрисайтовой адресации туннелей). По протоколу ISATAP выполняется инкапсуляция IPv6-пакетов в IPv4-пакеты для передачи по с IPv4-сети. Поддержка данного функционала позволяет устройству устанавливать связь с удаленными IPv6-хостами.

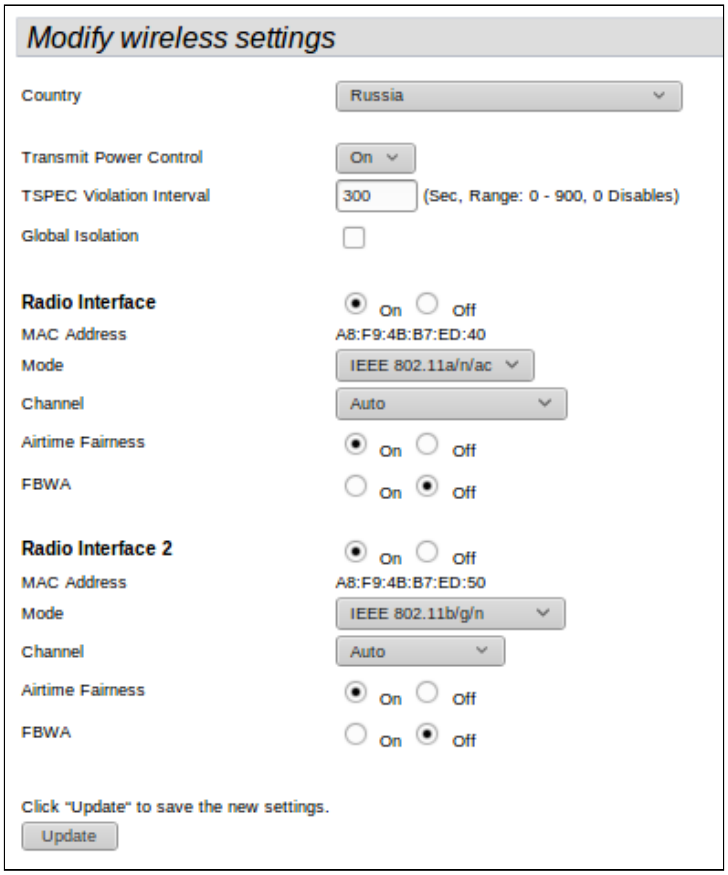


- *ISATAP Status* – режим работы протокола ISATAP:
  - *Enabled* – разрешена работа по протоколу ISATAP;
  - *Disabled* – запрещена работа по протоколу ISATAP.
- *ISATAP Capable Host* – IP-адрес или имя хоста, задается строка до 253 символов, по умолчанию – isatap;
- *ISATAP Query Interval* – интервал времени опроса DNS, принимает значения 120-3600, по умолчанию – 120;
- *ISATAP Solicitation Interval* – интервал времени между сообщениями запроса, принимает значения 120-3600, по умолчанию – 120;
- *ISATAP IPv6 Link Local Address* – локальный IPv6-адрес устройства;
- *ISATAP IPv6 Global Address* – глобальный IPv6-адрес устройства.

Кнопка «Update» используется для сохранения настроек.

5.4 Подменю «Wireless Settings»

В подменю «Wireless Settings» выполняются настройки беспроводной Wi-Fi сети. Устройство имеет 2 независимых физических радиоинтерфейса, способных работать в своем режиме и диапазоне каждый. Для WOP-2ac SFP, WOP-2ac GPON, WEP-2ac, WOP-2ac зафиксированы диапазоны: 5 ГГц только на первом радиоинтерфейсе, 2,4 ГГц только на втором радиоинтерфейсе. В представленном разделе меню приводится раздельная настройка для каждого интерфейса.



- *Country* – название страны, в которой работает точка доступа. В зависимости от указанного значения будут применены ограничения к полосе частот и мощности передатчика, которые действуют в данной стране. От установленной страны зависит список доступных частотных каналов и, следовательно, это влияет на автоматический выбор канала в режиме Channel = Auto. Если используется клиентское оборудование, лицензированное для использования в другом регионе, возможно, установить связь с точкой доступа в таком случае не удастся.

> Выбор неправильного региона может привести к проблемам совместимости с разными клиентскими устройствами.

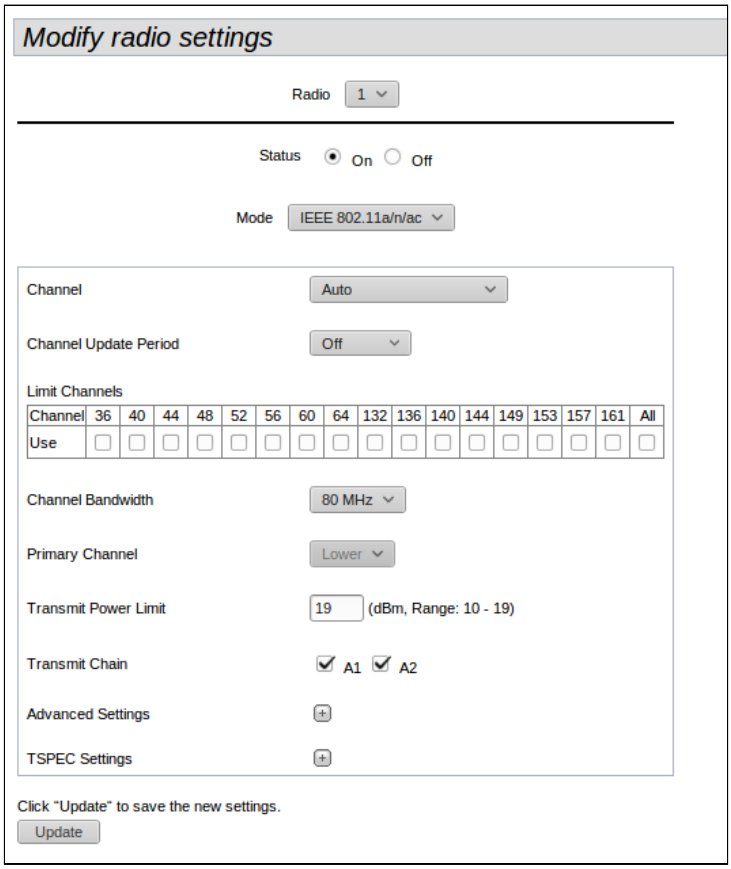
- *Transmit Power Control* – настройка режима ограничения параметра Transmit Power Limit:
  - *On* – максимальное значение ЭИИМ ограничивается в соответствии с законодательством РФ и не превышает 100 мВт (16 дБм излучаемой передатчиком мощности для диапазона 2,4 ГГц, 19 дБм излучаемой передатчиком мощности – для 5 ГГц).
  - *Off* – максимальное значение ЭИИМ ограничивается физическими характеристиками передатчика Для всех устройств WOP/WEP-2ac, максимальное значение ЭИИМ для диапазона 2,4 ГГц - 18 дБм, для диапазона 5 ГГц – 21 дБм.
- *TSPEC Violation Interval* – интервал времени, выделенный для точки доступа, чтобы сообщить через систему логирования или SNMP о присоединенных клиентах, которые не поддерживают обязательные процедуры допуска;
- *Global Isolation* – при установленном флаге включена изоляция трафика между клиентами разных VAP и разных радиоинтерфейсов;
- *Radio Interface* – состояние радиоинтерфейса:
  - *On* – при установленном флаге радиоинтерфейс активен;
  - *Off* – при установленном флаге радиоинтерфейс выключен.
- *MAC Address* – MAC-адрес радиоинтерфейса;
- *Mode* – выбор режима работы беспроводного интерфейса;
- *Channel* – номер канала для работы беспроводной сети. При выборе значения «auto» автоматически определяется канал с меньшим уровнем помех;

- *Airtime fairness* – функция эфирной радиодоступности:
  - *On* – при установленном флаге функция активна. Эфирное время равномерно распределяется между пользователями;
  - *Off* – функция выключена.
- *FBWA* – проприетарная технология, позволяющая выбирать для приема и передачи данных центральную частоту, а не установленный канал по стандартам IEEE 802.11. По стандартам IEEE 802.11 management и data трафик может использовать разную центральную частоту (актуально только при использовании ширины канала 40/80 МГц, технология доступна только для Outdoor устройств).
  - On – технология включена;
  - Off – технология выключена.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.5 Подменю «Radio»

В подменю «Radio» выполняются расширенные настройки беспроводной Wi-Fi сети для каждого радиоинтерфейса.



- *Radio* – выбор беспроводного Wi-Fi интерфейса;
- *Status* – состояние конфигурируемого Wi-Fi интерфейса:
  - *On* – при установленном флаге Wi-Fi интерфейс включен;
  - *Off* – при установленном флаге Wi-Fi интерфейс выключен;
- *Mode* – выбор режима работы радиоинтерфейса:
  - *IEEE 802.11b/g* – частотный диапазон 2,4 ГГц, максимальная скорость передачи 54 Мбит/с;
  - *IEEE 802.11b/g/n* – частотный диапазон 2,4 ГГц, максимальная скорость передачи 450 Мбит/с;
  - *2.4 Ghz IEEE 802.11n* – частотный диапазон 2,4 ГГц, максимальная скорость передачи 450 Мбит/с. Возможно подключение клиентов только с поддержкой стандарта IEEE 802.11n;
  - *IEEE 802.11a* – частотный диапазон 5 ГГц, максимальная скорость передачи 54 Мбит/с;

  - *IEEE 802.11a/n/ac* – частотный диапазон 5 ГГц, максимальная скорость передачи 1300 Мбит/с;
  - *IEEE 802.11n/ac* – частотный диапазон 5 ГГц, максимальная скорость передачи 1300 Мбит/с. Возможно подключение клиентов только с поддержкой стандарта IEEE 802.11n/ac;
- *Channel* – выбор радиоканала для работы Wi-Fi интерфейса. При выборе значения «*Auto*» автоматически определяется канал с наименьшим количеством работающих точек доступа на данном канале с учетом заданного региона;
- *Channel Update Period* – период времени, через который будет происходить автовыбор оптимального канала;
- *Limit Channels* – список каналов, которые ТД может выбирать для работы в режиме «*Auto*»;
- *Channel Bandwidth* – ширина полосы пропускания;
- *Primary Channel* – параметр может быть изменен только при пропускной способности статически заданного канала 40 МГц. Канал 40 МГц можно считать состоящим из двух каналов по 20 МГц, которые граничат в частотной области. Эти два канала 20 МГц называют первичным и вторичным каналами. Первичный канал используется клиентами, которые поддерживают только полосу пропускания канала 20 МГц:
  - *Upper*– первичным каналом будет верхний канал 20 МГц в полосе 40 МГц;
  - *Lower*– первичным каналом будет нижний канал 20 МГц в полосе 40 МГц.
- *Transmit Power Limit* – мощность передатчика радиоинтерфейса, в дБм. При включенном режиме *Transmit Power Control* в диапазоне 2,4 ГГц принимает значения от 8 до 16, по умолчанию – 16, в диапазоне 5 ГГц принимает значения от 1 до 19, по умолчанию – 19. При отключенном *режиме Transmit Power Control «Outdoor»* принимает значения в диапазоне 2.4ГГц от 8 до 18, по умолчанию – 18, в диапазоне 5ГГц от 1 до 21, по умолчанию - 21;
- *Transmit Chain*– флаги активности антенн. При установленном флаге соответствующая антенна включена.

> Клиентские Wi-Fi устройства могут не поддерживать некоторые частотные каналы. Рекомендуется назначать частотные каналы 1-11 для диапазона 2,4 ГГц и 36-48 для диапазона 5 ГГц, если нет информации о каналах, поддерживаемых клиентами.

> При установке частотного канала из диапазона 52-144 включение интерфейса Wi-Fi происходит через 1 минуту.

Чтобы перейти к расширенному списку параметров, нажмите "+" напротив "Advanced settings":

OBSS Coexistence: On
DFS Support: Off
Multidomain Regulatory Mode: Enable
Short Guard Interval Supported: No
STBC Mode: Auto
Protection: Auto
Beacon Interval: 100 (Msec, Range: 20 - 2000)
DTIM Period: 2 (Range: 1-255)
Fragmentation Threshold: 2346 (Range: 256-2346, Even Numbers)
RTS Threshold: 2347 (Range: 0-65535)
Maximum Stations: 200 (Range: 0-200)
VLAN List: Add, Remove Selected
(Range: 1-4094, 20 vlan-ids max)
Fixed Multicast Rate: Auto Mbps
Frame-burst Support: Off [Boosts Downstream Throughput]
ARP Suppression: On
DHCP Snooping Mode: Ignore
MCS Rate Set:
VHT NSS2 MCS0-MCS8 (13 - 156 Mbps)
VHT NSS2 MCS0-MCS7 (13 - 130 Mbps)
VHT NSS1 MCS0-MCS8 (6.5 - 78 Mbps)
VHT NSS1 MCS0-MCS7 (6.5 - 65 Mbps)
MCS15 (130 Mbps)
MCS14 (117 Mbps)

Legacy Rate Sets

Rate (Mbps)	54	48	36	24	18	12	9	6
Supported	✓	✓	✓	✓	✓	✓	✓	✓
Basic				✓		✓		✓

Broadcast/Multicast Rate Limiting
Rate Limit: 50 (packets per second)
Rate Limit Burst: 75 (packets per second)
VHT Features
TSPEC Settings

Click "Update" to save the new settings.
Update

- *OBSS Coexistence*– режим автоматической смены ширины канала с 40 МГц на 20 МГц при загруженном радиоэфире:
  - *On* – при установленном флаге режим включен;
  - *Off* – при установленном флаге режим выключен;
- *DFS Support* – механизм динамического выбора частоты. Требует от беспроводных устройств сканировать радиоэфир и избегать использования каналов, совпадающих с каналами, на которых работают радиолокационные системы в 5 ГГц диапазоне. Поле доступно, только если выбран

режим работы радиоинтерфейса на частоте 5 ГГц.
    - *On* – при установленном флаге поддержка механизма включена;
    - *Off* – при установленном флаге поддержка механизма выключена;
- *Multidomain Regulatory Mode* – режим передачи устройством информации о выставленном регионе в служебных сообщениях Beacon frame:
    - *Enable*– режим включен;
    - *Disable* – режим выключен;
- *Short Guard Interval Supported* – поддержка укороченного защитного интервала. Это поле доступно, только если выбранный режим работы радиоинтерфейса включает в себя 802.11n. Уменьшение защитного интервала увеличивает пропускную способность:
    - *Yes*– точка доступа передает данные, используя 400 нс защитный интервал при общении с клиентами, которые также поддерживают короткий защитный интервал;
    - *No*– точка доступа передает данные, используя 800 нс защитный интервал;
- *STBC Mode*– метод простанственно-временного блочного кодирования, направленный на повышение надежности передачи данных. Поле доступно, только если выбранный режим работы радиоинтерфейса включает в себя 802.11n:
    - *Yes*– точка доступа передает один поток данных через несколько антенн;
    - *No* – точка доступа не передает один и тот же поток данных через несколько антенн;
- *Protection* – режим работы предотвращения межстанционной интерференции:
    - *Auto* – режим включен;
    - *Off* – режим выключен;
- *Beacon Interval* – период посылки маячковых фреймов. Фреймы передаются для обнаружения точки доступа в эфире, принимает значения 20-2000 мс, по умолчанию - 100 мс;
- *DTIM Period* – временной интервал, по истечении которого широковещательные и мультикастовые пакеты, помещенные в буфере, будут доставлены беспроводным клиентам. При выставлении большего значения позволяет больше экономить энергию мобильных клиентов, однако повышает задержку для мультикастового аудио- и видеотрафика. Принимает значения 1-255 мс, по умолчанию – 4 мс;
- *Fragmentation Threshold* – порог фрагментации фрейма, в байтах. Принимает значения 256-2346, по умолчанию – 2346;
- *RTS Threshold* – указывает число байт, через которое посылается запрос на передачу (Request to Send). Уменьшение данного значения может улучшить работу точки доступа при большом количестве подключенных клиентов, однако это уменьшает общую пропускную способность беспроводной сети. Принимает значения 0-2347, по умолчанию – 2347;
- *Maximum stations* – максимальное число подключенных клиентов. Принимает значения 0-200, по умолчанию – 200;
- DHCP Snooping Mode - управление политикой обработки опции 82:
    - *Ignore* – на точке доступа отключена обработка опции 82;
    - *Replace* – точка доступа подставляет или заменяет значение опции 82.
        - DHCP Option 82 Circuit ID - свободная строка ввода значения опции 82 (ограничение в 52 символа). Если оставить стоку пустой, ТД автоматически подставляет значение в формате:
            - _Agent Circuit ID = \[mac-адрес точки ; SSID\];
            - _Remote ID = \[mac-адрес клиента\] - подставляется автоматически.
    - *Remove* – ТД удаляет значение опции 82.
- *VLANlist* – список VLAN, разрешенных для передачи в эфир (используется совместно с режимом VlanTrunk на VAP). Настройка VLAN list используется в том случае, если в сторону клиентского устройства нужно передать не один VLAN, а несколько. Настройка актуальна для режима работы VAP – VlanTrunk. Максимум – 20;
- *Fixed Multicast Rate* – выбор фиксированной скорости передачи мультикастового трафика, при выборе значения «auto» выбор скорости выполняется автоматически;
- *Frame-burst Support* – режим, позволяющий увеличить пропускную способность для нисходящего потока;
- *ARP suppression* – механизм конвертирования ARP-запросов из Broadcast в Unicast;

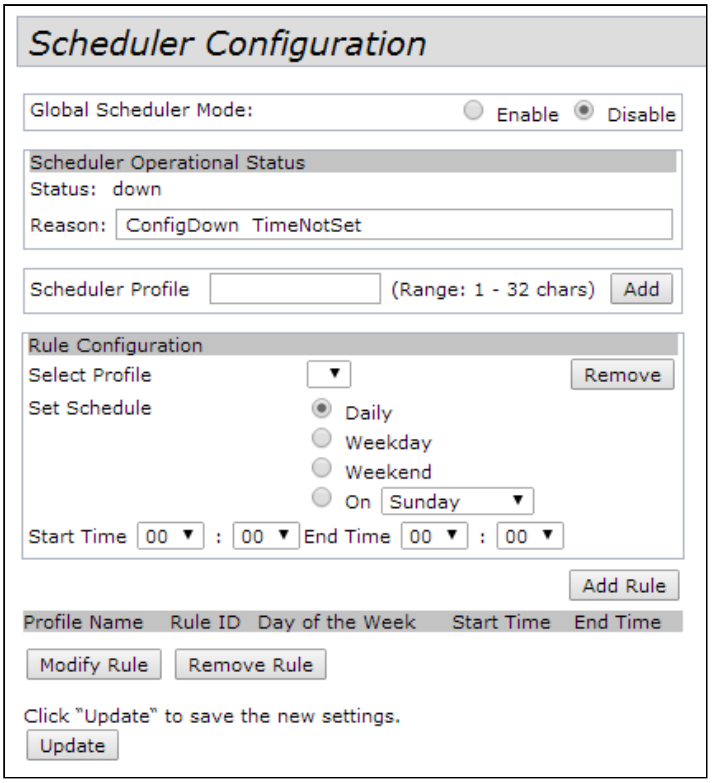
- MCS Rate Set - выбор поддерживаемых канальных скоростей беспроводной передачи данных, определяемых спецификациями стандартов IEEE 802.11n/ac;
- *Legacy Rate Sets* – поддерживаемые и транслируемые точкой доступа наборы канальных скоростей;
- *Broadcast/Multicast Rate Limit* – при установленном флаге выполняется ограничение передачи широковещательного/мультикастового трафика по беспроводной сети. Для редактирования будут доступны следующие поля:
    - *Rate limit* – порог для скорости передачи данных, пакет/с;
    - *Rate limit Burst* – максимальное значение всплеска трафика, пакет/с.
- *Tspec Mode* – регулирует общий режим Tspec на точке доступа.
    - *On* – точка доступа обрабатывает Tspec-запросы от клиентов. Используйте эту настройку, если точка доступа обрабатывает трафик от QoS-совместимых устройств, таких как сертифицированный телефоны Wi-Fi.
    - *Off* – точка доступа игнорирует Tspec-запросы от клиентов. Используйте эту настройку, если вы не хотите использовать Tspec для QoS-совместимых устройств.
- *Tspec Voice ACMMode* – регламентирует обязательный контроль допуска (ACM) для категории голосового трафика (Voice).
    - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока голосового трафика Voice.
    - *Off* – клиент может отправлять и получать голосовой трафик Voice, не требуя допускаемой Tspec; точка доступа игнорирует запросы Voice Tspec от клиентов.
- *Tspec VoiceACM Limit* – определяет предел объема Voice-трафика.
- *Tspec FBT Voice ACM Limit* – определяет верхний предел объема Voice-трафика для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS.
- *Tspec Video ACMMode* – регламентирует обязательный контроль допуска (ACM) для категории Video-трафика.
    - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока Video-трафика.
    - *Off* – клиент может отправлять и получать Video-трафик без необходимости запроса.
- *Tspec Video ACM Limit* – определяет верхний предел объема Video-трафика
- *Tspec FBT Video ACM Limit* – определяет верхний предел объема Video-трафика для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS.
- *Tspec BE ACM Mode* – регламентирует обязательный контроль допуска для категории BE-трафика.
    - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока трафика категории BE.
    - *Off* – клиент может отправлять и получать трафик категории BE, без необходимости запроса.
- *Tspec BE ACM Limit* – определяет верхний предел объема трафика категории BE для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS.
- *Tspec BK ACMMode* – регламентирует обязательный контроль допуска для категории BK-трафика.
    - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока трафика категории BK.
    - *Off* – клиент может отправлять и получать трафик категории BK без необходимости запроса.
- *Tspec BK ACM Limit* – определяет верхний предел объема трафика категории BK для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS.
- *Tspec AP Inactivitytimeout*– время, по истечению которого, будут удаляться неактивные клиенты с точки доступа (проверяется поток downlink).
- *Tspec Stationinactivitytimeout* – время, по истечению которого, будут удаляться неактивные клиенты с точки доступа (проверяется поток uplink).
- *Tspec Legacy WMM QueueMapMode* – выберите *Вкл*, чтобы получать трафик различных категорий на очередях, работающих в АКМ.
- *VHT Features* – функция включения/выключения Broadcom расширения в VHT. Функция VHT включает поддержку 256QAM, поддерживается для 802.11ac.

Предупреждение
Настраивать состав используемых антенн допускается только для устройств WOP-2ac. Для WEP-2ac настройка скрыта.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.6 Подменю «Scheduler»

В подменю «Scheduler» выполняется настройка планировщика работы точек доступа. С помощью настроек данного меню можно сконфигурировать время работы определенного радиоинтерфейса или виртуальной точки доступа.



- *Global Scheduler Mode* – включение/выключение планировщика:
  - *Enable* – при установленном флаге планировщик включен;
  - *Disable* – при установленном флаге планировщик выключен;

Scheduler Operational Status – в разделе выполняется просмотр о состоянии работы планировщика:

- *Status* – статус работы планировщика;
- *Reason* – дополнительная информация о состоянии работы планировщика:
    - *IsActive* – в рабочем состоянии;
    - *ConfigDown* – планировщик выключен, отсутствуют глобальные настройки;
    - *TimeNotSet* – планировщик выключен, на устройстве не установлено системное время;
    - *ManagedMode* – планировщик выключен, устройство в режиме управления;
    - *Scheduler Profile* – имя создаваемого профиля планировщика, задается от 1-32 символов.

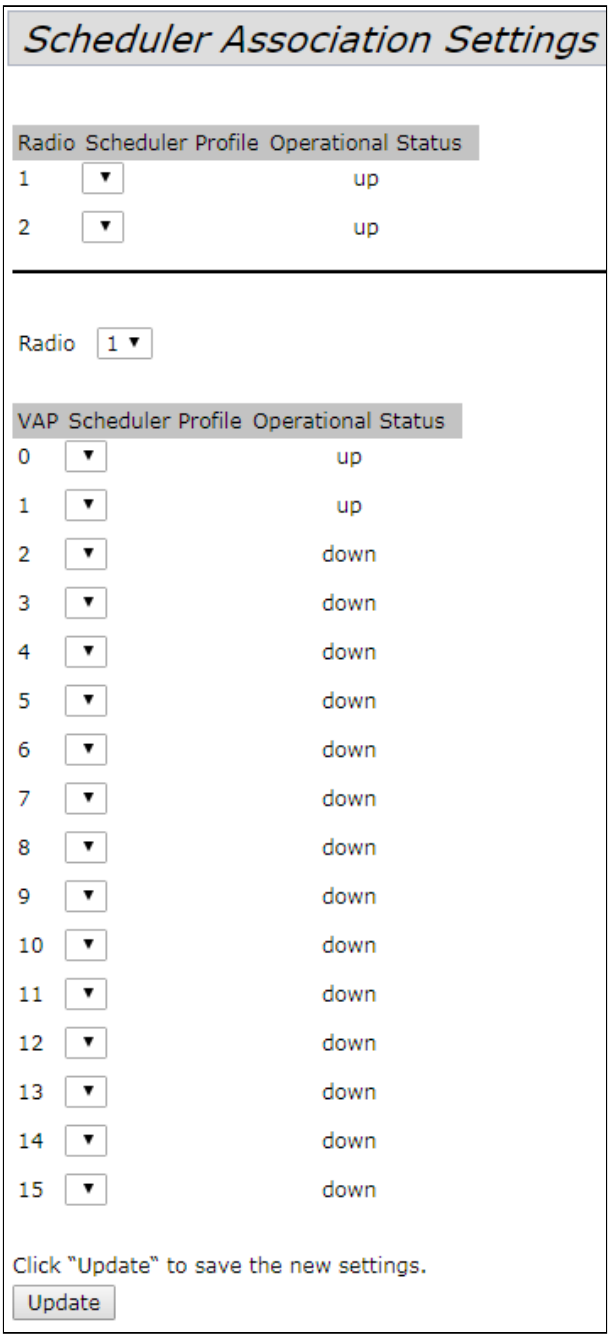
Для добавления профиля в систему укажите имя в поле «Scheduler Profile» и нажмите кнопку «Add».
Rule Configuration – в разделе выполняется настройка параметров профиля планировщика:

- *Select Profile* – имя созданного профиля, для которого будет выполняться настройка параметров;
- *Set Schedule* – день недели работы планировщика:
    - *Daily* – ежедневно;
    - *Weekday* – рабочие дни;
    - *Weekend* – выходные дни;
    - *On* – определенный день, выбор осуществляется из выпадающего списка;
- *Start Time* – время включения радиоинтерфейса, задается в виде часы:минуты;
- *End Time* – время выключения радиоинтерфейса, задается в виде часы:минуты.

Для сохранения нового правила профиля нажмите кнопку «Add Rule». Для удаления правила выберите правило в списке и нажмите кнопку «Remove Rule». Для изменения настроек правила выберите правило и нажмите кнопку «Modify Rule».
Нажмите кнопку «Update» для сохранения внесенных изменений.

5.7 Подменю «Scheduler Association»

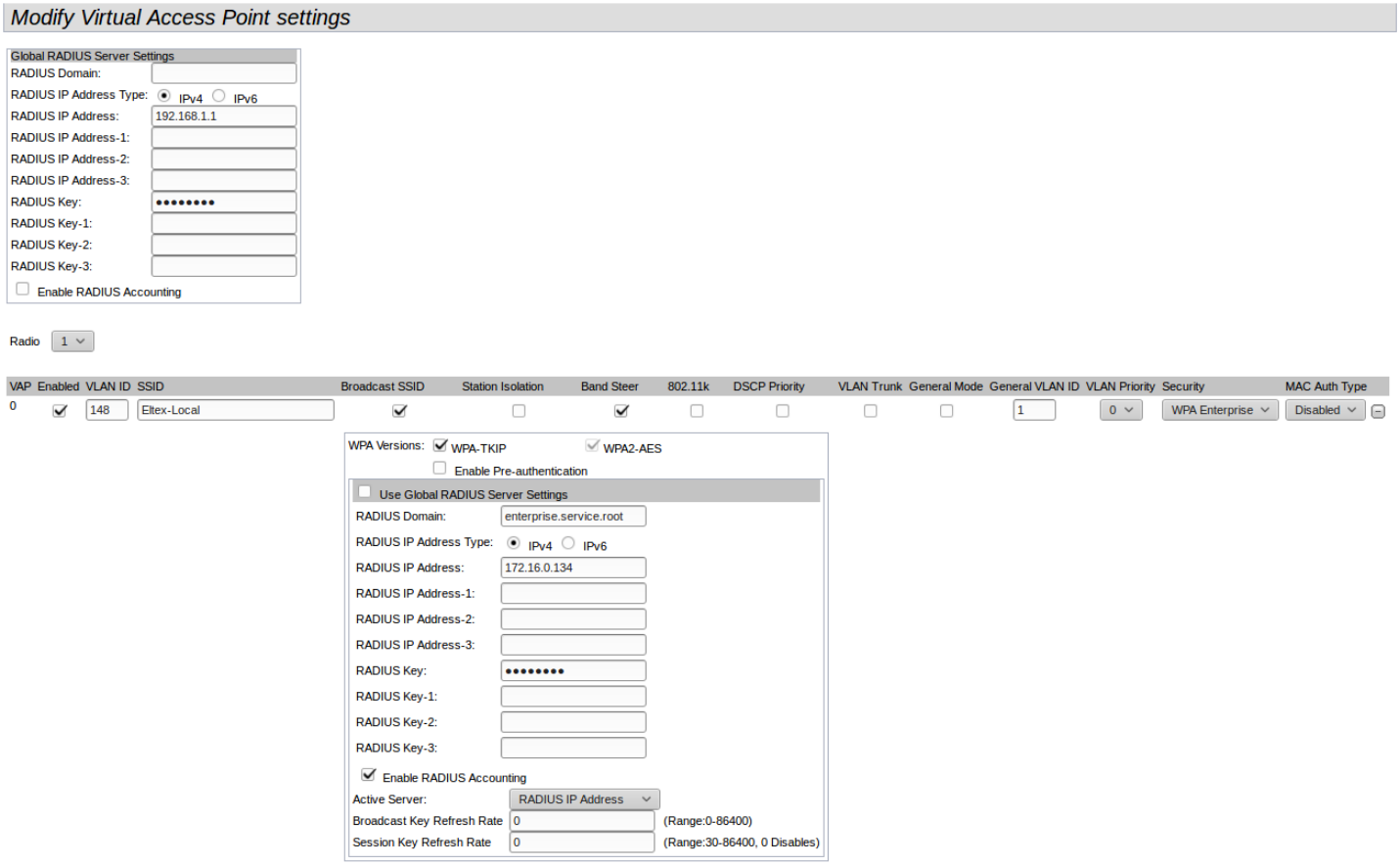
В разделе «Scheduler Association» выполняется привязка правил планировщика к виртуальным точкам доступа или радиоинтерфейсам.



Нажмите кнопку «Update» для сохранения внесенных изменений.

5.8 Подменю «VAP»

В разделе «VAP» выполняется настройка виртуальных точек доступа на Wi-Fi интерфейсах и настройка параметров RADIUS-сервера. Может быть сконфигурировано до 16 точек доступа на каждом Wi-Fi интерфейсе.



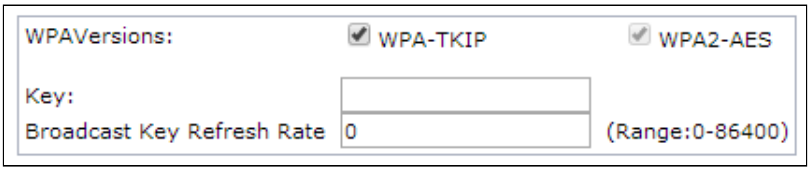
Global RADIUS server settings – в разделе выполняются глобальные настройки авторизации по RADIUS-протоколу:

- *RADIUS Domain* – домен пользователя;
- *RADIUS IP address Type* – выбор протокола IPv4 или IPv6 для доступа на сервер RADIUS;
- *RADIUS IP Address* – адрес RADIUS-сервера. При недоступности основного RADIUS-сервера, запросы будут отправляться на резервные;
- *RADIUS Key* – пароль для авторизации на RADIUS-сервере;
- *Enable RADIUS accounting* – при установленном флаге будут отправляться сообщения «Accounting» на RADIUS-сервер.

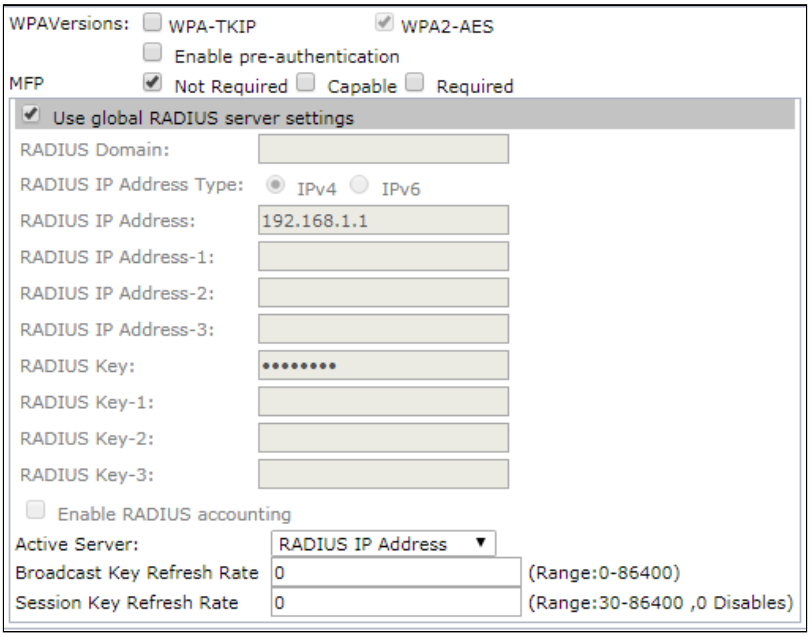
Настройка точек доступа:

- *Radio* – выбор настраиваемого радиоинтерфейса;
- *VAP* – порядковый номер виртуальной точки доступа;
- *Enabled* – при установленном флаге виртуальная точка доступа включена, иначе – выключена:
- *VLANID* – номер VLAN, к которому привязана виртуальная точка доступа;
- *SSID* – имя беспроводной сети;
- *BroadcastSSID* – при установленном флаге включено вещание в эфир имени SSID, иначе – выключено;
- *Station Isolation* – при установленном флаге включена изоляция клиентов друг от друга в пределах одного SSID;

- *BandSteer* – при установленном флаге активно приоритетное подключение клиента к 5 ГГц сети. Для работы этой функции нужно настроить радиоинтерфейсы точки доступа на разные частоты 2.4 ГГц и 5 ГГц, создать VAP с одинаковым SSID на каждом радиоинтерфейсе, и активировать на них параметр «BandSteer»;
- *802.11k* – включить поддержку стандарта 802.11k на виртуальной точке доступа;
- *DSCPPriority* - при установленном флаге источником приоритета для выбора очереди будут данные DSCP, при снятом – 802.1p;
- *VLAN trunk* – при установленном флаге используется транковый порт для подключения абонента;
- *General Mode* - при установленном флаге будет использоваться General порт для подключения клиентского оборудования - прием и передача тегированного и нетегированного трафика;
- *General VLAN ID* - номер VLAN, который будет сниматься в сторону клиентского оборудования/в который будет заворачиваться нетегированный трафик;
- *VLANPriority* – приоритет 3-го уровня, который будет назначаться на пакеты, проходящие через данный VAP с радио эфира в сторону проводной сети;
- *Security* – режим безопасности доступа к беспроводной сети:
    - *None* – не использовать шифрование для передачи данных. Точка открыта для доступа любого клиента;
    - WPA Personal – шифрование WPA и WPA2, при выборе данного способа будут доступны следующие настройки:



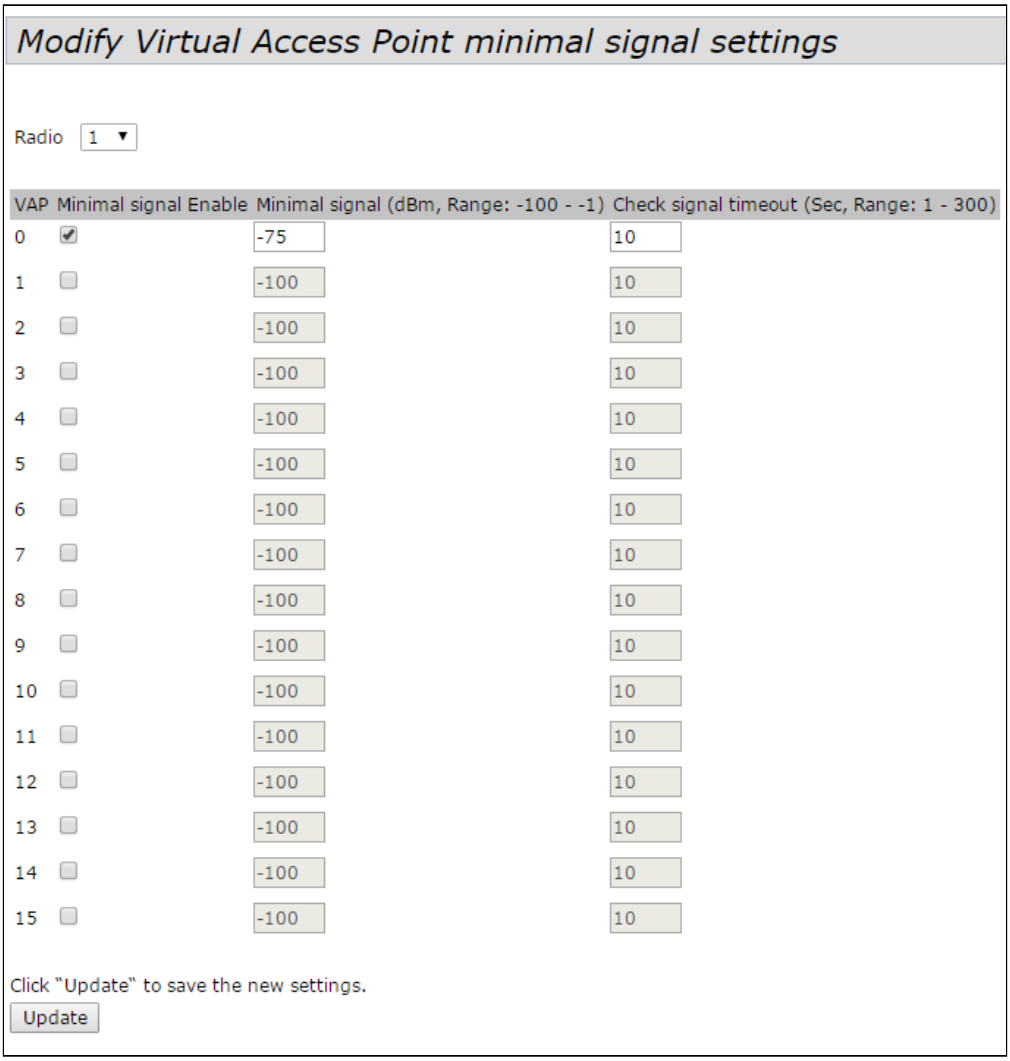
    - *WPAVersions* – версия шифрования: WPA-TKIP, WPA2-AES.
    - *KEY* – WPA-ключ. Длина ключа составляет от 8 до 63 символов.
    - *Broadcast Key Refresh Rate* – интервал обновления широковещательного ключа. Принимает значения 0-86400, по умолчанию – 0.
    - *MFP* – защита управляющих кадров: *Not Required* – не использовать; *Capable* – опционально; *Required* – использовать;
- *WPAEnterprise* – режим сертификации устройств беспроводной связи, при котором клиент авторизуется на централизованном RADIUS-сервере. Для настройки данного режима безопасности требуется указать параметры RADIUS-сервера (возможно использование до 4 RADIUS-серверов одновременно, но с указанием одного активного на данный момент). Также требуется указать домен, версии протоколов режима безопасности и ключи для каждого RADIUS-сервера.



- *MAC Auth Type* – режим аутентификация клиентов по MAC-адресу:
  - *Disabled* – не использовать аутентификацию клиентов по MAC-адресу;
  - *RADIUS* – использовать аутентификацию клиентов по MAC-адресу с помощью RADIUS-сервера;
  - *Local* – использовать аутентификацию клиентов по MAC-адресу с помощью локального списка адресов, сформированного на данной точке доступа.

5.9 Подменю «VAP Minimal Signal»

В разделе выполняется настройка функции отключения клиентского Wi-Fi оборудования при низком уровне сигнала, принимаемом от него.

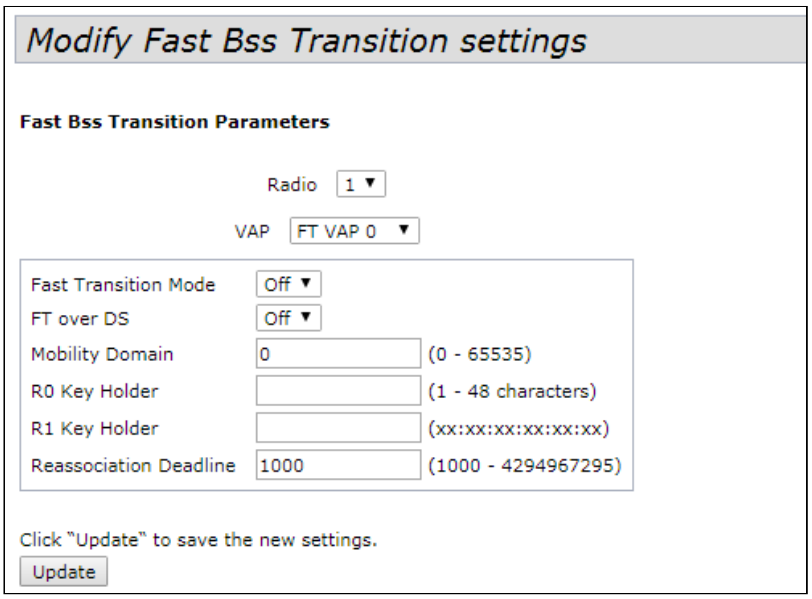


- *Radio* – выбор настраиваемого радиоинтерфейса;
- *VAP* – номер виртуальной точки доступа;
- *Minimal signal Enabled* – при установленном флаге включена функция Minimal Signal;
- *Minimal signal, dBm* – уровень сигнала в дБм, ниже которого происходит отключение клиентского оборудования;
- *Check signal timeout, s* – период времени, по истечении которого принимается решение об отключении клиентского оборудования.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.10 Подменю «Fast Bss Transition»

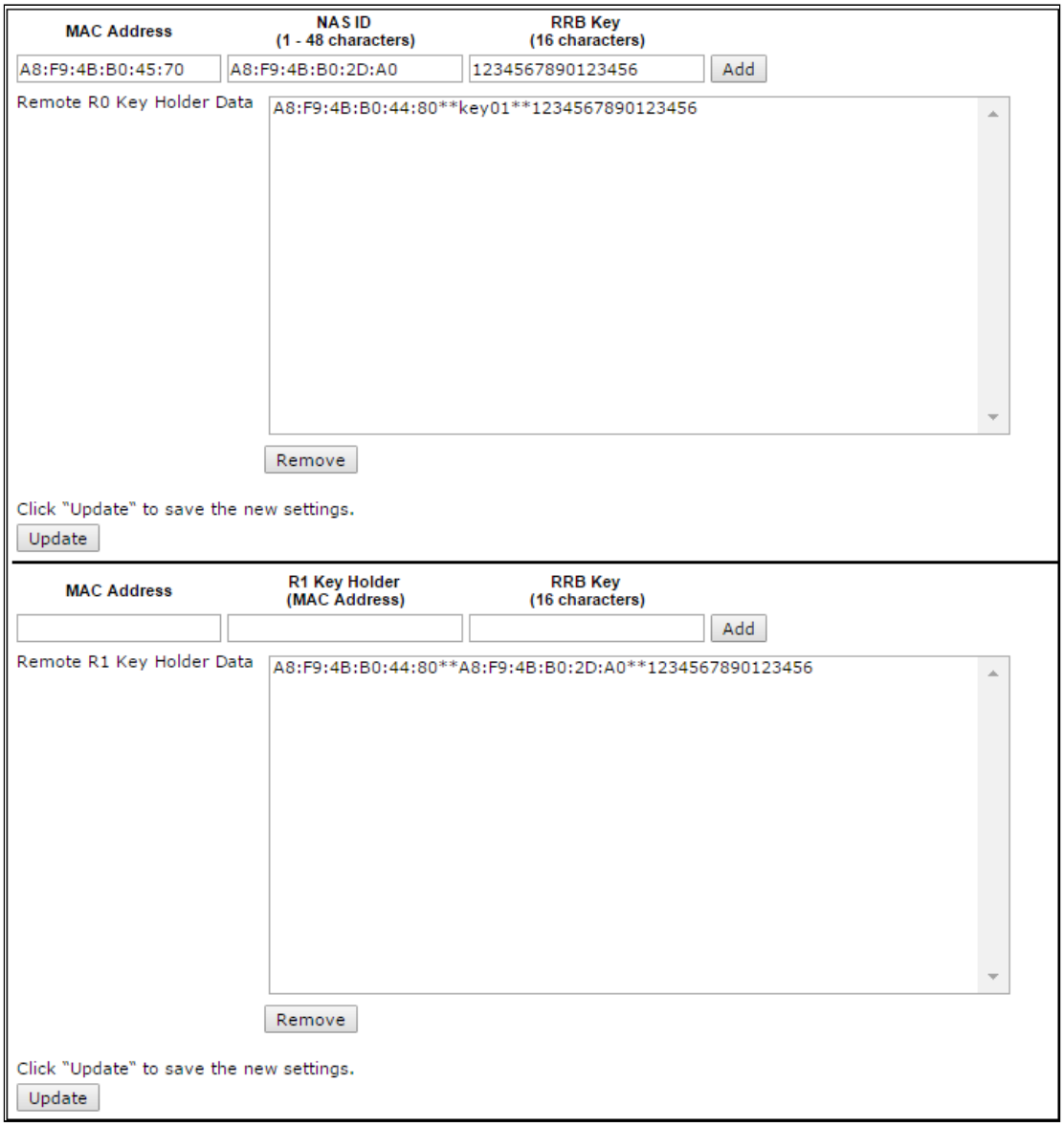
В подменю «Fast Bss Transition» производится задание параметров и настройка роуминга 802.11r между базовыми станциями.



Параметры Fast Bss Transition:

- *Radio* – выбор радиоинтерфейса, на котором будет настроен FBT;
- *VAP* – номер виртуальной точки доступа, на которой будет настроен FBT;
- *Fast Transition Mode* – активация функции быстрой передачи базового набора служб для ускорения процесса аутентификации на точке доступа:
  - *On* – функция включена;
  - *Off* – функция выключена.
- *FT over DS* – включение механизма обмена между базовыми станциями через проводную сеть. Клиент при необходимости совершить роуминг отправляет на текущую точку доступа FT Action Request frame с необходимыми авторизационными данными. Текущая точка доступа инкапсулирует данный фрейм и перенаправляет на целевую точку доступа через проводную сеть. Целевая точка доступа подтверждает возможность быстрой аутентификации инкапсулированным сообщением текущей точки доступа FT Action Response frame. Текущая точка доступа пересылает это сообщение клиенту. После окончания процесса клиент отсылает на целевую точку доступа запрос Reassociation. При отключенной функции *FT-over-DS* работает *FT-over-AIR*, в таком случае авторизация клиента на целевой ТД происходит с использованием стандартных фреймов аутентификации:
  - *On* – функция включена;
  - *Off* – функция выключена.
- *Mobility Domain identifier (MDID)* – номер группы (0 - 65535), в рамках которой может быть совершен роуминг;
- *R0 Key Holder* – ключ PMK-R0, до 48 символов. Также используется в качестве идентификатора NAS, который будет отправляться в сообщении Radius Access Request;
- *R1 Key Holder* – ключ PMK-R1 в формате MAC-адреса xx:xx:xx:xx:xx:xx;
- *Reassociation Deadline, ms* – максимальное разрешенное время ожидания запроса "Reassociation" от станции. По умолчанию используется значение 1000 мс.

Нажмите кнопку «Update» для сохранения внесенных изменений.
После указания основных параметров необходимо настроить взаимодействие с точками доступа, между которыми будет осуществляться роуминг, задав MAC-адреса и ключи.



- *MAC Address* – MAC-адрес точки доступа, участвующей в роуминге;
- *NAS ID* – идентификатор NAS, принимает значение, указанное в R0 Key Holder;
- *RRB key* – ключ для шифрования RRM-сообщений длиной 16 символов.

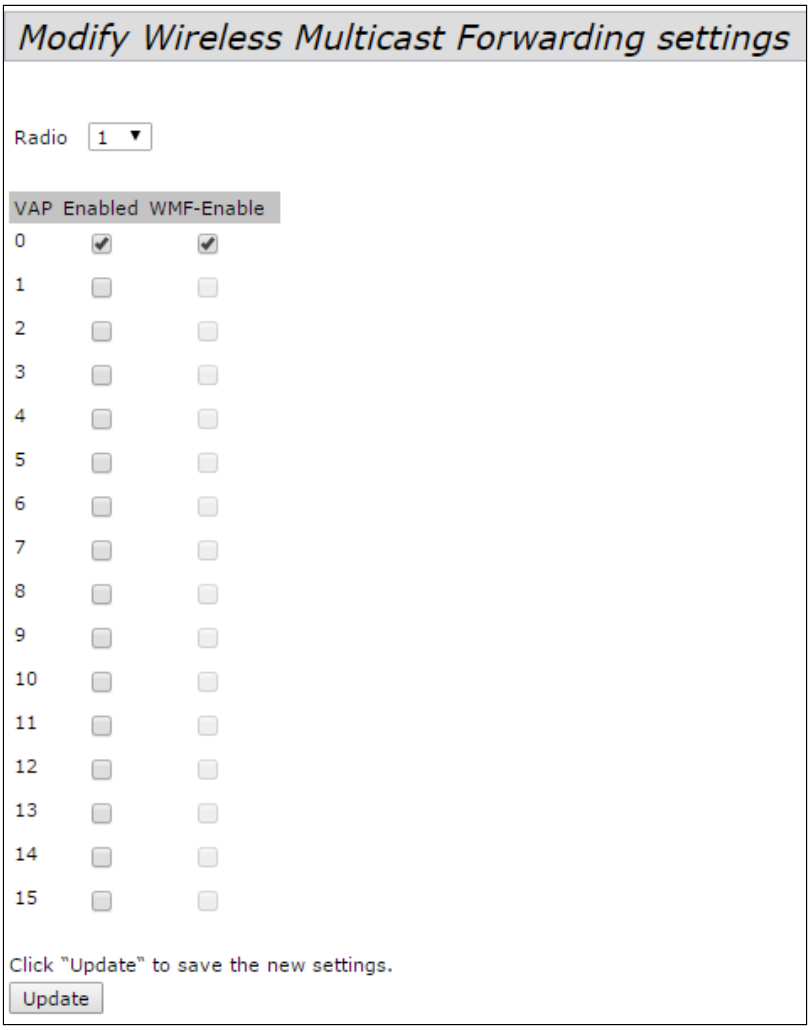
Для добавления записи в таблицу нажмите кнопку «Add».

Для удаления записи из таблицы выделите строку и нажмите кнопку «Remove».

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.11 Подменю «Wireless Multicast Forwarding»

В разделе «Wireless Multicast Forwarding» выполняется настройка перенаправления multicast-пакетов.

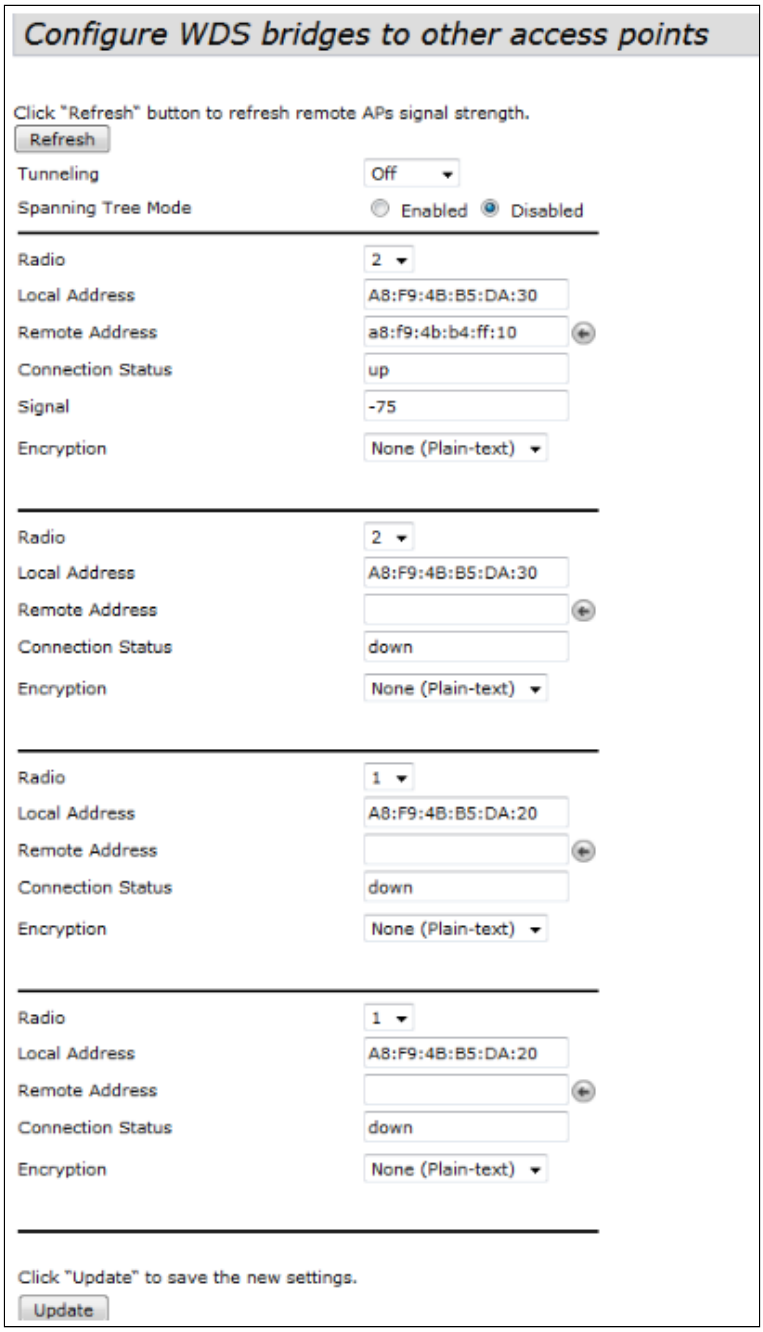


- *Radio* – выбор радиоинтерфейса;
- *VAP* – номер виртуальной точки доступа;
- *Enabled* – при установленном флаге виртуальная точка доступа будет активна, иначе – не активна;
- *WMF-Enable* – при установленном флаге будет активна функция перенаправления multicast-пакетов на виртуальной точке доступа, иначе – не активна.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.12 Подменю «WDS»

В разделе «WDS» выполняется настройка связи между точками доступа по беспроводной сети.



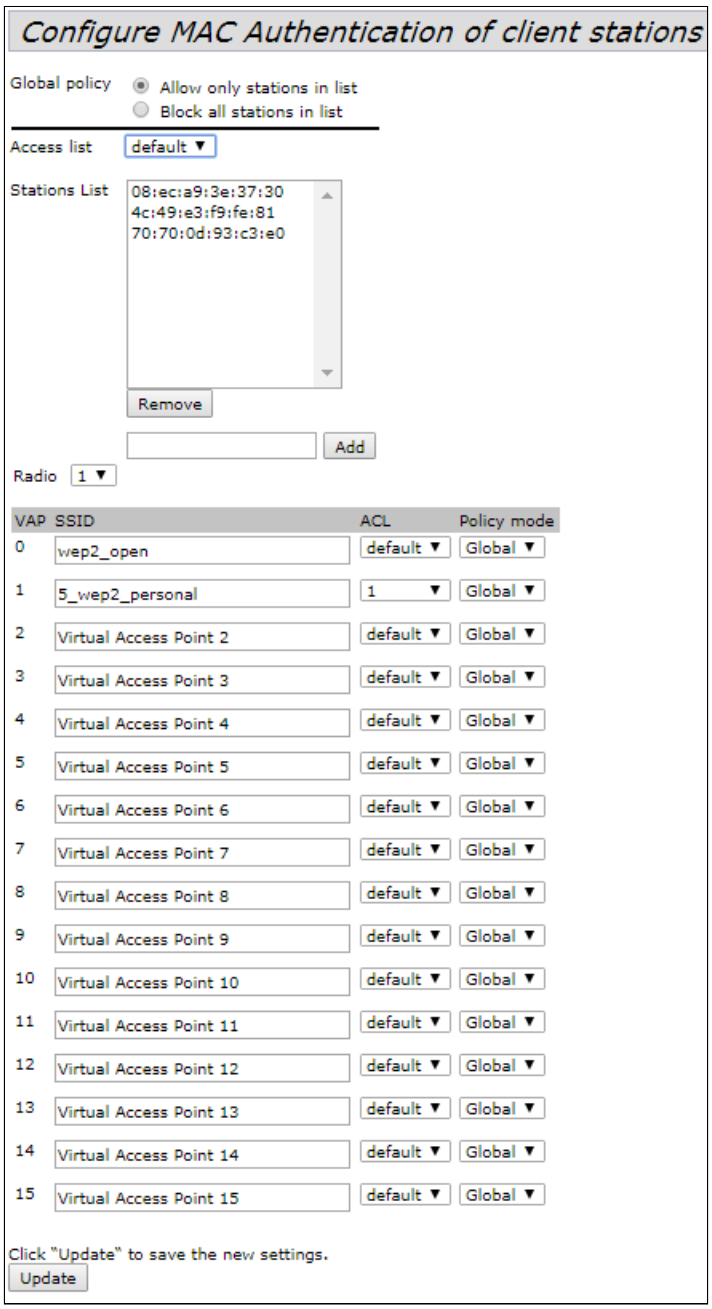
- *Tunneling* – опция доступна только при использовании GRE:
  - *Off* – GRE не используется, опция Tunneling выключена;
  - *Master* – точка подключается в сеть через Ethernet-интерфейс;
  - *Slave* – точка подключается к Master по радиоинтерфейсу;
- *Spanning tree mode* – режим работы протокола STP для предотвращения петель в сети:
  - *Enabled* – при установленном флаге протокол STP разрешен для использования. Рекомендуется включить при использовании WDS;
  - *Disable* – при установленном флаге протокол STP запрещен;
- *Radio* – выбор радиоинтерфейса;
- *Local Address* – просмотр MAC-адреса текущего радиоинтерфейса;
- *Remote Address* – адрес точки доступа, с которой предусматривается совместная работа;
- *Connection Status* – статус соединения;

- *Signal* – уровень с которым видна встречная ТД;
- *Encryption* – выбор режима шифрования:
    - *None* – не использовать шифрование;
    - *WPA (PSK)* – шифрование WPA и WPA2, при выборе данного способа будут доступны следующие настройки:
        - *SSID* – имя Wi-Fi сети;
        - *KEY* – WPA-ключ. Длина ключа составляет от 8 до 63 символов.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.13 Подменю «MAC Authentication»

В разделе «MAC Authentication» выполняется настройка белых/черных списков MAC-адресов клиентов, которым разрешено/запрещено подключаться к данной точке доступа.



- *Global policy* – выбор списка фильтрации MAC-адресов при аутентификации;
- *Allow only stations in list* – при установленном флаге будет формироваться белый список MAC-адресов;
- *Block all stations in list* – при установленном флаге будет формироваться черный список MAC-адресов.
- *Access list* – выбор списков MAC-адресов;
- *Stations List* – список MAC-адресов клиентов, которым разрешен/запрещен доступ;

Для добавления MAC-адреса в разделе «access List» выберите список фильтрации и введите MAC-адрес, который нужно добавить в список. Нажмите кнопку «Add».

Для удаления MAC-адреса в разделе «Station List» выберите запись и нажмите кнопку «Remove».

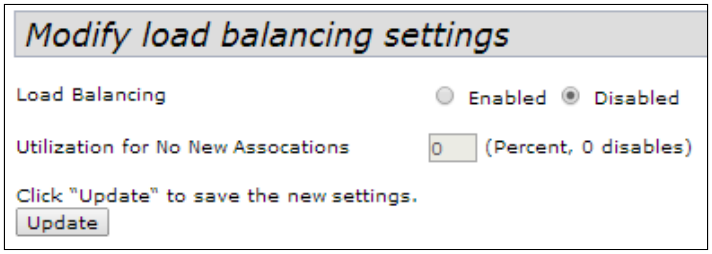
- *Radio* – выбор радио интерфейса точки доступа;

- *VAP* – номер виртуальной точки доступа;
- SSID – имя виртуальной точки доступа;
- *ACL* – выбор списка MAC-адресов для привязки его к выбранному SSID;
- *Policy mode* – настройка белых/черных списков MAC-адресов:
    - Global – для текущего SSID выбранный список Mac-адресов будет соответствовать глобальному флагу;
    - Allow – для текущего SSID выбранный список будет являться белым(доступ разрешен);
    - Block – для текущего SSID выбранный список будет являться черным(доступ запрещен).

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.14 Подменю «Load Balancing»

В разделе «Load Balancing» выполняется конфигурирование ограничения возможности подключения к точке доступа в зависимости от утилизации канала.

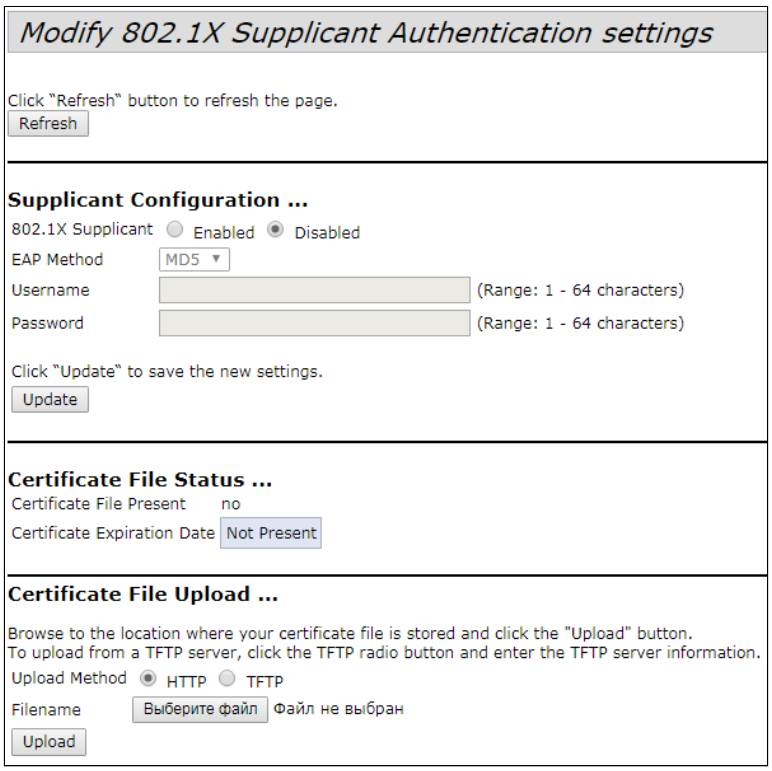


- *Load Balancing* – балансировка нагрузки:
    - *Enabled* – балансировка нагрузки включена;
    - *Disabled* – балансировка нагрузки выключена.
- *Utilization for No New Associations* – уровень утилизации полосы пропускания точки доступа, при превышении которой происходит запрет на подключение новых клиентов, задается в %. По умолчанию – 0.

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.15 Подменю «Authentication»

В разделе «Authentication» производится настройка точки доступа в режим клиента по протоколу 802.1X для прохождения процедуры аутентификации на вышестоящем оборудовании.



Supplicant Configuration – в разделе выполняется настройка параметров аутентификации:

- *802.1X Supplicant* – включить/выключить работу точки доступа в режиме клиента по протоколу 802.1X:
  - *Enabled* – включить;
  - *Disabled* – выключить;
- *EAP Method* – алгоритм шифрования при аутентификации пользователя;
- *Username* – имя пользователя, задается строка 1-64 символов;
- *Password* – пароль, задается стройка 1-64 символов.

Certificate File Status – в разделе можно просмотреть информацию о состоянии HTTP SSL сертификата.

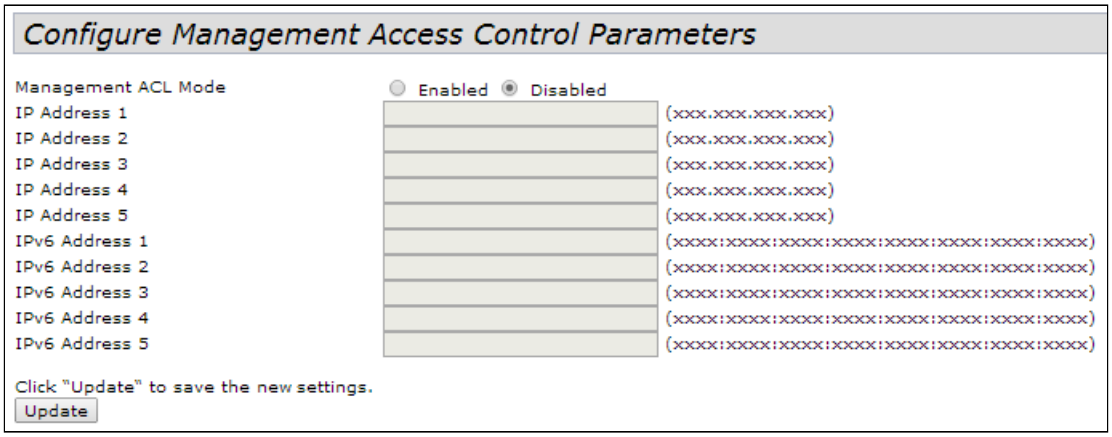
Certificate File Upload – в разделе выполняется загрузка файла HTTP SSL Certificate.

- *Upload Method* – метод загрузки файла HTTP SSL сертификата:
  - *HTTP* – загрузка сертификата через HTTP. При выборе этого способа нажмите кнопку «Выберите файл», укажите файл, который нужно загрузить в устройство;
  - *TFTP* – загрузка сертификата через TFTP. При указании этого способа нужно заполнить следующие поля:
    - *Filename* – имя файла сертификата;
    - *Server IP* – IP-адрес сервера.

Для загрузки сертификата нажмите кнопку «Upload».

5.16 Подменю «Management ACL»

В разделе «Management ACL» выполняется настройка списков доступа управления устройством Web, Telnet, SSH, SNMP.

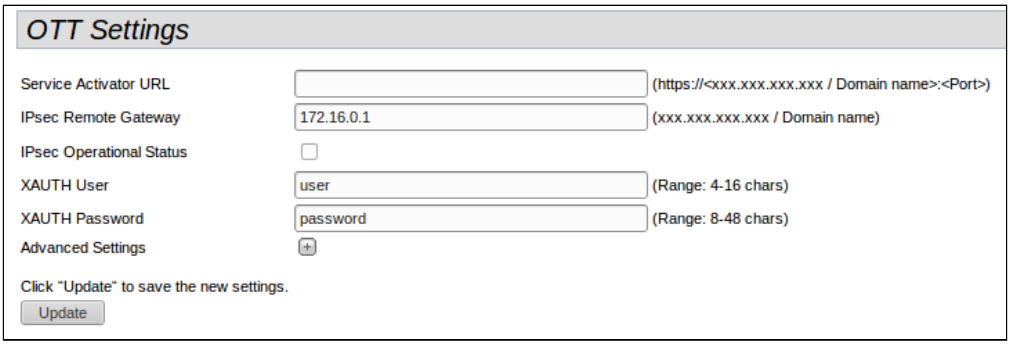


- *Management ACL Mode* – использование списков доступа к управлению устройством:
  - *Enabled* – при установленном флаге функционал включен;
  - *Disabled* – при установленном флаге функционал отключен;
- *IP Address* – список хостов IPv4, которые имеют доступ к управлению устройством;
- *IPv6 Address* – список хостов IPv4, которые имеют доступ к управлению устройством.

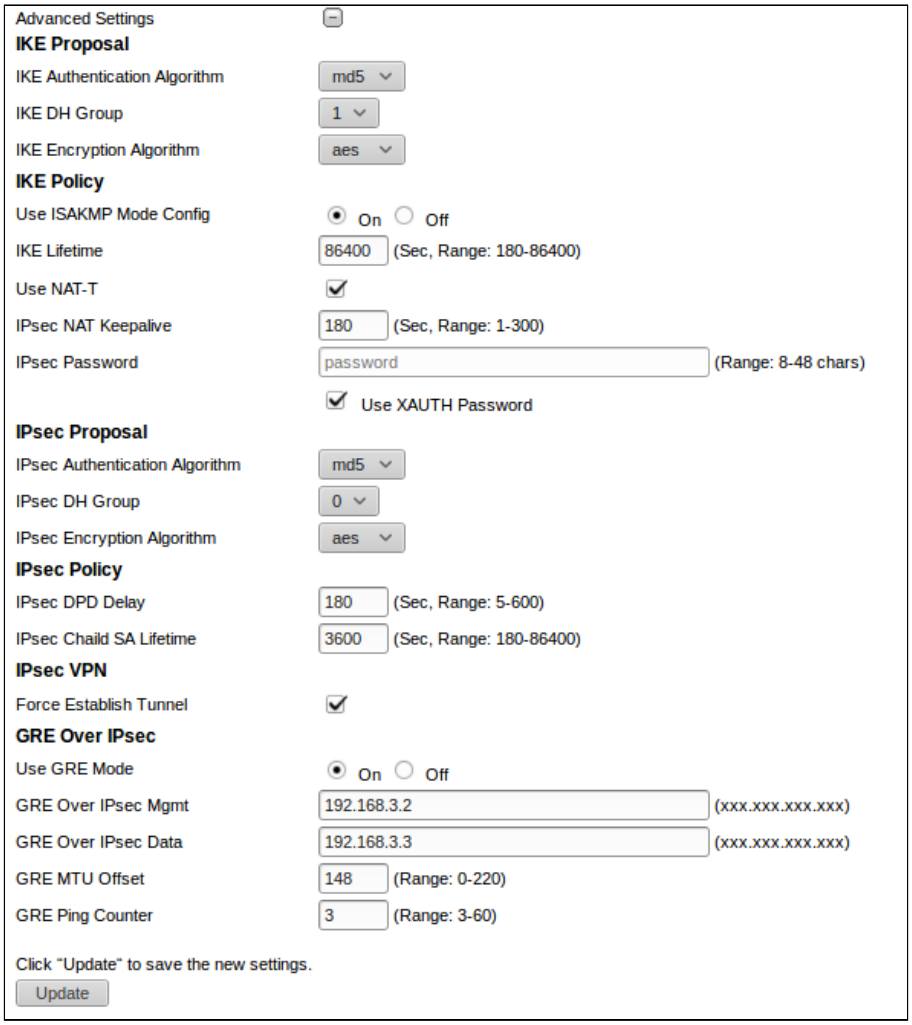
Для применения и сохранения настроек в энергонезависимую память нажмите «Update».

5.17 Подменю «OTT Settings»

В разделе **«OTT Settings»** выполняется настройка параметров OTT (over the top) для построения IPsec, либо GRE-туннелей внутри IPSec соединения от ТД.



- *Service Activator URL* – адрес сервис-активатора, задается в формате IP-адреса или доменного имени;
- *IPsec Remote Gateway* – шлюз для IPsec, задается в формате IP-адреса или доменного имени;
- *IPsec Operation Status* – состояние конфигурируемого IPsec-соединения;
- *XAUTH User* – имя пользователя для расширенной авторизации, необходимо для работы механизма mode config (диапазон: 4-16 символов);
- *XAUTH Password* – пароль пользователя для расширенной авторизации, необходимо для работы механизма mode config (диапазон: 8-48 символов);



- *IKE Authentication Algorithm* – выбор алгоритма хэширования IKE, предназначен для проверки целостности данных;
- *IKE DH Group* – выбор алгоритма Диффи-Хеллмана, используется чтобы установить общий секрет в незащищенной сети;
- *IKE Encryption Algorithm* – выбор алгоритма шифрования для 1 фазы подключения IPsec;
- *Use ISAKMP Mode Config* – активируем режим автоматического получения вирутального адреса, удалённой подсети, адресов для поднятия GRE-туннелей от ESR, к которому подключаемся по IPSec;
- *IKE Lifetime* – время жизни IKE (фаза 1), должен быть идентичен по обе стороны IKE/IPsec соединения (диапазон: 180-86400 секунд);
- *Use NAT-T* – необходимо включить флаг, если ТД находится за NAT;
- *IPsec NAT Keepalive* – периодичность отправки пакетов keepalive при работе через NAT, чтобы NAT-трансляция сохранялась на вышестоящих роутерах при длительной неактивности со стороны клиента. (диапазон: 0-300 секунд);
- *IPsec Password* – пароль для IKE/ISPEC-соединения (диапазон: 8-48 символов);
- *IPsec Authentication Algorithm* – выбор алгоритма хэширования IPsec, предназначен для проверки целостности данных;
- *IPsec DH Group* – выбор алгоритма Диффи-Хеллмана, используется чтобы установить общий секрет в незащищенной сети;
- *IPsec Encryption Algorithm* – выбор алгоритма шифрования для 1 фазы подключения IPsec;
- *IPsec DPD Delay* – интервал отправки пакетов обнаружения разрыва соединения. При отсутствии с противоположной стороны IPsec VPN ответов на 5 пакетов подряд, ТД сочтет VPN развалившимся и произведёт перезапуск IPsec VPN со своей стороны. (диапазон: 5-600 секунд);
- *IPsec Chaild SA Lifetime* – время жизни IPsec VPN SA (фаза 2), должен быть одинаковым с обеих сторон туннеля IKE/IPsec и ниже, чем IKE Lifetime (диапазон: 180-86400 секунд);

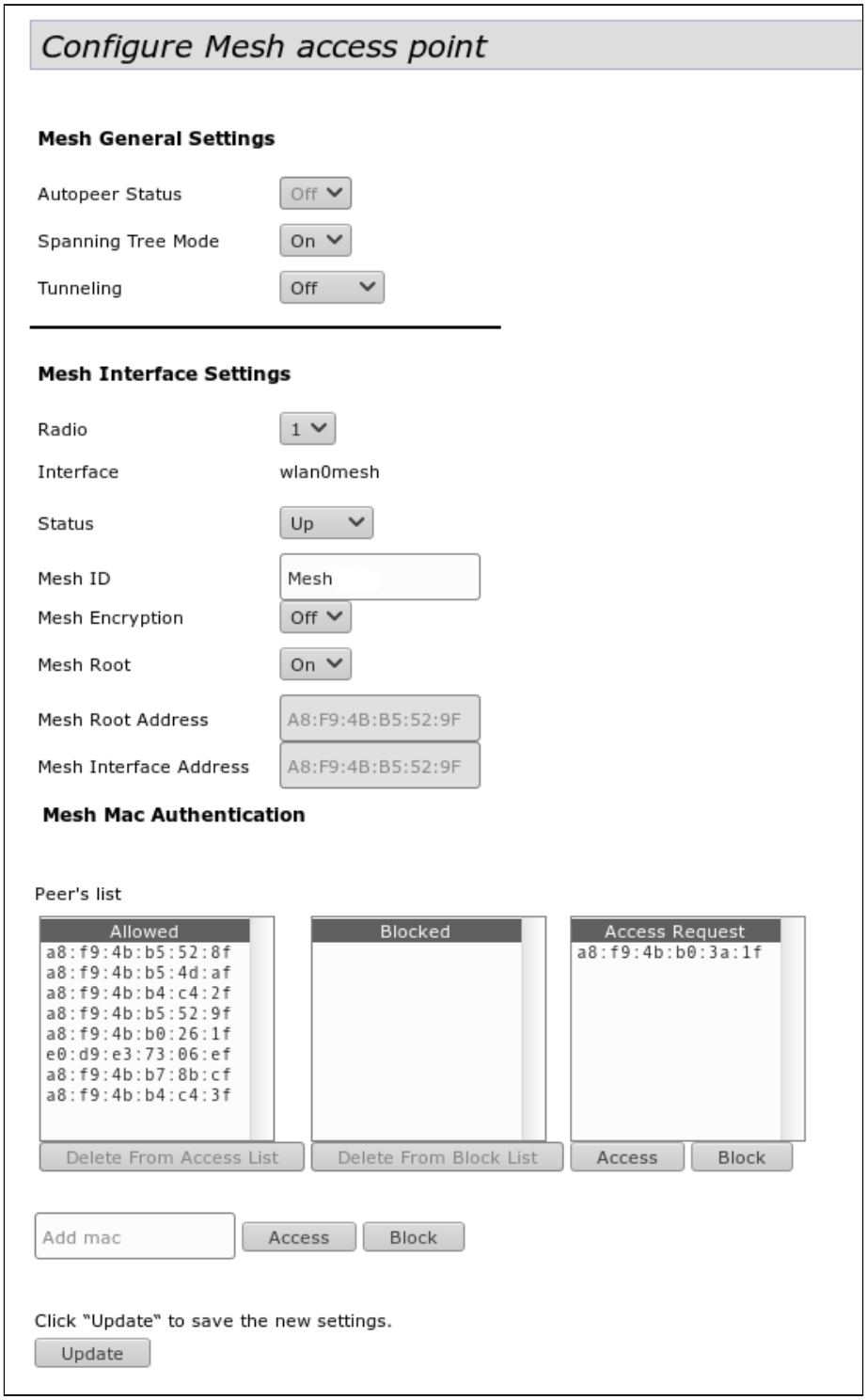
- *Force Establish Tunnel* – включить, чтобы установить соединение IPsec VPN немедленно. Иначе, VPN-соединение IPsec будет установлено по запросу;
- *Use GRE Mode* – включить или отключить GRE через IPsec;
- *GRE Over IPsec Mgmt* – IP-адрес GRE для туннеля управления;
- *GRE Over IPsec Data* – IP-адрес GRE для туннеля управления данными;
- *GRE MTU Offset* – определяет уменьшение MTU для GRE-туннелей. GRE-туннелям будет назначено MTU исходя из расчета 1500 - *GRE MTU Offset*;
- *GRE Ping Counte*r – чтобы проверить, что туннель GRE все еще жив, отправляется ping на GRE IP-management каждые 10 секунд. Это значение определяет, сколько пакетов пинга может быть потеряно, до того, как ТД перезапустит соединение IPsec (диапазон: 3-60).

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.18 Подменю «Mesh»*

В разделе "**Mesh**" выполняется настройка связи между точками доступа по беспроводной Mesh-сети.

> * Подменю доступно, если на точке доступа установлено ПО с поддержкой Mesh (WOP-2ac-1.14.0.X-MESH.tar.gz и более поздние версии).



Mesh General Settings – в данном разделе выполняется настройка общих Mesh параметров.

- *Autopeer Status* – статус автоконфигурирования точек доступа. Должен быть отключен на проводной точке (Root) и включен на беспроводных;
- *Spanning Tree Mode* – режим работы протокола STP для предотвращения петель в сети;

- *Tunneling* – опция доступна только при использовании GRE:
  - *Off* – GRE не используется, опция Tunneling выключена;
  - *Master* – точка подключается в сеть через Ethernet-интерфейс;
  - *Slave* – точка подключается к Master по радиоинтерфейсу.

Mesh Interface Settings – в данном разделе выполняется настройка параметров интерфеса для организации Mesh.

- *Radio* - выбор радиоинтерфейса для организации Mesh;

На точках типа WOP-2ac Mesh поддержан только на Radio 1 (5 ГГц).

- *Interface* - интерфейс, используемый для организации Mesh;
- *Status* – состояние конфигуриремого Mesh-интерфейса;
- *Mesh id* – имя Mesh-сети;
- *Mesh Encryption* – использование Mesh-сети с шифрованием (on – включить, off – выключить);
- *Mesh Root* – назначить точку доступа контроллером в Mesh сети(должна быть точкой ввода/проводной);
- *Root Address* – MAC-адрес интерфейса точки доступа, являющийся контроллером (заполняется автоматически);
- *Mesh interface Address* – MAC-адрес Mesh-интерфейса конфигурируемой точки доступа.

Mesh Mac Authentication – в разделе выполняется добавление/удаление участников Mesh-сети.

- *Allowed* – точкам доступа добавленным в список "Allowed" разрешен доступ в Mesh-сеть;
- *Blocked* – точкам доступа добавленным в список "Blocked" запрещен доступ в Mesh-сеть;
- *Access Request*– список точек доступа приславших запрос на подключение в Mesh-сеть:
  - *Access*– добавление точки доступа в "белый" список (доступ разрешен);
  - *Block*– добавление точки доступа в "черный" список (доступ запрещен).
- *Delete from Access List* – удалить выделенный MAC-адрес из списка разрешенных;
- *Delete from Block List* – удалить выделенный MAC-адрес из списка запрещенных.

Для того, чтобы добавить точку доступа в список *Allowed/Blocked вручную, необходимо ввести MAC-адрес точки в поле "Add mac" и нажать соотвествующую кнопку:*

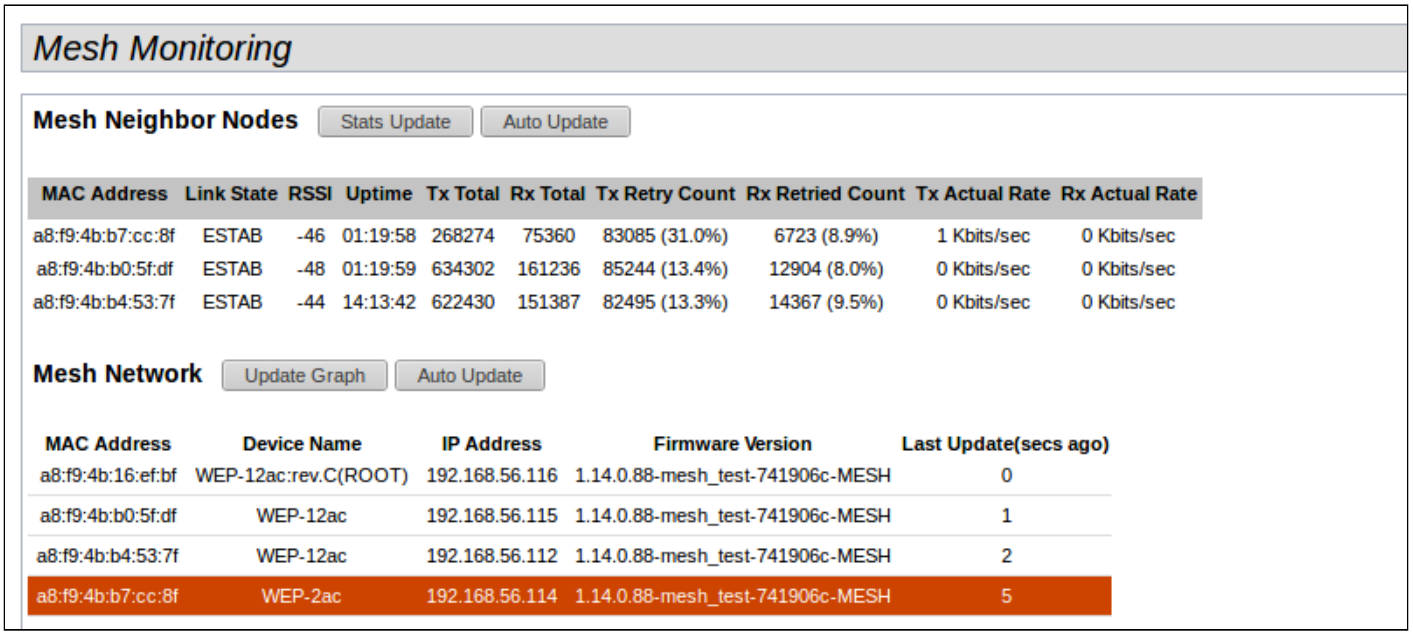
- *Access, если точку необходимо добавить в "белый" список,*
- *Block для добавления точки в "черный" список.*

Нажмите кнопку «Update» для сохранения внесенных изменений.

5.19 Подменю «Mesh Monitoring»*

В разделе "**Mesh Monitoring**" отображается статистика и состояние соединений в Mesh-сети.

* Подменю доступно, если на точке доступа установлено ПО с поддержкой Mesh (WOP-2ac-1.14.0.X-MESH.tar.gz и более поздние версии).



MAC Address	Link State	RSSI	Uptime	Tx Total	Rx Total	Tx Retry Count	Rx Retried Count	Tx Actual Rate	Rx Actual Rate
a8:f9:4b:b7:cc:8f	ESTAB	-46	01:19:58	268274	75360	83085 (31.0%)	6723 (8.9%)	1 Kbits/sec	0 Kbits/sec
a8:f9:4b:b0:5f:df	ESTAB	-48	01:19:59	634302	161236	85244 (13.4%)	12904 (8.0%)	0 Kbits/sec	0 Kbits/sec
a8:f9:4b:b4:53:7f	ESTAB	-44	14:13:42	622430	151387	82495 (13.3%)	14367 (9.5%)	0 Kbits/sec	0 Kbits/sec

MAC Address	Device Name	IP Address	Firmware Version	Last Update(secs ago)
a8:f9:4b:16:ef:bf	WEP-12ac:rev.C(ROOT)	192.168.56.116	1.14.0.88-mesh_test-741906c-MESH	0
a8:f9:4b:b0:5f:df	WEP-12ac	192.168.56.115	1.14.0.88-mesh_test-741906c-MESH	1
a8:f9:4b:b4:53:7f	WEP-12ac	192.168.56.112	1.14.0.88-mesh_test-741906c-MESH	2
a8:f9:4b:b7:cc:8f	WEP-2ac	192.168.56.114	1.14.0.88-mesh_test-741906c-MESH	5

Mesh Neighbor Nodes – в разделе отображается таблица со статистикой соединений с соседними точками доступа.

Stats Update – при нажатии на кнопку произойдет обновление статистики в таблице;

Auto update – автоматическое обновление таблицы (данные обновляются раз в секунду);

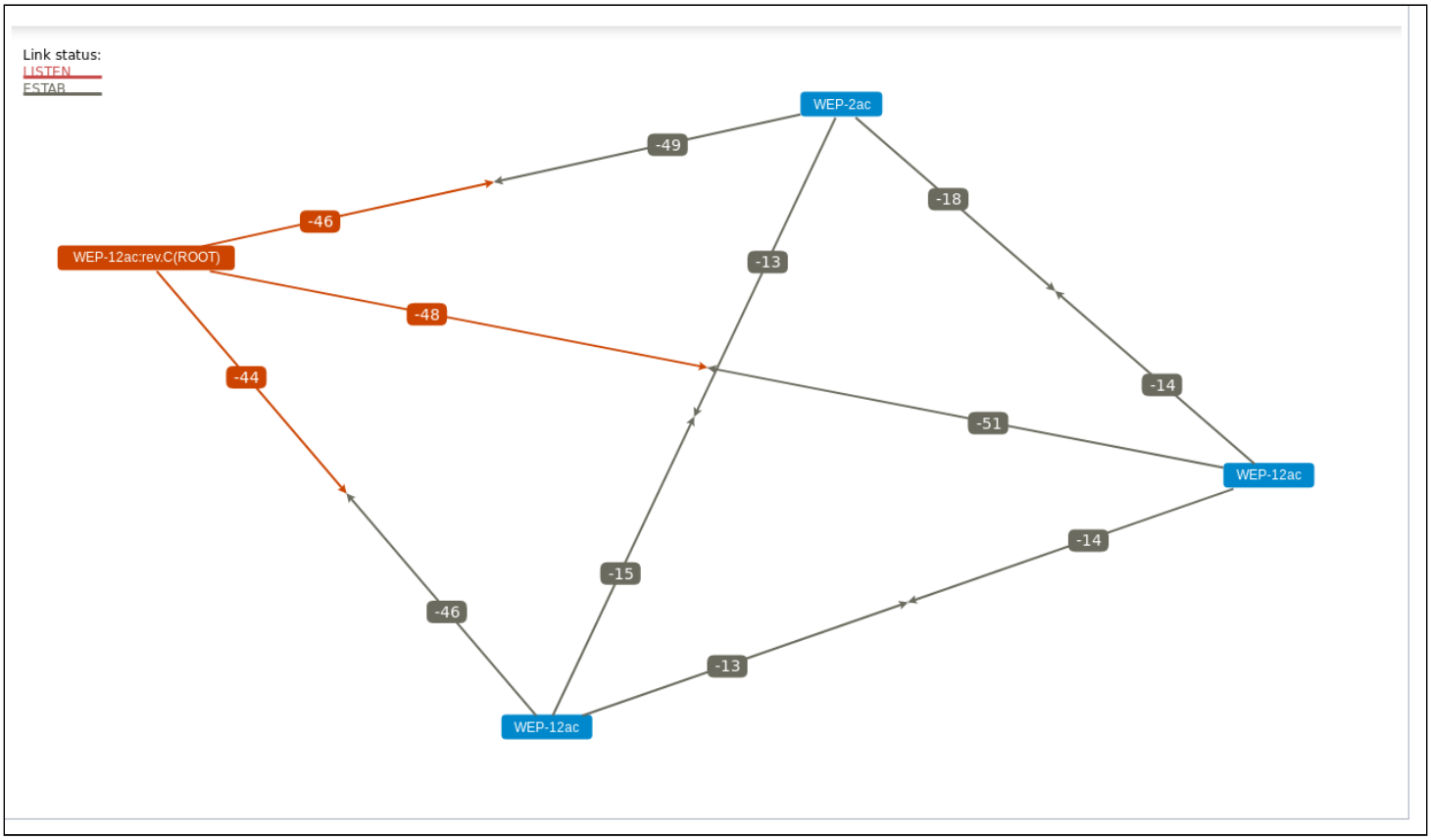
- *MAC Address* – MAC-адрес Mesh-интерфейса соседней точки доступа;
- *Link State* – состояние соединения;
- *RSSI* – уровень сигнала от соседней точки доступа;
- *Uptime* – продолжительность соединения с точкой доступа;
- *Tx Total* – количество успешно отправленных пакетов;
- *Rx Total* – количество успешно принятых пакетов;
- *Tx Retry Count* – количество повторно отправленных пакетов;
- *Rx Retried Count* – количество принятых пакетов, отправленных повторно;
- *Tx Actual Rate* – текущая скорость передачи данных, в кбит/с;
- *Rx Actual Rate* – текущая скорость приема данных, в кбит/с.

Mesh Network – в разделе отображается таблица с информацией об участниках Mesh-сети.

> ⓘ Отображается только на устройстве, являющимся контроллером Mesh-сети (Root AP).

- *Update Graph* – при нажатии на кнопку произойдет обновление информации в таблице и графе;
- *Auto update* – автоматическое обновление таблицы и графа (данные обновляются каждые 10 секунд);
- *Mac Address* – MAC-адрес Mesh-интерфейса участника сети;
- *Device Name* – системное имя устройства;
- *IP Address* – IP-адрес устройства;
- *Firmware Version* – версия программного обеспечения;
- *Last Update* – время последней синхронизации с устройством.

Также в разделе мониторинга располагается граф с построенной схемой Mesh-сети. На основании таблицы и графа можно произвести анализ сети. Это позволит оценить правильность расположения точек доступа по территории покрытия и укажет на проблемные места, а также поможет производить мониторинг сети в режиме реального времени.

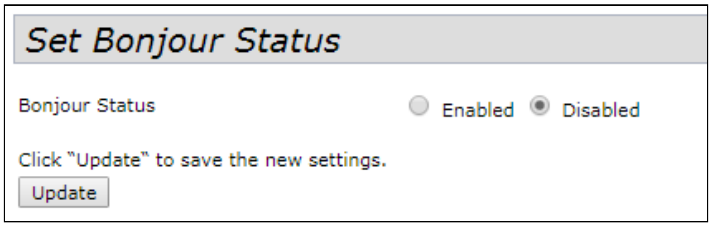

Link status:
LISTEN
ESTAB
WEP-2ac
-49
-18
-46
WEP-12ac:rev.C(ROOT)
-13
-48
-44
-14
-51
WEP-12ac
-14
-15
-46
-13
WEP-12ac

6 Меню «Services»

В меню «Services» выполняется настройка встроенных служб точки доступа.

6.1 Подменю «Bonjour»

В разделе «Bonjour» выполняется настройка услуги Bonjour, которая позволяет беспроводным точкам доступа и их сервисам обнаруживать друг друга внутри локальной сети, используя записи в multicast Domain Name System (mDNS).

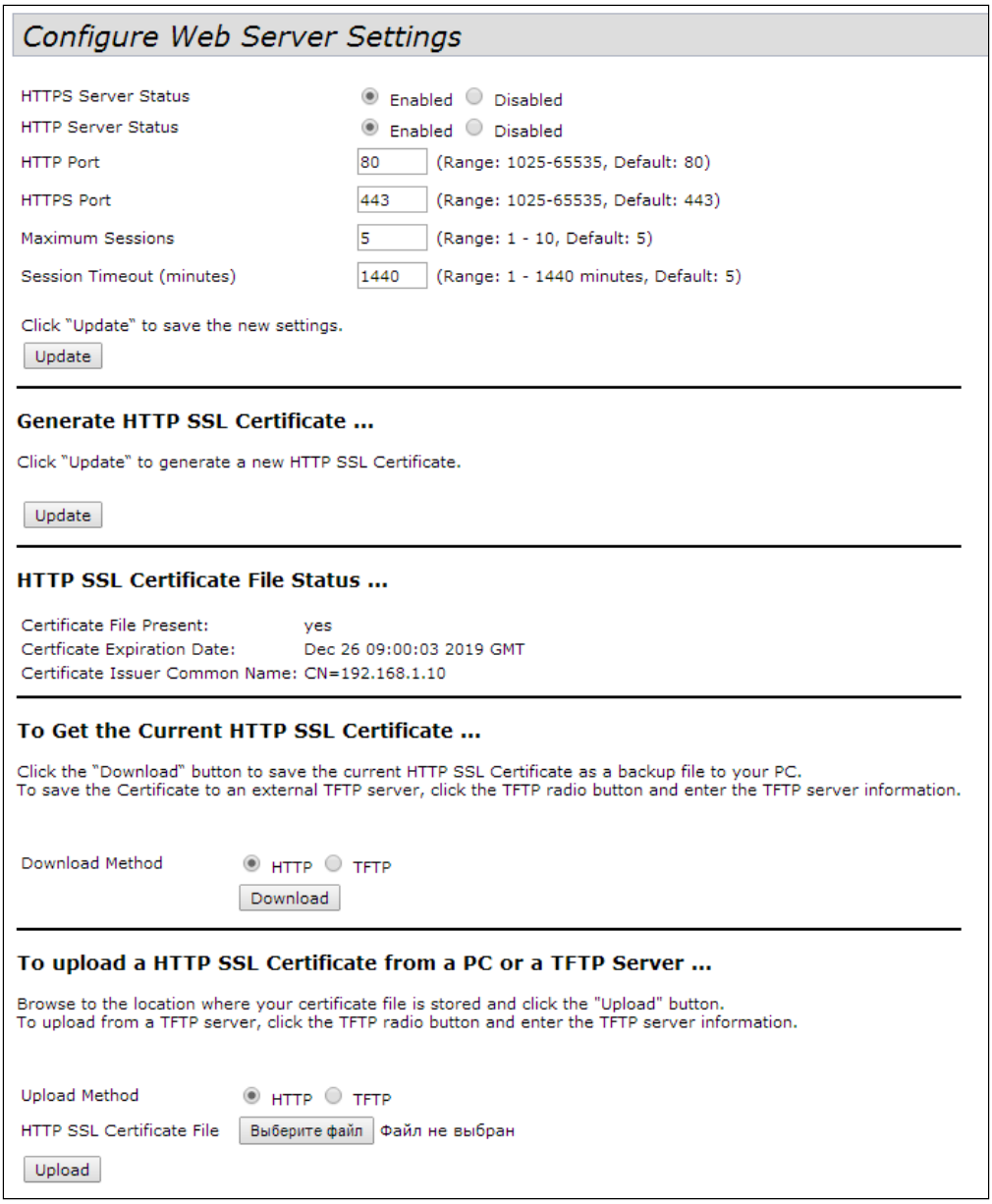


- *Bonjour Status* – состояние услуги Bonjour:
  - *Enabled* – при установленном флаге услуга активна;
  - *Disabled* – при установленном флаге услуга выключена.

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.2 Подменю «Web Server»

В разделе «Web Serves» выполняются настройки доступа к точке доступа через web-интерфейс.



- *HTTPS Server Status* – состояние сервера HTTPS:
  - *Enabled* – при установленном флаге подключение к Web-интерфейсу устройства будет по защищенному протоколу HTTP (HTTPS);
  - *Disabled* – при установленном флаге подключение к Web-интерфейсу устройства не доступно по протоколу HTTPS;
- *HTTP Server Status* – состояние сервера HTTP, этот параметр не зависит от состояния настроек параметра «HTTPS Server Status»:
  - *Enabled* – при установленном флаге подключение к Web-интерфейсу устройства будет разрешено по протоколу HTTP;
  - *Disabled* – при установленном флаге подключение к Web-интерфейсу устройства не доступно по протоколу HTTP;
- *HTTP Port* – номер порта для передачи HTTP-трафика, принимает значения 1025-65535. По умолчанию установлено 80;
- *HTTPS Port* – номер порта для передачи HTTPS-трафика, принимает значения 1025-65535. По умолчанию установлено 443;

- *Maximum Sessions* – количество Web-сессий, включая HTTP и HTTPs, которые могут быть одновременно запущенны, принимает значения 1-10 сессий. По умолчанию установлено 5;
- *Session Timeout (minutes)* – период времени, по истечении которого система автоматически выполнит выход из Web -интерфейса, если пользователь не был активен. Принимает значения (1-1440). По умолчанию 60 минут.

Нажмите кнопку «Update» для сохранения внесенных изменений.

Generate HTTP SSL Certificate – в данном разделе при нажатии на кнопку «Update» выполняется генерация нового HTTP SSL сертификата для безопасного доступа к Web-серверу. Это нужно выполнить при получении IP-адреса, чтобы имя сертификата совпадало с IP-адресом устройства. При создании нового сертификата будет запущен web-сервер безопасности. Защищенное соединение не будет функционировать, пока новый сертификат не будет применен в браузере.

HTTP SSL Certificate File Status – в данном разделе приводится информация о HTTP SSL сертификате:

- *Certificate FilePresent* – указывает, присутствует ли сертификат SSL HTTP;
- *Certificate Expiration Date* – дата, до которой сертификат действителен;
- Certificate IssuerCommon Name – имя сертификата.

To Get the Current HTTP SSL Certificate – в данном разделе выполняется сохранение текущего HTTP SSL сертификата, который в дальнейшем может быть использован как backup-файл:

- *Download Method* – метод сохранения HTTP SSL сертификата:
    - *HTTP* – файл будет сохранен по HTTP на компьютер;
    - *TFTP* – сертификат будет сохранен на TFTP-сервере, при указании этого способа нужно заполнить следующие поля:
        - *HTTP SSL Certificate File* – имя файла сертификата, задается строка до 256 символов, по умолчанию установлено Mini_httpd.pem;
        - *Server IP* – IPv4 или IPv6-адрес TFTP-сервера, который будет использоваться для загрузки файл. По умолчанию установлено 0.0.0.0.

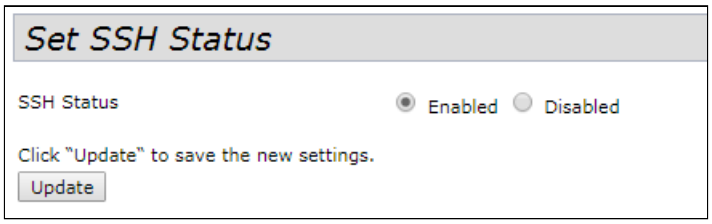
Нажмите кнопку «Download» для сохранения файла HTTP SSL сертификата.

To upload a HTTP SSL Certificate from a PC or a TFTP Server – в разделе выполняется загрузка файла HTTP SSL Certificate:

- *Upload Method* – метод загрузки файла HTTP SSL сертификата:
    - *HTTP* – по HTTP, при указании этого способа нажмите кнопку «Выберите файл», укажите файл, который нужно загрузить в устройство и нажмите кнопку «Upload»;
    - *TFTP* – через TFTP-сервер, при указании этого способа нужно заполнить следующие поля: HTTP SSL Certificate File; Server IP и нажать кнопку «Upload». Описание полей приведено выше.

6.3 Подменю «SSH»

В разделе «SSH» выполняется настройка доступа к устройству по протоколу SSH.
SSH – безопасный протокол удаленного управления устройствами. В отличие от Telnet протокол SSH шифрует весь трафик, включая передаваемые пароли.



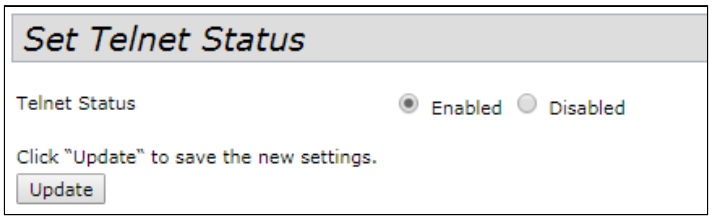
- *SSH Status* – состояние доступа к устройству по протоколу SSH:
  - *Enabled* – при установленном флаге доступ разрешен;
  - *Disabled* – при установленном флаге доступ запрещен.

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.4 Подменю «Telnet»

В разделе «Telnet» выполняется настройка доступа к устройству по протоколу Telnet.

Telnet – протокол, предназначенный для организации управления по сети. Позволяет удаленно подключиться к шлюзу с компьютера для настройки и управления.



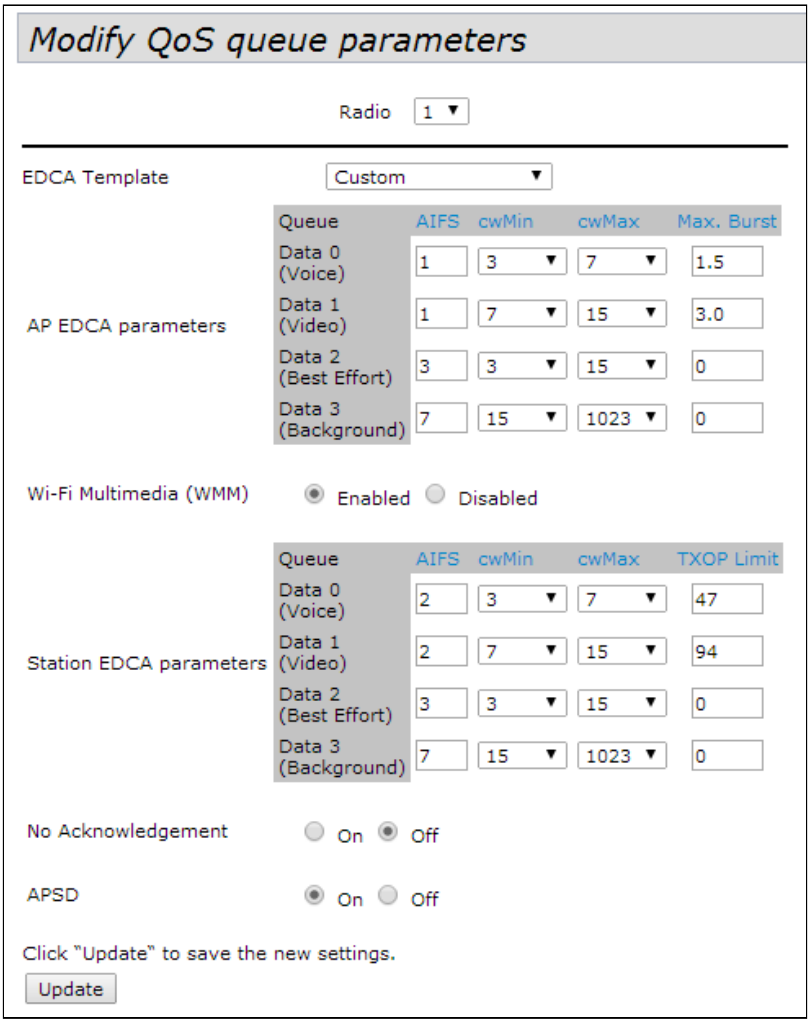
- *Telnet Status* – состояние доступа к устройству по протоколу Telnet:
  - *Enabled* – при установленном флаге доступ разрешен;
  - *Disabled* – при установленном флаге доступ запрещен.

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.5 Подменю «QoS»

В подменю «QoS» настраиваются функции обеспечения качества обслуживания (Quality of Service). Настройка параметров QoS выполняется для каждого радиоинтерфейса.

QoS используется для обеспечения минимальных задержек в передаче данных таких сервисов, как передача голоса по IP (VoIP), видео в режиме реального времени и других сервисов, чувствительных ко времени передачи данных.



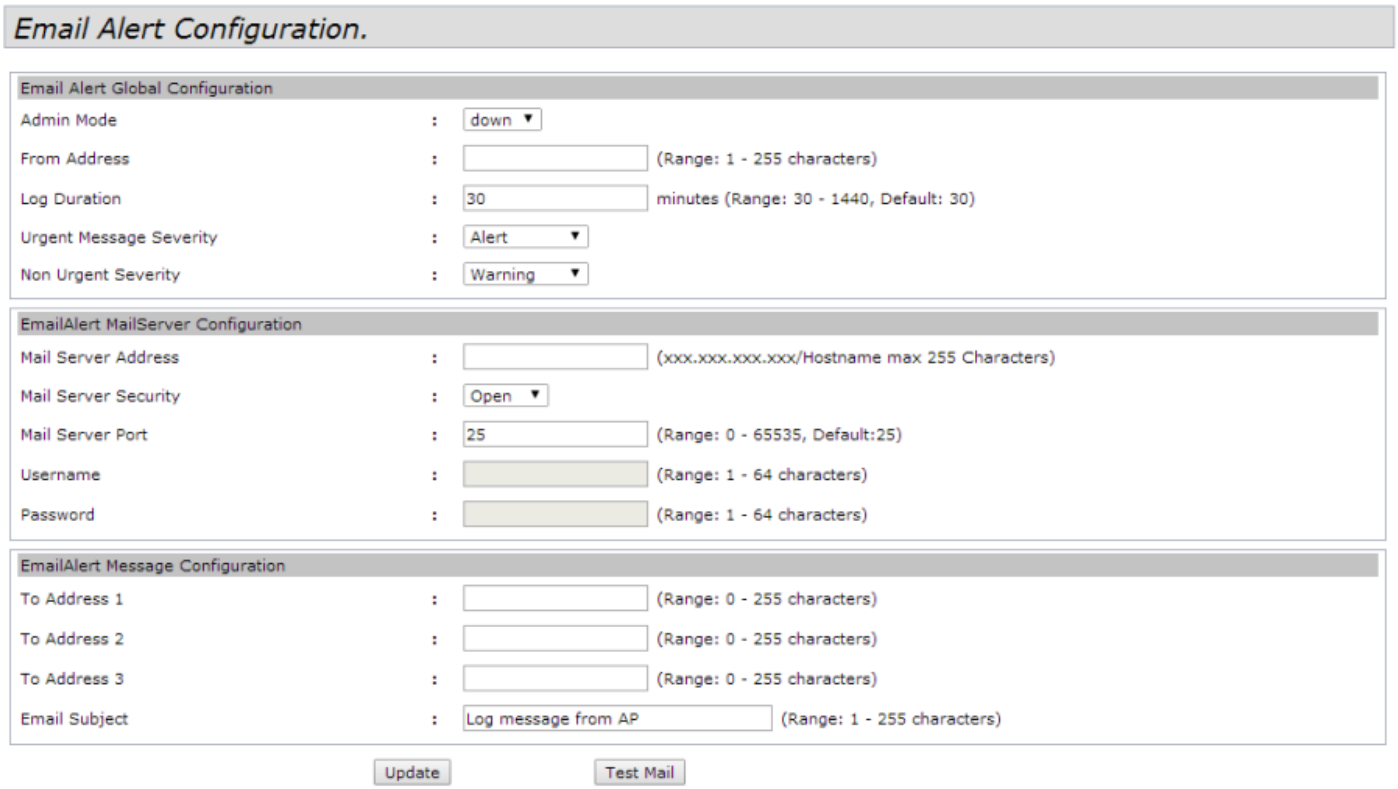
- *Radio* – радиоинтерфейс, для которого будут выполняться настройки параметров QoS;
- *EDCA Template* – шаблон с предопределенными параметрами EDCA:
  - *Default* – настройки по умолчанию;
  - *Optimized for Voice* – оптимальные настройки для передачи голоса;
  - *Custom* – пользовательские настройки;
- *AP EDCA parameters* – таблица настроек параметров точки доступа (трафик передается от точки доступа к клиенту):
  - *Queue* – предопределенные очереди для различного рода трафика:
    - *Data 0 (Voice)* – высокоприоритетная очередь, минимальные задержки. В данной очереди автоматически обрабатываются данные, чувствительные к времени, такие как: VoIP, потоковое видео;
    - *Data 1 (Video)* – высокоприоритетная очередь, минимальные задержки. В данной очереди автоматически обрабатываются видеоданные, чувствительные к времени;
    - *Data 2 (best effort)* – среднеприоритетная очередь, средняя пропускная способность и задержка. В данную очередь отправляется большинство традиционных IP-данных;
    - *Data 3 (Background)* – низкоприоритетная очередь, высокая пропускная способность.
  - *AIFS* (Arbitration Inter-Frame Spacing) – определяет время ожидания кадров (фреймов) данных, измеряется в слотах, принимает значения (1-15);
  - *cwMin* – начальное значение времени ожидания перед повторной отправкой кадра, задается в миллисекундах, принимает значения 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. Значение cwMin не может превышать значение cwMax;
  - *cwMax* – максимальное значение времени ожидания перед повторной отправкой кадра, задается в миллисекундах, принимает значения 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. Значение cwMax должно быть больше значения cwMin;

    - *Max. Burst Length* – параметр используется только для данных, передаваемых от точки доступа до станции клиента. Максимальная длина пакета, разрешенная для очередей в беспроводной сети, принимает значения 0-999;
- *Wi-Fi MultiMedia (WMM)* – состояние работы функции WiFi Multimedia, которая позволяет оптимизировать передачу мультимедийного трафика по беспроводной среде:
    - *Enable* – функция включена;
    - *Disable* – функция выключена;
- *Station EDCA parameters* – таблица настроек параметров станции клиента (трафик передается от станции клиента до точки доступа):
    - Описание параметров *Queue, AIFS, cwMin, cwMax* приведено выше;
    - *TXOP Limit* – параметр используется только для данных, передаваемых от станции клиента до точки доступа. Возможность передачи – интервал времени, в миллисекундах, когда клиентская WME-станция имеет права инициировать передачу данных по беспроводной среде к точке доступа, максимальное значение 65535 миллисекунд;
- *No Acknowledgement* – при установленном флаге «On» точка доступа не должна признавать кадры QosNoAck как значение класса обслуживания;
- *APSD* – при установленном флаге «On» будет включен режим экономии энергии доставки APSD, который является методом управления питания. Данный режим рекомендуется, если для VoIP-телефонов доступ к сети предоставляется через точку доступа.

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.6 Подменю «Email Alert»

В разделе «Email Alert» выполняется настройка отсылки сервисной информации по электронной почте (Email).



В разделе «**Email Alert Global Configuration**» задаются глобальные настройки для функции отправки Email-сообщений.

- *Admin Mode* – состояние функции отправки Email-сообщений на точке доступа:
  - *Up* – функция включена;
  - *Down* – функция отключена;
- *From Address* – почтовый адрес отправителя, например, AP23@foo.com. Задается строка до 255 символов;
- *Log Duration* – интервалы времени отправки некритичных сообщений, принимает значения 30-1440. По умолчанию – 30;
- *Urgent Message Severity* – уровень важности сообщений, которые будут отправлены немедленно;
- *Non Urgent Severity* – уровень важности сообщений, которые будут оправлены в интервалах «Log Duration.

В разделе «**EmailAlert MailServer Configuration**» выполняется настройка параметров почтового сервера и клиента.

- *Mail Server Address* – адрес почтового сервера, задается строка вида XXX.XXX.XXX.XXX;
- *Mail Server Security* – протокол аутентификации на почтовом сервере: Open, TLSv1. По умолчанию – Open;
- *Mail Server Port* – номер порта почтового сервера, принимает значения 0-65535. По умолчанию установлено – 25;
- *Username* – имя почтового клиента, задается строка до 64 символов;
- Password – пароль почтового клиента, задается строка до 64 символов.

В разделе «**EmailAlert Message Configuration**» выполняется настройка параметров аварийного сообщения:

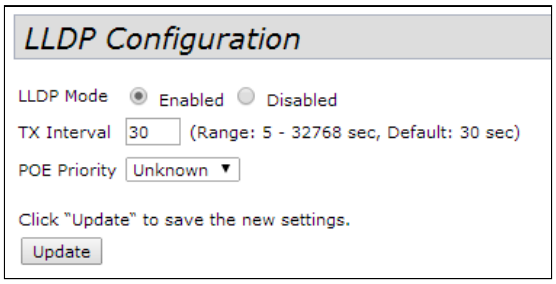
- *To Address 1* – адрес первого получателя сообщений;
- *To Address 2* – адрес второго получателя сообщений;
- *To Address 3* – адрес третьего получателя сообщений;
- *Email Subject* – текст в теме письма.

Нажмите кнопку «Update» для сохранения внесенных изменений.

Для отправки тестового сообщения нажмите кнопку «Test Mail».

6.7 Подменю «LLDP»

В разделе «LLDP» выполняется настройка работы протокола LLDP (Link Layer Discovery Protocol).

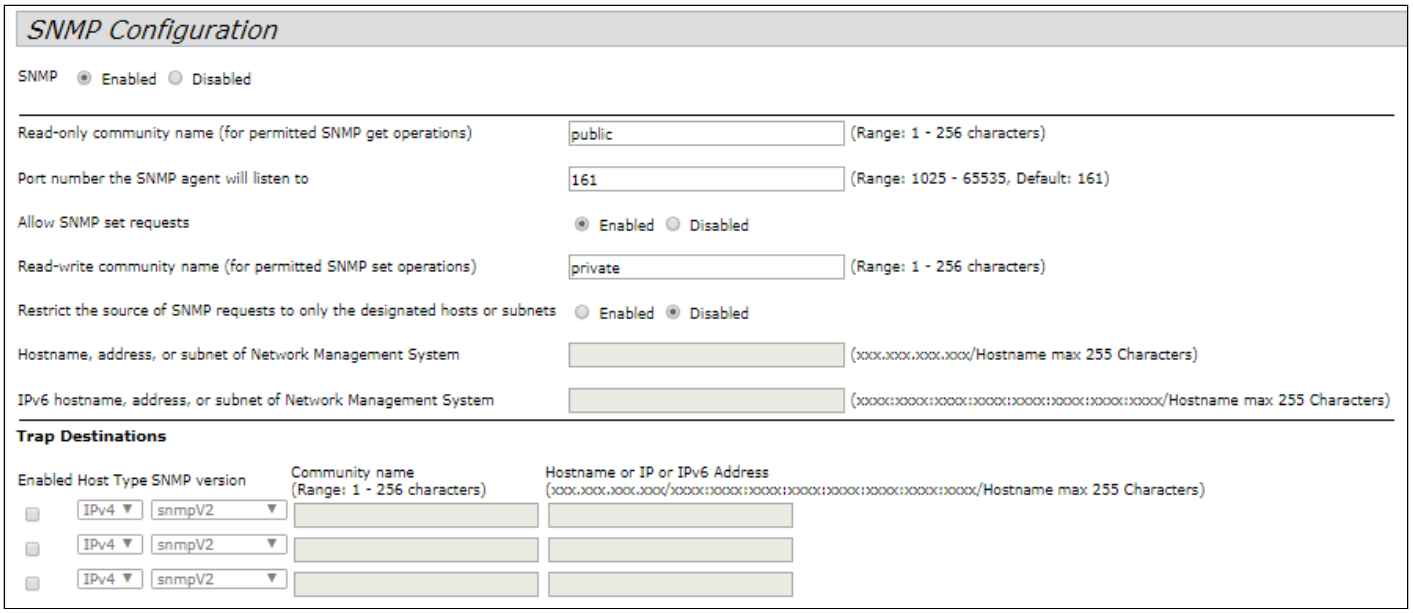


- *LLDP Mode* – состояние работы протокола LLDP:
  - *Enabled* – при установленном флаге LLDP активен;
  - *Disabled* – при установленном флаге LLDP выключен;
- *TX Interval* – интервал посылки LLDP-сообщений, принимает значения 5-32768. По умолчанию установлено – 30 секунд;
- *POE Priority* – приоритет, пересылаемый в поле «Extended Power Information».

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.8 Подменю «SNMP»

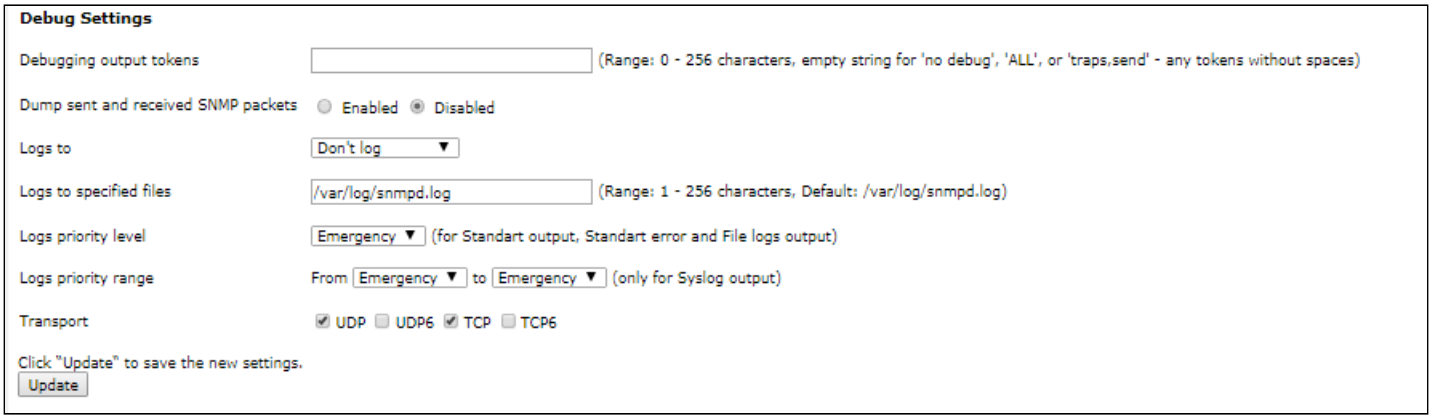
В разделе «SNMP» выполняется настройка управления устройством по SNMP.



- *SNMP* – включение/выключение управления устройством по SNMP:
  - *Enabled* – при установленном флаге SNMP активен;
  - *Disabled* – при установленном флаге SNMP выключен;
- *Read-only community name* – пароль для read-only запросов, задается строка до 256 символов;
- *Port number the SNMP agent will listen to* – номер порта приема/отправки SNMP-сообщений, принимает значения 1025-65535, по умолчанию 161;
- *Allow SNMP set requests* – разрешить/запретить конфигурирование устройства по SNMP:
  - *Enabled* – разрешить конфигурирование устройства по SNMP;
  - *Disabled* – запретить конфигурирование устройства по SNMP;
- *Read-write community name* – пароль для read-write запросов, задается строка до 256 символов;
- *Restrict the source of SNMP requests to only the designated hosts or subnets* – принимать SNMP запросы только с указанных адресов, задается IP-адрес в виде XXX.XXX.XXX.XXX или имя хоста;
- *Hostname, address, or subnet of Network Management System* – имя, адрес или подсеть IPv4, из которой разрешено принимать SNMP-запросы;
- *IPv6 hostname, address, or subnet of Network Management System* – имя, адрес или подсеть IPv6, из которой разрешено принимать SNMP-запросы;
- *Community name* – строка, ассоциированная с передающимися трапами;
- *Enabled Host Type SNMP version* – сопоставление адресов получателей SNMP-трапов с версиями SNMP-трапов, а также версией IP-протокола.

Нажмите кнопку «Update» для сохранения внесенных изменений.

В подразделе "**Debug Settings**" выполняется настройка отправки отладочных сообщений.

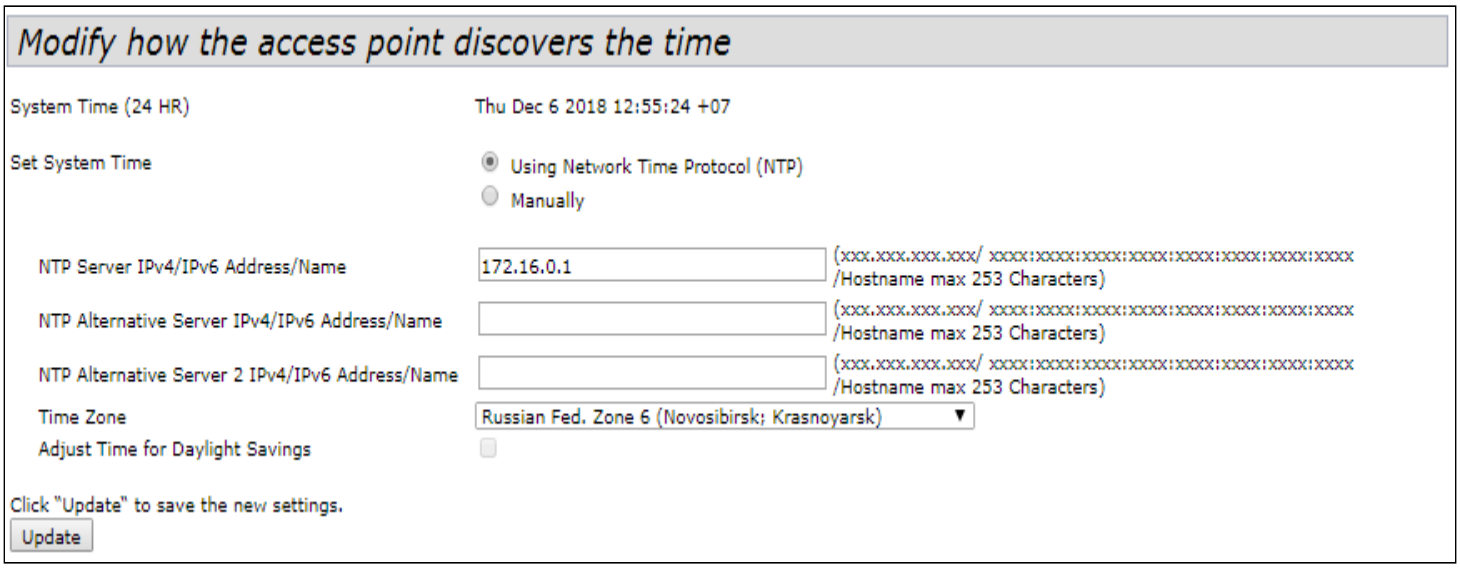


- *Debugging output tokens* – идентификатор группы отладочных сообщений;
- *Dump sent and received SNMP packets* – вывод в лог содержимого принимаемых и передаваемых SNMP-сообщений;
- *Logs to* – указание места вывода лога:
  - *Don't log* – не выводить лог;
  - Standart error, standart output – вывод в консоль;
  - File – вывод в файл;
  - Syslog – Syslog-вывод;
- *Logs to specified files* – указание файла для вывода лога;
- *Logs priority level* – выбор уровня выводимых логов, указывается при выводе лога в консоль или файл;
- *Logs priority range* – указание диапазона уровней логов для Syslog-вывода;
- *Transport* – транспортный протокол, используемый для передачи SNMP-сообщений.

Нажмите кнопку «Update» для сохранения внесенных изменений.

6.9 Подменю «Time Settings (NTP)»

В разделе «Time Settings (NTP)» выполняется настройка локального времени устройства.



- *System Time* – текущее системное время;
- *Set System Time* – выбор способа установки времени:
  - *UsingNetworkTimeProtocol (NTP)* – автоматическая установка с помощью NTP-протокола.
  - *Manually* – ручная установка времени.

Автоматическая установка с помощью NTP-протокола (выбрано UsingNetworkTimeProtocol (NTP)):

- *NTP Server IPv4/IPv6 Address/Name* – IPv4-адрес, IPv6-адрес или имя хоста NTP-сервера. Если не указать сервер – будет использоваться имя сервера полученного в опции DHCP;
- *NTP Alternative Server IPv4/IPv6 Address/Name* и *NTP Alternative Server 2 IPv4/IPv6 Address/Name* – укажите IPv4-адреса, IPv6-адреса или имена хостов дополнительных NTP-серверов. Если не указать сервер – будет использоваться имя сервера полученного в опции DHCP;

Ручная установка времени (выбрано Manually):

- *System Date* – установка даты;
- *System Time (24 HR)* – установка времени системы в 24-часовом формате;

- *Time Zone* – временная зона, по умолчанию установлено – Russia(Moscow);
- *Adjust Time for Daylight Savings* – при установленном флаге выполняется автоматический переход на летнее время (DST). При выставленном флаге, будут доступны следующие поля:
  - DST Start (24 HR) – установить время перехода на зимнее время;
  - DST End (24 HR) – установить время перехода на летнее время;
  - DST Offset (minutes) – установить разницу во времени (в минутах).

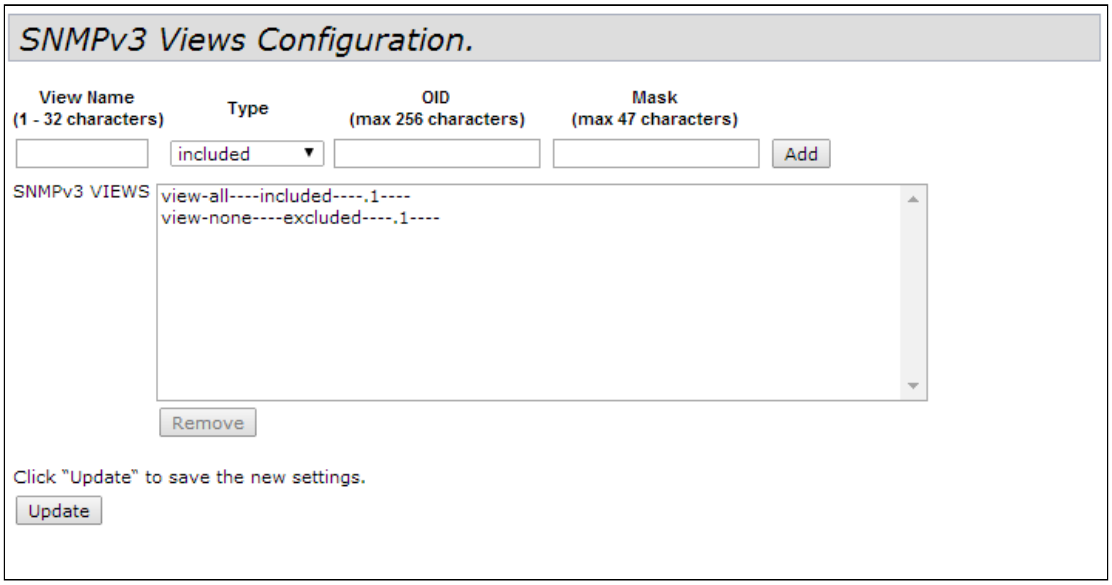
Нажмите кнопку «Update» для сохранения внесенных изменений.

7 Меню «SNMPv3»

Меню «SNMPv3» предназначено для конфигурирования прав взаимодействия с функционалом устройства при помощи протокола SNMPv3.

7.1 Подменю «SNMPv3 Views»

В подменю «SNMPv3 Views» формируется описание дерева или поддерева OID, а также включение или исключение поддерева из обзора.

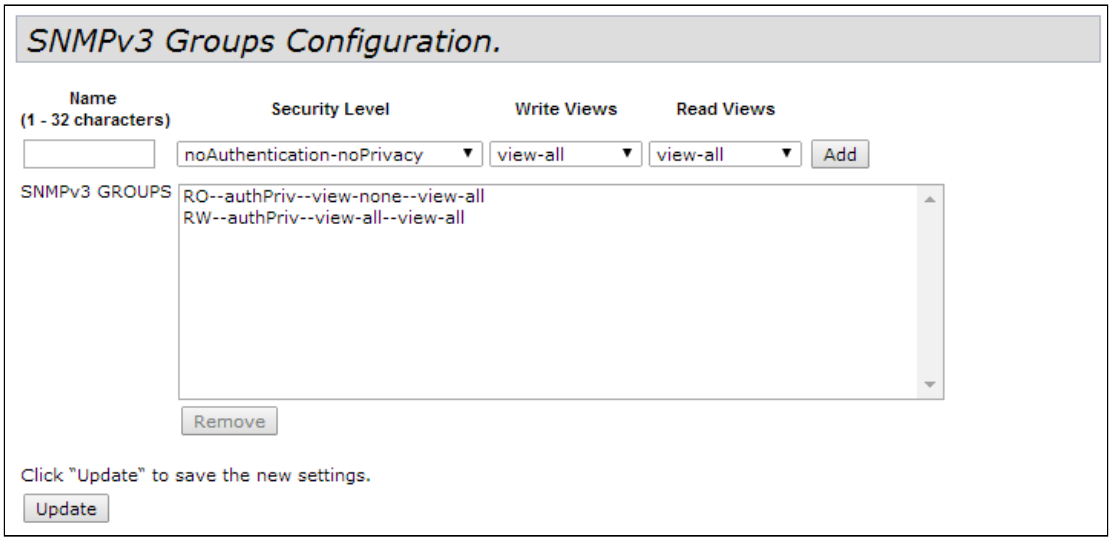


- *View Name* – имя дерева или поддерева MIB, задается строка до 32 символов;
- *Type* – включить или исключить поддерево MIB из обзора:
  - include – включить;
  - excluded – исключить;
- *OID* – строка OID, описывающая поддерево, включаемое или исключаемое из обзора, задается строка до 256 символов;
- *Mask* – маска, задается в формате xx.xx.xx(.).. размером не более 47 символов, используется для формирования необходимого поддерева в рамках указанного OID;
- *SNMPv3 VIEWS* – список существующих правил.

Для добавления правила нажмите кнопку «Add».
Для удаления правила в поле «SNMPv3 VIEWS» выберите запись и нажмите кнопку «Remove».
Нажмите кнопку «Update» для применения и сохранения внесенных изменений.

7.2 Подменю «SNMPv3 Groups»

В подменю «SNMPv3 Groups» выполняется формирование групп с различными уровнями безопасности, примененными к правилам обзора деревьев и поддеревьев.

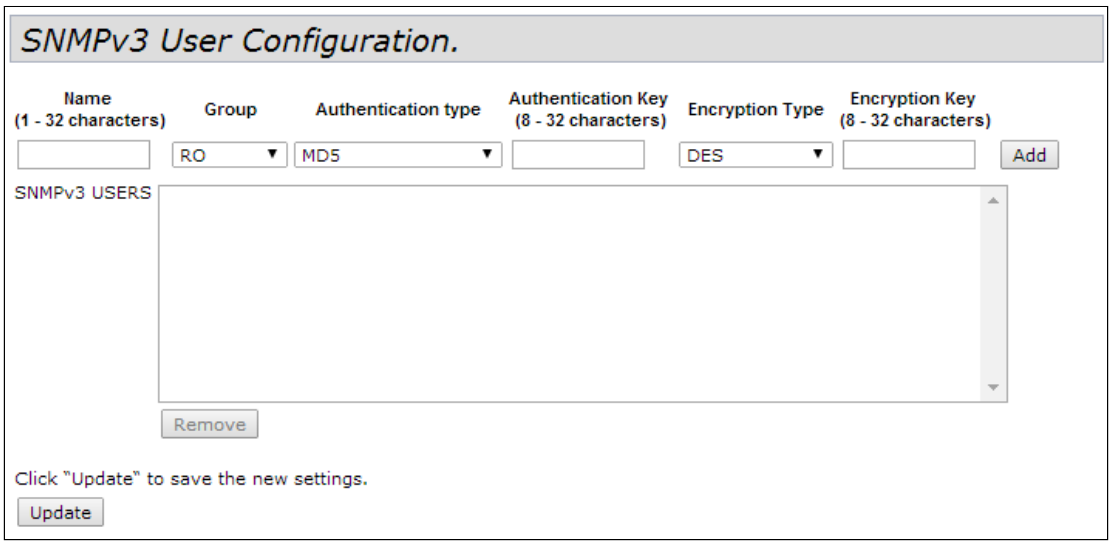


- *Name* – имя группы, задается строка до 32 символов;
- *Sequrity Level* – уровень безопасности для группы:
  - *noAuthentication-noPrivacy* – не используется аутентификация и шифрование данных;
  - *Authentication-noPrivacy* – используется аутентификация, но не используется шифрование данных. При отправке SNMP-сообщений для аутентификации используется MD5 ключ и пароль;
  - *Authentication-Privacy* – используется аутентификация и шифрование данных. При отправке SNMP-сообщений для аутентификации используется MD5 ключ/пароль, для шифрования данных используется DES ключ/пароль;
- *Write Views* – выбор дерева/поддерева OID, доступного для записи:
  - *write-all* – группа может создавать, изменять и удалять базы MIB;
  - *write-none* – группе не разрешено создавать, изменять и удалять базы MIB;
- *Read Views* - выбор дерева/поддерева OID, доступного для чтения:
  - *write-all* – группе разрешен просмотр и чтение всех MIB файлов;
  - *write-none* – группе не разрешен просмотр и чтение MIB файлов;
- *SNMPv3 GROUPS* – список существующих групп.

Для добавления группы нажмите кнопку «Add».
Для удаления группы в поле «SNMPv3 GROUPS» выберите запись и нажмите кнопку «Remove».
Нажмите кнопку «Update» для применения и сохранения внесенных изменений.

7.3 Подменю «SNMPv3 Users»

В подменю «SNMPv3 Users» происходит создание пользователей и параметров их доступа, работающих с устройством по протоколу SNMPv3.



- *Name* – имя пользователя, задается строка до 32 символов;
- *Group* – группа, созданная в подменю «SNMPv3 Groups»;
- *Authentication type* – тип аутентификации для использования SNMP-запросов:
  - *MD5* – требовать проверку подлинности по алгоритму MD5 для SNMPv3-запросов пользователя;
  - *None* – при передачи SNMPv3-запросов от данного пользователя не требуется аутентификация;
- *Authentication Key* – ключ аутентификации, задается строка от 8 до 32 символов. Используется, если в поле «Authentication type» выбрать значение «MD5»;
- *Encryption Type* – тип шифрования:
  - *DES* – использовать алгоритм шифрования DES для SNMPv3-запросов пользователя;
  - *None* – при передачи SNMPv3-запросов от данного пользователя шифрование не требуется;
- *Encryption Key* – ключ шифрования, задается строка от 8 до 32 символов. Используется, если в поле «Encryption Type» выбрать значение «DES».

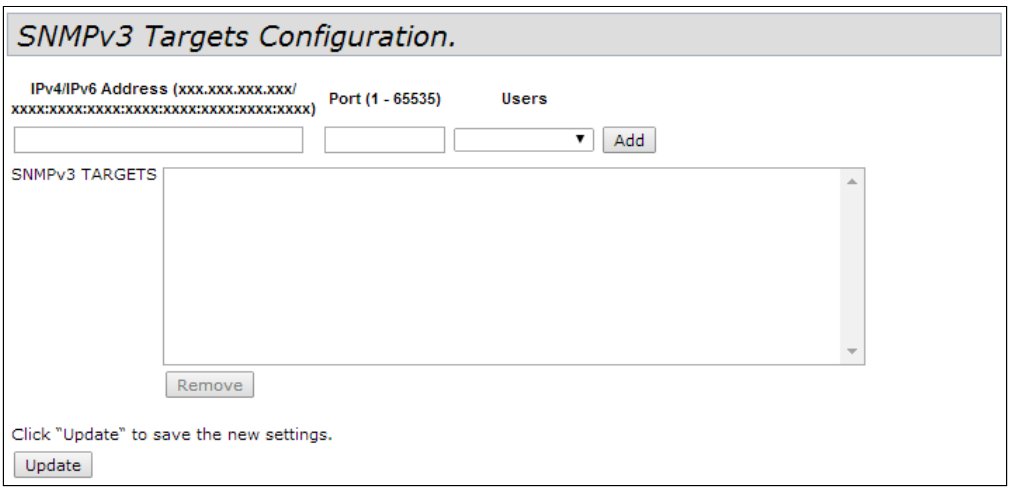
Для добавления пользователя нажмите кнопку «Add».

Для удаления пользователя в поле «SNMPv3 USERS» выберите запись и нажмите кнопку «Remove».

Нажмите кнопку «Update» для применения и сохранения внесенных изменений.

7.4 Подменю «SNMPv3 Targets»

В подменю «SNMPv3 Targets» выполняется настройка трапов от устройства на определенный IP-адрес, порт UDP и пользователя.



- *IPv4/IPv6 Address* – адрес IPv4 или IPv6, на который будут отправлены трапы;
- *Port* – порт UDP, на который будут отправлены трапы, принимает значения 1-65535;
- *Users* – имя пользователя, которому будут отправлены трапы.

Для добавления правила отправки трапов нажмите кнопку «Add».

Для удаления правила отправки трапов в поле «SNMPv3 TARGETS» выберите запись и нажмите кнопку «Remove».

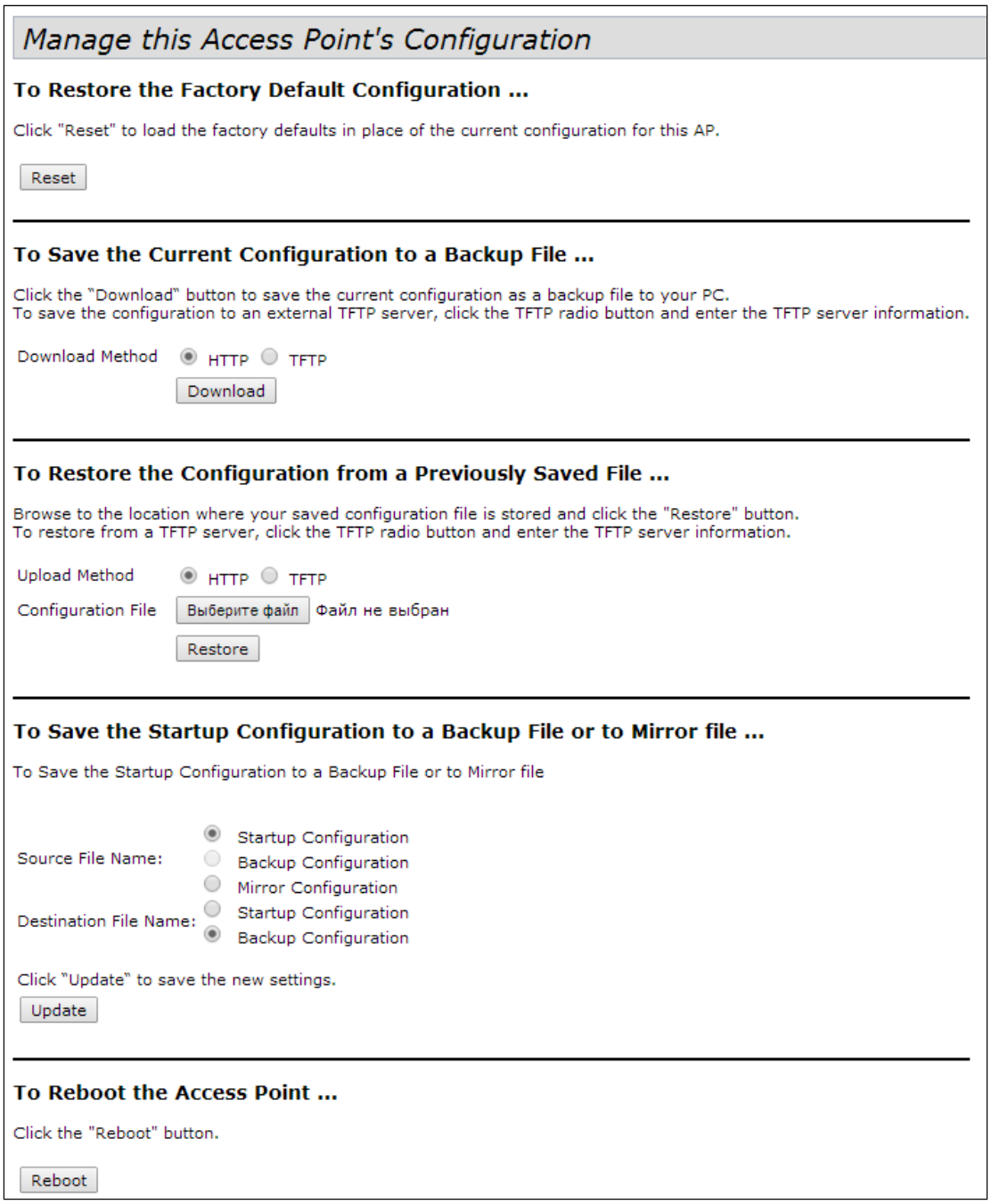
Нажмите кнопку «Update» для применения и сохранения внесенных изменений

8 Меню «Maintenance»

Данный раздел Web -интерфейса предназначен для общего управления устройством: выгрузка, загрузка, установка конфигурации по умолчанию, обновление ПО, перезагрузка устройства, а также для операций отладки: сниффинга трафика, проходящего через точку доступа и выгрузка диагностической информации по устройству.

8.1 Подменю «Configuration»

В подменю «Configuration» производится загрузка и выгрузка конфигурации устройства, а также сброс устройства к конфигурации по умолчанию и перезагрузка устройства.



Reset – сброс устройства к заводским настройкам. После сброса устройство автоматически перезагрузится. Это займет несколько минут.

Сброс к заводским настройкам приведет к удалению всей конфигурации устройства, в том числе и IP-адреса для доступа к устройству. После выполнения данной операции возможна потеря связи с устройством.

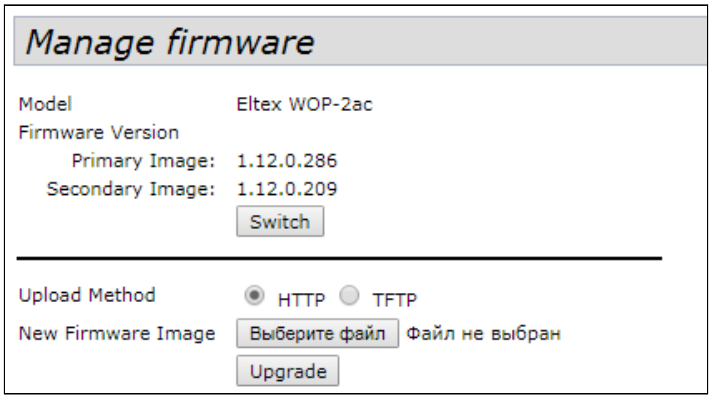
- **Reboot** – программная перезагрузка устройства.Выгрузка текущей конфигурации в backup файл. Выгрузка конфигурации устройства может осуществляться двумя методами: выгрузка через HTTP (на ПК) и выгрузка через TFTP-протокол (на сторонний TFTP-сервер);
  - **Выгрузка через HTTP.** Установите флаг «Download Method» в значение «HTTP». Нажмите «Download» и в диалоговом окне выберите путь для сохранения файла на ПК;
  - **Выгрузка через TFTP.** Установите флаг «Download Method» в значение «TFTP». В поле «Configuration File» укажите имя файла, в котором будет сохранена конфигурация устройства. Имя файла обязательно должно содержать расширение .xml. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором будет сохранен backup-файл. Нажмите «Download» для начала выгрузки файла.
- **Загрузка сохраненной конфигурации в устройство.** Загрузка конфигурации в устройство может осуществляться двумя методами: загрузка через HTTP (с ПК) и загрузка через TFTP-протокол (со стороннего TFTP-сервера).

  При загрузке backup-файла конфигурации в устройстве произойдет применение всех параметров из файла, включая Management VLAN и IP. В случае если будет загружен файл конфигурации другого устройства, то вследствие применения чужого IP или Management VLAN может пропасть связь с устройством.

  - **Загрузка через HTTP.** Установите флаг «Upload Method» в значение HTTP. Нажмите «Выберите файл» и в диалоговом окне выберите путь к сохраненному файлу backup на ПК. Нажмите «Restore» для начала загрузки файла конфигурации в устройство.
  - **Загрузка через TFTP.** Установите флаг «Upload Method» должен быть установлен в значение TFTP. В поле «Filename» укажите имя файла, который будет загружен в устройство. Имя файла обязательно должно содержать расширение .xml. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором сохранен backup-файл. Нажмите «Restore» для начала загрузки файла.
- **Выгрузка текущей конфигурации в backup-файл в энергонезависимую память устройства и загрузка сохраненной конфигурации из энергонезависимой памяти устройства.**
  - **Source File Name** – имя файла источника конфигурации (Startup или Backup).
  - **Destination File Name** – имя файла, в который будет записана выбранная конфигурация.

8.2 Подменю «Upgrade»

В подменю «Upgrade» выполняется обновление и смена ПО устройства. В физической памяти устройства одновременно содержится два образа ПО. Если один из образов устройства вышел из строя, то загрузка будет выполнена с другого образа ПО. Одновременно в устройстве может быть активен только один образ.



- *Model* – модель устройства;
- *Primary Image* – версия ПО активного образа (текущая версия ПО);
- *Secondary Image* – версия ПО резервного образа (не используется в данный момент);
- *Switch* – загрузить ПО устройства с резервного образа. При выполнении данной операции активный образ перейдет в резервное состояние, а резервный – в активное. Устройство автоматически перезагрузится и установит в качестве активного резервное ПО.

Обновление ПО устройства. При обновлении ПО устройства файл прошивки загружается на устройство и становится активным (Primary Image). При этом текущий образ перемещается на позицию «Secondary Image». Автоматически происходит перезагрузка устройства и оно загружается с ПО, которое соответствует загруженному образу.
Загрузка файла ПО на устройство может производиться через HTTP или TFTP-протокол.

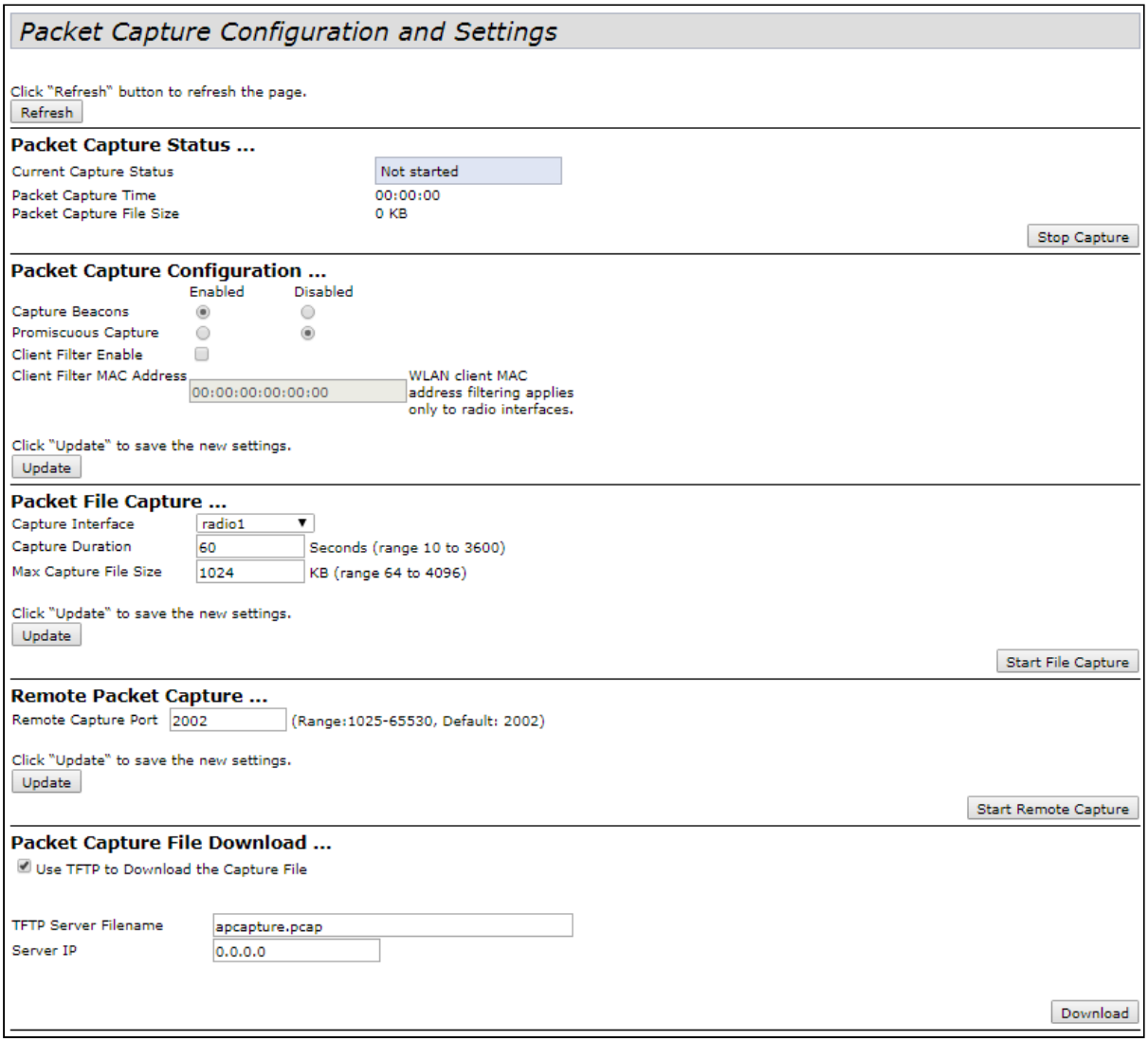
- **Загрузка через HTTP.** Установите флаг «Upload Method» в значение HTTP. Нажмите «Выберите файл» и в диалоговом окне выберите путь к файлу ПО на ПК. Нажмите «Upgrade» для начала загрузки выбранного файла ПО в устройство.

Загрузка через TFTP. Установите флаг «Upload Method» в значение TFTP. В поле «Image Filename» укажите имя файла ПО, который будет загружен в устройство. Имя файла обязательно должно содержать расширение .tar. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором сохранен файл ПО. Нажмите «Upgrade» для начала загрузки файла.

> В процессе обновления ПО устройства не отключайте питание устройства, а также не обновляйте и не меняйте текущую web-страницу с прогресс-баром обновления.

8.3 Подменю «Packet Capture»

В подменю «Packet Capture» реализована возможность формирования и выгрузки дампа трафика с одного из интерфейсов устройства в файл с форматом PCAP. После выбора параметров записи дампа трафика, старта записи, остановки записи и выгрузки файла дамп можно проанализировать специальными программами, например, Wireshark.



Для обновления информации на странице нажмите кнопку «Refresh».

Packet Capture Status – в разделе выполняется просмотр информации и остановка записи дампа трафика.

- *Current Capture Status* – текущий статус записи дампа трафика (запись запущена/остановлена);
- *Packet Capture Time* – время записи дампа трафика;
- *Packet Capture File Size* – размер записанного дампа трафика.

Для остановки записи дампа трафика нажмите кнопку «Stop Capture».

Packet Capture Configuration – в разделе выполняется настройка параметров записи дампа трафика:

- *Capture Beacons* – если установлен флаг в положение «Enabled» - записывать в дамп Beacon-пакеты, если установлен флаг в положение «Disabled» - не записывать;
- *Promiscuous Capture* – записывать в дамп все принимаемые радиоинтерфейсом пакеты, включая пакеты, непредназначенные для данной точки доступа;
- *Client Filter Enable* – записывать в дамп только те пакеты, которые приходят от определенного пользователя;
- *Client Filter MAC Address* – MAC-адрес клиента, трафик которого должен отфильтровываться в дамп.

Нажмите кнопку «Update» для сохранения внесенных изменений.

Packet File Capture – в разделе выполняется настройка параметров запуска записи дампа трафика:

- *Capture Interface* – имя интерфейса устройства, с которого будет производиться запись дампа трафика (eth0 - GE1, eth1 – GE2, wlan0vap1 – виртуальная сеть 1 на беспроводном интерфейсе 0);
- *Capture Duration* – длительность записи дампа (от 10 секунд до 1 часа);
- *Max Capture File Size* – максимальный размер дампа (от 64 до 4096KB);
- *Update* – применение параметров запуска записи трафика;
- *Start File Capture* – запуск записи дампа трафика с установленными параметрами.

Remote Packet Capture – в разделе выполняется удаленная запись дампа трафика:

Устройство поддерживает протокол RPCAP, позволяющий производить запись дампа трафика с интерфейса устройства на удаленной машине в режиме онлайн.

- *Remote Capture Port* – номер порта (от 1025 до 65530), который служит для подключения удаленной машины.

Для применения параметра «Remote Capture Port» нажмите кнопку «Update».

Для старта RPCAP-сервера на устройстве нажмите кнопку «Start Remote Capture».

После старта RPCAP-сервера на удаленной машине нужно подключиться к точке доступа, используя Management IP на порт Remote Capture Port, используя RPCAP-протокол. Например, это можно выполнить с помощью программы Wireshark. Затем, необходимо получить список интерфейсов для сниффинга от устройства, выбрать один из них и запустить снятие дампа с удаленного интерфейса.

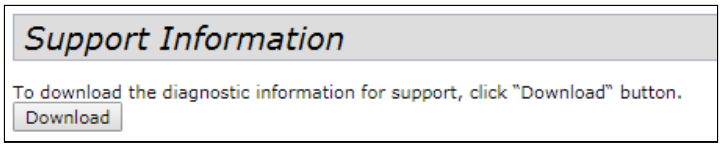
Packet Capture File Download – в разделе выполняется выгрузка записанного дампа трафика:

Выгрузка дампа может производиться через HTTP или TFTP-протокол.

- *Выгрузка через HTTP*. Флаг *«Use TFTP to download the capture file»* должен быть снят. Нажмите «Download» и в диалоговом окне выберите путь для сохранения дампа на ПК;
- *Выгрузка через TFTP. Флаг «Use TFTP to download the capture file»* должен быть установлен. В поле «TFTP Server Filename» укажите имя файла, в котором будет сохранен дамп трафика на TFTP-сервере. Имя файла обязательно должно содержать расширение .pcap. В поле «Server IP» укажите IP-адрес TFTP-сервера, на который будет отправлен дамп трафика. Нажмите «Download» для начала выгрузки дампа.

8.4 Подменю «Support Information»

В подменю «Support Information» выполняется выгрузка из устройства в виде текстового файла всей информации о нем (количество памяти, запущенные процессы, конфигурация) на текущий момент для последующего анализа состояния устройства, диагностики, выявления проблем.



- *Download* – выгрузка текстового файла в RTF-формате из устройства по протоколу HTTP на компьютер. После нажатия данной кнопки появляется диалоговое окно, в котором требуется указать путь на локальном компьютере для сохранения файла.

9 Меню «Cluster»

В меню «CLUSTER» описывается работа и настройка устройств в режиме кластера. Режим кластера позволяет настраивать в сети всего одну точку доступа (мастер). Остальные точки при включении будут находить в сети мастера и копировать с него конфигурацию. В последующем при внесении изменений в конфигурацию одной из точек доступа эти изменения будут применены для всех точек, находящихся в кластере.

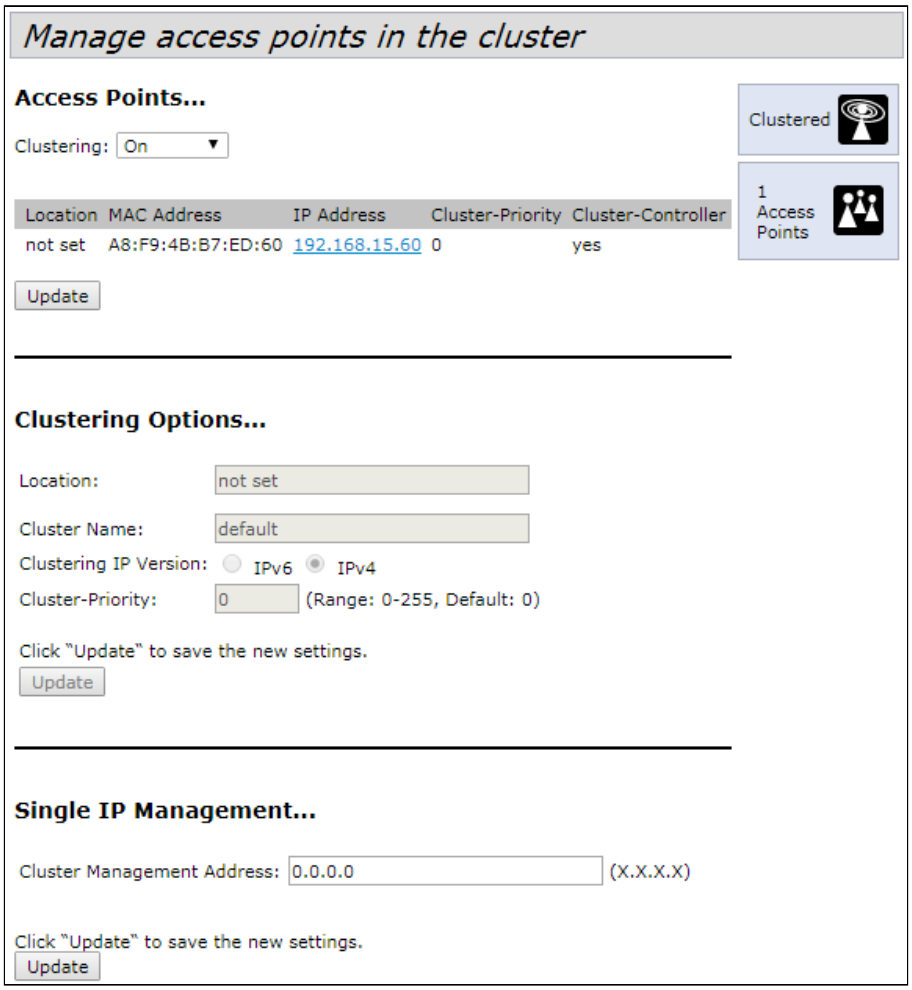
- Устройство может работать в кластере только если отключены WDS (Wireless Distribution System) и WGB (Work Group Bridge).

- Для работы в кластере Management Ethernet интерфейс всех точек должен находиться внутри одной сети.

- Режим работы в кластере включен на устройстве по умолчанию.

9.1 Подменю «Access Points»

В подменю «Access Points» выполняется включение/выключение режима кластера, мониторинг состояния режима и состава точек доступа в кластере, конфигурирование базовых параметров кластера.



В первом блоке настройки выполняется просмотр состояния работы в режиме кластера и запуск/остановка работы устройства в режиме кластера.

- *Clustering* – режим работы кластера:
  - *Off* – кластер выключен;
  - On – кластер включен;
  - SoftWLC – кластер выключен, режим для работы с SoftWLC.

Нажмите кнопку «Update» для сохранения внесенных изменений.

Clustering Options – в разделе выполняется настройка базовых параметров кластера.

- *Location* – описание физического расположения точки доступа. Используется для отображения в различных таблицах мониторинга для удобства анализа и управления сетью. Данный пункт меню доступен для изменения только при выключенном режиме кластера;
- *Cluster Name* – имя кластера. Точка доступа будет подключаться только к тому кластеру, имя которого прописано в её «Cluster Name». Данный пункт меню доступен для изменения только при выключенном режиме кластера;
- *Clustering IP Version* – используемая версия протокола IP для обмена управляющей информацией между устройствами кластера;

- *Cluster-Priority* – приоритет точки в кластере, принимает значения 0-255, по умолчанию установлено значение «0». Поддерживается только для IPv4-сетей. Чем выше значение, тем выше приоритет кластера.

Нажмите кнопку «Update» для сохранения внесенных изменений.

Single IP Management – устанавливается дополнительный адрес мастера в кластере.

Мастер в кластере определяется кластером по внутреннему алгоритму, и впоследствии бывает трудно определить мастера и подключиться. В случае установления соединения по данному Single Management IP-адресу, пользователь гарантированно подключается именно к тому устройству, которое является мастером в кластере. В случае смены мастера в кластере, Single Management также переходит на новую точку доступа.

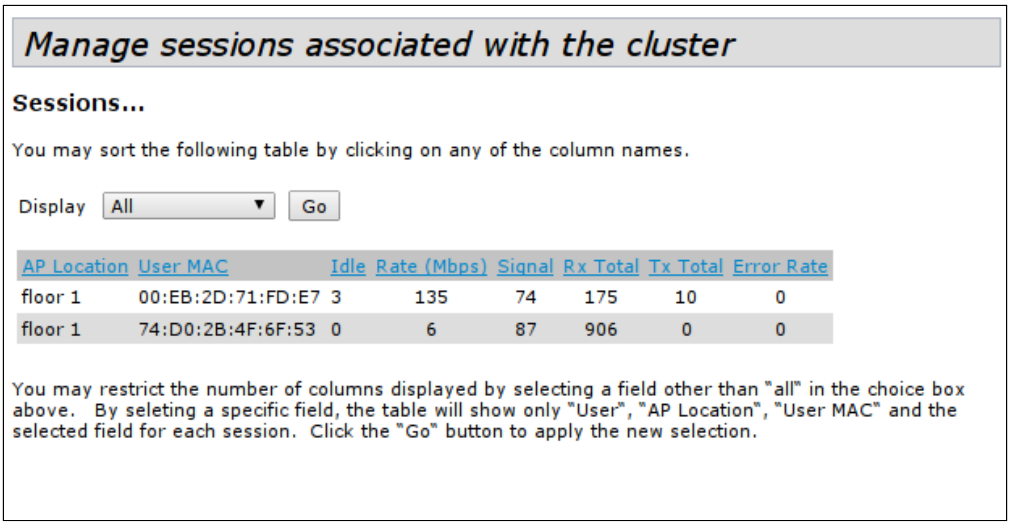
- *Cluster Management Address* – адрес, по которому будет доступен мастер кластера. Должен находиться в подсети кластера.

Нажмите кнопку «Update» для сохранения внесенных изменений.

В дальнейшем все пункты из меню «Cluster» будут описываться для режима включенного кластера.

9.2 Подменю «Sessions»

В подменю «Sessions» выполняется просмотр параметров сессий клиентов, подключенных к точкам доступа, находящимся в кластере. Каждый клиет определяется MAC-адресом и точкой доступа, к которой осуществляется его текущее подключение.
В таблице подменю «Session» может быть указано максимум 20 клиентов, просмотреть всех клиентов, подключенных к данной точке доступа можно в меню «Status» -> «Client Associations». Для просмотра статистики в раздлеле «Display» выберите нужное значение и нажмите кнопку «Go».



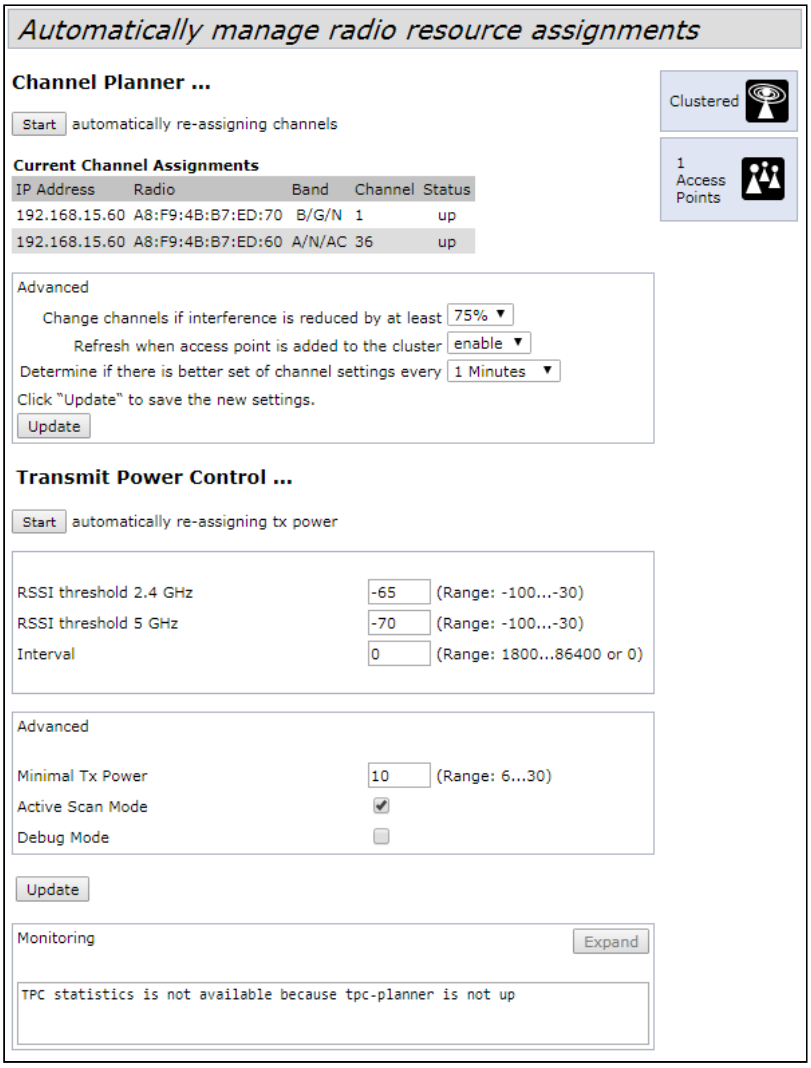
- *AP Location* – местоположение точки доступа. Значение получено от описания местоположения, указанного на вкладке «Basic Settings»;
- *User MAC* – MAC-адрес беспроводного устройства клиента;
- *Idle* – среднее время, которое устройство было в состоянии бездействия, то есть когда устройство не принимает или не передает данные;
- *Rate* – скорость передачи данных между точкой доступа и определенным клиентом, в Mbps;
- *Signal* – уровень сигнала, принимаемый от точки доступа;
- *Rx Total* – общее количество пакетов, полученных клиентом в течение данной сессии;
- *Tx Total* – общее количество пакетов, переданных от клиента в течение данной сессии;
- Error Rate – процент переотправленных пакетов.

9.3 Подменю «Radio Resource Management»

Данное подменю предназначено для управления автоматическим выбором каналов точек доступа.

В режиме кластера каждая точка доступа устанавливает номера каналов, на которых работают другие близлежащие точки доступа в этом же кластере, а также производит спектральный анализ зашумленности фона сторонними точками доступа. Через установленные интервалы времени точки доступа производят пересчет общей спектральной структуры среды и выбирают канал таким образом, чтобы он был наименее зашумленным, а точки доступа, области покрытия которых пересекаются, находились на разных каналах.

В таблице «**Current Channel Assignments**» приводится текущий список точек доступа в кластере и их параметры:



- *Start* – ручной запуск спектрального анализа среды и выбора оптимального канала для каждой точки доступа в кластере;
- *IP Address* – IP-адрес точки доступа в кластере;
- *Radio* – MAC-адрес радиоинтерфейса точки доступа в кластере;
- *Band* – набор стандартов, поддерживаемых радиоинтерфейсом точки доступа в кластере на данный момент;
- *Channel* - частотный канал в кластере;
- *Status* – состояние работы радиоинтерфейса точки доступа в кластере;
- *Locked* – блокировка смены канала. При установленном флаге в момент выбора оптимального канала всеми точками доступа данный радиоинтерфейс будет использовать прежний канал при любом исходе выбора оптимального канала.

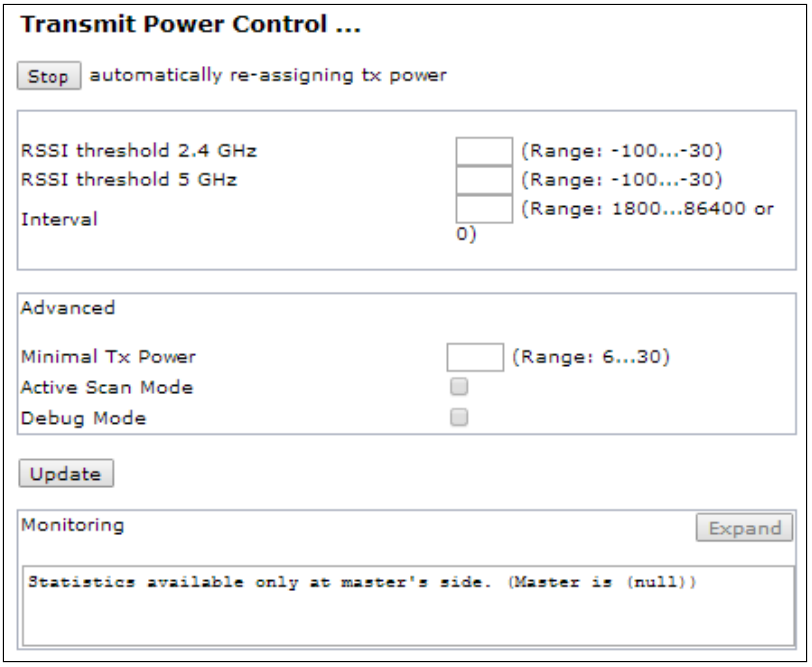
Нажмите кнопку «Apply» для применения изменений. Нажмите кнопку «Refresh» для обновления данных в таблице «Current Channel Assignments».
В таблице « **Proposed Channel Assignments** » приводится информация о возможных значениях канала, на который перейдет радиоинтерфейс точки доступа в случае запуска пересчета оптимальности выбора канала:

- *IP Address* – IP-адрес точки доступа в кластере;
- *Radio* – MAC-адрес радиоинтерфейса точки доступа в кластере;
- *Proposed Channel* – номер канала, на который перейдет радиоинтерфейс точки доступа в случае запуска пересчета оптимальности выбора канала.

Advanced – в разделе выполняются расширенные настройки:

- *Change channels if interference is reduced by at least* – процент выигрыша в уменьшении уровня шума для принятия решения перехода на другой канал. Если при анализе среды точка доступа обнаруживает, что при переходе на другой канал уровень шума снизится на величину, большую, чем указано в данном параметре, то выбор будет сделан в пользу перехода на другой канал. Диапазон настройки величины: от 5% до 75%;
- *Refresh when access point is added to the claster* – производить пересчет общей спектральной структуры среды и выбор оптимального канала для точек доступа, если к кластеру присоединяется новая точка доступа;
- *Determine if there is better set of channel settings every* – интервал времени, через который происходит пересчет общей спектральной структуры среды и выбор оптимального канала для точек доступа.

Нажмите кнопку «Update» для сохранения внесенных изменений.
В разделе «**Transmit Power Control**» точки доступа, состоящие в одном кластере, через установленные интервалы времени производят спектральный анализ эфира и производят перерасчет мощностей выставленных на точках доступа в кластере таким образом, чтобы оказывать как можно меньше влияния друг на друга. По умолчанию оптимизация проводится при изменении состава кластера.



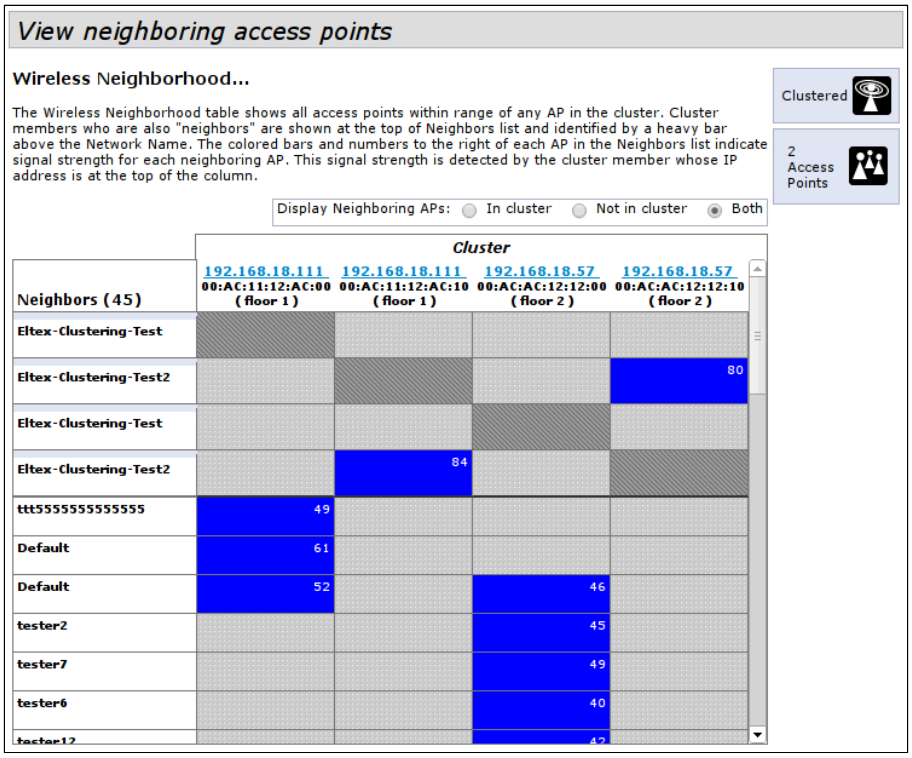
- *Start* – ручной запуск автоподстройки мощности для каждой точки доступа в кластере;
- *Stop* – остановка автоподстройки мощности;
- *RSSI threshold 2.4 GHz* – порог уровня RSSI в диапазоне 2.4 ГГц, принимает значения -100..-30, по умолчанию -65;
- *RSSI threshold 5 GHz* – порог уровня RSSI в диапазоне 5 ГГц, принимает значения -100..-30, по умолчанию -65;
- *Interval* – интервал времени между циклами оптимизации. Принимает значения: 1800...86400 секунд, по умолчанию 0 – оптимизация мощности проводится 1 раз, затем только при изменении состава кластера;
- *Minimal Tx Power* – минимальный выходной уровень мощности точки доступа, принимает значения 6...30, по умолчанию 10;
- *Active Scan Mode* – при установленном флаге, используется активный режим сканирования, при выключенном – пассивный;
- *Debug Mode* – при установленном флаге включается отправка отладочных сообщений в консоль точек доступа;

В окне Monitoring после окончания оптимизации автоподстройки мощности можно наблюдать результаты сканирования всех точек доступа в кластере, уровень влияния друг на друга, а так же

измененную выходную мощность точек доступа.
Нажмите кнопку «Update» для сохранения внесенных изменений.

9.4 Подменю «Wireless Neighborhood»

Подменю «**Wireless Neighborhood**» содержит таблицу соответствия точек доступа, находящихся в кластере, и беспроводных сетей, детектируемых этими устройствами. Данная таблица демонстрирует, какие беспроводные сети детектирует каждая точка доступа и какой уровень сигнала она от них принимает.
На основании данной таблицы можно произвести спектральный анализ всей сети и оценить влияние помех на каждую точку доступа. Это позволит оценить правильность расположения точек доступа по территории покрытия и укажет на проблемные места, в которых уровень помех может помешать качественному предоставлению услуг.



В верхней горизонтальной строке таблицы отображена информация по каждому радиоинтерфейсу точек доступа, находящихся в кластере. В левом вертикальном столбце таблицы расположена информация по беспроводным сетям, которые видны устройствам в кластере.
Уровень сигнала от каждой беспроводной сети указан в правом верхнем углу ячейки таблицы.

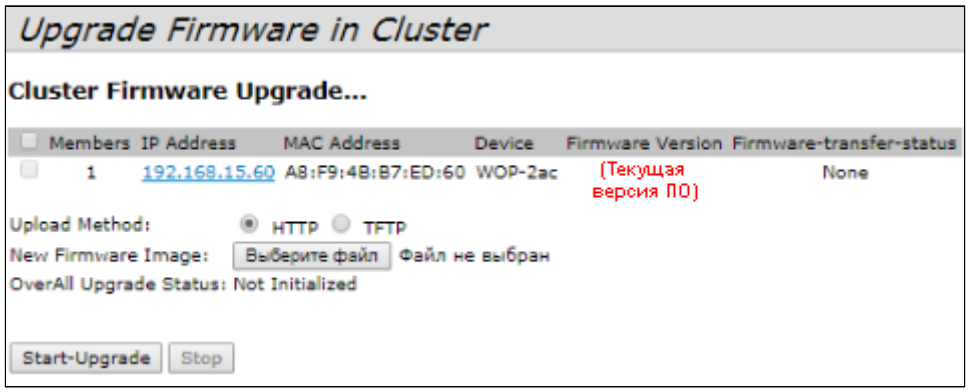
Таблица сформирована так, что в первых ее строках отображаются беспроводные сети, образованные самим кластером, далее идут имена сторонних сетей.

- *In cluster* – при установленном флаге в таблице будет отображаться информация о беспроводных сетях, находящихся только в кластере;
- *Not in cluster* – при установленном флаге в таблице будет отображаться информация только о сторонних беспроводных сетях;
- *Both* – при установленном флаге в таблице будет отображаться информация о всех сетях.

9.5 Подменю «Cluster Firmware Upgrade»

В подменю «**Cluster Firmware Upgrade**» можно выполнить обновление программного обеспечения на всех устройствах, входящих в кластер.

При обновлении ПО устройств кластера файл прошивки будет загружен на каждое устройство и установлен на позицию «Primary Image». Автоматически выполняется перезагрузка устройств с загрузкой ПО, которое соответствует новому образу. Установленное ранее на устройствах кластера ПО будет сохранено и перемещено на позицию «Secondary Image» (резервная версия ПО).



- *Upload Method* – метод загрузки файла ПО на устройства:
  - *загрузка через HTTP*. Установите флаг «Upload Method» в значение HTTP. Нажмите «Выберите файл» и в диалоговом окне выберите путь к файлу ПО на ПК. Нажмите «Upgrade» для начала загрузки выбранного файла ПО в устройство;
  - *загрузка через TFTP*. Установите флаг «Upload Method» в значение TFTP. В поле «Image Filename» укажите имя файла ПО, который будет загружен в устройство. Имя файла обязательно должно содержать расширение .tar. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором сохранен файл ПО. Нажмите «Upgrade» для начала загрузки файла;
- *New Firmware Image* – выбор файла, содержащего новую версию ПО;
- *Start-Upgrade* – начало обновления.

В процессе обновления ПО устройств не отключайте питание устройств, а также не обновляйте и не меняйте текущую web-страницу с прогресс-баром обновления.

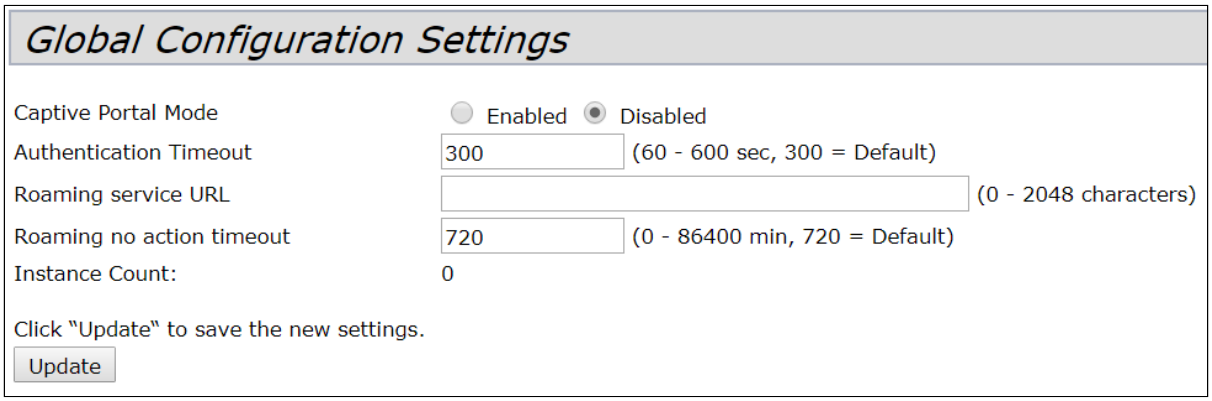
10 Меню «Captive Portal»

В меню «Captive portal» выполняется настройка специального портала, на который перенаправляются клиенты для прохождения авторизации при подключении к сети Интернет.

Таким образом можно, например, перевести Wi-Fi сеть в открытый режим, сняв шифрование, но ограничив доступ к сетевым ресурсам. Подключение к сетевым ресурсам будет реализовано через Web-авторизацию.

10.1 Подменю «Global Configuration»

В разделе «Global Configuration» выполняется настройка общих параметров портала и мониторинг текущего количества созданных объектов.

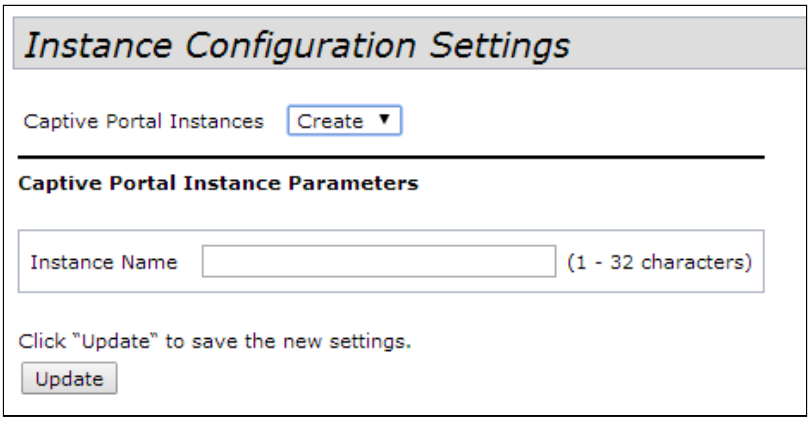


- *Captive Portal Mode* – состояние работы портала:
  - *Enabled* – при установленном флаге портал используется;
  - *Disabled* – при установленном флаге портал не используется.
- *Authentication Timeout* – период времени в секундах, в течение которого клиент может ввести авторизационные данные на странице портала для получения доступа к сети. Если интервал превышен, необходимо обновить страницу либо повторно подключиться к сети. Принимает значения (60–600) секунд. По умолчанию установлено – 300 секунд;
- *Roaming service URL* – адрес Service APB для поддержки роуминга в режиме hotspot. Задается в формате: "ws://host:port/path";
- *Roaming no action timeout, min* – время, через которое точка доступа удалит устаревшие/неактивные записи о клиентах в роуминге;
- *Instance Count – количество экз*емпляров портала, настроенных на точке доступа.Нажмите кнопку «Update» для сохранения внесенных *изменений.*

Нажмите кнопку «Update» для сохранения внесенных изменений.

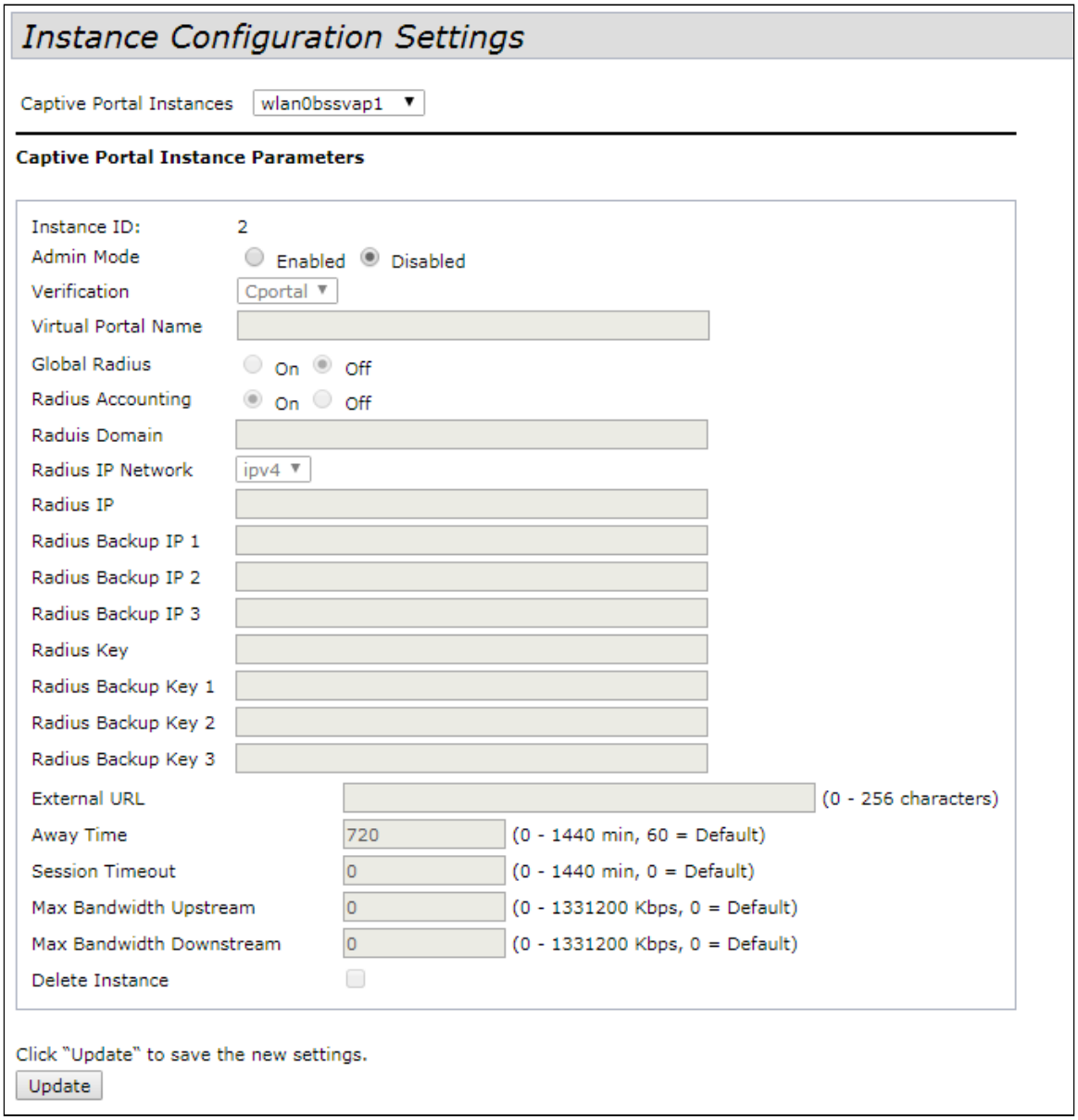
10.2 Подменю «Instance Configuration»

В разделе «Instance Configuration» создаются порталы и настраиваются параметры порталов.



Для создания нового портала в поле **«Captive Portal Instances»** необходимо выбрать пункт **«Create»** и в поле **«Instance Name»** указать имя нового портала (до 32 символов). Для создания портала нажать кнопку **«Update»**.

Для перехода к работе с порталом необходимо выбрать его имя в поле **«Captive Portal Instances»**:



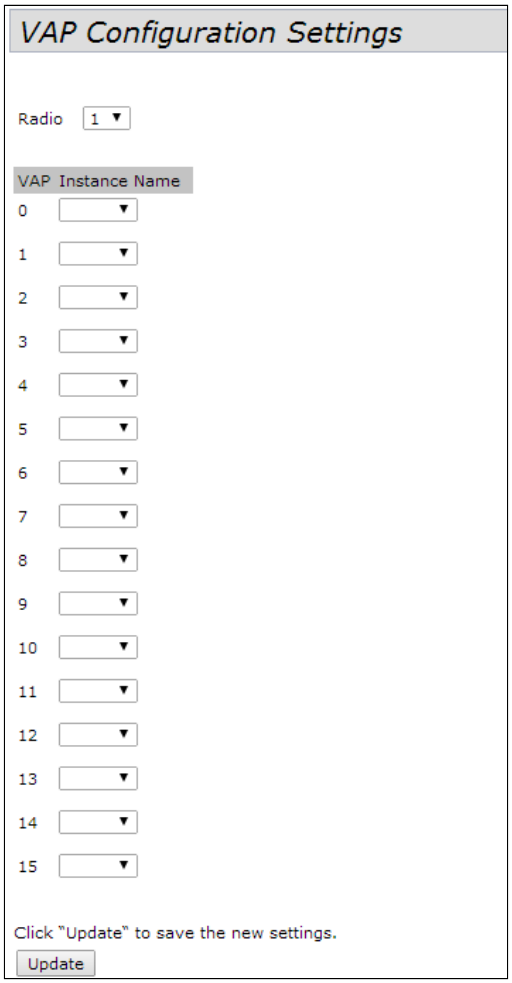
- *Instance ID* – номер портала;
- *Admin Mode* – режим работы портала:
  - *Enable* – включен;
  - *Disabled* – выключен;
- *Virtual Portal Name* – имя виртуального портала;
- *Global Radius* – глобальные настройки авторизации по RADIUS-протоколу:
  - *On* – включен;
  - *Off* – выключен;
- *Radius Accounting* – при включенной функции будут отправляться сообщения «Accounting» на RADIUS-сервер:
  - *On* – включен;
  - *Off* – выключен;
- *Raduis Domain* – домен пользователя;
- *Radius IP Network* – выбор протокола IPv4 или IPv6 для доступа на сервер RADIUS;
- *Radius IP* – адрес RADIUS-сервера. При недоступности основного RADIUS-сервера, запросы будут отправляться на резервные;
- *Radius Backup IP* – резервный адрес RADIUS-сервера;
- *Radius Key* – пароль для авторизации на RADIUS-сервере;
- *Radius Backup Key* – резервный пароль для авторизации на RADIUS-сервере;

- *External URL* – адрес внешнего Captive Portal, на который будет перенаправлен пользователь при подключении к hotspot;
- *Away Time* – время, в течение которого действительна запись аутентификации пользователя на базовой станции после его диссоциации. Если в течение этого времени клиент не пройдет аутентификацию повторно, запись будет удалена. Принимает значения 0-1440 минут, по умолчанию – 60 минут;
- *Session Timeout* – таймаут жизни сессии. Пользователь автоматически выходит из портала через указанный промежуток времени. Принимает значения 0-1440 минут. По умолчанию установлено значение «0» – таймаут не применяется;
- *Max Bandwidth Upstream* – максимальная скорость передачи трафика от абонента. Принимает значения 0-300 Мбит/с. По умолчанию установлено значение «0» – без ограничения;
- *Max Bandwidth Downstream* – максимальная скорость передачи трафика к абоненту. Принимает значения 0-300 Мбит/с. По умолчанию установлено значение «0» – без ограничения;
- *User mobility domain* – название группы, в рамках которой может быть совершен роуминг;
- *Delete Instance* – для удаления данного портала установите флаг и нажмите кнопку «Update».

Нажмите кнопку «Update» для сохранения внесенных изменений.

10.3 Подменю «VAP Configuration»

В разделе «VAP Configuration» выполняется привязка портала к виртуальным Wi-Fi сетям VAP.

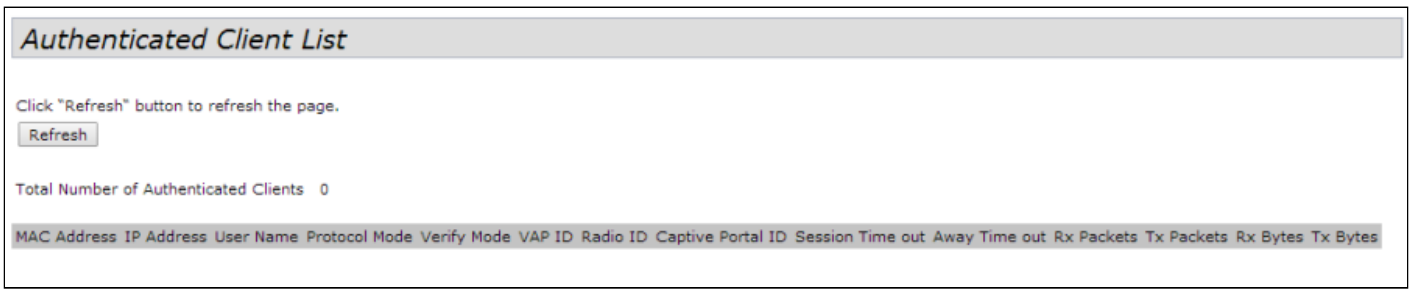


- *Radio* – номер Wi-Fi интерфейса, для которого производится настройка.

В таблице для каждой виртуальной сети назначается портал по его имени.
Нажмите кнопку «Update» для сохранения внесенных изменений.

10.4 Подменю «Authenticated Clients»

В разделе «Authenticated Clients» отображается список клиентов, которые успешно прошли аутентификацию на портале.



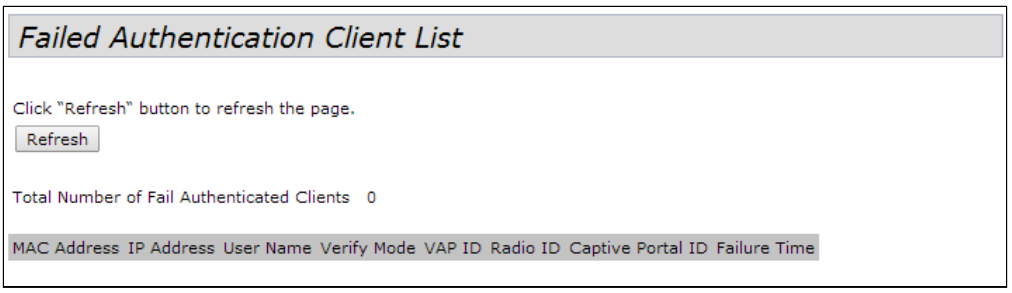
Для обновления информации на странице нажмите кнопку «Refresh».

- *Total Number of Authenticated Clients* – количество успешно авторизированных клиентов в данный момент;

- *MAC Address* – MAC-адрес клиента;
- *IP Address* – IP-адрес клиента;
- *User Name* – имя пользователя, с которым клиент прошёл аутентификацию на портале;
- *Protocol Mode* – протокол, используемый для соединения HTTP / HTTPS;
- *Verify Mode* – метод авторизации на портале;
- *VAP ID* – номер виртуальной сети;
- *Radio ID* – номер радиоинтерфейса;
- *Captive Portal ID* – имя портала, с которым ассоциирован клиент;
- *Session Timeout* – оставшееся время жизни сессии;
- *Away Timeout* – оставшееся время жизни записи аутентификации клиента;
- *Rx Packets* – количество принятых пакетов от клиента;
- *Tx Packets* – количество переданных клиенту пакетов;
- *Rx Bytes* – количество полученных байт UAP от пользователя;
- *Tx Bytes* – количество переданных байт UAP пользователем.

10.5 Подменю «Failed Authentication Clients»

В разделе «Failed Authentication Clients» приведен список клиентов с ошибкой авторизации на портале.



Для обновления информации на странице нажмите кнопку «Refresh».

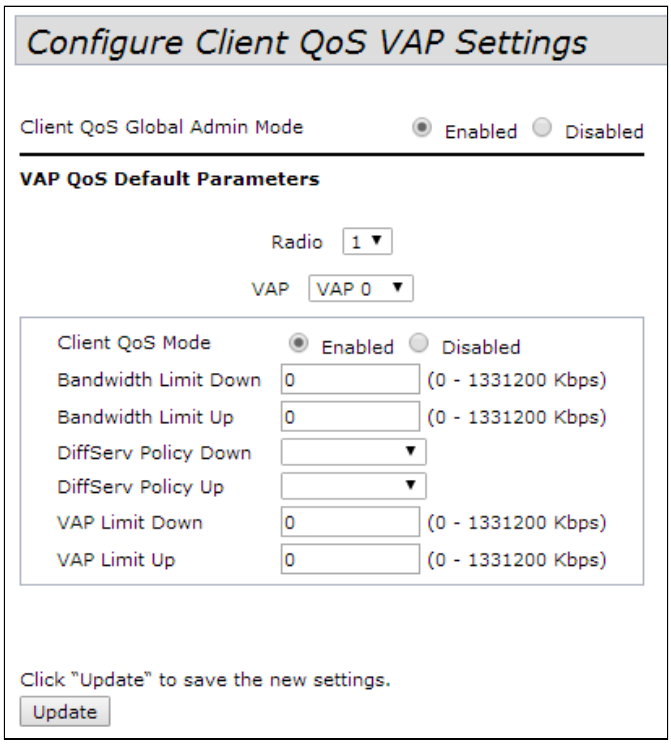
- *MAC Address* – MAC-адрес клиента;
- *IP Address* – IP-адрес клиента;
- *User Name* – имя пользователя, с которым клиент прошёл аутентификацию на портале;
- *Verify Mode* – метод авторизации на портале;
- *VAP ID* – номер виртуальной сети;
- *Radio ID* – номер радиоинтерфейса;
- *Captive Portal ID* – имя портала, с которым ассоциирован клиент;
- *Failure Time* – время, когда произошла ошибка.

11 Меню «Client QoS»

Меню «Client QoS» предназначено для более тонкой настройки QoS клиентских потоков трафика. Client QoS позволяет настроить приоритизацию отдельных потоков трафика, ограничить ширину полосы для каждого клиента.

11.1 Подменю «VAP QoS Parameters»

Подменю «VAP QoS Parameters» позволяет глобально включить использование всех настроек Client QoS (Class MAP, Policy MAP, Bandwidth Limit), назначить раннее сформированные правила приоритизации трафика.



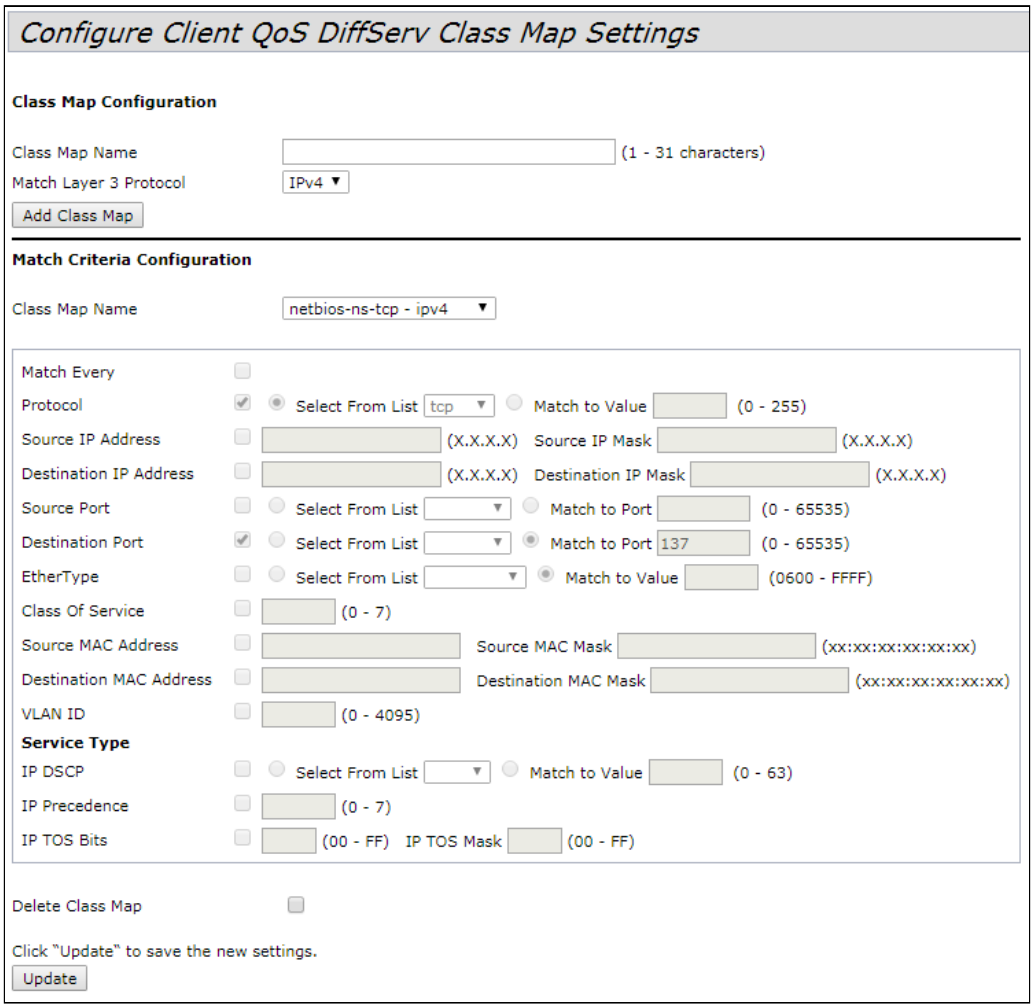
- *Client QoS Global Admin Mode* – использование Client QoS на всей точке доступа глобально:
  - *Enable* – включить;
  - *Disabled* – выключить;
- *Radio* – выбор радиоинтерфейса, на котором будет производиться настройка Client QoS;
- *VAP* – выбор виртуальной точки доступа, на которой будет производиться настройка Client QoS;
- *Client QoS Mode* – использование Client QoS на выбранной VAP:
  - *Enable* – включить;
  - *Disabled* – выключить;
- *Bandwidth Limit Down* – ограничение ширины полосы трафика от точки доступа к каждому клиенту, бит/с. Диапазон возможных значений: 0 – 4294967295 бит/с. Если назначен 0, то ограничение полосы трафика не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;
- *Bandwidth Limit Up* – ограничение ширины полосы трафика от каждого клиента до точки доступа. Единица измерения: бит/с. Диапазон возможных значений: 0 – 4294967295 бит/с. Если назначен 0, то ограничение полосы трафика не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;
- *DiffServ Policy Down* – имя профиля Policy, который должен быть применен к трафику, идущему от точки доступа к клиенту;
- *DiffServ Policy Up* – имя профиля Policy, который должен быть применен к трафику, идущему клиента к точке доступа.

- *VAP Limit Down* – ограничение ширины полосы трафика от точки доступа к клиентам (в сумме), подключенным к данному VAP, бит/с. Диапазон возможных значений: 0 – 4294967295 бит/с. Если назначен 0, то ограничение не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;
- *VAP Limit Up* – ограничение ширины полосы трафика от клиентов (в сумме) до точки доступа, бит/с. Диапазон возможных значений: 0 – 4294967295 бит/с. Если назначен 0, то ограничение не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с.

Нажмите кнопку «Update» для сохранения внесенных изменений.

11.2 Подменю «Class Map»

В подменю «Class Map» выполняется настройка классификации трафика. На основе уникальных особенностей пакетов определенного потока трафика формируется класс принадлежности пакетов к данному потоку. В дальнейшем этот класс будет использован для операций приоритизации различных потоков, объединенных по общему признаку.



Class Map Configuration – в разделе выполняется создание профиля классификации трафика.

- *Class Map Name* – имя класса трафика;
- *Match Layer 3 Protocol* – протокол, по которому будет происходить классификация (IPv4 или IPv6). В зависимости от выбора протокола будет предложен различный набор полей, по которым будет выполняться классификация трафика.

Для создания нового класса трафика укажите в поле «Class Map Name» имя класса и нажмите кнопку «Add Class Map».

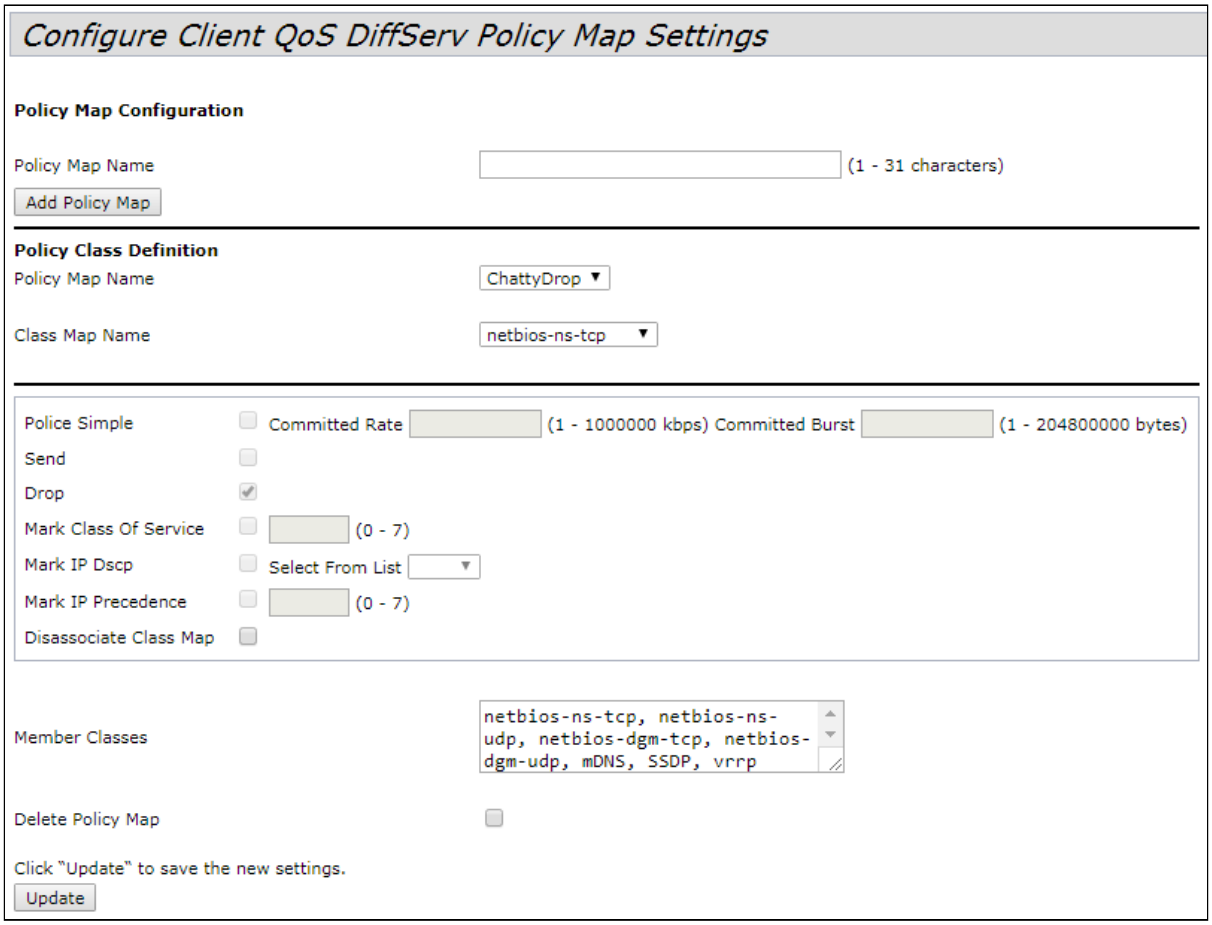
Match Criteria Configuration – в разделе выполняется настройка критериев для класса трафика.

- *Class Map Name* – выбор класса трафика, для которого будет происходить конфигурирование признаков принадлежности к классу;
- *Match Every* – при установленном флаге трафик будет отнесен к данному классу независимо от содержания полей в его заголовке. Если флаг не установлен, то требуется указать значения необходимых полей трафика, которые должны быть соотнесены с данным классом;
- *Protocol* – значение поля Protocol в IPv4-пакете;
- *Source IP Address* – значение IP-адреса отправителя пакета;
- *Source IP Mask* – маска, указывающая на значимость битов в IP-адресе, на основании которых классифицируется пакет;
- *Source IPv6 Prefix Len* – длина префикса IPv6-адреса отправителя;
- *Destination IP Address* – значение IP-адреса получателя пакета;
- *Destination IP Mask* – маска, указывающая на значимость битов в IP-адресе, на основании которых классифицируется пакет;
- *Destination IPv6 Prefix Len* – длина префикса IPv6-адреса получателя;
- *Source Port* – порт отправителя (Layer 4);
- *Destination Port* – порт получателя (Layer 4);
- *EtherType* – значение поля EtherType, указывающего тип протокола, используемого в пакете;
- *Class Of Service* – значение поля CoS, указывающего на приоритет пакета на Layer 2 пакета;
- *Source MAC Address* – значение MAC-адреса отправителя пакета;
- *Destination MAC Address* – значение MAC-адреса получателя пакета;
- *VLAN ID* – значение поля VLAN в пакете;
- *IP DSCP* – значение поля DSCP в IP-заголовке пакета;
- *IP Precedence* – значение поля Precedence в IP-заголовке пакета;
- *IP TOS Bits* – значение поля TOS в IP-заголовке пакета;
- *IP TOS Mask* – маска, указывающая на значимость битов в поле TOS, на основании которых классифицируется пакет;
- *Delete Class Map* – удалить класс трафика;
- *Update* – применить параметры класса трафика;
- *IPv6 Flow Label* – значение поля Flow Label.

Нажмите кнопку «Update» для сохранения внесенных изменений.

11.3 Подменю «Policy Map»

Подменю «Policy Map» предназначено для настройки ширины полосы пропускания для классифицированного по общему признаку потока трафика, маркирования приоритета данного класса трафика на уровне Layer 2 и Layer 3 (CoS, DSCP, Precedence), а также для принятия решения о пропуске данного трафика или о его блокировки. В подменю формируется профиль «Policy Map», для которого последовательно назначаются ранее созданные классификаторы трафика «Class Map». Для каждого классификатора указываются операции, которые необходимо произвести с данным типом трафика.



Policy Map Configuration – в разделе выполняется создание нового профиля Policy Map.

- *Policy Map Name* – имя профиля Policy Map.

Для добавления нового профиля введите имя профиля в поле «Police Map Name» и нажмите кнопку «Add Policy Map».

Policy Class Definition – в разделе выполняется настройка классификаторов трафика.

- *Policy Map Name* – имя профиля «Policy Map», в котором будет производиться дальнейшая настройка операций для классификаторов трафика;
- *Class Map Name* – классификатор трафика, ранее созданный в подменю «Class Map».

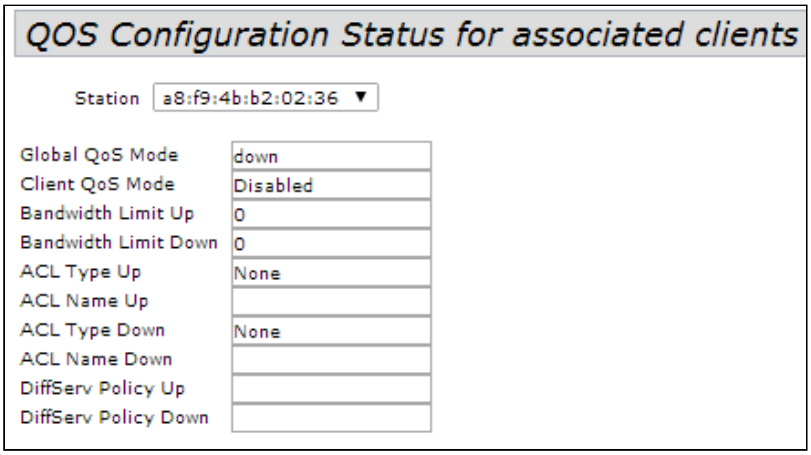
Операции, которые необходимо произвести с данным типом трафика:

- *Police Simple* – упрощенная настройка, при которой задаются два параметра:
  - *Committed Rate* – гарантированная скорость передачи для данного вида трафика;
  - *Committed Burst* – ограничение скачков трафика;
- *Send* – при установленном флаге все пакеты соответствующего потока трафика будут переданы, если критерии Class Map выполняются;
- *Drop* – при установленном флаге все пакеты соответствующего потока трафика будут отброшены, если критерии Class Map выполняются;
- *Mark Class Of Service* – при установленном флаге все пакеты соответствующего потока трафика будут маркироваться заданным значением CoS (целое число от 0 до 7);
- *Mark IP Dscp* – при установленном флаге все пакеты соответствующего потока трафика будут маркироваться заданным значением IP-DSCP. Значение можно выбрать из списка или указать;
- *Mark IP Precedence* – при установленном флаге все пакеты соответствующего потока трафика будут маркироваться заданным значением IP Precedence (целое число от 0 до 7);
- *Disassociate Class Map* – установите флаг и нажмите кнопку «Update», чтобы удалить привязку данного Class Map и Policy Map;

- *Member Classes* – список всех Class Map, которые связаны с выбранной Policy Map. Если класс не связан с политикой, это поле пустое;
- *Delete Policy Map* – установите флаг и нажмите кнопку «Update», чтобы удалить Policy Map, указанную в Policy Map Name.

11.4 Подменю «Client Configuration»

В этом разделе можно просмотреть текущую конфигурацию QoS.

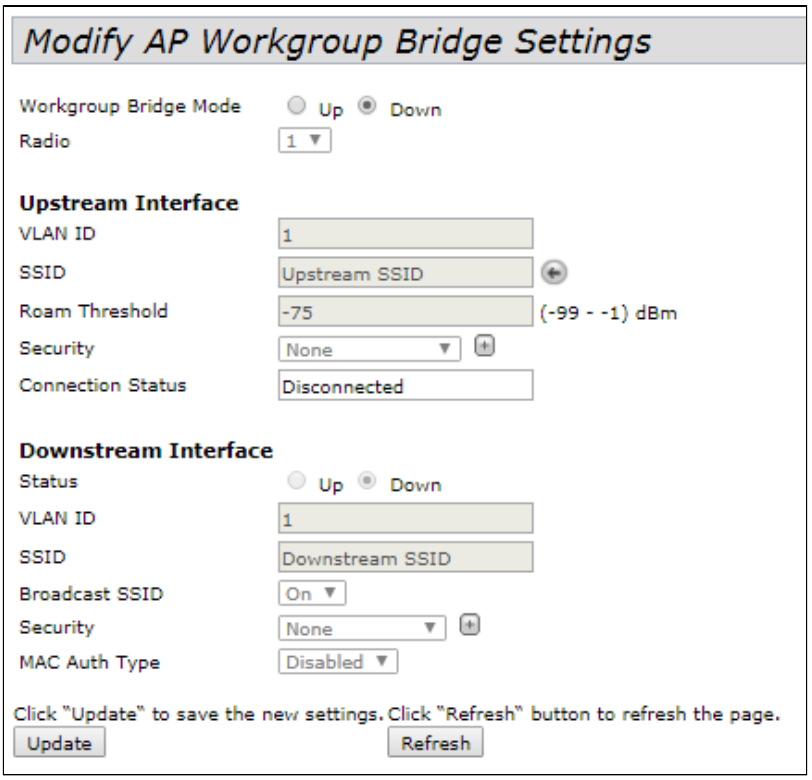


- *Station* – выбор интерфейса по MAC-адресу;
- *Global QoS Mode* – использование Client QoS на всей точке доступа глобально:
  - *Up* – включено;
  - *Down* – выключено;
- *Client QoS* Mode – использование Client QoS на выбранной VAP:
  - *Enable* – включено;
  - *Disabled* – выключено;
- *Bandwidth Limit Up* – ограничение ширины полосы трафика от каждого клиента до точки доступа, в бит/с;
- Bandwidth Limit Down – ограничение ширины полосы трафика от точки доступа к каждому клиенту, бит/с;
- ACL Type Up – тип трафика от клиента к точке доступа, для которого будут применяться правила ACL;
- ACL Name Up – имя профиля ACL, который должен быть применен к трафику, идущему от клиента к точке доступа;
- ACL Type Down – тип трафика от точки доступа к клиенту, для которого будут применяться правила ACL;
- ACL Name Down – имя профиля ACL, который должен быть применен к трафику, идущему от точки доступа к клиенту;
- DiffServ Policy Up – имя профиля Policy, который должен быть применен к трафику, идущему от клиента к точке доступа;
- DiffServ Policy Down – имя профиля Policy, который должен быть применен к трафику, идущему от точки доступа к клиенту.

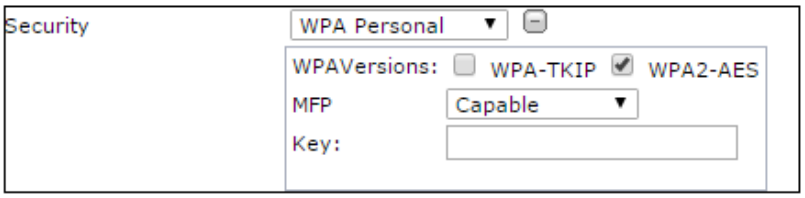
12 Меню «Work Group Bridge»

12.1 Подменю «Work group bridge»

Подменю «Work group bridge» предназначено для настройки устройства в режим беспроводного клиента с использованием одного из беспроводных интерфейсов. При настройке режима клиента кластер на устройстве должен быть отключен.

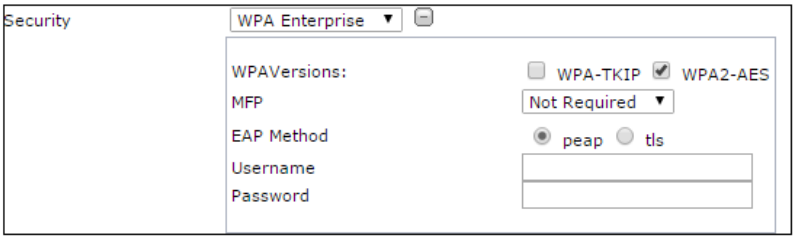


- *WorkGroupBridgeMode* – включение/выключение режима клиента на интерфейсе;
- *Radio* – выбор беспроводного интерфейса, на котором включается режим клиента;
- *UpstreamInterface* – настройки интерфейса, который будет являться беспроводным клиентом и подключаться к сторонней точке доступа;
- *VLANID* – номер VLAN, используемый на точке доступа;
- *SSID* – имя точки доступа, к которой происходит подключение;
- *Roamthreshold* – минимальный уровень сигнала от точки доступа, при котором происходит подключение к точке;
- *Security* – режим безопасности точки доступа, к которой происходит подключение:
  - *None* – не использовать шифрование для передачи данных. Точка открыта для доступа любого клиента;
  - *WPAPersonal* – режим подключения к точке доступа с использованием механизма безопасности WPA-TKIP или WPA2-AES. При выборе данного режима для редактирования будут доступны следующие настройки:



    - *WPAVersions* – версия используемого протокола безопасности (WPA или WPA2);
    - *MFP* – защита управляющих кадров: Not Required – не использовать; Capable – опционально; Required – использовать;

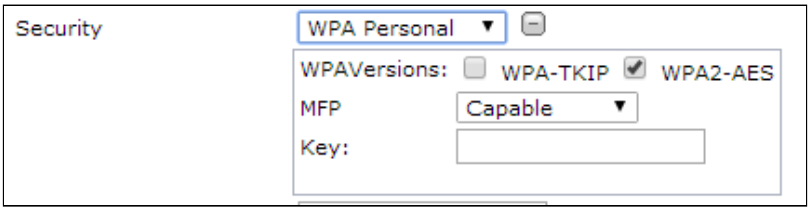
    - *Key* – ключ/пароль, необходимый для авторизации на точке доступа.
  - *WPAEnterprise* – режим подключения к точке доступа с использованием авторизации и аутентификации на вышестоящем сервере. При выборе данного режима для редактирования будут доступны следующие настройки:



    - *WPAVersions* – версия используемого протокола безопасности: WPA-TKIP, WPA2-AES;
    - *MFP* – защита управляющих кадров: *Not Required* – не использовать; *Capable* – опционально; *Required* – использовать;
    - *EAP Method* – выбор протокола аутентификации (peap или tls);
    - *Username* – имя пользователя, используемое при авторизации на сервере;
    - *Password* – пароль пользователя, используемый при авторизации на сервере.
- *Connection Status* – статус подключения к точке доступа.

В разделе «**Downstream Interface**» выполняются настройки интерфейса, выступающего в качестве точки доступа.

- *Status* – включение/выключение downstream-интерфейса:
  - *Up* – интерфейс включен;
  - *Down* – интерфейс выключен.
- *VLANID* – номер VLAN, в котором будет передаваться сетевой трафик для данной точки доступа;
- *SSID* – имя точки доступа;
- *BroadcastSSID* – включить/выключить вещание точки доступа:
  - *On* – вещание включено;
  - *Off* – вещание выключено.
- *Security* – режим безопасности создаваемой точки доступа;
  - *None* – не использовать шифрование для передачи данных. Точка открыта для доступа любого клиента;
  - *WPA Personal* – режим подключения к точке доступа с использованием механизма безопасности WPA или WPA2. При выборе данного режима к редактированию доступны следующие пункты:



    - *WPAVersions* – версия используемого протокола безопасности (WPA-TKIP или WPA2-AES).

Если выбран WPA-TKIP, то для настройки будут доступны поля:

- *Key* – ключ/пароль, необходимый для авторизации на точке доступа;
- *Broadcast Key Refresh Rate* – интервал времени обновления группового ключа, принимает значения 0-86400.

Если выбран WPA2-AES, то для настройки будут доступны поля:

- *Key* – ключ/пароль, необходимый для авторизации на точке доступа;
- *Broadcast Key Refresh Rate* – интервал времени обновления группового ключа, принимает значения 0-86400;

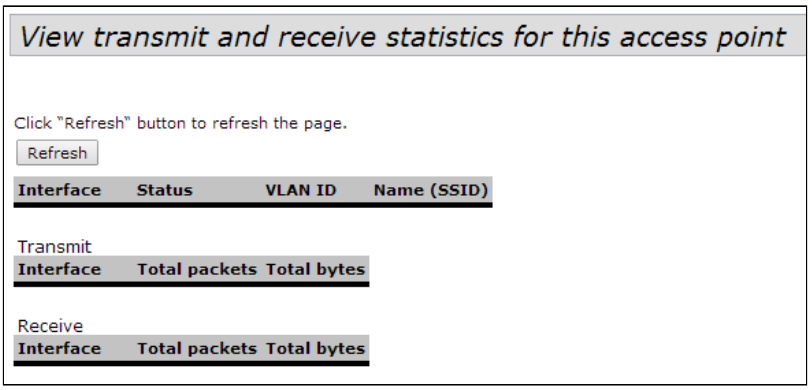
    - *MFP* – защита управляющих кадров: *Not Required* – не использовать; *Capable* – опционально; *Required* – использовать;
- *MAC Auth Type* – режим аутентификации пользователей с учетом их MAC-адреса:
    - *Disabled* – не использовать аутентификацию пользователей по MAC-адресу;
    - *RADIUS* – использовать аутентификацию пользователей по MAC-адресу с помощью RADIUS-сервера;
    - *Local* – использовать аутентификацию пользователей по MAC-адресу с помощью локального списка адресов, сформированного на данной точке доступа.

Нажмите кнопку «Update» для сохранения внесенных изменений.
Для обновления информации на странице нажмите кнопку «Refresh».

12.2 Подменю «Workgroup Bridge Transmit/Receive»

В подменю «Workgroup Bridge Transmit/Receive» представлена статистика по переданному/принятому трафику на интерфейсах, сформированных в режиме Work Group Bridge.

Для обновления информации на странице нажмите кнопку «Refresh».



- *Interface* – имя интерфейса;
- *Status* – статус работы интерфейса;
- *VLAN ID* – номер VLAN, назначенного на интерфейс;
- *Name(SSID)* – имя беспроводной сети, сконфигурированной для интерфейса.

В разделе **«Transmit»** выполняется просмотр статистики по переданному трафику.

В разделе **«Receive»** выполняется просмотр статистики по принятому трафику.

- *Interface* – имя интерфейса;
- *Total packets* – общее количество переданных/принятых пакетов;
- *Total bytes* – общее количество переданных/принятых байт.

13 Список изменений

Версия документа	Дата выпуска	Содержание изменений
Версия 1.20	07.12.2020	Синхронизация с версией ПО 1.20.0
Версия 1.19	09.04.2020	Синхронизация с версией ПО 1.19.3
Версия 1.18	24.02.2020	Синхронизация с версией ПО 1.19.0
Версия 1.17	01.10.2019	Синхронизация с версией ПО 1.18.1 Изменены разделы: 5.19 Подменю «Mesh»
Версия 1.16	05.06.2019	Синхронизация с версией ПО 1.17.0 Изменены разделы: 5.5 Подменю «Radio» 5.8 Подменю «VAP»
Версия 1.15	12.02.2019	Синхронизация с версией ПО 1.16.0
Версия 1.14	30.11.2018	Синхронизация с версией ПО 1.15.0
Версия 1.13	10.08.2018	Синхронизация с версией ПО 1.14.0 Добавлены разделы: • 5.11 Подменю «Passpoint» • 5.19 Подменю «Mesh» • 5.20 Подменю «Mesh Monitoring»
Версия 1.12	08.05.2018	Синхронизация с версией ПО 1.12.2 Изменены разделы: • 5.4 Подменю «Wireless Settings» • 5.5 Подменю «Radio» Добавлены разделы: • 5.17 Подменю «OTT Settings»
Версия 1.11	27.12.2017	Синхронизация с версией ПО 1.11.4
Версия 1.10	30.10.2017	Синхронизация с версией ПО 1.11.2 Изменены: • 4.3 Подменю «Transmit/Receive» • 4.5 Подменю «Client Association» • 4.10 Подменю «Radio Statistic»
Версия 1.9	01.07.2017	Синхронизация с версией ПО 1.10.0

Версия документа	Дата выпуска	Содержание изменений
Версия 1.8	02.02.2017	Синхронизация с версией ПО 1.9.0 Изменено: • 5.5 Подменю «Radio» • 9.3 Подменю «Radio Resource Management»
Версия 1.7	20.09.2016	Синхронизация с версией ПО 1.8.0
Версия 1.6	27.07.2016	Синхронизация с версией ПО 1.7.0 Добавлены разделы: • 4.6 Подменю «TSPEC Client Associations» • 4.8 Подменю «TSPEC Status and Statistics» • 4.9 Подменю «TSPEC AP Statistics» Изменены разделы: • 5.5 Подменю «Radio»
Версия 1.5	06.07.2016	Синхронизация с версией ПО 1.6.5
Версия 1.4	16.05.2016	Синхронизация с версией ПО 1.6.4 Изменено: • 5.4 Подменю "Wireless Settings" • 5.5 Подменю "Radio"
Версия 1.3	26.02.2016	Синхронизация с версией ПО 1.6.3 Изменены: • 5.5 Подменю «Radio» • 5.8 Подменю «VAP» • 11.1 Подменю «Global Configuration» • 11.2 Подменю «Instrance Congiguration»
Версия 1.2	14.10.2015	Синхронизация с версией ПО 1.6.2 Добавлены: • 5.9 Подменю "VAP Minimal Signal" • 5.10 Подменю "Fast Bss Transition" Изменены: • 4.5 Подменю «Client Associations» • 5.4 Подменю "Wireless Settings" • 5.5 Подменю "Radio" • 5.8 Подменю "VAP" • 6.2 Подменю «Web Server» • 6.8 Подменю «SNMP» • 8.1 Подменю «Configuration» • 10.1 Подменю «Access Points» • 11.2 Подменю «Instance Configuration» • 12.1 Подменю «VAP QoS Parametrs» • 12.3 Подменю «Policy Map» • 13.1 Подменю «Work group bridge»

Версия документа	Дата выпуска	Содержание изменений
Версия 1.1	26.03.2015	Синхронизация с версией ПО 1.5.0. Добавлены: • 4.4 Подменю «Wireless Multicast Forwarding Statistic» • 5.10 Подменю «Wireless Multicast Forwarding» • 10.5 Подменю «Cluster Firmware Upgrade» • 12.4 Подменю «Client Configuration» Изменены: • 4.3 Подменю «Transmit/Receive» • 4.5 Подменю «Client Associations» • 4.6 Подменю «Rogue AP Detection» • 5.8 Подменю «VAP» • 5.10 Подменю «WDS» • 10.1 Подменю «Access Points» • 11.2 Подменю «Instance Configuration» • 13.1 Подменю «Work group bridge»
Версия 1.0	23.09.2014	Первая публикация
Версия программного обеспечения 1.20.0		

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Форма обратной связи на сайте: https://eltex-co.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: https://eltex-co.ru/

Технический форум: https://eltex-co.ru/forum

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex-co.ru/support/downloads