

Беспроводная точка доступа

# WEP-2ac, WEP-2ac Smart

Руководство по эксплуатации

Версия ПО 1.25.7

IP-адрес: 192.168.1.10

Username: admin

Password: password

## Содержание

<b>1</b>	<b>Введение .....</b>	<b>6</b>
1.1	Аннотация.....	6
1.2	Условные обозначения .....	6
<b>2</b>	<b>Описание изделия .....</b>	<b>7</b>
2.1	Назначение .....	7
2.2	Характеристика устройства.....	7
2.3	Технические параметры устройства.....	9
2.4	Диаграмма направленности встроенных антенн .....	11
2.5	Конструктивное исполнение .....	11
2.5.1	Основная панель устройства .....	12
2.6	Световая индикация .....	13
2.7	Сброс к заводским настройкам .....	13
2.8	Комплект поставки .....	13
<b>3</b>	<b>Правила и рекомендации по установке устройства .....</b>	<b>14</b>
3.1	Инструкции по технике безопасности .....	14
3.2	Рекомендации по установке .....	14
3.3	Расчет необходимого числа точек доступа .....	15
3.4	Выбор каналов соседствующих точек .....	15
3.5	Установка устройства.....	17
3.5.1	Порядок крепления на стену .....	17
3.5.2	Порядок крепления на фальшпотолок .....	18
3.5.3	Порядок снятия устройства с кронштейна.....	18
<b>4</b>	<b>Управление устройством через web-интерфейс .....</b>	<b>19</b>
4.1	Начало работы.....	19
4.2	Основные элементы web-интерфейса .....	20
4.3	Меню «Basic Settings» .....	21
4.4	Меню «Status».....	23
4.4.1	Подменю «Interfaces» .....	23
4.4.2	Подменю «Events» .....	25
4.4.3	Подменю «Transmit/Receive» .....	27
4.4.4	Подменю «Wireless Multicast Forwarding Statistic» .....	29
4.4.5	Подменю «Client Associations» .....	31
4.4.6	Подменю «TSPEC Client Associations» .....	33
4.4.7	Подменю «Rogue AP Detection».....	34
4.4.8	Подменю «TSPEC Status and Statistics».....	36
4.4.9	Подменю «TSPEC AP Statistics» .....	39

4.4.10	Подменю «Radio Statistics».....	40
4.4.11	Подменю «Email Alert Status».....	41
4.5	Меню «Manage» .....	42
4.5.1	Подменю «Ethernet Settings».....	42
4.5.2	Подменю «Management IPv6».....	43
4.5.3	Подменю «IPv6 Tunnel».....	44
4.5.4	Подменю «Wireless Settings» .....	45
4.5.5	Подменю «Radio» .....	46
4.5.6	Подменю «Scheduler».....	53
4.5.7	Подменю «Scheduler Association».....	54
4.5.8	Подменю «VAP» .....	55
4.5.9	Подменю «VAP Minimal Signal».....	59
4.5.10	Подменю «Fast Bss Transition» .....	60
4.5.11	Подменю «Passpoint» .....	61
4.5.12	Подменю «Wireless Multicast Forwarding» .....	67
4.5.13	Подменю «WDS».....	68
4.5.14	Подменю «MAC Authentication» .....	70
4.5.15	Подменю «Load Balancing».....	72
4.5.16	Подменю «Authentication».....	72
4.5.17	Подменю «Management ACL» .....	73
4.5.18	Подменю «OTT Settings» .....	74
4.5.19	Подменю «Mesh»* .....	77
4.5.20	Подменю «Mesh Monitoring»* .....	79
4.6	Меню «Services».....	80
4.6.1	Подменю «Bonjour» .....	80
4.6.2	Подменю «Web Server».....	81
4.6.3	Подменю «SSH».....	83
4.6.4	Подменю «Telnet» .....	83
4.6.5	Подменю «QoS».....	84
4.6.6	Подменю «Email Alert» .....	86
4.6.7	Подменю «LLDP» .....	87
4.6.8	Подменю «SNMP».....	88
4.6.9	Подменю «Time Settings (NTP)» .....	90
4.7	Меню «SNMPv3».....	91
4.7.1	Подменю «SNMPv3 Views» .....	91
4.7.2	Подменю «SNMPv3 Groups».....	92
4.7.3	Подменю «SNMPv3 Users».....	93

4.7.4	Подменю «SNMPv3 Targets» .....	94
4.8	Меню «Maintenance».....	94
4.8.1	Подменю «Configuration» .....	94
4.8.2	Подменю «Upgrade» .....	96
4.8.3	Подменю «Packet Capture».....	97
4.8.4	Подменю «Support Information» .....	99
4.9	Меню «Cluster» .....	99
4.9.1	Подменю «Access Points».....	100
4.9.2	Подменю «Sessions» .....	102
4.9.3	Подменю «Radio Resource Management».....	103
4.9.4	Подменю «Wireless Neighborhood».....	106
4.9.5	Подменю «Cluster Firmware Upgrade».....	107
4.10	Меню «Captive Portal».....	108
4.10.1	Подменю «Global Configuration».....	108
4.10.2	Подменю «Instance Configuration» .....	109
4.10.3	Подменю «VAP Configuration» .....	111
4.10.4	Подменю «Authenticated Clients» .....	112
4.10.5	Подменю «Failed Authentication Clients» .....	112
4.11	Меню «Client QoS».....	113
4.11.1	Подменю «VAP QoS Parameters» .....	113
4.11.2	Подменю «Class Map» .....	114
4.11.3	Подменю «Policy Map».....	115
4.11.4	Подменю «Client Configuration».....	117
4.12	Меню «Workgroup Bridge».....	118
4.12.1	Подменю «Workgroup Bridge» .....	118
4.12.2	Подменю «Workgroup Bridge Transmit/Receive».....	121
<b>5</b>	<b>Управление устройством с помощью командной строки.....</b>	<b>122</b>
5.1	Подключение к CLI через COM-порт .....	122
5.2	Подключение по протоколу Telnet.....	123
5.3	Подключение по проколу Secure Shell.....	124
5.4	Начало работы в CLI точки доступа.....	126
5.4.1	Правила пользования командной строкой .....	126
5.4.2	Условные обозначения интерфейсов .....	127
5.4.3	Сохранение изменений в конфигурации.....	128
5.5	Описание команд CLI .....	129
5.5.1	Команда get.....	129
5.5.2	Команда set .....	130

5.5.3	Команды add .....	130
5.5.4	Команда remove.....	130
5.5.5	Дополнительные команды .....	131
5.6	Настройка точки доступа через CLI.....	132
5.6.1	Настройка сетевых параметров .....	132
5.6.2	Настройка беспроводных интерфейсов.....	133
5.6.3	Настройка виртуальных точек доступа Wi-Fi (VAP) .....	138
5.6.4	Настройка Cluster .....	147
5.6.5	Настройка WDS .....	148
5.6.6	Настройка WGB.....	149
5.6.7	Настройка Radar .....	152
5.6.8	Системные настройки .....	153
5.6.9	Настройка сервиса APB.....	155
5.6.10	Мониторинг .....	156
<b>6</b>	<b>Приложение. Список основных классов и подклассов команд.....</b>	<b>173</b>
<b>7</b>	<b>Список изменений.....</b>	<b>238</b>

# 1 Введение

## 1.1 Аннотация

Современные тенденции развития связи диктуют операторам необходимость поиска наиболее оптимальных технологий, позволяющих удовлетворить стремительно возрастающие потребности абонентов, сохраняя при этом преемственность бизнес-процессов, гибкость развития и сокращение затрат на предоставление различных сервисов. Беспроводные технологии все больше набирают обороты и к данному моменту в короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей ШПД, сопоставимых по скорости с проводными сетями с высокими критериями к качеству предоставления услуг. Устройства WEP-2ac и WEP-2ac Smart являются точками доступа Wi-Fi Enterprise-класса. Основное предназначение WEP-2ac и WEP-2ac Smart – установка внутри зданий в качестве точки доступа к различным ресурсам с созданием бесшовной беспроводной сети из нескольких идентичных точек доступа («Роуминг»), если территория покрытия достаточно велика.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, конструктивное исполнение, правила безопасной эксплуатации, а также рекомендации по установке и настройке устройств WEP-2ac и WEP-2ac Smart.

## 1.2 Условные обозначения

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

✘ Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

## 2 Описание изделия

### 2.1 Назначение

Для возможности предоставления доступа пользователей к высокоскоростной безопасной беспроводной сети разработаны беспроводные точки доступа WEP-2ac и WEP-2ac Smart (далее «устройство»).

Основным назначением устройств является создание беспроводной сети передачи данных L2-уровня на стыке с проводной сетью. WEP-2ac и WEP-2ac Smart подключаются к проводной сети через 10/100/1000M Ethernet-интерфейс и с помощью своих радиоинтерфейсов создают беспроводной высокоскоростной доступ для устройств, поддерживающих технологию Wi-Fi в диапазоне 2.4 и 5 ГГц.

Устройства содержат 2 радиоинтерфейса для организации двух физических беспроводных сетей.

WEP-2ac и WEP-2ac Smart поддерживают современные требования к качеству сервисов и позволяют передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Обеспечение приоритизации происходит на основе ключевых технологий QoS: CoS (специальные метки в поле VLAN-пакета) и ToS (метки в поле IP-пакета). Но кроме стандартных практик приоритизации, устройства позволяют задавать требования к качеству передачи трафика практически по любому полю пакета, начиная от MAC и заканчивая TCP/UDP-портом. Та же гибкость сохраняется при применении правил ACL и шейпинга трафика, что позволяет в полной мере управлять доступом, качеством сервисов и ограничениями, как для всех абонентов, так и для каждого в частности.

Устройство ориентировано на установку в офисы (госучреждения, конференц-залы, лаборатории, гостиницы и др.). Возможность создания виртуальных точек доступа с различными типами шифрования позволяет устанавливать WEP-2ac и WEP-2ac Smart в организациях, где требуется разграничение прав доступа между обычными пользователями и выделенными группами пользователей.

### 2.2 Характеристика устройства

#### **Интерфейсы:**

- 1 порт Ethernet 10/100/1000BASE-T(RJ-45) с поддержкой PoE+;
- Wi-Fi 2.4 ГГц IEEE 802.11b/g/n;
- Wi-Fi 5 ГГц IEEE 802.11a/n/ac;
- Console RJ-45.

#### **Функции:**

##### *Возможности WLAN:*

- поддержка стандартов IEEE 802.11a/b/g/n/ac;
- агрегация данных, включая A-MPDU (Tx/Rx) и A-MSDU (Rx);
- приоритеты и планирование пакетов на основе WMM;
- динамический выбор частоты (DFS);
- поддержка скрытого SSID;
- 32 виртуальные точки доступа;
- обнаружение сторонних точек доступа;
- Workgroup Bridge;
- поддержка WDS;
- поддержка MESH;
- поддержка APSD.

##### *Сетевые функции:*

- автоматическое согласование скорости, дуплексного режима и переключения между режимами MDI и MDI-X;
- поддержка VLAN;

- поддержка 802.11k/r;
- DHCP-клиент;
- поддержка IPv6;
- поддержка LLDP;
- поддержка ACL;
- поддержка SNMP;
- поддержка GRE.

#### Работа в режиме кластера:

- организация кластера емкостью до 64 точек доступа;
- автоматическая синхронизация конфигураций точек доступа в кластере;
- автоматическое обновление ПО точек доступа в кластере;
- Single Management IP – единый адрес для управления точками доступа в кластере;
- автоматическое распределение частотных каналов между точками доступа;
- автоматическое распределение уровня излучаемой мощности между точками доступа.

#### Функции QoS:

- приоритет и планирование пакетов на основе профилей;
- ограничение пропускной способности для каждого SSID;
- изменение параметров WMM для каждого радиointерфейса.

#### Безопасность:

- e-mail-информирование о системных событиях;
- централизованная авторизация через RADIUS-сервер (802.1X WPA/WPA2 Enterprise);
- WPA/WPA2;
- поддержка Captive Portal;
- поддержка Internet Protocol Security (IPsec);
- поддержка WIDS/WIPS.

На рисунке 1 приведена схема применения оборудования WEP-2ac.

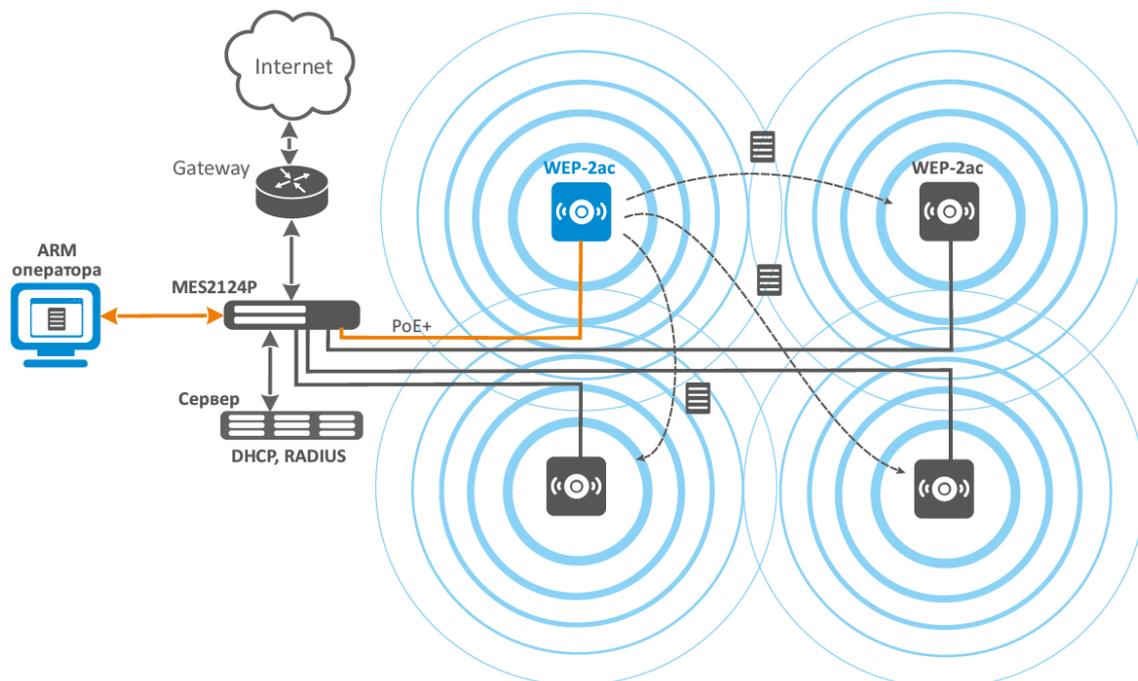


Рисунок 1 – Функциональная схема использования WEP-2ac

## 2.3 Технические параметры устройства

Таблица 1 – Основные технические параметры

<b>Параметры WAN-интерфейса Ethernet</b>	
Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T
<b>Параметры беспроводного интерфейса</b>	
Стандарты	802.11a/b/g/n/ac
Частотный диапазон, МГц	2400–2483.5 МГц; 5150–5350 МГц, 5470–5850 МГц
Модуляция	BPSK, QPSK, 16QAM, 64QAM, 256QAM
Рабочие каналы	802.11b/g/n: 1-13 (2412–2472 МГц) 802.11a/ac: 36-64 (5170–5330 МГц) 100-144 (5490–5730 МГц) 149-165 (5735–5835 МГц)
Скорость передачи данных, Мбит/с	6, 9, 12, 18, 24, 36, 48, 54, MCS0-MCS15, MCS0-9 NSS1, MCS0-9 NSS2 802.11n: до 144,4 Мбит/с (канал 20 МГц), до 300 Мбит/с (канал 40 МГц) 802.11ac: до 866,7 Мбит/с (80 МГц)
Максимальная мощность передатчика	2.4 ГГц: 18 дБм <sup>1</sup> 5 ГГц: 21 дБм <sup>1</sup>
Коэффициент усиления встроенных антенн	2.4 ГГц: ~5 дБи 5 ГГц: ~5 дБи
Чувствительность приемника	2.4 ГГц: до -98 дБм 5 ГГц: до -94 дБм
Безопасность	централизованная авторизация через RADIUS-сервер (802.1X WPA/WPA2 Enterprise); 64/128/152-битное WEP-шифрование данных, WPA/WPA2; поддержка Captive Portal; e-mail-информирование о системных событиях
Поддержка 2x2 MIMO	
<b>Управление</b>	
Удаленное управление	web-интерфейс, Telnet, SNMP, SSH, система управления EMS; Обновление ПО и конфигурирование посредством DHCP Autoprovisioning
Ограничение доступа	по паролю, по IP-адресу, аутентификация через RADIUS-сервер
<b>Общие параметры</b>	
NAND	128 МБ NAND Flash
RAM	256 МБ DDR3 RAM
Питание	PoE+ 48 В/54 В (IEEE 802.3at-2009)
Потребляемая мощность	не более 13 Вт

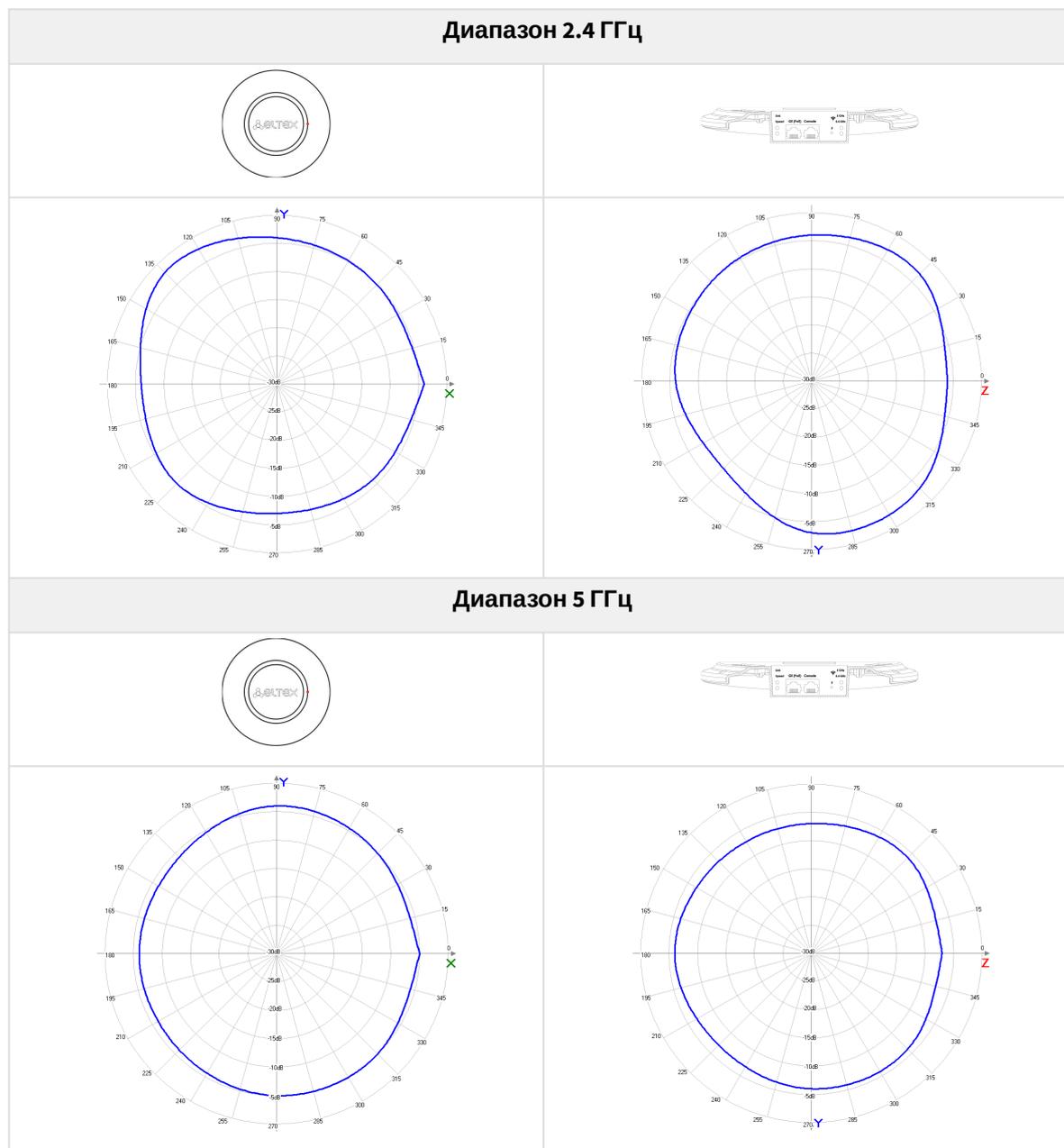
Рабочий диапазон температур	от +5 до +40 °C
Относительная влажность при температуре 25 °C	до 80 %
Габариты WEP-2ac (диаметр × высота)	200 × 40 мм
Габариты WEP-2ac Smart (диаметр × высота)	200 × 43 мм
Масса	не более 0,4 кг

---

<sup>1</sup>Определяется регуляторами Transmit Power Limit и Transmit Power Control

## 2.4 Диаграмма направленности встроенных антенн

На рисунках ниже представлены диаграммы направленности встроенных антенн устройства.



- ✓ Для WEP-2ac Smart в диапазоне 5 ГГц смарт-антенна использует метод «переключения луча» – это более 700 шаблонов диаграмм направленности, которые динамически меняются в процессе работы точки доступа. WEP-2ac Smart постоянно оценивает расположение клиентов и источников радиопомех, а затем выбирает из 700 шаблонов оптимальную для каждого момента времени диаграмму направленности.

## 2.5 Конструктивное исполнение

Устройства WEP-2ac и WEP-2ac Smart выполнены в пластиковом корпусе.

### 2.5.1 Основная панель устройства

Внешний вид панели устройства приведен на рисунке 2.

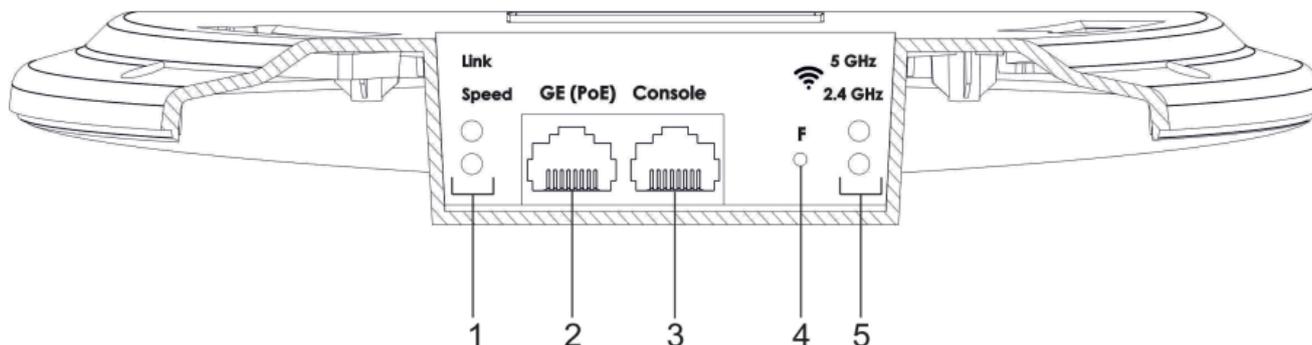


Рисунок 2 – Внешний вид основной панели WEP-2ac и WEP-2ac Smart

На основной панели устройств WEP-2ac и WEP-2ac Smart расположены следующие световые индикаторы, разъемы и органы управления (таблица 2).

Таблица 2 – Описание индикаторов, портов и органов управления

Элемент панели		Описание
1	Link/Speed	световая индикация состояния порта GE (PoE)
2	GE (PoE)	порт GE для подключения питания PoE+
3	Console	консольный порт RS-232 для локального управления устройством
4	F	функциональная кнопка
5	Wi-Fi	индикаторы активности соответствующих Wi-Fi модулей

## 2.6 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов **Wi-Fi, LAN, Power**. Перечень состояний индикаторов приведен в таблице 3.

Таблица 3 – Световая индикация состояния устройства

Индикатор	Состояние индикатора	Состояние устройства
Wi-Fi	зеленый, горит постоянно	сеть Wi-Fi-активна
	зеленый, мигает	процесс передачи данных по беспроводной сети
LAN	горит зеленый светодиод (10, 100 Мбит/с)/ горит оранжевый светодиод (1000 Мбит/с)	установлено соединение с подключенным сетевым устройством
	мигает зеленый светодиод	процесс пакетной передачи данных по LAN-интерфейсу
Power (на верхней панели устройства)	зеленый, горит постоянно	включено питание устройства, нормальная работа
	оранжевый, горит постоянно	устройство загружено, но не получен IP-адрес по DHCP
	красный, горит постоянно	загрузка устройства

## 2.7 Сброс к заводским настройкам

Для сброса устройства к заводским настройкам необходимо в загруженном состоянии нажать и удерживать кнопку «F», пока индикатор «Power» не начнет мигать. После этого произойдет автоматическая перезагрузка устройства. При заводских установках будет запущен DHCP-клиент. В случае, если адрес не будет получен по DHCP, то у устройства будет заводской ip-адрес – 192.168.1.10, маска подсети – 255.255.255.0.

## 2.8 Комплект поставки

В комплект поставки входят:

- беспроводная точка доступа WEP-2ac/WEP-2ac Smart;
- комплект крепежа;
- руководство по эксплуатации на CD-диске (опционально);
- сертификат соответствия;
- памятка о документации;
- паспорт.

## 3 Правила и рекомендации по установке устройства

В данном разделе описаны инструкции по технике безопасности, рекомендации по установке, процедура установки и порядок включения устройства.

### 3.1 Инструкции по технике безопасности

1. Не устанавливайте устройство рядом с источниками тепла и в помещениях с температурой ниже 5 °С или выше 40 °С.
2. Не используйте устройство в помещениях с высокой влажностью. Не подвергайте устройство воздействию дыма, пыли, воды, механических колебаний или ударов.
3. Не вскрывайте корпус устройства. Внутри устройства нет элементов, предназначенных для обслуживания пользователем.

 Во избежание перегрева компонентов устройства и нарушения его работы запрещается закрывать вентиляционные отверстия посторонними предметами и размещать предметы на поверхности оборудования.

### 3.2 Рекомендации по установке

1. Рекомендуемое устанавливаемое положение: горизонтальное, на потолке.
2. Перед установкой и включением устройства необходимо проверить устройство на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.
3. Если устройство находилось длительное время при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре. После длительного пребывания устройства в условиях повышенной влажности перед включением выдержать в нормальных условиях не менее 12 часов.
4. При размещении устройства для обеспечения зоны покрытия сети Wi-Fi с наилучшими характеристиками учитывайте следующие правила:
  - a. Устанавливайте устройство в центре беспроводной сети.
  - b. Минимизируйте число преград (стены, потолки, мебель и другое) между точкой доступа и другими беспроводными сетевыми устройствами.
  - c. Не устанавливайте устройство вблизи (порядка 2 м) электрических и радиоустройств.
  - d. Не рекомендуется использовать радиотелефоны и другое оборудование, работающее на частоте 2.4 ГГц или 5 ГГц, в радиусе действия беспроводной сети Wi-Fi.
  - e. Препятствия в виде стеклянных/металлических конструкций, кирпичных/бетонных стен, а также емкости с водой и зеркала могут значительно уменьшить радиус действия Wi-Fi сети. Не рекомендуется размещение со внутренней стороны фальшпотолка, так как металлический каркас вызывает многолучевое распространение сигнала и затухание при прохождении через решетку каркаса фальшпотолка.
5. При размещении нескольких точек, радиус соты должен пересекаться с соседней сотой на уровне от -65 до -70 дБм. Допускается уменьшение уровня сигнала до -75 дБм на границах сот, если не предполагается использование VoIP, потокового видеовещания и другого чувствительного к потерям трафика в беспроводной сети.

### 3.3 Расчет необходимого числа точек доступа

При выборе количества необходимых точек доступа для покрытия помещения необходимо произвести оценку требуемой зоны охвата. Для более точной оценки необходимо произвести радиоисследование помещения. Приблизительный радиус охвата уверенного приема точек доступа WEP-2ac и WEP-2ac Smart при монтаже на потолке в типовых офисных помещениях: 2.4 ГГц – 40-50 м, 5 ГГц – 20-30 м. При полном отсутствии препятствий радиус охвата: 2.4 ГГц – до 100 м, 5 ГГц – до 60 м. В таблице 4 приведены приблизительные значения затухания.

Таблица 4 – Значения затухания

Материал	Изменение уровня сигнала, дБ	
	2.4 ГГц	5 ГГц
Оргстекло	-0,3	-0,9
Кирпич	-4,5	-14,6
Стекло	-0,5	-1,7
Гипсокартон	-0,5	-0,8
ДСП	-1,6	-1,9
Фанера	-1,9	-1,8
Штукатурка с металлической сеткой	-14,8	-13,2
Шлакоблок	-7	-11
Метал. решетка (ячейка 13*6мм, металл 2мм)	-21	-13

### 3.4 Выбор каналов соседствующих точек

Во избежание межканальной интерференции между соседствующими точками доступа рекомендуется установить неперекрывающиеся каналы.

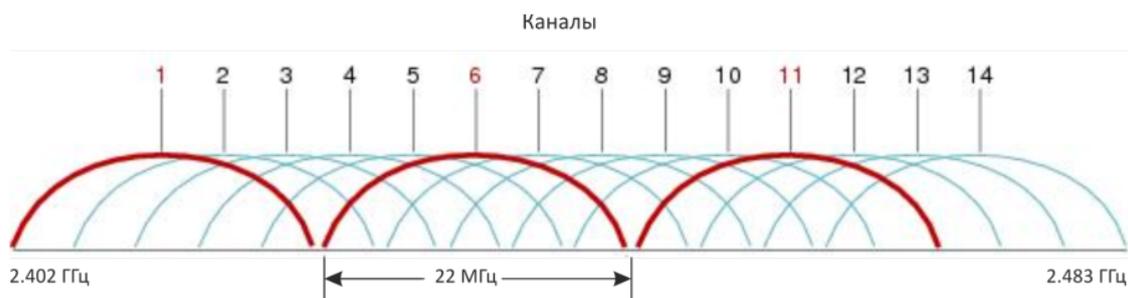


Рисунок 3 – Общая диаграмма перекрытия частотных каналов в 2.4 ГГц

Пример схемы распределения каналов между соседними точками в диапазоне 2.4 ГГц при ширине канала в 20 МГц приведен на рисунке 4.

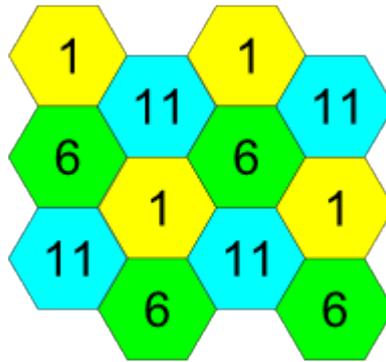


Рисунок 4 – Схема распределения каналов между соседними точками доступа в диапазоне 2.4 ГГц при ширине канала в 20 МГц

Аналогично рекомендуется сохранять данный механизм распределения каналов при расположении точек между этажами (рисунок 5).

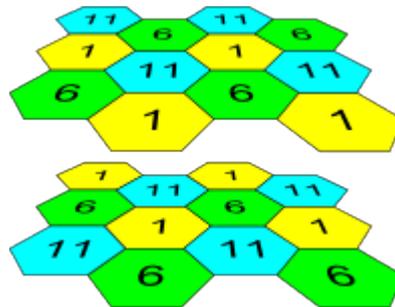


Рисунок 5 – Схема распределения каналов между соседними точками доступа, расположенными между этажами

При использовании ширины канала 40 МГц в диапазоне 2.4 ГГц нет неперекрывающихся каналов. В таких случаях стоит выбрать максимально отдаленные друг от друга каналы.

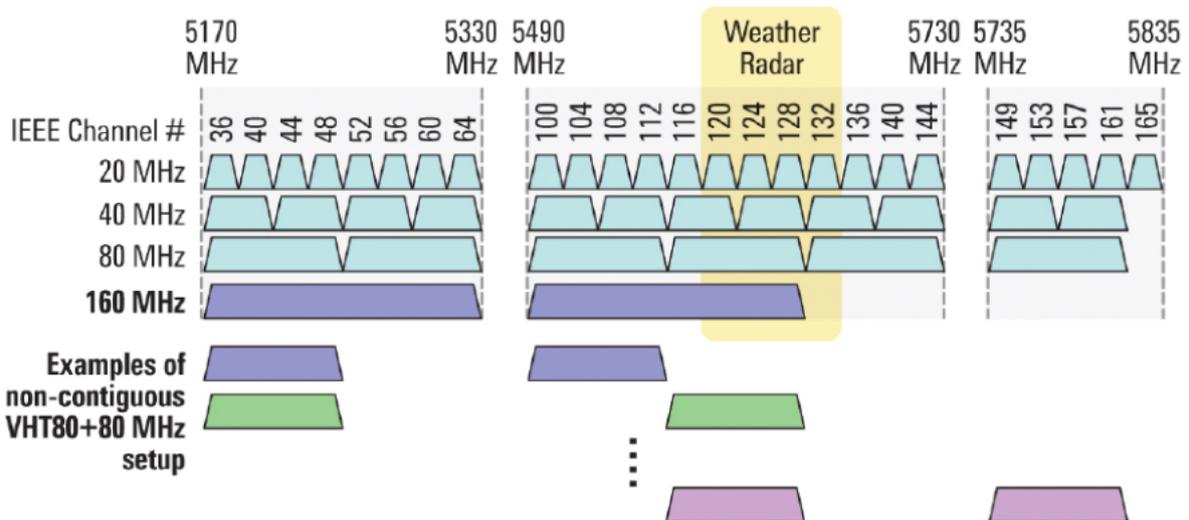


Рисунок 6 – Каналы, используемые в диапазоне 5 ГГц при ширине канала 20, 40, 80 МГц

### 3.5 Установка устройства

Устройство может быть установлено на плоской поверхности (стена, потолок) при соблюдении инструкции по технике безопасности и рекомендаций, приведенных выше.

В комплект поставки устройства входит крепеж для установки устройства на плоскую поверхность.

#### 3.5.1 Порядок крепления на стену

1. Закрепите пластиковый кронштейн (входит в комплект поставки) на стене:

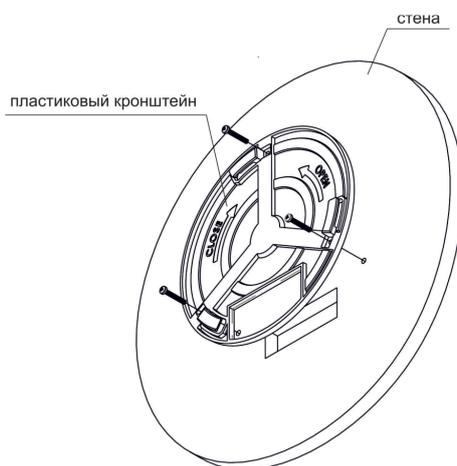


Рисунок 7 – Крепление кронштейна на стене

- Пример расположения пластикового кронштейна показан на рисунке 7.
- При установке кронштейна нужно пропустить провода в соответствующие пазы на кронштейне, рисунок 7.
- Совместите три отверстия для винтов на кронштейне с такими же отверстиями на поверхности. С помощью отвертки прикрепите кронштейн винтами к поверхности.

2. Установите устройство:

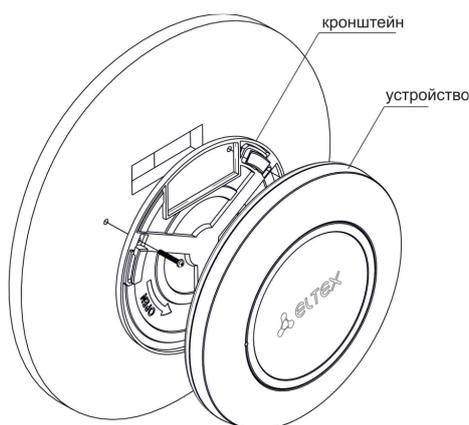
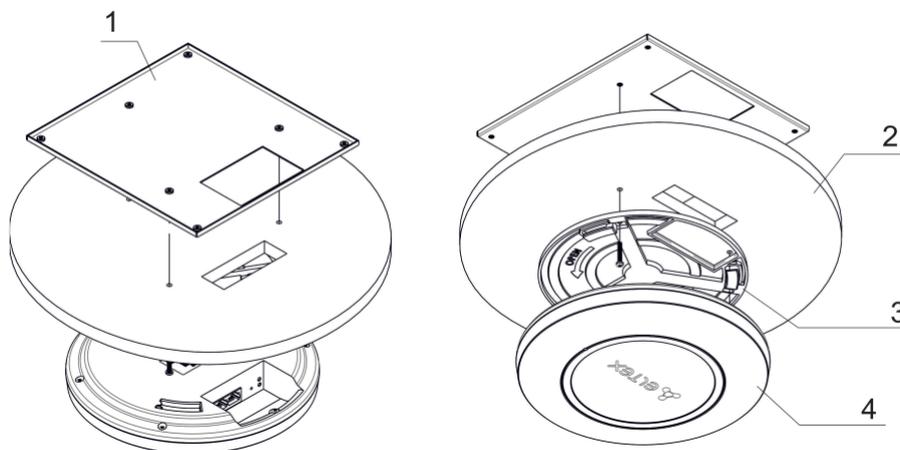


Рисунок 8 – Установка устройства (вид спереди)

- Подключите кабеля к соответствующим разъемам устройства. Описание разъемов приведено в разделе [Конструктивное исполнение](#).
- Совместите устройство с кронштейном и зафиксируйте положение, поворачивая по часовой стрелке.

### 3.5.2 Порядок крепления на фальшпотолок

- ✘ Не рекомендуется размещение со внутренней стороны фальшпотолка, так как металлический каркас вызывает многолучевое распространение сигнала и затухание при прохождении через решетку каркаса фальшпотолка.



1 – металлический кронштейн; 2 – панель Армстронг; 3 – пластиковый кронштейн; 4 – устройство.

Рисунок 9 – Монтаж устройства на фальшпотолок

1. Закрепите металлический и пластиковый кронштейны на потолке (рисунок 9).
  - a. Пластиковый кронштейн (3) соединяется на фальшпотолке с металлическим (1) в следующем порядке: металлический кронштейн -> панель Армстронг -> пластиковый кронштейн.
  - b. В панели Армстронг прорезается отверстие, размером с отверстие металлического кронштейна. Через данное отверстие заводятся провода.
  - c. Совместите отверстия на металлическом кронштейне, панели Армстронг и пластиковом кронштейне. Далее совместите три отверстия для винтов на пластиковом кронштейне с такими же отверстиями на металлическом кронштейне. С помощью отвертки соедините кронштейны винтами.
2. Установите устройство.
  - a. Подключите кабеля к соответствующим разъемам устройства. Описание разъемов приведено в разделе [Конструктивное исполнение](#).
  - b. Совместите устройство с пластиковым кронштейном и зафиксируйте положение, поворачивая устройство по часовой стрелке.

### 3.5.3 Порядок снятия устройства с кронштейна

Для снятия устройства с кронштейна:

1. Поверните устройство против часовой стрелки (рисунок 7).
2. Снимите устройство.

## 4 Управление устройством через web-интерфейс

### 4.1 Начало работы

Для начала работы нужно подключиться к устройству по интерфейсу GE через web-браузер:

1. Откройте web-браузер, 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.  
По умолчанию устройство может получить адрес по DHCP. До этого оно доступно по заводскому IP-адресу.

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



The screenshot shows a login page for the ELTEX device. At the top center is the ELTEX logo, which consists of a blue stylized 'E' icon followed by the word 'ELTEX' in a bold, blue, sans-serif font. Below the logo, there are two input fields: the first is labeled 'User Name' and the second is labeled 'Password'. Both fields are empty and have a light blue border. Below these fields is a button labeled 'Logon' in a grey, rounded rectangular box.

3. Введите имя пользователя в строке «User Name» и пароль в строке «Password».

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

4. Нажмите кнопку «Logon». В окне браузера откроется начальная страница web-интерфейса устройства.

## 4.2 Основные элементы web-интерфейса

На рисунке ниже представлены элементы навигации web-интерфейса.



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.

### 4.3 Меню «Basic Settings»

В меню «**Basic Settings**» отображается основная информация об устройстве. Имеющиеся в данном меню разделы предоставляют возможность сменить пароль доступа к устройству и настроить скорость порта Console.

*Provide basic settings*

---

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

These fields show information specific to this access point.

IP Address:	192.168.15.118
MAC Address:	E0:D9:E3:51:DE:00
Firmware Version:	<b>(Текущая версия ПО )</b>
Uptime:	0 days, 1 hours, 42 minutes
CPU Usage:	70.70%
Memory Usage:	98MB/249MB (39%)

---

**2 Device Information**

Product Identifier:	WLAN-EAP
Hardware Version:	3v0
Serial Number :	WP19000305
Device Name:	Eltex-AP
Device Description:	WEP-2ac Smart

**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 процент загрузки процессора за последние 10 секунд;
- *Memory Usage* – процент 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.

**3 Provide Network Settings ...**  
These settings apply to this access point.

New Password

Confirm new password

---

**4 Serial Settings ...**

Baud Rate

---

**5 System Settings ...**

System Name

System Contact

System Location

Click "Update" to save the new settings.

**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. По умолчанию параметр равен 115200. Может принимать значения 9600, 19200, 38400, 57600, 115200.

**System Settings** – в разделе можно изменить системные настройки устройства.

- *System Name* – системное имя устройства;
- *System Contact* – контактная информация для связи с администратором;
- *System Location* – информация о физическом местоположении устройства.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.4 Меню «Status»

В меню «**Status**» отражается текущее состояние системы, приводится информация о состоянии интерфейсов устройства, регистрируемых на устройстве событиях, подключенных клиентах, радиоокружении и радиостатистике устройства.

### 4.4.1 Подменю «Interfaces»

В подменю «**Interfaces**» представлена информация о текущем состоянии проводных интерфейсов и настройках беспроводной сети.

Для быстрого перехода в меню настроек проводного интерфейса «*Wired Settings*» или беспроводного интерфейса «*Wireless Settings*» нажмите на ссылку «*Edit*» в соответствующем разделе.

*View settings for network interfaces*

Click "Refresh" button to refresh the page.

**Wired Settings** [\( Edit \)](#)

**Internal Interface**

MAC Address	E0:D9:E3:51:E4:E1
VLAN ID	1
IP Address	192.168.44.29
Subnet Mask	255.255.255.0
IPv6 Address	::
IPv6 Address Status	
IPv6 Autoconfigured Global Addresses	
IPv6 Link Local Address	
IPv6-DNS-1	::
IPv6-DNS-2	::
DNS-1	172.16.0.1
DNS-2	172.16.0.3
Default Gateway	192.168.43.1

[Show interfaces table](#)

---

**Wireless Settings** [\( Edit \)](#)

**Radio One**

Status	On
MAC Address	E0:D9:E3:51:E4:E0
Mode	IEEE 802.11a/n/ac
Channel	48 (5240 MHz)
Operational bandwidth, MHz	20
Transmit Power Output, dBm	19.25

[Show interfaces table](#)

**Radio Two**

Status	On
MAC Address	E0:D9:E3:51:E4:F0
Mode	IEEE 802.11b/g/n
Channel	6 (2437 MHz)
Operational bandwidth, MHz	20
Transmit Power Output, dBm	15.00

[Show interfaces table](#)

**Wired Settings** – приводится информация о текущем состоянии проводного интерфейса:

- *MAC Address* – MAC-адрес Ethernet-интерфейса устройства;
- *VLAN ID* – номер VLAN для управления устройством;
- *IP Address* – IP-адрес управления устройства;
- *Subnet Mask* – маска IPv4-сети управления;
- *IPv6 Address* – IPv6-адрес управления устройства;
- *IPv6 Autoconfigured Global Addresses* – список сконфигурированных автоматически IPv6-адресов;
- *IPv6 Link Local Address* – автоматически сконфигурированный локальный IPv6-адрес;
- *IPv6-DNS-1* – адрес первого DNS-сервера в IPv6-сети;
- *IPv6-DNS-2* – адрес второго DNS-сервера в IPv6-сети;
- *DNS-1* – адрес первого DNS-сервера в IPv4-сети;
- *DNS-2* – адрес второго DNS-сервера в IPv4-сети;
- *Default Gateway* – шлюз по умолчанию в IPv4-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 согласно стандартам IEEE 802.11;
- *Channel* – номер беспроводного канала, на котором работает радиоинтерфейс;
- *Operational bandwidth* – ширина полосы частот канала, на котором работает радиоинтерфейс, МГц;
- *Transmit Power Output* – фактическая излучаемая мощность передатчика, дБм.

Wireless Settings <a href="#">( Edit )</a>				
<b>Radio One</b>				
Status	On			
MAC Address	E8:28:C1:C1:27:60			
Mode	IEEE 802.11a/n/ac			
Channel	157 (5785 MHz)			
Operational Bandwidth, MHz	80			
Transmit Power Output, dBm	19.25			
<a href="#">Hide interfaces table</a>				
Interface	Status	MAC Address	VLAN ID	Name (SSID)
wlan0:vap0	up	E8:28:C1:C1:27:60	1505	Eltex VAP
wlan0:vap1	down	E8:28:C1:C1:27:61	1	Virtual Access Point 1
wlan0:vap2	down	E8:28:C1:C1:27:62	1	Virtual Access Point 2
wlan0:vap3	down	E8:28:C1:C1:27:63	1	Virtual Access Point 3
wlan0:vap4	down	E8:28:C1:C1:27:64	1	Virtual Access Point 4
wlan0:vap5	down	E8:28:C1:C1:27:65	1	Virtual Access Point 5
wlan0:vap6	down	E8:28:C1:C1:27:66	1	Virtual Access Point 6
wlan0:vap7	up	E8:28:C1:C1:27:67	1	Virtual Access Point 7
wlan0:vap8	down	E8:28:C1:C1:27:68	1	Virtual Access Point 8
wlan0:vap9	down	E8:28:C1:C1:27:69	1	Virtual Access Point 9
wlan0:vap10	down	E8:28:C1:C1:27:6A	1	Virtual Access Point 10
wlan0:vap11	down	E8:28:C1:C1:27:6B	1	Virtual Access Point 11
wlan0:vap12	down	E8:28:C1:C1:27:6C	1	Virtual Access Point 12
wlan0:vap13	down	E8:28:C1:C1:27:6D	1	Virtual Access Point 13
wlan0:vap14	down	E8:28:C1:C1:27:6E	1	Virtual Access Point 14
wlan0:vap15	down	E8:28:C1:C1:27:6F	1	Virtual Access Point 15
wlan0wds0	down	-	-	-
wlan0wds1	down	-	-	-
wlan0wds2	down	-	-	-
wlan0wds3	down	-	-	-
<b>Radio Two</b>				
Status	Off			
MAC Address	E8:28:C1:C1:27:70			
Mode	IEEE 802.11b/g/n			
<a href="#">Show interfaces table</a>				

При нажатии на ссылку «**Show interfaces table**» в разделах «*Wired Settings*» и «*Wireless Settings*» становится доступной таблица интерфейсов, содержащая следующую информацию:

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

Для того чтобы скрыть таблицу нажмите на ссылку «**Hide interfaces table**».

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.2 Подменю «Events»

В подменю «**Events**» можно просмотреть список событий, происходящих с устройством, а также настроить перенаправление событий на сторонний SYSLOG-сервер.

*View events generated by this access point*

<p><b>Options</b></p> <p>Persistence <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>Severity <input type="text" value="7"/> (Range : 1 - 512)</p> <p>Depth <input type="text" value="512"/> (Range : 1 - 512)</p> <p>Click "Update" to save the new settings.</p> <p><input type="button" value="Update"/></p>	<p><b>Relay Options</b></p> <p>Relay Log <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled</p> <p>Relay Host <input type="text"/> (xxx.xxx.xxx.xxx/xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/ Hostname max 253 Characters)</p> <p>Relay Port <input type="text" value="514"/> (Range: 1 - 65535, Default: 514)</p> <p>Click "Update" to save the new settings.</p> <p><input type="button" value="Update"/></p>
--	---

---

**Events**

Click "Refresh" button to refresh the page.

Time Settings (NTP)	Type	Service	Description
Apr 20 2021 08:28:00	debug	hostapd[21316]	Station f2:2b:5a:02:68:5e associated, time = 0.001250
Apr 20 2021 08:28:00	debug	hostapd[21316]	station: f2:2b:5a:02:68:5e associated rssi -57(-57)
Apr 20 2021 08:28:00	info	hostapd[21316]	STA f2:2b:5a:02:68:5e associated with BSSID e8:28:c1:c1:27:60
Apr 20 2021 08:28:00	info	hostapd[21316]	Assoc request from f2:2b:5a:02:68:5e BSSID e8:28:c1:c1:27:60 SSID Eitex VAP
Apr 20 2021 08:27:20	info	dman[1233]	The AP startup configuration was updated successfully.
Apr 20 2021 08:27:20	debug	clusterd[1951]	dman sent notification that config has changed

Click "Clear All" to erase all events.

**Options** – в данном разделе выполняется настройка следующих 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 существующих уровней важности приведено в таблице ниже.

Таблица 5 – Описание категорий важности событий

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. При превышении данного порога происходит перезапись сообщения, которое хранится в

системе дольше всех, новым сообщением. Параметр принимает значения в диапазоне от 1 до 512. Значение по умолчанию – 512.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**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. Может быть задан IPv4-адрес, IPv6-адрес или доменное имя удаленного сервера.
- *Relay Port* – номер порта (layer 4), на который перенаправляются сообщения. Принимает значения в диапазоне от 1 до 65535. Значение по умолчанию – 514.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**Events** – в данном разделе можно просмотреть список информационных сообщений в реальном времени, содержащий следующую информацию:

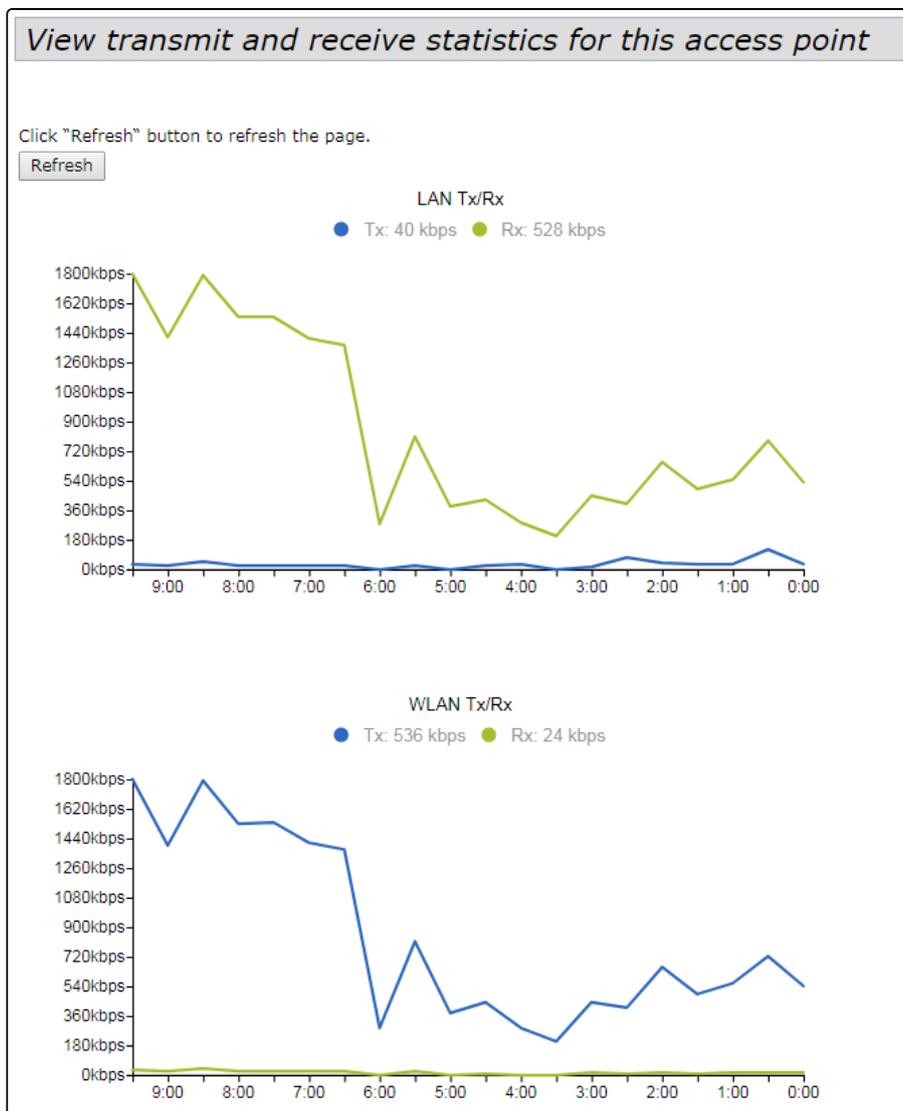
- *Time Setting (NTP)* – время, когда событие было сгенерировано;
- *Type* – уровень важности события (таблица 5);
- *Service* – имя процесса, сгенерировавшего сообщение;
- *Description* – описание события.

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

Для удаления всех сообщений нажмите кнопку «Clear All».

#### 4.4.3 Подменю «Transmit/Receive»

В подменю «**Transmit/Receive**» отображаются графики скорости приема/передачи трафика за последние 10 минут, а также информация о количестве переданного/полученного трафика с момента включения точки доступа.



#### 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.

Transmit					
Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	8715267	1529876381	0	0	0
isatap0	0	0	0	0	0
wlan0:vap0	5163390	4117748340	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	29704	11964655	0	0	0
wlan0:vap3	196384	58061993	2050	3094107	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	11045	9274028	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	313121	415719017	0	0	0
wlan1:vap2	7473043	10448367916	576124	869642147	0
wlan1:vap3	1563879	745541384	0	0	0
wlan1:vap4	0	0	0	0	0

Описание таблицы «Transmit»:

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

Receive					
Interface	Total packets	Total bytes	Total Drop Packets	Total Drop Bytes	Errors
LAN	20095269	17273106147	28727	0	16
isatap0	0	0	0	0	0
wlan0:vap0	1589456	244114016	0	0	0
wlan0:vap1	0	0	0	0	0
wlan0:vap2	6437	814291	0	0	0
wlan0:vap3	39272	6695565	0	0	0
wlan0:vap4	0	0	0	0	0
wlan0:vap5	0	0	0	0	0
wlan0:vap6	4486	434660	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	282058	21248406	0	0	0
wlan1:vap2	5041611	714677115	3525	4954835	0
wlan1:vap3	482182	69990869	0	0	0
wlan1:vap4	0	0	0	0	0

Описание таблицы «Receive»:

- *Interface* – имя интерфейса;
- *Total packets* – количество успешно принятых пакетов;
- *Total bytes* – количество успешно принятых байт;
- *Total Drop Packets* – количество пакетов, отброшенных при получении;
- *Total Drop Bytes* – количество байт, отброшенных при получении;
- *Errors* – количество ошибок.

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.4 Подменю «Wireless Multicast Forwarding Statistic»

В подменю «**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.

---

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					

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.

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 «IGMP Statistics»:

- *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.

#### 4.4.5 Подменю «Client Associations»

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

View list of currently associated client stations											
Click "Refresh" button to refresh the page.											
<input type="button" value="Refresh"/>											
Total Number of Associated Clients 3											
SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate Quality	Link Capacity	Status
Eltex-Local (wlan0)	<a href="#">58:48:22:a3:13:96</a>	192.168.40.149		00:02:10	-63	26 dB	-89 dBm	78%	74%	84%	Yes
Eltex-Guest (wlan1vap2)	<a href="#">e4:23:54:04:36:83</a>	192.168.41.88	android-89375627ba2fc0f3	00:00:08	-74	18 dB	-92 dBm	72%	72%	20%	Yes
Eltex-Local (wlan1vap3)	<a href="#">70:8b:cd:72:b4:5e</a>			00:00:04	-62	30 dB	-92 dBm	100%	100%	100% (not changed)	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;
- **Uptime** – продолжительность сессии клиента;
- **RSSI** – уровень принимаемого сигнала, дБм;
- **SNR** – уровень отношения сигнал/шум, дБ;
- **Noise** – уровень шума, дБм;
- **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 Authorized** – статус авторизации.

При нажатии на MAC-адрес клиента раскрывается подробная информация о его работе и статистика переданного/полученного трафика по данному клиенту.

## View list of currently associated client stations

Click "Refresh" button to refresh the page.

Refresh

Total Number of Associated Clients 3

SSID	Station	IP Address	Hostname	Uptime	RSSI	SNR	Noise	Link Quality	Rate	Quality	Link Capacity	Status																																																																																																																			
Eltex-Local (wlan0)	<a href="#">58:48:22:a3:13:96</a>	192.168.40.149		00:02:19	-62	27	-89	92%	100%	75%		Authorized Yes																																																																																																																			
Eltex-Guest (wlan1vap2)	<a href="#">58:48:22:a3:13:96</a>		58:48:22:a3:13:96									Yes																																																																																																																			
Eltex-Local (wlan1vap3)	<a href="#">58:48:22:a3:13:96</a>		802.11ac									Yes																																																																																																																			
<table border="1"> <tr> <td>MAC:</td> <td>58:48:22:a3:13:96</td> <td>Connection time:</td> <td>00:02:19</td> </tr> <tr> <td>AID:</td> <td>1</td> <td>Bandwidth:</td> <td>20MHz</td> </tr> <tr> <td>SSID:</td> <td>Eltex-Local</td> <td>PS Mode:</td> <td>on</td> </tr> <tr> <td>Mode:</td> <td>802.11ac</td> <td>Auth Mode:</td> <td>WPA2</td> </tr> <tr> <td>RSSI:</td> <td>-62</td> <td>Encryption:</td> <td>AES-CCMP</td> </tr> <tr> <td>VLAN:</td> <td>148</td> <td>Listen Interval:</td> <td>10</td> </tr> <tr> <td>Tx actual rate:</td> <td>1</td> <td>Rx actual rate:</td> <td>0</td> </tr> <tr> <td>Tx/Rx Packets:</td> <td colspan="3">83388/16329</td> </tr> <tr> <td>Tx/Rx Drop Packets:</td> <td colspan="3">0/0</td> </tr> <tr> <td>Tx/Rx Bytes:</td> <td colspan="3">43398215/2132001</td> </tr> <tr> <td>Tx/Rx Drop Bytes:</td> <td colspan="3">0/0</td> </tr> <tr> <td>Tx/Rx Rate:</td> <td colspan="3">6/1 Mbps</td> </tr> <tr> <td colspan="4">Tx/Rx Statistics:</td> </tr> <tr> <td></td> <td>MCS</td> <td>Rx Pkts</td> <td>Tx Pkts</td> <td>Tx Succ Pkts</td> <td>Tx Retries</td> <td>Tx Period Retries</td> </tr> <tr> <td></td> <td>1mbps</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>2mbps</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>5mbps5</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>6mbps</td> <td>856</td> <td>136302</td> <td>10721</td> <td>92.1%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>9mbps</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>11mbps</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>12mbps</td> <td>1686</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> <tr> <td></td> <td>18mbps</td> <td>0</td> <td>0</td> <td>0</td> <td>0.0%</td> <td>0.0%</td> </tr> </table>													MAC:	58:48:22:a3:13:96	Connection time:	00:02:19	AID:	1	Bandwidth:	20MHz	SSID:	Eltex-Local	PS Mode:	on	Mode:	802.11ac	Auth Mode:	WPA2	RSSI:	-62	Encryption:	AES-CCMP	VLAN:	148	Listen Interval:	10	Tx actual rate:	1	Rx actual rate:	0	Tx/Rx Packets:	83388/16329			Tx/Rx Drop Packets:	0/0			Tx/Rx Bytes:	43398215/2132001			Tx/Rx Drop Bytes:	0/0			Tx/Rx Rate:	6/1 Mbps			Tx/Rx Statistics:					MCS	Rx Pkts	Tx Pkts	Tx Succ Pkts	Tx Retries	Tx Period Retries		1mbps	0	0	0	0.0%	0.0%		2mbps	0	0	0	0.0%	0.0%		5mbps5	0	0	0	0.0%	0.0%		6mbps	856	136302	10721	92.1%	0.0%		9mbps	0	0	0	0.0%	0.0%		11mbps	0	0	0	0.0%	0.0%		12mbps	1686	0	0	0.0%	0.0%		18mbps	0	0	0	0.0%	0.0%
MAC:	58:48:22:a3:13:96	Connection time:	00:02:19																																																																																																																												
AID:	1	Bandwidth:	20MHz																																																																																																																												
SSID:	Eltex-Local	PS Mode:	on																																																																																																																												
Mode:	802.11ac	Auth Mode:	WPA2																																																																																																																												
RSSI:	-62	Encryption:	AES-CCMP																																																																																																																												
VLAN:	148	Listen Interval:	10																																																																																																																												
Tx actual rate:	1	Rx actual rate:	0																																																																																																																												
Tx/Rx Packets:	83388/16329																																																																																																																														
Tx/Rx Drop Packets:	0/0																																																																																																																														
Tx/Rx Bytes:	43398215/2132001																																																																																																																														
Tx/Rx Drop Bytes:	0/0																																																																																																																														
Tx/Rx Rate:	6/1 Mbps																																																																																																																														
Tx/Rx Statistics:																																																																																																																															
	MCS	Rx Pkts	Tx Pkts	Tx Succ Pkts	Tx Retries	Tx Period Retries																																																																																																																									
	1mbps	0	0	0	0.0%	0.0%																																																																																																																									
	2mbps	0	0	0	0.0%	0.0%																																																																																																																									
	5mbps5	0	0	0	0.0%	0.0%																																																																																																																									
	6mbps	856	136302	10721	92.1%	0.0%																																																																																																																									
	9mbps	0	0	0	0.0%	0.0%																																																																																																																									
	11mbps	0	0	0	0.0%	0.0%																																																																																																																									
	12mbps	1686	0	0	0.0%	0.0%																																																																																																																									
	18mbps	0	0	0	0.0%	0.0%																																																																																																																									

- *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, дБм;
- *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 Bytes* – 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»: off – клиент активен, on – клиент находится в «спящем» режиме;
- *Auth Mode* – тип безопасности;
- *Encryption* – тип шифрования;
- *Listen Interval* – количество beacon frame спустя которые клиент должен проверить наличие для него трафика (в случае сна);
- *Rx actual rate* – текущая скорость передачи данных в сторону точки доступа, в кбит/с.

Описание таблицы «Tx/Rx Statistics»:

- *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* – процент дублированных пакетов в сторону клиента;
- *Tx Period Retries* – процент повторно отправленных пакетов за последний период (10 секунд).

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.6 Подменю «TSPEC Client Associations»

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

**View TSPEC Client Association Status and Statistics**

Click "Refresh" button to refresh the page.

Status

Network	Station	TS Identifier	Access Category	Direction	User Priority	Medium Time	Excess Usage Events	VAP	MAC Address	SSID
---------	---------	---------------	-----------------	-----------	---------------	-------------	---------------------	-----	-------------	------

Statistics

Network	Station	TS Identifier	Access Category	Direction	From Station		To Station	
					Packets	Bytes	Packets	Bytes

- *Network* – имя беспроводного интерфейса и имя виртуальной точки доступа на интерфейсе, к которой подключен клиент. Например, запись wlan0var2 означает, что клиент связан с Radio1 виртуальной точкой доступа VAP2; запись wlan1 означает, что клиент связан с VAP0 на Radio2;
- *Station* – MAC-адрес клиента;
- *TS Identifier* – TSPEC идентификатор потока трафика. Может принимать значение от 0 до 7;
- *Access Category* – категория доступа (Voice или Video);
- *Direction* – направление трафика (Uplink/Downlink/Bidirectional);
- *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.

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.7 Подменю «Rogue AP Detection»

В подменю «**Rogue AP Detection**» отображается информация обо всех беспроводных точках доступа, которые устройство детектирует вокруг себя.

**View Rogue AP Detection**

Click "Refresh" button to refresh the page.

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

Click "Update" to save the new settings.

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

**Dangerous AP List**

Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel [BandWidth]	Channel Blocks	Signal	Beacons	Last Beacon	Rates
<input type="button" value="Grant"/>	e8:28:c1:da:cb:88	wlan0	100	AP	Virtual Access Point 7	Off	Off	5	44 [20]	44		1	Tue Apr 20 09:06:34 2021	6,9,12,18,24,36,48,54
<input type="button" value="Grant"/>	e8:28:c1:da:cb:82	wlan1	100	AP	2ac-portal	Off	Off	2.4	1 [20]	1 - 3		38	Tue Apr 20 09:06:36 2021	1,2,5,5,6,9,11,12,18,24,36,48,54

Для обновления информации на странице нажмите кнопку «Refresh».

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

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**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 «Known AP List».
- *MAC* – MAC-адрес точки доступа;
- *Radio* – радиоинтерфейс, которым была обнаружена сторонняя точка доступа;
- *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: *Off* – выключено, *On* – 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 точка доступа;
- *Signal* – уровень сигнала, принимаемый от точки доступа, дБм. При наведении указателя на графическое изображение сигнала демонстрируются 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														
Action	MAC	Radio	Beacon Int.	Type	SSID	Privacy	WPA	Band	Channel [BandWidth]	Channel Blocks	Signal	Beacons	Last Beacon	Rates
Delete	e8:28:c1:da:cb:86	wlan0	100	AP	2ac-portal	Off	5	44 [20]	44		1	Tue Apr 20 09:06:34 2021		

**Save Known AP List to a file**  
Save

**Import Known AP List from a file**  
 Replace  Merge  
 Обзор... Файл не выбран. Import

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

Чтобы удалить точку доступа из данного списка нажмите на кнопку «Delete», после удаления из списка «Known AP List» точка попадет в список обнаруженных 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* – импортируемый список доверенных точек доступа полностью заменит текущий список доверенных точек доступа;
- *Merge* – доверенные точки доступа из импортируемого списка будут добавлены к точкам доступа, находящимся в импортируемом списке в данный момент времени.

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

## 4.4.8 Подменю «TSPEC Status and Statistics»

В подменю «**TSPEC Status and Statistics**» отображается информация о TSPEC-сессиях на радиointерфейсах.

View TSPEC Status and Statistics						
Click "Refresh" button to refresh the page.						
<input type="button" value="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

Описание таблиц «AP Status» и «VAP Status»:

- *Interface* – имя интерфейса;
- *Access Category* – категория доступа (Voice, Video, Best Effort, Background);
- *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* – среднее время простоя полосы в данной категории.

Transmit								
Radio	Access Category	Total Packets	Total Bytes					
wlan0	Best Effort	0	0					
wlan0	Background	0	0					
wlan0	Voice	0	0					
wlan0	Video	0	0					
wlan1	Best Effort	0	0					
wlan1	Background	0	0					
wlan1	Voice	0	0					
wlan1	Video	0	0					
Interface	Total Voice Packets	Total Voice Bytes	Total Video Packets	Total Video Bytes	Total Best Effort Packets	Total Best Effort Bytes	Total Background Packets	Total Background Bytes
wlan0:vap0	0	0	0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0	0	0	0
wlan0:vap2	0	0	0	0	0	0	0	0
wlan0:vap3	0	0	0	0	0	0	0	0
wlan0:vap4	0	0	0	0	0	0	0	0
wlan0:vap5	0	0	0	0	0	0	0	0
wlan0:vap6	0	0	0	0	0	0	0	0
wlan0:vap7	0	0	0	0	0	0	0	0
wlan0:vap8	0	0	0	0	0	0	0	0
wlan0:vap9	0	0	0	0	0	0	0	0
wlan0:vap10	0	0	0	0	0	0	0	0
wlan0:vap11	0	0	0	0	0	0	0	0
wlan0:vap12	0	0	0	0	0	0	0	0
wlan0:vap13	0	0	0	0	0	0	0	0
wlan0:vap14	0	0	0	0	0	0	0	0
wlan0:vap15	0	0	0	0	0	0	0	0
wlan1:vap0	0	0	0	0	0	0	0	0
wlan1:vap1	0	0	0	0	0	0	0	0

Описание таблиц «Transmit»:

- *Radio* – имя радиointерфейса;
- *Access Category* – категория доступа (Voice, Video, Best Effort, Background);
- *Total Packets* – общее количество пакетов данной категории доступа, отправленных радиointерфейсом;
- *Total Bytes* – общее количество байтов данной категории доступа, отправленных радиointерфейсом;
- *Interface* – номер виртуальной точки доступа;
- *Total Voice Packets* – общее количество пакетов категории Voice, отправленных с данной VAP;
- *Total Voice Bytes* – общее количество байтов категории Voice, отправленных с данной VAP;
- *Total Video Packets* – общее количество пакетов категории Video, отправленных с данной VAP;
- *Total Video Bytes* – общее количество байтов категории Video, отправленных с данной VAP;
- *Total Best Effort Packets* – общее количество пакетов категории Best Effort, отправленных с данной VAP;
- *Total Best Effort Bytes* – общее количество байтов категории Best Effort, отправленных с данной VAP;
- *Total Background Packets* – общее количество пакетов категории Background, отправленных с данной VAP;
- *Total Background Bytes* – общее количество байтов категории Background, отправленных с данной VAP.

Receive								
Radio	Access Category	Total Packets	Total Bytes					
wlan0	Best Effort	0	0					
wlan0	Background	0	0					
wlan0	Voice	0	0					
wlan0	Video	0	0					
wlan1	Best Effort	0	0					
wlan1	Background	0	0					
wlan1	Voice	0	0					
wlan1	Video	0	0					
Interface	Total Voice Packets	Total Voice Bytes	Total Video Packets	Total Video Bytes	Total Best Effort Packets	Total Best Effort Bytes	Total Background Packets	Total Background Bytes
wlan0:vap0	0	0	0	0	0	0	0	0
wlan0:vap1	0	0	0	0	0	0	0	0
wlan0:vap2	0	0	0	0	0	0	0	0
wlan0:vap3	0	0	0	0	0	0	0	0
wlan0:vap4	0	0	0	0	0	0	0	0
wlan0:vap5	0	0	0	0	0	0	0	0
wlan0:vap6	0	0	0	0	0	0	0	0
wlan0:vap7	0	0	0	0	0	0	0	0
wlan0:vap8	0	0	0	0	0	0	0	0
wlan0:vap9	0	0	0	0	0	0	0	0
wlan0:vap10	0	0	0	0	0	0	0	0
wlan0:vap11	0	0	0	0	0	0	0	0
wlan0:vap12	0	0	0	0	0	0	0	0
wlan0:vap13	0	0	0	0	0	0	0	0
wlan0:vap14	0	0	0	0	0	0	0	0
wlan0:vap15	0	0	0	0	0	0	0	0
wlan1:vap0	0	0	0	0	0	0	0	0
wlan1:vap1	0	0	0	0	0	0	0	0

Описание таблиц «Receive»:

- *Radio* – имя радиоинтерфейса;
- *Access Category* – категория доступа (Voice, Video, Best Effort, Background);
- *Total Packets* – общее количество пакетов данной категории доступа, принятых радиоинтерфейсом;
- *Total Bytes* – общее количество байт данной категории доступа, принятых радиоинтерфейсом;
- *Interface* – номер виртуальной точки доступа;
- *Total Voice Packets* – общее количество пакетов категории Voice, принятых на данной VAP;
- *Total Voice Bytes* – общее количество байт категории Voice, принятых на данной VAP;
- *Total Video Packets* – общее количество пакетов категории Video, принятых на данной VAP;
- *Total Video Bytes* – общее количество байт категории Video, принятых на данной VAP;
- *Total Best Effort Packets* – общее количество пакетов категории Best Effort, принятых на данной VAP;
- *Total Best Effort Bytes* – общее количество байт категории Best Effort, принятых на данной VAP;
- *Total Background Packets* – общее количество пакетов категории Background, принятых на данной VAP;
- *Total Background Bytes* – общее количество байтов категории Background, принятых на данной VAP.

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.9 Подменю «TSPEC AP Statistics»

В подменю «**TSPEC AP Statistics**» отображается статистика по количеству переданного/полученного потоков трафика различных категорий (Voice, Video, Best Effort, Background).

**View TSPEC AP Statistics**

Click "Refresh" button to refresh the page.

**TSPEC Statistics Summary for Voice ACM**

Total Voice TS Accepted	0
Total Voice TS Rejected	0

---

**TSPEC Statistics Summary for Video ACM**

Total Video TS Accepted	0
Total Video TS Rejected	0

---

**TSPEC Statistics Summary for Best Effort ACM**

Total Best Effort TS Accepted	0
Total Best Effort TS Rejected	0

---

**TSPEC Statistics Summary for Background ACM**

Total Background TS Accepted	0
Total Background TS Rejected	0

- *TSPEC Statistics Summary for Voice ACM* – общее количество принятых (Accepted) и отклоненных (Rejected) потоков трафика категории Voice;
- *TSPEC Statistics Summary for Video ACM* – общее количество принятых (Accepted) и отклоненных (Rejected) потоков трафика категории Video;
- *TSPEC Statistics Summary for Best Effort ACM* – общее количество принятых (Accepted) и отклоненных (Rejected) потоков трафика категории Best Effort;
- *TSPEC Statistics Summary for Background ACM* – общее количество принятых (Accepted) и отклоненных (Rejected) потоков трафика категории Background.

Для обновления информации на странице нажмите кнопку «Refresh».

## 4.4.10 Подменю «Radio Statistics»

В подменю «**Radio Statistics**» отображается подробная информация о пакетах и байтах, переданных/полученных по беспроводному интерфейсу.

### View Radio Statistics

Click "Refresh" button to refresh the page.

Radio 1     Radio 2

WLAN Packets Received:	4293459	WLAN Bytes Received:	828073107
WLAN Packets Transmitted:	9720109	WLAN Bytes Transmitted:	7728537587
WLAN Packets Receive Dropped:	1847	WLAN Bytes Receive Dropped:	2696185
WLAN Packets Transmit Dropped:	55726	WLAN Bytes Transmit Dropped:	81298424
Fragments Received:	126939	Fragments Transmitted:	8894441
Multicast Frames Received:	48590	Multicast Frames Transmitted:	725984
Duplicate Frame Count:	112438	Failed Transmit Count:	114919
Transmit Retry Count:	88349	Multiple Retry Count:	29411
RTS Success Count:	6037615	RTS Failure Count:	301616
ACK Failure Count:	698557	FCS Error Count:	41080635
Transmitted Frame Count:	15158478	WEP Undecryptable Count:	1437

Выставьте флаг у наименования радиоинтерфейса, по которому необходимо вывести подробную информацию (Radio 1 или Radio 2):

- *WLAN Packets Received* – общее количество пакетов, полученных точкой доступа через данный радиоинтерфейс;
- *WLAN Bytes Received* – общее количество байт, полученных точкой доступа через данный радиоинтерфейс;
- *WLAN Packets Transmitted* – общее количество, пакетов переданных точкой доступа через данный радиоинтерфейс;
- *WLAN Bytes Transmitted* – общее количество байт, переданных точкой доступа через данный радиоинтерфейс;
- *WLAN Packets Receive Dropped* – количество пакетов, полученных точкой доступа через данный радиоинтерфейс, которые были отброшены;
- *WLAN Bytes Receive Dropped* – количество байт, полученных точкой доступа через данный радиоинтерфейс, которые были отброшены;
- *WLAN Packets Transmit Dropped* – количество пакетов, переданных точкой доступа через данный радиоинтерфейс, которые были отброшены;
- *WLAN Bytes Transmit Dropped* – количество байт, переданных точкой доступа через данный радиоинтерфейс, которые были отброшены;
- *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);

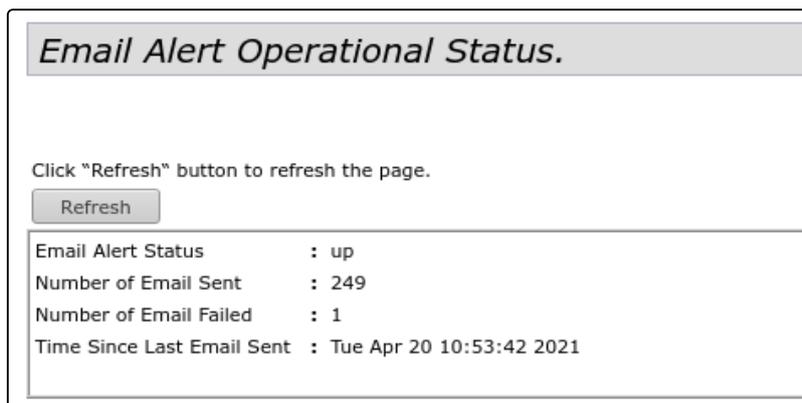
- *ACK Failure Count* – количество пакетов, на которые не пришли подтверждения о успешном приеме (ACK);
- *FCS Error Count* – количество кадров, не прошедших проверку контрольной суммы;
- *Transmitted Frame Count* – количество успешно переданных кадров;
- *WEP Undecryptable Count* – количество пакетов, которые не удалось расшифровать (WEP).

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.4.11 Подменю «Email Alert Status»

В подменю «**Email Alert Status**» приводится информация об отправленных по электронной почте сообщениях, сгенерированных на основе журнала событий.

Настроить отправку сообщений можно в подменю «Email Alert», расположенном в меню «Services».



- *Email Alert Status* – статус работы оповещения по электронной почте о работе устройства:
  - *Up* – оповещение включено;
  - *Down* – оповещение выключено.
- *Number of Email Sent* – общее количество сообщений, отправленных на данный момент;
- *Number of Email Failed* – общее количество сообщений, которые были потеряны, на данный момент;
- *Time Since Last Email Sent* – дата и время отправки последнего сообщения.

Для обновления информации на странице нажмите кнопку «Refresh».

## 4.5 Меню «Manage»

### 4.5.1 Подменю «Ethernet Settings»

В подменю «**Ethernet Settings**» выполняются сетевые настройки устройства.

### Modify Ethernet (Wired) settings

Hostname  (Range : 1 - 63 characters)

---

**Internal Interface Settings**

MAC Address

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

Untagged VLAN  Enabled  Disabled

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

Connection Type

Static IP Address  .  .  .

Subnet Mask  .  .  .

Default Gateway  .  .  .

DNS Nameservers  Dynamic  Manual

.  .  .

.  .  .

Click "Update" to save the new settings.

- *Hostname* – сетевое имя устройства. Может содержать от 1 до 63 символов и состоять из латинских заглавных и строчных букв, цифр, знака дефис «-» (обратите внимание, что дефис не может быть последним символом в сетевом имени устройства);
- *MAC Address* – MAC-адрес Ethernet-интерфейса устройства;
- *Management VLAN ID* – идентификатор VLAN, используемый для доступа к устройству. Принимает значения от 1 до 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 от 1 до 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 сетевые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static IP» для редактирования станут доступны следующие параметры:
    - *Static IP Address* – IP-адрес устройства в сети провайдера;
    - *Subnet Mask* – маска внешней подсети;

- *Default Gateway* – IP-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):
  - *Dynamic* – будут использованы DNS-сервера, полученные по DHCP;
  - *Manual* – необходимо указать DNS-сервера вручную.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.2 Подменю «Management IPv6»

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

### Modify Management IPv6

---

**Management IPv6**

IPv6 Connection Type DHCPv6 ▾

IPv6 Admin Mode  Enabled  Disabled

IPv6 Auto Config Admin Mode  Enabled  Disabled

Static IPv6 Address  (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Static IPv6 Address Prefix Length  (Range: 0 - 128, Default: 0)

Static IPv6 Address Status

IPv6 Autoconfigured Global Addresses

IPv6 Link Local Address

Default IPv6 Gateway  (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

IPv6 DNS Nameservers  Dynamic  Manual

(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Click "Update" to save the new settings.

- *IPv6 Connection Type* – выбор использования статического (*Static IPv6*) или динамического (DHCPv6) IPv6-адреса устройства;
- *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.

При установке типа «*Static IPv6*» в параметре «*IPv6 Connection Type*» для редактирования становятся доступными следующие параметры:

- *Static IPv6 Address* – статический IPv6-адрес устройства. Точка доступа может иметь статический IPv6-адрес, даже если адреса уже были настроены автоматически через «Auto Config»;
- *Static IPv6 Address Prefix Length* – префикс статического IPv6-адреса. Принимает значение от 0 до 128. По умолчанию – 0;
- *Static IPv6 Address Status* – просмотр рабочего статуса статически сконфигурированного IPv6-адреса. Параметр принимает следующие 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):
  - *Dynamic* – будут использованы DNS-сервера, полученные по DHCP;
  - *Manual* – необходимо указать DNS-сервера вручную.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.3 Подменю «IPv6 Tunnel»

В подменю «**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 IPv4-сети. Поддержка данного функционала позволяет устройству устанавливать связь с удаленными IPv6-хостами.

### Modify IPv6 Tunnel Settings

---

**IPv6 Tunnel**

ISATAP Status  Enabled  Disabled

ISATAP Capable Host  (xxx.xxx.xxx.xxx / Hostname max 253 characters, Default: isatap)

ISATAP Query Interval  sec. (Range: 120-3600, Default: 120)

ISATAP Solicitation Interval  sec. (Range: 120-3600, Default: 120)

ISATAP IPv6 Link Local Address

ISATAP IPv6 Global Address

Click "Update" to save the new settings.

- *ISATAP Status* – режим работы протокола ISATAP:
  - *Enabled* – разрешена работа по протоколу ISATAP;
  - *Disabled* – запрещена работа по протоколу ISATAP.
- *ISATAP Capable Host* – IP-адрес или DNS-имя маршрутизатора ISATAP. Значение – isatap;
- *ISATAP Query Interval* – интервал времени между DNS-запросами. Принимает значение от 120 до 3600 секунд. По умолчанию – 120 секунд;
- *ISATAP Solicitation Interval* – интервал времени между сообщениями опроса маршрутизатора ISATAP. Принимает значения от 120 до 3600 секунд. По умолчанию – 120 секунд;
- *ISATAP IPv6 Link Local Address* – локальный IPv6-адрес устройства;
- *ISATAP IPv6 Global Address* – глобальный IPv6-адрес устройства.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.4 Подменю «Wireless Settings»

В подменю «**Wireless Settings**» выполняются настройки беспроводной Wi-Fi сети. Устройство имеет 2 независимых физических радиоинтерфейса, каждый из которых работает в своем режиме и диапазоне. Radio 1 работает в диапазоне 5 ГГц, Radio 2 – в диапазоне 2.4 ГГц.

В представленном разделе меню приводится отдельная настройка для каждого радиоинтерфейса.

- *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, что влияет на автоматический выбор канала в режиме Channel = Auto. Если клиентское оборудование лицензировано 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 диапазона 5 ГГц).
  - *Off* – максимальное значение ЭИИМ ограничивается физическими характеристиками передатчика. Для устройств WEP-2ac и WEP-2ac Smart максимальное значение ЭИИМ для диапазона 2.4 ГГц – 18 дБм, для диапазона 5 ГГц – 21 дБм.
- *TSPEC Violation Interval* – интервал времени в секундах, за который точка доступа должна сообщить через журнал событий или посредством SNMP-trap о присоединенных клиентах, которые не поддерживают обязательные процедуры допуска. Принимает значение от 0 до 900 секунд. По умолчанию – 300 секунд;

- *Global Isolation* – при установленном флаге включена изоляция трафика между клиентами разных VAP и разных радиointерфейсов;
- *Radio Interface* – состояние радиointерфейса:
  - *On* – при установленном флаге радиointерфейс активен;
  - *Off* – при установленном флаге радиointерфейс выключен.
- *MAC Address* – MAC-адрес радиointерфейса;
- *Mode* – выбор режима работы беспроводного интерфейса согласно стандартам IEEE 802.11;
- *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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.5 Подменю «Radio»

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

### Modify radio settings

Radio 1

---

Status  On  Off

Mode IEEE 802.11a/n/ac

Channel Auto

Channel Update Period Off

Limit Channels

Channel	36	40	44	48	52	56	60	64	132	136	140	144	149	153	157	161	All
Use	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>												

Channel Bandwidth 80 MHz

Primary Channel Lower

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

Advanced Settings +

TSPEC Settings +

Click "Update" to save the new settings.

Update

- *Radio* – выбор беспроводного Wi-Fi интерфейса. Radio 1 работает в диапазоне 5 ГГц, Radio 2 работает в диапазоне 2.4 ГГц;
- *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 беспроводного интерфейса согласно стандартам IEEE 802.11.
  - Для Radio 1, работающего в диапазоне 5 ГГц:
    - *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 866 Мбит/с;
- *IEEE 802.11n/ac* – частотный диапазон 5 ГГц, максимальная скорость передачи 866 Мбит/с. Возможно подключение клиентов только с поддержкой стандартов IEEE 802.11n/ac.
- Для Radio 2, работающего в диапазоне 2.4 ГГц:
  - *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 300 Мбит/с;
  - *2.4 GHz IEEE 802.11n* – частотный диапазон 2.4 ГГц, максимальная скорость передачи 300 Мбит/с. Возможно подключение клиентов только с поддержкой стандарта IEEE 802.11n.
- *Channel* – выбор радиоканала для работы Wi-Fi интерфейса. При выборе значения «Auto» автоматически определяется и выставляется наименее зашумленный канал (с учетом заданного региона), на котором работает наименьшее количество точек доступа;
- *Channel Update Period* – период времени, через который будет происходить автоматический выбор оптимального канала;
- *Limit Channels* – список каналов, из которых точка доступа может выбрать оптимальный для работы канал в режиме «Auto»;
- *Channel Bandwidth* – ширина полосы пропускания;
- *Primary Channel* – параметр может быть изменен только при ширине канала (Channel Bandwidth), равной 40 МГц. Канал 40 МГц можно считать состоящим из двух каналов по 20 МГц, которые граничат в частотной области. Эти два канала по 20 МГц называют первичным и вторичным каналами. Первичный канал используется клиентами стандарта IEEE 802.11n, 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* – регулировка мощности сигнала передатчика Wi-Fi в дБм.
  - При включенном режиме *Transmit Power Control* параметр принимает следующие значения:
    - в диапазоне 2.4 ГГц (Radio 2) – от 8 до 16, по умолчанию – 16;
    - в диапазоне 5 ГГц (Radio 1) на WEP-2ac – от 1 до 19, на WEP-2ac Smart – от 11 до 19, по умолчанию – 19.
  - При отключенном режиме *Transmit Power Control* параметр принимает следующие значения:
    - в диапазоне 2.4 ГГц (Radio 2) – от 8 до 18, по умолчанию – 18;
    - в диапазоне 5 ГГц (Radio 1) на WEP-2ac – от 1 до 21, на WEP-2ac Smart – от 11 до 21, по умолчанию – 21.

✓ Клиентские Wi-Fi устройства могут не поддерживать некоторые частотные каналы. Если нет информации о каналах, поддерживаемых клиентами, рекомендуется назначать частотные каналы 1-11 для диапазона 2.4 ГГц и 36-48 для диапазона 5 ГГц.

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

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)

- *OBSS Coexistence* – режим автоматической смены ширины канала с 40 МГц на 20 МГц при загруженном радиоэфире:
  - *On* – режим включен;
  - *Off* – 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 для редактирования только в настройках интерфейса Radio 1, работающего в диапазоне частот 5 ГГц. Параметр может принимать значения:
  - *On* – поддержка механизма включена;
  - *Off* – 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. Уменьшение защитного интервала увеличивает пропускную способность. Поле доступно для редактирования при условии, что выбранный режим работы радиоинтерфейса включает в себя стандарт IEEE 802.11n. Параметр может принимать значения:
  - *Yes* – точка доступа передает данные, используя защитный интервал в 400 нс при общении с клиентами, которые также поддерживают короткий защитный интервал;
  - *No* – точка доступа передает данные, используя защитный интервал в 800 нс.
- *STBC Mode* – метод пространственно-временного блочного кодирования, направленный на повышение надежности передачи данных. Поле доступно для редактирования при условии, что выбранный режим работы радиоинтерфейса включает в себя стандарт IEEE 802.11n. Параметр может принимать следующие значения:
  - *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. Параметр принимает значение от 20 до 2000 мс. По умолчанию – 100 мс.

DTIM Period	<input type="text" value="2"/> (Range: 1-255)
Fragmentation Threshold	<input type="text" value="2346"/> (Range: 256-2346, Even Numbers)
RTS Threshold	<input type="text" value="2347"/> (Range: 0-65535)
Maximum Stations	<input type="text" value="200"/> (Range: 0-200)
VLAN List	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Remove Selected"/> (Range: 1-4094, 20 vlan-ids max)
Fixed Multicast Rate	<input type="button" value="Auto"/> Mbps
Frame-burst Support	<input type="button" value="Off"/> [Boosts Downstream Throughput]

- *DTIM Period* – интервал времени перед отправкой сигнала беспроводному клиенту, находящемуся в спящем режиме, для сообщения о том, что пакет данных ожидает доставки. Параметр принимает значения от 1 от 255 мс. По умолчанию – 2 мс;
- *Fragmentation Threshold* – порог фрагментации фрейма в байтах. Параметр принимает значения от 256 от 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. Параметр принимает значения от 0 до 2347. По умолчанию – 2347;
- *Maximum Stations* – максимально допустимое число подключаемых к радиоинтерфейсу клиентов. Параметр принимает значения от 0 до 200, где 0 – ограничение выключено. По умолчанию – 0;
- *VLAN List* – 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. Максимальное количество VLAN, которое можно указать в списке – 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.

DHCP Replication	<input type="button" value="On"/>																											
ARP Suppression	<input type="button" value="On"/>																											
DHCP Snooping Mode	<input type="button" value="Ignore"/>																											
MCS Rate Set	<input type="button" value="VHT NSS2 MCS0-MCS8 (13 - 156 Mbps)"/> <input type="button" value="VHT NSS2 MCS0-MCS7 (13 - 130 Mbps)"/> <input type="button" value="VHT NSS1 MCS0-MCS8 (6.5 - 78 Mbps)"/> <input type="button" value="VHT NSS1 MCS0-MCS7 (6.5 - 65 Mbps)"/> <input type="button" value="MCS15 (130 Mbps)"/> <input type="button" value="MCS14 (117 Mbps)"/>																											
Legacy Rate Sets	<table border="1"> <tr> <td>Rate (Mbps)</td> <td>54</td> <td>48</td> <td>36</td> <td>24</td> <td>18</td> <td>12</td> <td>9</td> <td>6</td> </tr> <tr> <td>Supported</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Basic</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </table>	Rate (Mbps)	54	48	36	24	18	12	9	6	Supported	<input checked="" type="checkbox"/>	Basic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>							
Rate (Mbps)	54	48	36	24	18	12	9	6																				
Supported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>																				
Basic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>																				
<input type="checkbox"/> Broadcast/Multicast Rate Limiting	Rate Limit <input type="text" value="50"/> (packets per second) Rate Limit Burst <input type="text" value="75"/> (packets per second)																											
VHT Features	<input type="checkbox"/>																											
TSPEC Settings	<input type="button" value="±"/>																											

- *DHCP Replication* – репликация DHCP-пакетов в сторону клиента при «on» – unicast, при «off» – broadcast;
- *ARP Suppression* – механизм конвертирования ARP-запросов из Broadcast в Unicast;
- *DHCP Snooping Mode* – управление политикой обработки опции 82:
  - *Ignore* – на точке доступа отключена обработка опции 82. Это значение установлено по умолчанию;
  - *Remove* – точка доступа удаляет значение опции 82;
  - *Replace* – точка доступа подставляет или заменяет значение опции 82. При установке данного значения становятся доступными для редактирования следующие параметры:
    - *DHCP Option 82 CID Format*:
      - *String* – точка доступа меняет содержимое Circuit-ID на значение, которое настраивается вручную в поле «DHCP Option 82 CID String»;
      - *APMAC-SSID* – точка доступа меняет содержимое Circuit-ID на запись вида <MAC-адрес точки доступа>;<имя SSID, к которому подключен клиент>. Это значение установлено по умолчанию;
      - *SSID* – точка доступа меняет содержимое Circuit-ID на имя SSID, к которому подключен клиент.
  - *DHCP Option 82 CID String* – значение от 1 до 52 символов, которое будет передаваться в Circuit-ID в случае, если в параметре «DHCP Option 82 CID Format» указано «String». Допускаются только латинские буквы и цифры, знаки «.», «-», «\_»;

✓ Если в параметре «DHCP Option 82 CID Format» установлено значение «String» и при этом поле «DHCP Option 82 CID String» осталось пустым, то точка доступа будет менять содержимое Circuit-ID на значение По умолчанию – «APMAC-SSID».

- *DHCP Option 82 RID Format*:
  - *String* – точка доступа меняет содержимое Remote-ID на значение, которое настраивается вручную в поле «DHCP Option 82 RID String»;
  - *ClientMAC* – точка доступа меняет содержимое Remote-ID на MAC-адрес клиентского устройства. Это значение установлено по умолчанию;
  - *APMAC* – точка доступа меняет содержимое Remote-ID на свой MAC-адрес;
  - *APdomain* – точка доступа меняет содержимое Remote-ID на имя последнего по дереву домена, указанного в параметре AP-Location, прописанного в настройках устройства.
- *DHCP Option 82 RID String* – значение от 1 до 63 символов, которое будет передаваться в Remote-ID в случае, если в параметре «DHCP Option 82 RID Format» указано «String». Допускаются только латинские буквы и цифры, знаки «.», «-», «\_».

✓ Если в параметре «DHCP Option 82 RID Format» установлено значение «String» и при этом поле «DHCP Option 82 RID String» осталось пустым, то точка доступа будет менять содержимое Remote-ID на значение По умолчанию – «ClientMAC».

- *DHCP Option 82 MAC Format* – параметр определяет формат MAC-адресов, которые передаются в CID и RID. Может принимать значения:
  - *default* – MAC-адрес передается в обычном формате, таком же, как в опции "Client-Ethernet-Address" DHCP-пакета. В этом случае MAC-адрес, как правило, имеет нижний регистр букв, а в качестве разделителя выступает ":"; например "aa:bb:cc:dd:ee:ff". В пакете он будет передаваться в ASCII-кодировке. Это значение установлено по умолчанию;
  - *radius* – MAC-адрес передается в RADIUS-формате. В этом случае все буквы переводятся в верхний регистр, в качестве разделителя выступает "-". Пример "AA-BB-CC-DD-EE-FF". В пакете он будет передаваться в ASCII кодировке.

- *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. При установке флага становятся доступными для редактирования следующие поля:
  - *Rate Limit* – порог скорости передачи данных, пак/с. По умолчанию – 50 пак/с.;
  - *Rate Limit Burst* – максимальное значение всплеска трафика, пак/с. По умолчанию – 75 пак/с.
- *VHT Features* – функция включения/выключения поддержки VHT скоростей. Функция VHT включает поддержку 256QAM. Поддерживается для стандарта IEEE 802.11ac.

TSPEC Settings		
TSPEC Mode		Off ▼
TSPEC Voice ACM Mode		Off ▼
TSPEC Voice ACM Limit	20	(Percent, Range: 0 - 90)
TSPEC Fbt Voice ACM Limit	0	(Percent, Range: 0 - 90)
TSPEC Video ACM Mode		Off ▼
TSPEC Video ACM Limit	15	(Percent, Range: 0 - 90)
TSPEC Fbt Video ACM Limit	0	(Percent, Range: 0 - 90)
TSPEC BE ACM Mode		Off ▼
TSPEC BE ACM Limit	0	(Percent, Range: 0 - 90)
TSPEC BK ACM Mode		Off ▼
TSPEC BK ACM Limit	0	(Percent, Range: 0 - 90)
TSPEC AP Inactivity Timeout	30	(Sec, Range: 0 - 120, 0 Disables)
TSPEC Station Inactivity Timeout	30	(Sec, Range: 0 - 120, 0 Disables)
TSPEC Legacy WMM Queue Map Mode		Off ▼

Click "Update" to save the new settings.

Update

Для перехода к настройке параметров TSPEC, нажмите кнопку с изображением символа «+» напротив «TSPEC Settings»:

- *TSPEC Mode* – выбор режима работы TSPEC. По умолчанию – off (выключен). Может принимать значения:
  - *On* – точка доступа обрабатывает Tspec-запросы от клиентов. Используйте эту настройку, если точка доступа обрабатывает трафик от QoS-совместимых устройств, таких как сертифицированные 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 ACM Mode* – регламентирует обязательный контроль допуска (ACM) для категории голосового трафика (Voice). По умолчанию – off. Может принимать следующие значения:
  - *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 Voice ACM Limit* – определяет предел объема Voice трафика. Параметр принимает значения от 0 до 90%. По умолчанию – 20%;

- *TSPEC FBT Voice ACM Limit* – определяет верхний предел объема Voice трафика для клиентов в роуминге на данной точке доступа с помощью быстрого перехода BSS. Параметр принимает значения от 0 до 90%. По умолчанию – 0%;
- *TSPEC Video ACM Mode* – регламентирует обязательный контроль допуска (ACM) для категории Video-трафика. По умолчанию – off. Может принимать следующие значения:
  - *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. Параметр принимает значения от 0 до 90%. По умолчанию – 15%;
- *TSPEC FBT Video ACM Limit* – определяет верхний предел объема Video-трафика для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS. Параметр принимает значения от 0 до 90%. По умолчанию – 0%;
- *TSPEC BE ACM Mode* – регламентирует обязательный контроль допуска для категории Best Effort трафика. По умолчанию – off. Может принимать следующие значения:
  - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока трафика категории Best Effort;
  - *Off* – клиент может отправлять и получать трафик категории Best Effort без необходимости запроса.
- *TSPEC BE ACM Limit* – определяет верхний предел объема трафика категории Best Effort для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS. Параметр принимает значения от 0 до 90%. По умолчанию – 0%;
- *TSPEC BK ACM Mode* – регламентирует обязательный контроль допуска для категории Background-трафика. По умолчанию – off. Может принимать следующие значения:
  - *On* – клиенту требуется отправить запрос к точке доступа перед отправкой или получением потока трафика категории Background;
  - *Off* – клиент может отправлять и получать трафик категории Background без необходимости запроса.
- *TSPEC BK ACM Limit* – определяет верхний предел объема трафика категории Background для клиентов в роуминге на этой точке доступа с помощью быстрого перехода BSS. Параметр принимает значения от 0 до 90%. По умолчанию – 0%;
- *TSPEC AP Inactivity Timeout* – время, по истечению которого будут удаляться неактивные клиенты с точки доступа (проверяется поток downlink). Параметр принимает значения от 0 до 120 секунд. По умолчанию – 30 секунд;
- *TSPEC Station Inactivity Timeout* – время, по истечению которого будут удаляться неактивные клиенты с точки доступа (проверяется поток uplink). Параметр принимает значения от 0 до 120 секунд. По умолчанию – 30 секунд;
- *TSPEC Legacy WMM Queue Map Mode* – выберите *On*, чтобы получать трафик различных категорий на очередях, работающих в АКМ.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.6 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* – планировщик включен;
  - *Disable* – планировщик выключен.

**Scheduler Operational Status** – в разделе приводится информация о состоянии работы планировщика:

- *Status* – статус работы планировщика. Параметр принимает значения Up (Включен) или Down (Выключен). По умолчанию – Down;
- *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 находится в режиме управления.
- *Scheduler Profile* – имя создаваемого профиля планировщика. Может содержать от 1 до 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 ранее профиля, для которого будет выполняться настройка параметров;
- *Set Schedule* – день недели работы планировщика. Параметр может принимать следующие значения:
  - *Daily* – ежедневно;
  - *Weekday* – рабочие дни;
  - *Weekend* – выходные дни;
  - *On* – определенный день недели, выбор которого осуществляется из выпадающего списка. Может принимать значение Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
- *Start Time* – время включения радиоинтерфейса или VAP. Задается в виде часы:минуты;

- *End Time* – время выключения радиointерфейса или VAP. 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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.7 Подменю «Scheduler Association»

В подменю «**Scheduler Association**» выполняется привязка созданных в подменю «Scheduler» правил планировщика к VAP или радиointерфейсам.

### Scheduler Association Settings

Radio	Scheduler Profile	Operational Status
1	<input type="text" value=""/>	up
2	<input type="text" value=""/>	up

---

Radio

VAP	Scheduler Profile	Operational Status
0	<input type="text" value="test"/>	up
1	<input type="text" value=""/>	down
2	<input type="text" value=""/>	down
3	<input type="text" value=""/>	down
4	<input type="text" value=""/>	down
5	<input type="text" value=""/>	down
6	<input type="text" value=""/>	down
7	<input type="text" value=""/>	up
8	<input type="text" value=""/>	down
9	<input type="text" value=""/>	down
10	<input type="text" value=""/>	down
11	<input type="text" value=""/>	down
12	<input type="text" value=""/>	down
13	<input type="text" value=""/>	down
14	<input type="text" value=""/>	down
15	<input type="text" value=""/>	down

Click "Update" to save the new settings.

В столбце «Scheduler Profile» напротив номера Radio или VAP, к которому необходимо применить созданное ранее правило планировщика, установите имя профиля планировщика.

Значения в столбце «Operational Status» носят информационный характер и указывают на статус, в котором находится VAP или радиointерфейс точки доступа: up – включен, down – выключен.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.8 Подменю «VAP»

В подменю «**VAP**» выполняется настройка виртуальных точек доступа на Wi-Fi интерфейсах, а также настройка параметров RADIUS-сервера. На каждом радиоинтерфейсе точки доступа может быть сконфигурировано до 16 виртуальных точек доступа.

**Global RADIUS Server Settings** – в данном 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 основного RADIUS-сервера. При недоступности основного RADIUS-сервера, запросы будут отправляться на резервные сервера указанные в полях *RADIUS IP Address-1*, *RADIUS IP Address-2*, *RADIUS IP Address-3*;
- *RADIUS IP Address-1, 2, 3* – резервные адреса RADIUS-сервера. При недоступности основного RADIUS-сервера запросы будут отправляться на резервные;
- *RADIUS Key* – пароль для авторизации на основном RADIUS-сервере;
- *RADIUS Key-1, 2, 3* – пароли для авторизации на резервных RADIUS-серверах;
- *Enable RADIUS Accounting* – при установленном флаге будут отправляться сообщения «Accounting» на RADIUS-сервер.

**Настройка виртуальных точек доступа:**

- *Radio* – выбор радиоинтерфейса, на котором необходимо настроить VAP. Radio 1 – настройка VAP в диапазоне 5 ГГц, Radio 2 – настройка VAP в диапазоне 2.4 ГГц;
- *VAP* – порядковый номер виртуальной точки доступа на радиоинтерфейсе;
- *Enabled* – при установленном флаге виртуальная точка доступа включена, иначе – выключена.
- *VLAN ID* – номер VLAN, с которого будет сниматься метка при передаче трафика Wi-Fi клиентам, подключенным к данной VAP. При прохождении трафика в обратную сторону на нетегированный трафик от клиентов будет навешиваться метка VLAN ID (при отключенном режиме VLAN Trunk);
- *SSID* – имя беспроводной сети;
- *Broadcast SSID* – при установленном флаге включено вещание в эфир имени SSID, иначе – выключено;

- *Station Isolation* – при установленном флаге включена изоляция трафика между клиентами в пределах одной VAP;
- *Band Steer* – при установленном флаге активно приоритетное подключение клиента к 5 ГГц сети. Для работы функционала необходимо создать VAP с одинаковым SSID на каждом радиointерфейсе и активировать на них параметр «Band Steer»;
- *802.11k* – включить поддержку стандарта 802.11k на VAP. Для работы роуминга 802.11k необходима поддержка стандарта со стороны клиентов. Использование функционала возможно только при использовании сервиса Airtune;
- *DSCP Priority* – при установленном флаге будет анализироваться приоритет из поля DSCP заголовка IP-пакета, при снятом флаге будет анализироваться приоритет из поля CoS (Class of Service) тегированных пакетов;
- *VLAN Trunk* – при установленном флаге беспроводному клиенту передается тегированный трафик;
- *General Mode* – при установленном флаге разрешается передача беспроводному клиенту нетегированного трафика совместно с тегированным (доступно при включенном режиме VLAN Trunk);
- *General VLAN ID* – с указанного VLAN ID будет сниматься метка, далее трафик этого VLAN будет передан клиенту без тега. При прохождении трафика в обратную сторону на нетегированный трафик будет навешиваться метка General VLAN ID;
- *Maximum Stations* – максимально допустимое число клиентов, подключаемых к SSID. Параметр принимает значения от 0 до 200, где 0 – ограничение выключено. По умолчанию – 0;
- *VLAN Priority* – приоритет 3-го уровня, который будет назначаться на пакеты, приходящие от клиента, подключенного к данной VAP, и передаваемые далее в проводную сеть;
- *Security* – режим безопасности доступа к беспроводной сети:
  - *None* – не использовать шифрование для передачи данных. Точка доступна для подключения любого клиента;
  - *WPA Personal* – шифрование WPA и WPA2. При выборе данного режима доступны следующие настройки:

WPA Versions:	<input type="checkbox"/> WPA-TKIP	<input checked="" type="checkbox"/> WPA2-AES
Key:	<input type="text"/>	
Broadcast Key Refresh Rate	<input type="text" value="0"/>	(Range:0-86400)
MFP	<input checked="" type="checkbox"/> Not Required	<input type="checkbox"/> Capable <input type="checkbox"/> Required

- *WPA Versions* – 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 от 0 до 86400. По умолчанию – 0;
- *MFP* – настройка режима защиты клиентских фреймов:
  - *Not Required* – не использовать защиту;
  - *Capable* – использовать защиту при наличии возможности;
  - *Required* – использовать защиту обязательно, все клиенты должны поддерживать CCX5.

WPA Versions: <input type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES	
<input type="checkbox"/> Enable Pre-authentication	
MFP	<input checked="" type="checkbox"/> Not Required <input type="checkbox"/> Capable
<input type="checkbox"/> Use Global RADIUS Server Settings	
RADIUS Domain:	<input type="text"/>
RADIUS IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
RADIUS IP Address:	<input type="text" value="192.168.1.1"/>
RADIUS IP Address-1:	<input type="text"/>
RADIUS IP Address-2:	<input type="text"/>
RADIUS IP Address-3:	<input type="text"/>
RADIUS Key:	<input type="text" value="*****"/>
RADIUS Key-1:	<input type="text"/>
RADIUS Key-2:	<input type="text"/>
RADIUS Key-3:	<input type="text"/>
<input type="checkbox"/> Enable RADIUS Accounting	
Active Server:	<input type="text" value="RADIUS IP Address"/> <input type="button" value="v"/>
Broadcast Key Refresh Rate	<input type="text" value="0"/> (Range:0-86400)
Session Key Refresh Rate	<input type="text" value="0"/> (Range:30-86400, 0 Disables)

- **WPA Enterprise** – режим шифрования канала 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. При выборе данного режима будет доступна следующая настройка:
  - **WPA Versions** – версия шифрования: WPA-TKIP, WPA2-AES;
  - **Enable Pre-authentication** – при установленном флаге используется процедура предварительной проверки подлинности для беспроводных клиентов WPA2. Предварительная аутентификация позволяет мобильному клиенту аутентифицироваться на другой, расположенной поблизости точке доступа, оставаясь "привязанным" к своей первичной точке доступа. В этом случае сокращается время, в течение которого связь для клиента, выполняющего роуминг, не доступна при ожидании проверки подлинности RADIUS в процессе переадресации;
  - **MFP** – настройка режима защиты клиентских фреймов:
    - **Not Required** – не использовать защиту;
    - **Capable** – использовать защиту при наличии возможности.
  - **Use Global RADIUS Server Settings** – при установке флага будут использоваться настройки Global RADIUS Server Settings, указанные в верхней части страницы. Чтобы использовать отдельный RADIUS-сервер для VAP, снимите флажок и введите IP-адрес, пароль RADIUS-сервера и другие данные в следующие поля:
    - **RADIUS Domain** – домен пользователя;
    - **RADIUS IP Address Type** – выбор протокола IPv4 или IPv6 для доступа на сервер RADIUS;
    - **RADIUS IP Address** – адрес основного RADIUS-сервера. При недоступности основного RADIUS-сервера, запросы будут отправляться на резервные сервера указанные в полях **RADIUS IP Address-1**, **RADIUS IP Address-2**, **RADIUS IP Address-3**;
    - **RADIUS IP Address-1, 2, 3** – резервные адреса RADIUS-сервера. При недоступности основного RADIUS-сервера запросы будут отправляться на резервные;
    - **RADIUS Key** – пароль для авторизации на основном RADIUS-сервере;
    - **RADIUS Key-1, 2, 3** – пароли для авторизации на резервных RADIUS-серверах;
    - **Enable RADIUS Accounting** – при установленном флаге будут отправляться сообщения «Accounting» на RADIUS-сервер.

- *Active Server* – выберите, к какому из четырех RADIUS-серверов должен обратиться VAP для аутентификации беспроводных клиентов;
- *Broadcast Key Refresh Rate* – интервал обновления широковещательного (группового) ключа для клиентов данного VAP. Параметр принимает значения от 0 до 86400 секунд. По умолчанию – 0. Значение 0 указывает на то, что широковещательный ключ не обновляется. Широковещательный ключ не обновляется, когда на VAP включен Fast Transition (IEEE 802.11r);
- *Session Key Refresh Rate* – интервал обновления сессионных ключей для каждого клиента данного VAP. Параметр принимает значения от 30 до 86400 секунд. По умолчанию – 0. Значение 0 указывает на то, что сессионный ключ не обновляется.
- *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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.9 Подменю «VAP Minimal Signal»

В подменю «**VAP Minimal Signal**» выполняется настройка функции отключения клиентского Wi-Fi оборудования при низком уровне сигнала, принимаемом от него. Применяется для оптимизации бесшовности роуминга на сети.

*Modify Virtual Access Point minimal signal settings*

Radio  ▾

VAP	Minimal signal Enable	Minimal signal (dBm, Range: -100 - -1)	Check signal timeout (Sec, Range: 1 - 300)
0	<input checked="" type="checkbox"/>	<input type="text" value="-75"/>	<input type="text" value="10"/>
1	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
2	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
3	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
4	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
5	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
6	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
7	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
8	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
9	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
10	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
11	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
12	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
13	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
14	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>
15	<input type="checkbox"/>	<input type="text" value="-100"/>	<input type="text" value="10"/>

Click "Update" to save the new settings.

- *Radio* – выбор настраиваемого радиointерфейса;
- *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. Принимает значение от -100 до -1;
- *Check signal timeout, s* – период времени, по истечении которого принимается решение об отключении клиентского оборудования. Принимает значения от 1 до 300 секунд. По умолчанию – 10 секунд.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.10 Подменю «Fast Bss Transition»

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

**Fast Bss Transition Parameters**

Radio  ▼

VAP  ▼

Fast Transition Mode	<input type="text" value="Off"/> ▼	
FT over DS	<input type="text" value="Off"/> ▼	
Mobility Domain	<input type="text" value="0"/>	(0 - 65535)
R0 Key Holder	<input type="text"/>	(1 - 48 characters)
R1 Key Holder	<input type="text"/>	(xx:xx:xx:xx:xx:xx)
Reassociation Deadline	<input type="text" value="1000"/>	(1000 - 4294967295)

Click "Update" to save the new settings.

#### Параметры Fast Bss Transition

- *Radio* – выбор радиointерфейса, 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. При необходимости совершить роуминг клиент 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 точке доступа FT Action Response Frame. Текущая точка доступа пересылает это сообщение клиенту. После окончания процесса клиент отправляет на целевую точку доступа запрос Reassociation. При отключенной функции *FT over DS* работает *FT over AIR*, в таком случае авторизация клиента на целевой точке доступа происходит с использованием стандартных фреймов аутентификации:
  - *On* – функция включена;
  - *Off* – функция выключена.
- *Mobility Domain* – номер группы, в рамках которой может быть совершен роуминг. Принимает значения от 0 до 65535. По умолчанию – 0;
- *R0 Key Holder* – ключ PMK-R0. Может содержать от 1 до 48 символов. Дополнительно 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* – максимальное разрешенное время ожидания запроса «Reassociation» от станции. Принимает значения от 1000 до 4294967295 мс. По умолчанию – 1000 мс.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

После указания основных параметров необходимо настроить взаимодействие с точками доступа, между которыми будет осуществляться роуминг, задав MAC-адреса точек доступа и ключи.

- *MAC Address* – MAC-адрес точки доступа, участвующей в роуминге;
- *NAS ID* – идентификатор NAS, принимает значение, указанное в R0 Key Holder;
- *R1 Key Holder* – ключ PMK-R1 в формате MAC-адреса xx:xx:xx:xx:xx:xx;
- *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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.11 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),
- 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)

- *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. Доступна при типах аутентификации: *Acceptance of Term and Conditions*, *HTTP/HTTPS Redirection*, *DNS Redirection*.

## 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.

<b>Roaming Consortium List</b>	
<b>OUI Name</b>	<b>Is Beacon</b>
<input type="text" value="Not Configured"/>	<input type="button" value="No"/> ▾
<input type="text" value="Not Configured"/>	<input type="button" value="No"/> ▾
<b>3GPP Cellular Network Information List</b>	
<b>Country Code</b>	<b>Network Code</b>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>
<b>Domain List</b>	
<b>1</b> <input type="text" value="Not Configured"/>	<b>2</b> <input type="text" value="Not Configured"/>
<b>3</b> <input type="text" value="Not Configured"/>	<b>4</b> <input type="text" value="Not Configured"/>

### 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.

Realm List:				
Realm Name	Encoding	EAP and Auth Information		
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>	<input type="text" value="Not Configured"/>	<input type="button" value="Modify"/>	<input type="button" value="Reset"/>

### 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.

Passpoint ANQP Parameters Configurations :	
<b>Passpoint ANQP Parameters</b>	
Passpoint Status	<input type="text" value="Disabled"/>
Passpoint Capability	<input type="text" value="Release 1"/>
DGAF Disabled Status	<input type="text" value="Disabled"/>
ANQP 4 frame	<input type="text" value="Disabled"/>
Gas Come Back Delay	<input type="text" value="0"/>
Proxy ARP Status	<input type="text" value="Disabled"/>
Operating Class Indicator	<input type="text" value="Operating Class 81"/>
Anonymous NAI	<input type="text" value="Not Configured"/>
L2 Traffic Inspection	<input type="text" value="Enabled"/>
ICMPv4 Echo	<input type="text" value="Enabled"/>
<b>Operator Friendly Name List</b>	
<b>Operator Name</b>	<b>Language Code</b>
<input type="text" value="Not Configured"/>	<input type="text" value="ENG"/>
<input type="text" value="Not Configured"/>	<input type="text" value="ENG"/>
<b>QoS Map ID</b>	<input type="text" value="0"/>
<b>NAI Home Realm Query List</b>	
<b>Home Realm</b>	<b>Encoding</b>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>
<input type="text" value="Not Configured"/>	<input type="text" value="RFC4282"/>

## 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 точка доступа 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).

Connection Capability List :		
Protocol	Port	Status
Select ▼	Select ▼	Select ▼
Select ▼	Select ▼	Select ▼
Select ▼	Select ▼	Select ▼
Select ▼	Select ▼	Select ▼

## 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.

OSU Provider List:							
OSU SSID : <input type="text" value="OSU"/>							
	OSU Friendly Name	OSU Desc	OSU Language Code	OSU Server URI	OSU NAI	OSU Method	OSU Icon
#1	<input type="text" value="SP Red Test Only!eng"/>	<input type="text" value="Free service for te"/>		<input type="text" value="https://osu-serve"/>	<input type="text"/>	<input type="text" value="SOAP-XML"/>	<input type="text" value="7"/>
	1-1 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	1-2 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	1-3 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
#2	<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>		<input type="text"/>	<input type="text"/>	<input type="text" value="OMA-DM"/>	<input type="text" value="0"/>
	2-1 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	2-2 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	2-3 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
#3	<input type="text" value="Not Configured"/>	<input type="text" value="Not Configured"/>		<input type="text"/>	<input type="text"/>	<input type="text" value="OMA-DM"/>	<input type="text" value="0"/>
	3-1 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	3-2 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>
	3-3 <input type="text"/>	<input type="text"/>	<input type="text"/>				<input type="text" value="Select"/>

### 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* – метод онлайн-регистрации;
- *OSU Icon* – логотип провайдера.

WAN Metrics Information :							
Link Status	Symmetric Link	At Capacity	Down Link Speed	Up Link Speed	Down Link Load	Up Link Load	Lmd
<input type="text"/>	: <input type="text"/>	: <input type="text"/>	= <input type="text"/>	> <input type="text"/>	= <input type="text"/>	> <input type="text"/>	= <input type="text"/>

### Информация о метрике WAN (WAN Metrics Information)

- *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 несимметрично (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).

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.5.12 Подменю «Wireless Multicast Forwarding»

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

*Modify Wireless Multicast Forwarding settings*

Radio

VAP	Enabled	WMF-Enable
0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="checkbox"/>	<input type="checkbox"/>

Click "Update" to save the new settings.

- *Radio* – выбор радиointерфейса;
- *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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### 4.5.13 Подменю «WDS»

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

**✘** WDS не может быть настроен, если на точке настроен WGB или включен режим кластера.

**✘** Для корректной работы WDS необходимо, чтобы на точках доступа была установлена одинаковая версия программного обеспечения.

#### Configure WDS bridges to other access points

Click "Refresh" button to refresh remote APs signal strength.

Tunneling  ▼

Spanning Tree Mode  Enabled  Disabled

---

<p>Interface wlan0wds0</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>	<p>Interface wlan0wds4</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>
<p>Interface wlan0wds1</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>	<p>Interface wlan0wds5</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>
<p>Interface wlan0wds2</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>	<p>Interface wlan0wds6</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>
<p>Interface wlan0wds3</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>	<p>Interface wlan0wds7</p> <p>Radio <input style="border: 1px solid gray; padding: 2px 5px; margin-left: 5px;" type="button" value="1"/> <span style="margin-left: 10px;">▼</span></p> <p>Local Address <input style="width: 100%; border: 1px solid gray;" type="text" value="E8:28:C1:C1:27:60"/></p> <p>Remote Address <input style="width: 100%; border: 1px solid gray;" type="text"/> <span style="float: right;">↔</span></p> <p>Connection Status <input style="width: 100%; border: 1px solid gray;" type="button" value="down"/></p> <p>Encryption <input style="width: 100%; border: 1px solid gray;" type="button" value="None (Plain-text)"/></p>

Click "Update" to save the new settings.

- *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 радиointерфейсу.
- *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 радиointерфейса. Radio 1 – WDS будет построен в диапазоне 5 ГГц, Radio 2 – WDS будет построен в диапазоне 2.4 ГГц;
- *Local Address* – просмотр MAC-адреса текущего радиointерфейса;
- *Remote Address* – MAC-адрес радиointерфейса точки доступа, с которой предусматривается совместная работа. MAC-адрес радиointерфейса можно посмотреть на вкладке «Status»/«Interfaces»;
- *Connection Status* – статус соединения;
- *Signal* – уровень сигнала, с которым текущая точка доступа видит встречную точку доступа, с которой построен WDS, дБм;
- *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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

Для обновления информации на странице нажмите кнопку «Refresh».

## 4.5.14 Подменю «MAC Authentication»

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

### Configure MAC Authentication of client stations

Global policy  Allow only stations in list  
 Block all stations in list

---

Access List

Radio

VAP	SSID	ACL	Policy Mode
0	Eltex-Local	default ▼	Global ▼
1	000111_TestLength	default ▼	Global ▼
2	BRAS-Guest	default ▼	Global ▼
3	Eltex-Guest	default ▼	Global ▼
4	test_80211r_5g	default ▼	Global ▼
5	1.11.4_802111r	default ▼	Global ▼
6	1.11.4_802111r_26	default ▼	Global ▼
7	Virtual Access Point 7	default ▼	Global ▼
8	Virtual Access Point 8	default ▼	Global ▼
9	Virtual Access Point 9	default ▼	Global ▼
10	Virtual Access Point 10	default ▼	Global ▼
11	Virtual Access Point 11	default ▼	Global ▼
12	Virtual Access Point 12	default ▼	Global ▼
13	Virtual Access Point 13	default ▼	Global ▼
14	Virtual Access Point 14	default ▼	Global ▼
15	Virtual Access Point 15	default ▼	Global ▼

Click "Update" to save the new settings.

- *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  ▼

New acl name  (1 - 32 characters)

Click "Update" to save the new settings.

- *Access List* – выбор существующих списков MAC-адресов или создание нового списка:
  - *Create* – создание нового списка:
    - *New acl name* – введите имя нового списка MAC-адресов и нажмите кнопку «Update» для его создания.

- *Default* – стандартный пустой список MAC-адресов. При выборе данного списка или любого другого ранее созданного списка для редактирования будут доступны следующие поля:
  - *Delete Access List* – при установке флага и последующем нажатии на кнопку «Update» выбранный *Access List* будет удален. Список *default* удалить нельзя;
  - *Stations List* – список MAC-адресов клиентов, которым разрешен/запрещен доступ.

Для добавления MAC-адреса в список фильтрации в параметре «Access List» выберите нужный список и введите MAC-адрес, который нужно добавить. Далее нажмите кнопку «Add». MAC-адрес появится в разделе «Station List» .

Для удаления MAC-адреса из списка в разделе «Station List» выберите запись и нажмите на 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 (устройствам из списка разрешен доступ);
  - *Block* – для текущего SSID выбранный список будет являться черным (устройствам из списка запрещен доступ).

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.15 Подменю «Load Balancing»

В подменю «**Load Balancing**» выполняется настройка ограничения возможности подключения клиентов 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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.16 Подменю «Authentication»

В подменю «**Authentication**» производится настройка точки доступа в режиме 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. Возможные значения: MD5, PEAP, TLS;
- *Username* – имя пользователя. Параметр может содержать от 1 до 64 символов;
- *Password* – пароль. Параметр может содержать от 1 до 64 символов.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

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

- *Certificate File Present* – указывает, присутствует ли файл сертификата HTTP SSL. Возможные значения: yes, no. По умолчанию сертификат отсутствует – no;
- *Certificate Expiration Date* – дата, указывающая на то, когда истечет срок действия файла сертификата HTTP SSL. Если сертификат отсутствует, отображается сообщение «Not Present».

**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 вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.5.17 Подменю «Management ACL»

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

### Configure Management Access Control Parameters

Management ACL Mode  Enabled  Disabled

IP Address 1	<input type="text"/>	(xxx.xxx.xxx.xxx)
IP Address 2	<input type="text"/>	(xxx.xxx.xxx.xxx)
IP Address 3	<input type="text"/>	(xxx.xxx.xxx.xxx)
IP Address 4	<input type="text"/>	(xxx.xxx.xxx.xxx)
IP Address 5	<input type="text"/>	(xxx.xxx.xxx.xxx)
IPv6 Address 1	<input type="text"/>	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 2	<input type="text"/>	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 3	<input type="text"/>	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 4	<input type="text"/>	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)
IPv6 Address 5	<input type="text"/>	(xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Click "Update" to save the new settings.

- *Management ACL Mode* – использование списков доступа к управлению устройством:
  - *Enabled* – при установленном флаге функционал включен;
  - *Disabled* – при установленном флаге функционал отключен.
- *IP Address 1...5* – список хостов IPv4, которые имеют доступ к управлению устройством;
- *IPv6 Address 1...5* – список хостов IPv6, которые имеют доступ к управлению устройством.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.5.18 Подменю «OTT Settings»

В подменю «**OTT Settings**» выполняется настройка параметров OTT (Over the Top) для построения IPsec, либо GRE-туннелей внутри IPsec соединения от точки доступа.

OTT Settings	
Service Activator URL	<input type="text"/> (https://<xxx.xxx.xxx.xxx / Domain name>:<Port>)
IPsec Remote Gateway	<input type="text" value="172.16.0.1"/> (xxx.xxx.xxx.xxx / Domain name)
IPsec Operational Status	<input type="checkbox"/>
XAUTH User	<input type="text" value="user"/> (Range: 4-16 chars)
XAUTH Password	<input type="text" value="password"/> (Range: 8-48 chars)
Advanced Settings	<input type="button" value="⊖"/>

- *Service Activator URL* – адрес сервис-активатора, задается в формате `https://<xxx.xxx.xxx.xxx / Domain name>:<Port>`;
- *IPsec Remote Gateway* – шлюз для IPsec, задается в формате IP-адреса или доменного имени;
- *IPsec Operation Status* – установите флажок для включения конфигурируемого IPsec-соединения;
- *XAUTH User* – имя пользователя для расширенной авторизации, необходимо для работы механизма mode config. Параметр должен содержать от 4 до 16 символов;
- *XAUTH Password* – пароль пользователя для расширенной авторизации, необходимо для работы механизма mode config. Параметр должен содержать от 8 до 48 символов.

Чтобы перейти к расширенному списку параметров, нажмите кнопку с изображением символа «+» напротив «Advanced Settings»:

Advanced Settings <input type="button" value="⊖"/>	
<b>IKE Proposal</b>	
IKE Authentication Algorithm	<input type="text" value="md5"/>
IKE DH Group	<input type="text" value="1"/>
IKE Encryption Algorithm	<input type="text" value="aes"/>
<b>IKE Policy</b>	
Use ISAKMP Mode Config	<input type="radio"/> On <input checked="" type="radio"/> Off
IKE Lifetime	<input type="text" value="86400"/> (Sec, Range: 180-86400)
Use NAT-T	<input checked="" type="checkbox"/>
IPsec NAT Keepalive	<input type="text" value="180"/> (Sec, Range: 1-300)
IPsec Password	<input type="text" value="password"/> (Range: 8-48 chars)
<b>IKE Gateway</b>	
IPsec Local Address	<input type="text" value="192.168.2.10"/> (xxx.xxx.xxx.xxx)
IPsec Remote Network	<input type="text" value="192.168.3.0"/> (xxx.xxx.xxx.xxx)
IPsec Remote Mask	<input type="text" value="255.255.255.0"/> (xxx.xxx.xxx.xxx)

**IKE Proposal:**

- *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.

**IKE Policy:**

- *Use ISAKMP Mode Config* – активируем режим автоматического получения виртуального 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. Параметр принимает значения от 180 до 86400 секунд. По умолчанию – 86400 секунд;
- *Use NAT-T* – необходимо включить флаг, если точка доступа находится за NAT;
- *IPsec NAT Keepalive* – периодичность отправки пакетов keepalive при работе через NAT, чтобы NAT-трансляция сохранялась на вышестоящих роутерах при длительной не активности со стороны клиента. Параметр принимает значения от 0 до 300 секунд. По умолчанию – 180 секунд;
- *IPsec Password* – пароль для IKE/ISPEC-соединения. Параметр должен содержать от 8 до 48 символов;
- *Use XAUTH Password* – при установленном флаге для IKE/ISPEC-соединения будет использоваться заданный ранее *XAUTH Password*. Если флаг не установлен, будет использоваться пароль, указанный в поле *IPsec Password*. Поле доступно, если *Use ISAKMP Mode Config* включен.

**IKE Gateway** – раздел и все его параметры доступны для редактирования при условии, что параметр *Use ISAKMP Mode Config* находится в состоянии *off*:

- *IPsec Local Address* – адрес клиента, который использует в качестве IKE локальную сеть с маской подсети 255.255.255.255 (/32);
- *IPsec Remote Network* – удаленная IKE-подсеть;
- *IPsec Remote Mask* – маска удаленной IKE-подсети.

<b>IPsec Proposal</b>	
IPsec Authentication Algorithm	md5 ▾
IPsec DH Group	0 ▾
IPsec Encryption Algorithm	aes ▾
<b>IPsec Policy</b>	
IPsec DPD Delay	180 (Sec, Range: 5-600)
IPsec Child SA Lifetime	3600 (Sec, Range: 180-86400)
<b>IPsec VPN</b>	
Force Establish Tunnel	<input checked="" type="checkbox"/>
<b>GRE Over IPsec</b>	
Use GRE Mode	<input checked="" type="radio"/> On <input type="radio"/> Off
GRE Over IPsec Mgmt	192.168.3.2 (xxx.xxx.xxx.xxx)
GRE Over IPsec Data	192.168.3.3 (xxx.xxx.xxx.xxx)
GRE MTU Offset	148 (Range: 0-220)
GRE Ping Counter	3 (Range: 3-60)
Click "Update" to save the new settings.	
<input type="button" value="Update"/>	

**IPsec Proposal :**

- *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 Policy:**

- *IPsec DPD Delay* – интервал отправки пакетов обнаружения разрыва соединения. При отсутствии с противоположной стороны IPsec VPN ответов на 5 пакетов подряд, точка доступа сочтет VPN развалившимся и произведёт перезапуск IPsec VPN со своей стороны. Параметр принимает значения от 5 до 600 секунд. По умолчанию – 180 секунд;
- *IPsec Child SA Lifetime* – время жизни IPsec VPN SA (фаза 2), должен быть одинаковым с обеих сторон туннеля IKE/IPsec. Должен быть ниже, чем IKE Lifetime. Параметр принимает значения от 180 до 86400 секунд. По умолчанию – 3600 секунд.

**IPsec VPN:**

- *Force Establish Tunnel* – включить, чтобы установить соединение IPsec VPN немедленно. Иначе VPN-соединение IPsec будет установлено по запросу.

**GRE Over IPsec:**

- *Use GRE Mode* – включить или отключить GRE через IPsec. Во включенном состоянии для редактирования доступны параметры:
  - *GRE Over IPsec Mgmt* – IP-адрес GRE для туннеля управления;
  - *GRE Over IPsec Data* – IP-адрес GRE для туннеля управления данным;
  - *GRE MTU Offset* – определяет уменьшение MTU для GRE-туннелей. GRE-туннелям будет назначено MTU, исходя из расчета  $1500 - GRE\ MTU\ Offset$ . Параметр принимает значения от 0 до 220;
  - *GRE Ping Counter* – чтобы проверить, что туннель GRE все еще жив, каждые 10 секунд на GRE IP-management отправляется ping. Это значение определяет, сколько пакетов пинга может быть потеряно, до того, как точка доступа перезапустит соединение IPsec. Параметр принимает значения от 3 до 60.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.5.19 Подменю «Mesh»\*

В подменю «**Mesh**» выполняется настройка связи между точками доступа по беспроводной Mesh-сети.

- ✓ \* Подменю доступно, если на точке доступа установлено ПО с поддержкой Mesh (например, WEP-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-точке по радиointерфейсу.

**Mesh Interface Settings** – в данном разделе выполняется настройка параметров интерфейса для организации Mesh. Раздел доступен только на Root-точке, т.е. при нахождении параметра *Autopeer Status* в значении *off*.

- *Radio* – выбор радиointерфейса для организации Mesh;

- ✓ На точках типа WEP-2ac/WEP-2ac Smart Mesh поддержан только на Radio 1 (5 ГГц).

- *Interface* – интерфейс, используемый для организации Mesh;
- *Status* – состояние конфигурируемого 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, являющейся контроллером (заполняется автоматически);
- *Mesh Interface Address* – MAC-адрес Mesh-интерфейса конфигурируемой точки доступа.

**Mesh Mac Authentication**

Peer's list

Allowed	Blocked	Access Request
a8:f9:4b:b5:52:8f		a8:f9:4b:b0:3a:1f
a8:f9:4b:b5:4d:af		
a8:f9:4b:b4:c4:2f		
a8:f9:4b:b5:52:9f		
a8:f9:4b:b0:26:1f		
e0:d9:e3:73:06:ef		
a8:f9:4b:b7:8b:cf		
a8:f9:4b:b4:c4:3f		

Click "Update" to save the new settings.

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

- *Allowed* – точкам доступа добавленным в список «Allowed» разрешен доступ в Mesh-сеть:
  - *Delete From Access List* – удалить выделенный MAC-адрес из списка разрешенных.
- *Blocked* – точкам доступа добавленным в список «Blocked» запрещен доступ в Mesh-сеть:
  - *Delete From Block List* – удалить выделенный MAC-адрес из списка запрещенных.
- *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).

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

- *Access* – добавление точки доступа в «белый» список;
- *Block* – добавление точки доступа в «черный» список.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.5.20 Подменю «Mesh Monitoring»\*

В подменю «**Mesh Monitoring**» отображается статистика и состояние соединений в Mesh-сети.

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

### Mesh Monitoring

**Mesh Neighbor Nodes** Stats Update   Auto Update

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

**Mesh Network** Update Graph   Auto Update

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.

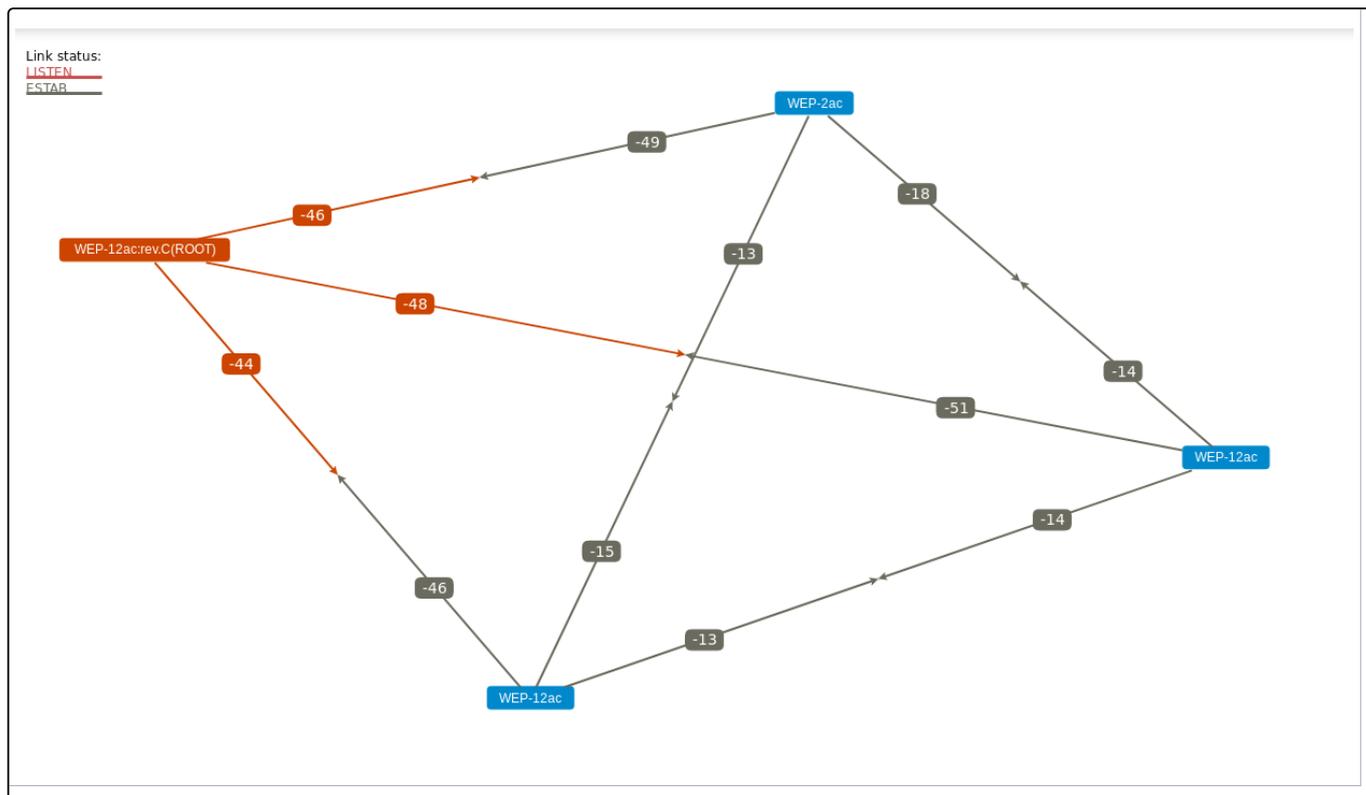
- ✓ Отображается только на устройстве, являющимся контроллером Mesh-сети (Root AP).

*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.

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.



## 4.6 Меню «Services»

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

### 4.6.1 Подменю «Bonjour»

В подменю «**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).

**Set Bonjour Status**

Bonjour Status  Enabled  Disabled

Click "Update" to save the new settings.

*Bonjour Status* – состояние услуги Bonjour:

- *Enabled* – при установленном флаге услуга активна;
- *Disabled* – при установленном флаге услуга выключена.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.6.2 Подменю «Web Server»

В подменю «**Web Server**» выполняются настройки доступа к точке доступа через web-интерфейс.

### Configure Web Server Settings

HTTPS Server Status  Enabled  Disabled

HTTP Server Status  Enabled  Disabled

HTTP Port  (Range: 1025-65535, Default: 80)

HTTPS Port  (Range: 1025-65535, Default: 443)

Maximum Sessions  (Range: 1 - 10, Default: 5)

Session Timeout (minutes)  (Range: 1 - 1440 minutes, Default: 5)

Click "Update" to save the new settings.

- *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. Параметр принимает значения от 1025 до 65535. По умолчанию – 80;
- *HTTPS Port* – номер порта для передачи HTTPS-трафика. Параметр принимает значения от 1025 до 65535. По умолчанию – 443;
- *Maximum Sessions* – количество web-сессий, включая HTTP и HTTPS, которые могут быть одновременно запущены. Параметр принимает значения от 1 до 10 сессий. По умолчанию – 5;
- *Session Timeout (minutes)* – период времени, по истечении которого система автоматически выполнит выход из web-интерфейса, если пользователь не был активен. Параметр принимает значения от 1 до 1440 минут. По умолчанию – 60 минут.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### Generate HTTP SSL Certificate ...

Click "Update" to generate a new HTTP SSL Certificate.

---

### HTTP SSL Certificate File Status ...

Certificate File Present:           yes

Certificate Expiration Date:       Dec 26 09:00:03 2019 GMT

Certificate Issuer Common Name: CN=192.168.1.10

**Generate HTTP SSL Certificate** – в данном разделе при нажатии на кнопку «Update» выполняется генерация нового HTTP SSL сертификата для безопасного доступа к web-серверу. Данное действие 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 File Present* – указывает, присутствует ли сертификат SSL HTTP;
- *Certificate Expiration Date* – дата, до которой сертификат действителен;
- *Certificate Issuer Common Name* – имя сертификата.

**To Get the Current HTTP SSL Certificate ...**

Click the "Download" button to save the current HTTP SSL Certificate as a backup file to your PC.  
To save the Certificate to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method  HTTP  TFTP

---

**To upload a HTTP SSL Certificate from a PC or a TFTP Server ...**

Browse to the location where your certificate file is stored and click the "Upload" button.  
To upload from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method  HTTP  TFTP

HTTP SSL Certificate File  Файл не выбран

**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;
  - *Server IP* – IPv4- или IPv6-адрес TFTP-сервера, который будет использоваться для загрузки файла.

Нажмите на 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 на устройство;
- *TFTP* – через TFTP-сервер, при указании этого способа нужно заполнить следующие поля:
  - *HTTP SSL Certificate File* – имя файла сертификата, задается строка до 256 символов;
  - *Server IP* – IPv4- или IPv6-адрес TFTP-сервера, который будет использоваться для загрузки файла.

Нажмите на кнопку «Upload» для загрузки файла на устройство.

#### 4.6.3 Подменю «SSH»

В подменю «**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.

*SSH Port* – номер порта доступа к устройству по протоколу SSH. Диапазон значений 1025-65535, порт по умолчанию: 22.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.6.4 Подменю «Telnet»

В подменю «**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.

*Telnet Port* – номер порта доступа к устройству по протоколу Telnet. Диапазон значений 1025-65535, порт по умолчанию: 23.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.6.5 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.

### Modify QoS queue parameters

Radio 1 ▼

---

EDCA Template Custom ▼

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3 ▼	7 ▼	1.5
Data 1 (Video)	1	7 ▼	15 ▼	3.0
Data 2 (Best Effort)	3	3 ▼	15 ▼	0
Data 3 (Background)	7	15 ▼	1023 ▼	0

AP EDCA parameters

Wi-Fi Multimedia (WMM)  Enabled  Disabled

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3 ▼	7 ▼	47
Data 1 (Video)	2	7 ▼	15 ▼	94
Data 2 (Best Effort)	3	3 ▼	15 ▼	0
Data 3 (Background)	7	15 ▼	1023 ▼	0

Station EDCA parameters

No Acknowledgement  On  Off

APSD  On  Off

Click "Update" to save the new settings.

Update

*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 и 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;
- *swMin* – начальное значение времени ожидания перед повторной отправкой кадра, задается в миллисекундах, принимает значения 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. Значение *swMin* не может превышать значение *swMax*;
- *swMax* – максимальное значение времени ожидания перед повторной отправкой кадра, задается в миллисекундах, принимает значения 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023. Значение *swMax* должно быть больше значения *swMin*;
- *Max. Burst* – 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*, *swMin*, *swMax* 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 питанием. Данный режим рекомендуется, если для VoIP-телефонов доступ к сети предоставляется через точку доступа.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.6.6 Подменю «Email Alert»

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

### Email Alert Configuration

**Email Alert Global Configuration**

Admin Mode :  (dropdown)

From Address :  (Range: 1 - 255 characters)

Log Duration :  minutes (Range: 30 - 1440, Default: 30)

Urgent Message Severity :  (dropdown)

Non Urgent Severity :  (dropdown)

**Email Alert Mail Server Configuration**

Mail Server Address :  (xxx.xxx.xxx.xxx/Hostname max 255 Characters)

Mail Server Security :  (dropdown)

Mail Server Port :  (Range: 0 - 65535, Default:25)

Username :  (Range: 1 - 64 characters)

Password :  (Range: 1 - 64 characters)

**Email Alert Message Configuration**

To Address 1 :  (Range: 0 - 255 characters)

To Address 2 :  (Range: 0 - 255 characters)

To Address 3 :  (Range: 0 - 255 characters)

Email Subject :  (Range: 1 - 255 characters)

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. Задается строка до 255 символов;
- *Log Duration* – интервалы времени отправки некритичных сообщений. Параметр принимает значения от 30 до 1440. По умолчанию – 30;
- *Urgent Message Severity* – уровень важности сообщений, которые будут отправлены немедленно;
- *Non Urgent Severity* – уровень важности сообщений, которые будут отправлены в интервалах «Log Duration».

В разделе «**Email Alert Mail Server 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. Параметр принимает значения от 0 до 65535. По умолчанию – 25;
- *Username* – имя почтового клиента, задается строка до 64 символов;

- Password – пароль почтового клиента, задается строка до 64 символов.

В разделе «**Email Alert 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.

Для отправки тестового сообщения нажмите кнопку «Test Mail».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.6.7 Подменю «LLDP»

В подменю «**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. Параметр принимает значения от 5 до 32768 секунд. По умолчанию – 30 секунд;
- *POE Priority* – приоритет, пересылаемый в поле «Extended Power Information».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.6.8 Подменю «SNMP»

В подменю «**SNMP**» выполняется настройка управления устройством по SNMP.

**SNMP Configuration**

SNMP  Enabled  Disabled

---

SNMP versions to use: All (Default: All)

Read-only Community Name (for Permitted SNMP Get Operations): \*\*\*\*\* (Range: 1 - 256 characters)

Port number the SNMP agent will listen to: 161 (Range: 1025 - 65535, Default: 161)

Allow SNMP set requests:  Enabled  Disabled

Read-write Community Name (for Permitted SNMP Set Operations): \*\*\*\*\* (Range: 1 - 256 characters)

Restrict the source of SNMP requests to only the designated hosts or subnets:  Enabled  Disabled

Hostname, Address, or Subnet of Network Management System:  (xxx.xxx.xxx.xxx/Hostname max 255 Characters)

IPv6 Hostname, Address, or Subnet of Network Management System:  (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters)

---

**Trap Destinations**

Enabled	Host Type	SNMP version	Community Name (Range: 1 - 256 characters)	Hostname or IP or IPv6 Address (xxx.xxx.xxx.xxx/xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/Hostname max 255 Characters)
<input checked="" type="checkbox"/>	IPv4	snmpV2	public	172.16.0.22
<input type="checkbox"/>	IPv4	snmpV2		
<input type="checkbox"/>	IPv4	snmpV2		

- **SNMP** – включение/выключение управления устройством по SNMP:
  - *Enabled* – при установленном флаге SNMP активен;
  - *Disabled* – при установленном флаге SNMP выключен.
- **SNMP versions to use** – используемая версия SNMP:
  - *All* – использование версий SNMPv1, SNMPv2, SNMPv3;
  - *SNMPv2* – использование версий SNMPv1, SNMPv2;
  - *SNMPv3* – использование версии SNMPv3.
- **Read-only community name** – пароль для read-only запросов, задается строка от 1 до 256 символов;
- **Port number the SNMP agent will listen to** – номер порта приема/отправки SNMP-сообщений. Параметр принимает значения от 1025 до 65535. По умолчанию – 161;
- **Allow SNMP set requests** – разрешить/запретить конфигурирование устройства по SNMP:
  - *Enabled* – разрешить конфигурирование устройства по SNMP:
    - **Read-write community name** – пароль для read-write запросов, задается строка от 1 до 256 символов.
  - *Disabled* – запретить конфигурирование устройства по SNMP.
- **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. Если включено, необходимо заполнить параметры:
  - **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.

**Trap Destinations** – настройка отправки SNMP-трапов на удаленный сервер:

- *Enabled* – включение отправки трапов;
- **Host Type** – укажите, является ли включенный узел узлом IPv4 или узлом IPv6;
- **SNMP version** – выбор версии протокола SNMP;
- **Community Name** – введите имя сообщества, задается строка от 1 до 256 символов;

- *Hostname or IP or IPv6 Address* – введите DNS-имя или IP-адрес сервера, на который точка доступа будет отправлять SNMP-трапы.

В подразделе «**Debug Settings**» выполняется настройка отправки отладочных сообщений.

**Debug Settings**

Debugging Output Tokens  (Range: 0 - 256 characters, empty string for 'no debug', 'ALL', or 'traps,send' - any tokens without spaces)

Dump Sent and Received SNMP Packets  Enabled  Disabled

Logs to

Logs to Specified Files  (Range: 1 - 256 characters, Default: /var/log/snmpd.log)

Logs Priority Level  (for Standart output, Standart error and File logs output)

Logs Priority Range From  to  (only for Syslog output)

Transport  UDP  UDP6  TCP  TCP6

Click "Update" to save the new settings.

- *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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.6.9 Подменю «Time Settings (NTP)»

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

### Modify how the access point discovers the time

System Time (24 HR) Mon Jul 3 2023 12:50:05 RFT

Set System Time  Using Network Time Protocol (NTP)  
 Manually

NTP Server IPv4/IPv6 Address/Name  (xxx.xxx.xxx.xxx/ xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx /Hostname max 253 Characters)

NTP Alternative Server IPv4/IPv6 Address/Name  (xxx.xxx.xxx.xxx/ xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx /Hostname max 253 Characters)

NTP Alternative Server 2 IPv4/IPv6 Address/Name  (xxx.xxx.xxx.xxx/ xxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx /Hostname max 253 Characters)

NTP Update Interval  (Range: 1 - 86400 sec, Default: 3600)

Time Zone  ▼

Adjust Time for Daylight Savings

Click "Update" to save the new settings.

- *System Time (24 HR)* – текущее системное время;
- *Set System Time* – выбор способа установки времени:
  - *Using Network Time Protocol (NTP)* – автоматическая установка с помощью NTP-протокола;
  - *Manually* – ручная установка времени.

Автоматическая установка с помощью NTP-протокола (выбрано Using Network Time Protocol (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;
- *NTP Update Interval* – параметр управления периодом синхронизации.

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).

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.7 Меню «SNMPv3»

В меню «**SNMPv3**» выполняется настройка SNMP протокола 3 версии.

### 4.7.1 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:
  - included – 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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.7.2 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;
- *Security 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:
  - *view-all* – группа может создавать, изменять и удалять базы MIB;
  - *view-none* – группе не разрешено создавать, изменять и удалять базы MIB.
- *Read Views* – выбор дерева/поддерева OID, доступного для чтения:
  - *view-all* – группе разрешен просмотр и чтение всех MIB файлов;
  - *view-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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### 4.7.3 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 передаче 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 передаче 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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.7.4 Подменю «SNMPv3 Targets»

В подменю «**SNMPv3 Targets**» выполняется настройка отправки 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. Параметр принимает значения от 1 до 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».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### 4.8 Меню «Maintenance»

Меню «**Maintenance**» предназначено для общего управления устройством: выгрузка, загрузка, установка конфигурации по умолчанию, обновление ПО, перезагрузка устройства, а также для операций отладки: sniffинга трафика, проходящего через точку доступа и выгрузки диагностической информации по устройству.

#### 4.8.1 Подменю «Configuration»

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

**Manage this Access Point's Configuration**

---

**To Restore the Factory Default Configuration ...**

Click "Reset" to load the factory defaults in place of the current configuration for this AP.

Save access settings

---

**To Save the Current Configuration to a Backup File ...**

Click the "Download" button to save the current configuration as a backup file to your PC. To save the configuration to an external TFTP server, click the TFTP radio button and enter the TFTP server information.

Download Method  HTTP  TFTP

---

**To Restore the Configuration from a Previously Saved File ...**

Browse to the location where your saved configuration file is stored and click the "Restore" button. To restore from a TFTP server, click the TFTP radio button and enter the TFTP server information.

Upload Method  HTTP  TFTP

Configuration File  Файл не выбран

**To Restore the Factory Default Configuration** – сброс устройства к заводским настройкам.

Чтобы сделать сброс всех настроек устройства на стандартные заводские установки, нажмите кнопку «Сброс». После сброса устройство автоматически перезагрузится. Весь процесс займет несколько минут.

Если активирован флаг **Save access settings**, то будут сохранены те параметры конфигурации, которые отвечают за доступ к устройству (настройка IP-адреса, настройки доступа по Telnet/SSH/SNMP/Netconf/Web). После сброса устройство автоматически перезагружено не будет.

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

**To Save the Current Configuration to a Backup File** – выгрузка текущей конфигурации в backup-файл с последующим скачиванием файла на удаленный сервер. Выгрузка файла конфигурации с устройства может осуществляться посредством протоколов HTTP и TFTP.

- **Выгрузка через HTTP.** Установите флаг «Download Method» в значение «HTTP». Нажмите кнопку «Download», 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 кнопку «Download» для начала выгрузки файла.

**To Restore the Configuration from a Previously Saved File** – загрузка ранее сохраненного файла конфигурации на точку доступа. Загрузка конфигурации на устройство может осуществляться посредством протоколов HTTP и TFTP.

- ✘ 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 кнопку «Restore» для начала загрузки файла конфигурации в устройство.
- **Загрузка через TFTP.** Установите флаг «Upload Method» в значение TFTP. В поле «Filename» укажите имя файла, который будет загружен на устройство. Имя файла обязательно должно содержать расширение .xml. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором сохранен backup-файл. Нажмите кнопку «Restore» для начала загрузки файла.

**To Save the Startup Configuration to a Backup File or to Mirror file ...**

To Save the Startup Configuration to a Backup File or to Mirror file

Source File Name:  Startup Configuration  
 Backup Configuration  
 Mirror Configuration

Destination File Name:  Startup Configuration  
 Backup Configuration

Click "Update" to save the new settings.

---

**To Reboot the Access Point ...**

Click the "Reboot" button.

**To Save the Startup Configuration to a Backup File or to Mirror file** – 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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**Rebooting the Access Point** – программная перезагрузка устройства.

Для перезагрузки устройства нажмите на кнопку «Reboot».

#### 4.8.2 Подменю «Upgrade»

В подменю «**Upgrade**» выполняется обновление и смена программного обеспечения (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.

**Manage firmware**

Model: Eltex WEP-2ac Smart

Firmware Version

Primary Image: **(Текущая версия ПО)**

Secondary Image: **(Версия ПО резервного образа)**

---

Upload Method:  HTTP  TFTP

New Firmware Image:  Файл не выбран.

- *Model* – модель устройства;
- *Firmware Version* – версия ПО 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 точка доступа 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 кнопку «Обзор...». В открывшемся диалоговом окне выберите путь к файлу ПО на ПК. Нажмите кнопку «*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 кнопку «*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.

#### 4.8.3 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, дампы можно проанализировать специальными программами, например, *Wireshark*.

Для обновления информации на странице нажмите кнопку «*Refresh*».

**Packet Capture Status** – в разделе выполняется просмотр информации о статусе записи дампа трафика и возможность остановки процесса.

- *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* – если установлен флаг в положение «Enabled» – записывать в дамп все принимаемые радиоинтерфейсом пакеты, включая пакеты, не предназначенные для данной точки доступа;
- *Client Filter Enable* – если установлен флаг в дамп будут записываться только те пакеты, которые приходят от определенного пользователя. При включении данной функции необходимо заполнить следующее поле:
  - *Client Filter MAC Address* – MAC-адрес клиента, трафик которого должен отфильтровываться в дамп.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**Packet File Capture ...**

Capture Interface:  (dropdown)

Capture Duration:  Seconds (range 10 to 3600)

Max Capture File Size:  KB (range 64 to 4096)

Click "Update" to save the new settings.

---

**Remote Packet Capture ...**

Remote Capture Port:  (Range:1025-65530, Default: 2002)

Click "Update" to save the new settings.

---

**Packet Capture File Download ...**

Use TFTP to Download the Capture File

TFTP Server Filename:

Server IP:

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

- *Capture Interface* – имя интерфейса устройства, с которого будет производиться запись дампа трафика (eth0 – GE1, wlan0var1 – виртуальная сеть 1 на беспроводном интерфейсе 0);
- *Capture Duration* – длительность записи дампа. Параметр принимает значения от 10 до 3600 секунд. По умолчанию – 60 секунд;
- *Max Capture File Size* – максимальный размер дампа. Параметр принимает значения от 64 до 4096 КВ. По умолчанию – 1024 КВ.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

Для начала записи дампа трафика в файл с установленными параметрами нажмите на кнопку «Start File Capture».

**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, который служит для подключения удаленной машины. Параметр принимает значения от 1025 до 65530. По умолчанию – 2002.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

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

После старта RPCAP-сервера на устройстве, необходимо на удаленной машине подключиться к точке доступа. Для удаленного подключения использовать RPCAP-протокол, указать IP-адрес устройства и порт, установленный в поле *Remote Capture Port*. Например, это можно выполнить с помощью программы Wireshark. Затем, необходимо получить список интерфейсов для sniffинга от устройства, выбрать один из них и запустить снятие дампа с удаленного интерфейса.

**Packet Capture File Download** – в разделе выполняется выгрузка записанного файла с дампом 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 кнопку «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 кнопку «Download» для начала выгрузки дампа.

#### 4.8.4 Подменю «Support Information»

В подменю «**Support Information**» выполняется выгрузка текущей информации об устройстве (количество памяти, запущенные процессы, конфигурация) в виде текстового файла. Данная информация может использоваться для 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.

#### 4.9 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 в сеть, будут находить в сети мастера и копировать с него конфигурацию. В последующем при внесении изменений в конфигурацию одной из точек доступа эти изменения применяется для всех точек, находящихся в кластере.

- ✓ Режим работы в кластере включен на устройстве по умолчанию.

- ✗ В кластер можно объединить только точки из одной группы:

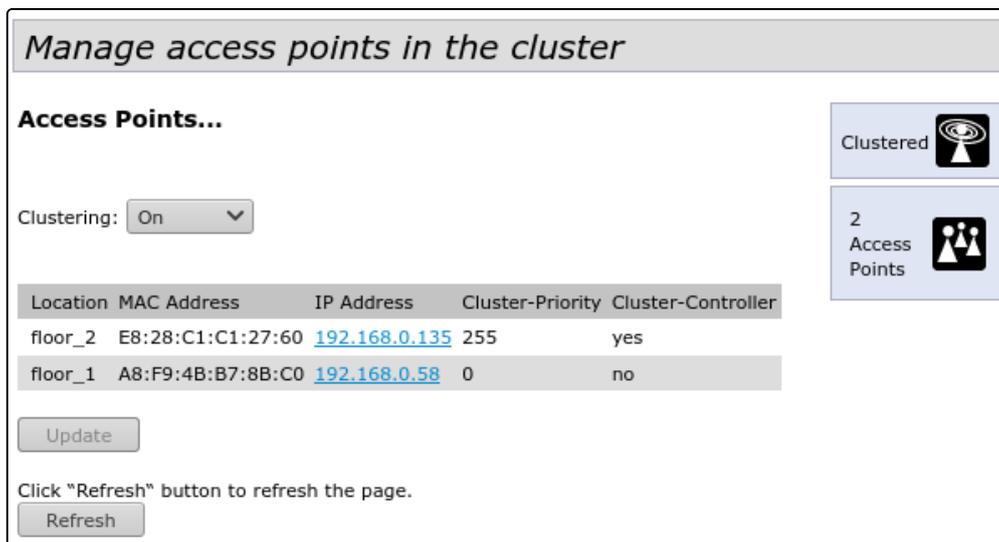
1 группа	WEP-12ac	WOP-12ac			
2 группа	WEP-2ac	WEP-2ac Smart	WOP-2ac	WOP-2ac SFP	WOP-2ac GPON

- ✓ 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.

#### 4.9.1 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 кластера и запуск/остановка работы устройства в данном режиме.

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

В таблице приводится список точек доступа, находящихся в одном кластере. Исходя из информации, представленной в таблице, можно узнать:

- *Location* – описание физического местоположения точки доступа. Заполняется на каждой точке доступа администратором в разделе «Clustering Options»;
- *MAC Address* – MAC-адрес точки доступа, находящейся в кластере;
- *IP Address* – IP-адрес точки доступа, находящейся в кластере;
- *Cluster-Priority* – приоритет точки доступа в кластере. Точка доступа с максимальным значением данного параметра становится Master-точкой. Параметр устанавливается на каждой точке доступа администратором в разделе «Clustering Options». Если параметр не установлен, Master-точкой в кластере становится точка доступа с наименьшим значением MAC-адреса;
- *Cluster-Controller* – параметр, указывающий какая точка доступа является в данном кластере Master-точкой. Параметр может принимать значения: *yes* – точка является Master-точкой; *no* – точка не является Master-точкой.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

Для обновления информации на странице нажмите кнопку «Refresh».

### Clustering Options...

Enter the location of this AP.

Location:

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

Cluster Name:

Clustering IP Version:  IPv6  IPv4

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

Click "Update" to save the new settings.

---

### Single IP Management...

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

Click "Update" to save the new settings.

**Clustering Options** – в разделе выполняется настройка базовых параметров кластера.

- ✓ Параметры раздела доступны для редактирования при условии, что кластер на точке выключен, т.е. параметр «Clustering» принимает значение *Off*

- *Location* – описание физического расположения точки доступа. Используется для отображения в таблицах мониторинга для удобства анализа и управления сетью;
- *Cluster Name* – имя кластера. Точка доступа будет подключаться только к тому кластеру, имя которого прописано в данном параметре. По умолчанию – default;
- *Clustering IP Version* – используемая версия протокола IP для обмена управляющей информацией между устройствами кластера;
- *Cluster-Priority* – приоритет точки в кластере. Параметр принимает значения от 0 до 255. По умолчанию – 0. Поддерживается только для IPv4-сетей. Мастером в кластере является та точка, у которой приоритет кластера выше. Если параметр не установлен, Master-точкой в кластере становится точка доступа с наименьшим значением MAC-адреса.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**Single IP Management** – в разделе выполняется установка дополнительного адреса мастера в кластере.

В процессе эксплуатации Master-точка кластера может меняться, что обусловлено различными ситуациями, например, Master-точка вышла из строя или в сеть была добавлена новая точка доступа с более высоким приоритетом или меньшим MAC-адресом. Для того, чтобы иметь возможность подключения к Master-точке независимо от того, какая именно точка является на данный момент мастером, необходимо назначить «Cluster Management Address».

В случае установления соединения по «Cluster Management Address», пользователь гарантированно подключается именно к тому устройству, которое является мастером в кластере. В случае смены мастера в кластере, «Cluster Management Address» также переходит на новую точку доступа.

- *Cluster Management Address* – уникальный IPv4-адрес, по которому будет доступна Master-точка кластера. Данный адрес должен находиться в подсети кластера и не совпадать с IP-адресом других устройств, находящихся в сети.

При установке данного параметра на одной точке кластера, все остальные точки, состоящие в кластере, узнают о данной настройке автоматически.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

**Secure Join Clustering...**

Secure Mode:  Enabled  Disabled

Pass Phrase:  (8 - 63 characters)

Reauthentication Timeout:  (Sec, Range: 300 - 86400)

Click "Update" to save the new settings.

**Secure Join Clustering** – в разделе выполняется настройка безопасности соединения кластера.

- ✓ Параметры раздела доступны для редактирования при условии, что кластер на точке выключен, т.е. параметр «Clustering» принимает значение *Off*. Настройки поддерживаются только для IPv4-сетей.

- *Secure Mode* – включение/отключение безопасности кластера. Если Enabled, то в кластер могут встать только те точки доступа, у которых совпадает пароль, указанный в поле «Pass Phrase»;
- *Pass Phrase* – пароль безопасности кластера. Пароль должен содержать от 8 до 63 символов. Допустимые символы: прописные и строчные буквы, цифры и специальные символы, такие как @ и #;
- *Reauthentication Timeout* – период времени через который будет происходить повторная аутентификация. Параметр принимает значения от 300 до 86400 секунд. По умолчанию – 300 секунд.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.9.2 Подменю «Sessions»

В подменю «**Sessions**» выполняется просмотр параметров сессий клиентов, подключенных к точкам доступа, находящимся в кластере. Каждый клиент определяется MAC-адресом и точкой доступа, к которой осуществляется его текущее подключение.

В таблице может быть указано максимум 20 клиентов. Просмотреть всех клиентов, подключенных к данной точке доступа можно в меню «Status» → «Client Associations».

*Manage sessions associated with the cluster*

**Sessions...**

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

Display

<a href="#">AP Location</a>	<a href="#">User MAC</a>	<a href="#">Rate (Mbps)</a>	<a href="#">Signal</a>	<a href="#">Rx Total</a>	<a href="#">Tx Total</a>	<a href="#">Error Rate</a>
floor_1	F2:2B:5A:02:68:5E	156	27	500	454	0
floor_1	14:36:C6:15:A4:11	65	22	18	38	0

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

- ✓ Вы можете ограничить количество отображаемых столбцов в таблице мониторинга, выберите в поле «Display» параметр, отличный от «All», и нажмите на кнопку «Go». При выборе определенного параметра в таблице для каждого клиента будут отображаться столбцы: «AP Location», «User MAC», и столбец с выбранным параметром.

- *AP Location* – описание физического местоположения точки доступа;
- *User MAC* – MAC-адрес беспроводного устройства клиента;
- *Rate* – скорость передачи данных между точкой доступа и определенным клиентом, Мбит/с;
- *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.

#### 4.9.3 Подменю «Radio Resource Management»

Подменю «**Radio Resource Management**» предназначено для управления автоматическим выбором каналов точек доступа.

В режиме кластера каждая точка доступа устанавливает номера каналов, на которых работают 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.

*Automatically manage radio resource assignments*

**Channel Planner ...**

automatically re-assigning channels

Clustered 

2 Access Points 

**Current Channel Assignments**

IP Address	Radio	Band	Channel	Status	Locked
192.168.0.135	E8:28:C1:C1:27:70	B/G/N	1	up	<input type="checkbox"/>
192.168.0.135	E8:28:C1:C1:27:60	A/N/AC	40	up	<input type="checkbox"/>
192.168.0.58	A8:F9:4B:B7:8B:D0	B/G/N	11	up	<input type="checkbox"/>
192.168.0.58	A8:F9:4B:B7:8B:C0	A/N/AC	36	up	<input type="checkbox"/>

Для того, чтобы запустить процесс спектрального анализа среды и выбора оптимального канала для каждой точки доступа в кластере, нажмите на кнопку «Start». Для остановки процесса нажмите на кнопку «Stop».

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

- *IP Address* – IP-адрес точки доступа в кластере;
- *Radio* – MAC-адрес радиointерфейса точки доступа в кластере;
- *Band* – набор стандартов, поддерживаемых радиointерфейсом точки доступа в кластере на данный момент;
- *Channel* – частотный канал в кластере;
- *Status* – состояние работы радиointерфейса точки доступа в кластере;
- *Locked* – блокировка смены канала. При установленном флаге, в момент выбора оптимального канала всеми точками доступа, данный радиointерфейс 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».

Proposed Channel Assignments ( 16 seconds ago )

IP Address	Radio	Proposed Channel
192.168.0.135	E8:28:C1:C1:27:70	1
192.168.0.58	A8:F9:4B:B7:8B:D0	11
192.168.0.135	E8:28:C1:C1:27:60	40
192.168.0.58	A8:F9:4B:B7:8B:C0	36

Advanced

Change channels if interference is reduced by at least

Refresh when access point is added to the cluster

Determine if there is better set of channel settings every

Click "Update" to save the new settings.

В таблице «**Proposed Channel Assignments**» приводится информация о возможных значениях канала, на который перейдет радиointерфейс точки доступа в случае запуска пересчета оптимальности выбора канала:

- *IP Address* – IP-адрес точки доступа в кластере;
- *Radio* – MAC-адрес радиointерфейса точки доступа в кластере;
- *Proposed Channel* – номер канала, на который перейдет радиointерфейс 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 cluster* – 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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### Transmit Power Control ...

automatically re-assigning tx power

RSSI Threshold 2.4 GHz  (Range: -100...-30)

RSSI Threshold 5 GHz  (Range: -100...-30)

Interval  (Range: 1800...86400 or 0)

**Advanced**

Minimal Tx Power  (Range: 6...30)

Active Scan Mode

Debug Mode

Monitoring

TPC statistics is not available because tpc-planner is not up

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.

Для запуска процесса автоподстройки мощности для каждой точки доступа в кластере нажмите на кнопку «Start». Для остановки процесса нажмите на кнопку «Stop».

- *RSSI Threshold 2.4 GHz* – порог уровня RSSI в диапазоне 2.4 ГГц. Параметр принимает значения от -100 до -30. По умолчанию -65;
- *RSSI Threshold 5 GHz* – порог уровня RSSI в диапазоне 5 ГГц. Параметр принимает значения от -100 до -30. По умолчанию -70;
- *Interval* – интервал времени между циклами оптимизации. Параметр принимает значения от 1800 до 86400 секунд. По умолчанию – 0, что означает, что оптимизация мощности проводится 1 раз, затем только при изменении состава кластера.

**Advanced** – в разделе выполняются расширенные настройки:

- *Minimal Tx Power* – минимальный выходной уровень мощности точки доступа. Параметр принимает значения от 6 до 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.

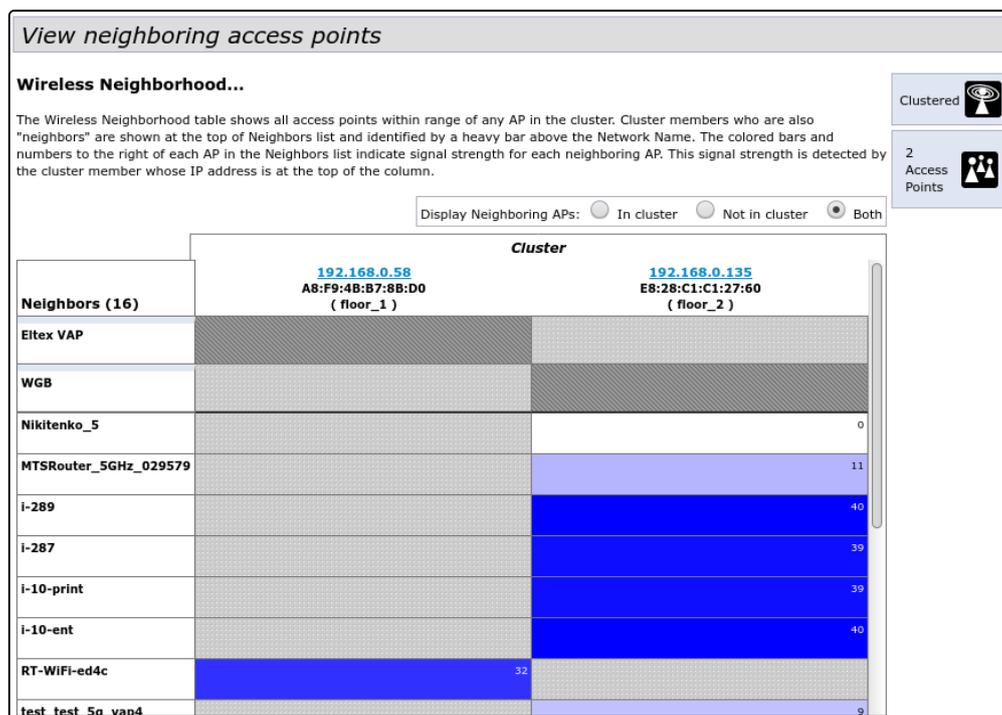
Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

В окне «Monitoring» после окончания оптимизации автоподстройки мощности можно наблюдать результаты сканирования всех точек доступа в кластере, уровень влияния точек друг на друга, а также измененную выходную мощность точек доступа.

#### 4.9.4 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 строке таблицы отображена информация по каждому радиоинтерфейсу точек доступа, находящихся в кластере. В крайнем левом столбце «Neighbors» 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.

Параметр «Display Neighboring APs» настраивает отображение информации в таблице:

- *In cluster* – при установленном флаге в таблице будет отображаться информация только о тех беспроводных сетях, которые настроены на точках доступа, находящихся в кластере;
- *Not in cluster* – при установленном флаге в таблице будет отображаться информация только о тех беспроводных сетях, которые настроены на точках доступа, не находящихся в кластере;
- *Both* – при установленном флаге в таблице будет отображаться информация о всех сетях.

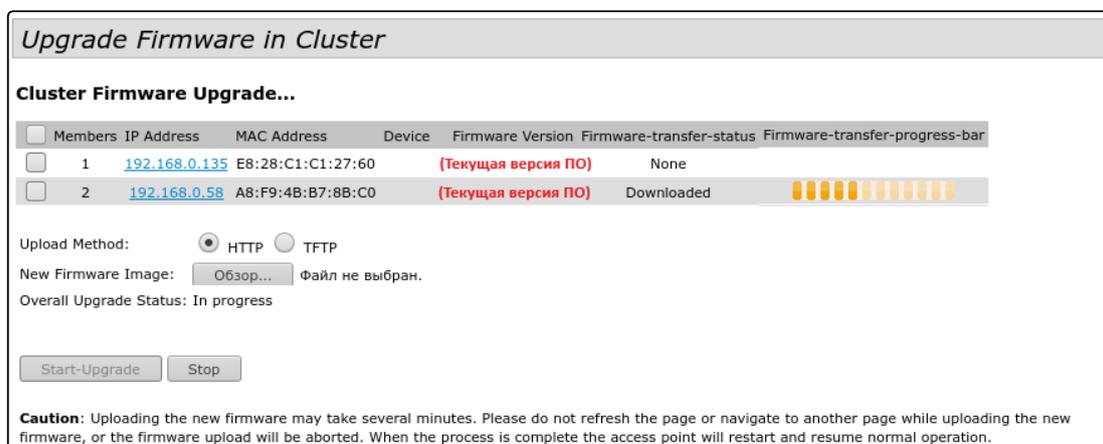
#### 4.9.5 Подменю «Cluster Firmware Upgrade»

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

✔ Параметры данного подменю доступны для просмотра и редактирования только на Master-точке кластера.

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

При обновлении ПО устройств кластера файл прошивки будет загружен на каждое устройство и установлен на позицию «Primary Image». В процессе обновления 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).



- *Members* – порядковый номер точки доступа, находящейся в кластере;
- *IP Address* – IP-адрес точки доступа, находящейся в кластере;
- *MAC Address* – MAC-адрес точки доступа, находящейся в кластере;
- *Device* – тип точки доступа;
- *Firmware Version* – текущая версия ПО точки доступа;
- *Firmware-transfer-status* – статус процесса обновления программного обеспечения на точке доступа;
- *Firmware-transfer-progress-bar* – статус процесса загрузки файла программного обеспечения на точку доступа.

**Обновление ПО устройств.** Загрузка файла ПО на устройство может производиться посредством HTTP или TFTP протоколов.

**Загрузка через HTTP.** Установите флаг «Upload Method» в значение HTTP. Нажмите кнопку «Обзор...». В открывшемся диалоговом окне выберите путь к файлу ПО на ПК. В крайнем левом столбце таблицы установите флаг напротив точек доступа, на которых необходимо обновить программное обеспечение. Нажмите кнопку «Start-Upgrade» для начала загрузки файла на устройства.

**Загрузка через TFTP.** Установите флаг «Upload Method» в значение TFTP. В поле «Image Filename» укажите имя файла ПО, который будет загружен на устройство. Имя файла обязательно должно содержать расширение .tar. В поле «Server IP» укажите IP-адрес TFTP-сервера, на котором сохранен файл ПО. В крайнем левом столбце таблицы установите флаг напротив точек доступа, на которых необходимо обновить программное обеспечение. Нажмите кнопку «Start-Upgrade» для начала загрузки файла.

Нажмите на кнопку «Stop» для прерывания процесса обновления устройства.

В поле «Overall Upgrade Status» отображается обобщенный статус процесса обновления программного обеспечения на точках доступа.

#### 4.10 Меню «Captive Portal»

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

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

##### 4.10.1 Подменю «Global Configuration»

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

*Global Configuration Settings*

Captive Portal Mode  Enabled  Disabled

Authentication Timeout  (60 - 600 sec, 300 = Default)

Roaming service URL  (0 - 2048 characters)

Roaming no action timeout  (0 - 86400 min, 720 = Default)

Instance Count: 32

Click "Update" to save the new settings.

- *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. Параметр принимает значения от 60 до 600 секунд. По умолчанию – 300 секунд;
- *Roaming Service URL* – адрес сервиса APB для поддержки роуминга в режиме hotspot. Задается в формате: "ws://host:port/path";
- *Roaming No Action Timeout* – время, через которое точка доступа удалит устаревшие/неактивные записи о клиентах в роуминге. Параметр принимает значения от 0 до 86400 минут. По умолчанию – 720 минут;
- *Instance Count* – количество экземпляров портала, настроенных на точке доступа.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

## 4.10.2 Подменю «Instance Configuration»

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

**Instance Configuration Settings**

Captive Portal Instances Create ▼

---

**Captive Portal Instance Parameters**

Instance Name  (1 - 32 characters)

Click "Update" to save the new settings.

Update

Для создания нового портала в поле «**Captive Portal Instances**» необходимо выбрать пункт «**Create**» и в поле «**Instance Name**» указать имя нового портала. Имя портала может содержать от 1 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 Configuration Settings**

Captive Portal Instances wlan0bssvap0 ▼

---

**Captive Portal Instance Parameters**

Instance ID: 1

Admin Mode  Enabled  Disabled

Verification Cportal ▼

Virtual Portal Name

Global Radius  On  Off

Radius Accounting  On  Off

Radius Domain

Radius IP Network ipv4 ▼

Radius IP

Radius Backup IP 1

Radius Backup IP 2

Radius Backup IP 3

Radius Key

Radius Backup Key 1

Radius Backup Key 2

Radius Backup Key 3

External URL  (0 - 256 characters)

Away Time  720 (0 - 1440 min, 60 = Default)

Session Timeout  0 (0 - 1440 min, 0 = Default)

Max Bandwidth Upstream  0 (0 - 1331200 Kbps, 0 = Default)

Max Bandwidth Downstream  0 (0 - 1331200 Kbps, 0 = Default)

Delete Instance

Click "Update" to save the new settings.

Update

- *Instance ID* – номер портала;
- *Admin Mode* – режим работы портала:
  - *Enable* – включен;
  - *Disabled* – выключен.
- *Verification* – метод проверки подлинности пользователя:
  - *Sportal* – метод, при котором проверку подлинности пользователя на Radius-сервере выполняет Captive Portal;
  - *RADIUS* – для авторизации пользователь должен быть прописан на Radius-сервере;
- *Virtual Portal Name* – имя виртуального портала;
- *Global Radius* – глобальные настройки авторизации по RADIUS-протоколу:
  - *Off* – выключен;
  - *On* – включен. Выбор данного варианта открывает возможность редактирования следующих полей:
    - *Radius Accounting* – при включенной функции будут отправляться сообщения «Accounting» на RADIUS-сервер:
      - *On* – включен;
      - *Off* – выключен.
    - *Radius Domain* – домен пользователя;
    - *Radius IP Network* – выбор протокола IPv4 или IPv6 для доступа на сервер RADIUS;
    - *Radius IP* – адрес основного RADIUS-сервера. При недоступности основного RADIUS-сервера, запросы будут отправляться на резервные RADIUS-сервера;
    - *Radius Backup IP 1, 2, 3* – адрес резервного RADIUS-сервера;
    - *Radius Key* – пароль для авторизации на основном RADIUS-сервере;
    - *Radius Backup Key 1, 2, 3* – пароль для авторизации на резервном RADIUS-сервере 1, 2, 3;
- *External URL* – адрес внешнего Captive Portal, на который будет перенаправлен пользователь при подключении к hotspot сети;
- *Away Time* – время, в течение которого действительна запись аутентификации пользователя на точке доступа после его диссоциации. Если в течение этого времени клиент не пройдет аутентификацию повторно, запись будет удалена. Параметр принимает значения от 0 до 1440 минут. По умолчанию – 60 минут;
- *Session Timeout* – таймаут жизни сессии. Пользователь автоматически выходит из портала через указанный промежуток времени. Параметр принимает значения от 0 до 1440 минут. По умолчанию 0 – таймаут не применяется;
- *Max Bandwidth Upstream* – максимальная скорость передачи трафика от абонента. Параметр принимает значения от 0 до 1331200 Kbps. По умолчанию 0 – без ограничения;
- *Max Bandwidth Downstream* – максимальная скорость передачи трафика к абоненту. Параметр принимает значения от 0 до 1331200 Kbps. По умолчанию 0 – без ограничения;
- *Delete Instance* – для удаления данного портала установите флаг и нажмите кнопку «Update». Дефолтные порталы удалить невозможно.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

### 4.10.3 Подменю «VAP Configuration»

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

### VAP Configuration Settings

Radio

VAP Instance Name	
0	<input type="text" value="wlan0bssvap0"/>
1	<input type="text" value="wlan0bssvap1"/>
2	<input type="text" value="wlan0bssvap2"/>
3	<input type="text" value="wlan0bssvap3"/>
4	<input type="text" value="wlan0bssvap4"/>
5	<input type="text" value="wlan0bssvap5"/>
6	<input type="text" value="wlan0bssvap6"/>
7	<input type="text" value="wlan0bssvap7"/>
8	<input type="text" value="wlan0bssvap8"/>
9	<input type="text" value="wlan0bssvap9"/>
10	<input type="text" value="wlan0bssvap10"/>
11	<input type="text" value="wlan0bssvap11"/>
12	<input type="text" value="wlan0bssvap12"/>
13	<input type="text" value="wlan0bssvap13"/>
14	<input type="text" value="wlan0bssvap14"/>
15	<input type="text" value="wlan0bssvap15"/>

Click "Update" to save the new settings.

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

В таблице для каждой виртуальной сети назначается портал по его имени.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.10.4 Подменю «Authenticated Clients»

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

<i>Authenticated Client List</i>													
Click "Refresh" button to refresh the page.													
<input type="button" value="Refresh"/>													
Total Number of Authenticated Clients 2													
MAC Address	IP Address	User Name	Protocol Mode	Verify Mode	VAP ID	Radio ID	Captive Portal ID	Session Time out	Away Time out	Rx Packets	Tx Packets	Rx Bytes	Tx Bytes
70:70:0d:93:c3:e0		79232566602	http	cportlad	2	1	3	0	88976 s	0	0	0	0
74:df:bf:ea:56:45		79139192546	http	cportlad	1	2	18	0	0	0	0	0	0

Для обновления информации на странице нажмите кнопку «Refresh».

- *Total Number of Authenticated Clients* – количество успешно авторизованных клиентов на данный момент времени;
- *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 радиointерфейса;
- *Captive Portal ID* – номер 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.

#### 4.10.5 Подменю «Failed Authentication Clients»

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

<i>Failed Authentication Client List</i>								
Click "Refresh" button to refresh the page.								
<input type="button" value="Refresh"/>								
Total Number of Fail Authenticated Clients 0								
MAC Address	IP Address	User Name	Verify Mode	VAP ID	Radio ID	Captive Portal ID	Failure Time	

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 радиointерфейса;
- *Captive Portal ID* – номер портала, с которым ассоциирован клиент;
- *Failure Time* – время, когда произошла ошибка.

## 4.11 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.

### 4.11.1 Подменю «VAP QoS Parameters»

Подменю «**VAP QoS Parameters**» позволяет глобально включить использование всех настроек Client QoS (Class MAP, Policy MAP, Bandwidth Limit), назначить ранее 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 пропускания от точки доступа к каждому клиенту, кбит/с. Параметр принимает значения от 0 до 866700 кбит/с. Если назначен 0, то ограничение полосы пропускания не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;
- *Bandwidth Limit Up* – ограничение ширины полосы пропускания от каждого клиента до точки доступа, кбит/с. Параметр принимает значения от 0 до 866700 кбит/с. Если назначен 0, то ограничение полосы пропускания не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;
- *DiffServ Policy Down* – имя профиля Policy, который должен быть применен к трафику, передаваемому в направлении от точки доступа к клиенту;
- *DiffServ Policy Up* – имя профиля Policy, который должен быть применен к трафику, передаваемому в направлении от клиента к точке доступа;
- *VAP Limit Down* – ограничение ширины полосы пропускания от точки доступа к клиентам (в сумме), подключенным к данному VAP, кбит/с. Параметр принимает значения от 0 до 866700 кбит/с. Если назначен 0, то ограничение не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с;

- *VAP Limit Up* – ограничение ширины полосы пропускания от клиентов (в сумме) до точки доступа, бит/с. Параметр принимает значения от 0 до 866700 кбит/с. Если назначен 0, то ограничение не применяется. Любое ненулевое значение округляется до величины, кратной 64 кбит/с.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.11.2 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 профиля;
- *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;
- *IPv6 Flow Label* – значение поля Flow Label.

Для удаления класса установите флаг напротив «Delete Class Map» и нажмите кнопку «Update».

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.11.3 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 блокировке.

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.

### Configure Client QoS DiffServ Policy Map Settings

---

**Policy Map Configuration**

Policy Map Name  (1 - 31 characters)

---

**Policy Class Definition**

Policy Map Name

Class Map Name

---

Police Simple  Committed Rate  (1 - 1000000 kbps) Committed Burst  (1 - 204800000 bytes)

Send

Drop

Mark Class Of Service   (0 - 7)

Mark IP Dscp  Select From List

Mark IP Precedence   (0 - 7)

Disassociate Class Map

---

Member Classes

Delete Policy Map

Click "Update" to save the new settings.

**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 на 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. Параметр принимает значение 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. Параметр принимает значение 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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

#### 4.11.4 Подменю «Client Configuration»

В подменю «**Client Configuration**» можно просмотреть текущую конфигурацию QoS, действующую для конкретного клиента, подключенного к точке доступа.

- *Station* – выбор клиента, подключенного к точке доступа;
- *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, 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.

## 4.12 Меню «Workgroup Bridge»

### 4.12.1 Подменю «Workgroup Bridge»

Подменю «**Workgroup Bridge**» предназначено для настройки устройства в режиме беспроводного клиента с использованием одного из беспроводных интерфейсов.

✘ WGB не может быть настроен, если на точке настроен WDS или включен режим кластера.

✘ Для корректной работы WGB необходимо, чтобы на точках доступа была установлена одинаковая версия программного обеспечения.

### Modify AP Workgroup Bridge Settings

Workgroup Bridge Mode  Up  Down

Radio  ▼

WGB ARP-Timeout  (1 - 1440 min, Default: 5)

**Upstream Interface**

VLAN ID

SSID  Ⓢ

Roam Threshold  (-99 - -1) dBm

Security  Ⓢ

Connection Status

**Downstream Interface**

Status  Up  Down

VLAN ID

SSID

Broadcast SSID  ▼

Security  Ⓢ

MAC Auth Type  ▼

Click "Update" to save the new settings. Click "Refresh" button to refresh the page.

- *Workgroup Bridge Mode* – включение/выключение режима клиента на интерфейсе:
  - *Up* – функционал включен;
  - *Down* – функционал выключен.
- *Radio* – выбор беспроводного интерфейса, на котором включается режим клиента. Radio 1 работает в диапазоне 5 ГГц, Radio 2 работает в диапазоне 2.4 ГГц;
- *WGB ARP-Timeout* – время жизни записи в ARP-таблице в режиме WGB. Параметр принимает значение от 1 до 1440 минут. По умолчанию – 5 минут.

**Upstream Interface** – настройка интерфейса, который будет являться беспроводным клиентом и подключаться к сторонней точке доступа;

- *VLAN ID* – номер VLAN, используемый на точке доступа;
- *SSID* – имя точки доступа, к которой происходит подключение;
- *Roam Threshold* – минимальный уровень сигнала от точки доступа, при котором происходит подключение к точке;

- **Security** – режим безопасности, настроенный на VAP точки доступа, к которой происходит подключение:
  - *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-TKIP или WPA2-AES. При выборе данного режима для редактирования будут доступны следующие настройки:

- *WPA Versions* – версия используемого протокола безопасности (WPA-TKIP или WPA2-AES);
- *MFP* – настройка режима защиты клиентских фреймов:
  - *Not Required* – не использовать защиту;
  - *Capable* – использовать защиту при наличии возможности;
  - *Required* – использовать защиту обязательно, все клиенты должны поддерживать CCX5.
- *Key* – ключ/пароль, необходимый для авторизации на точке доступа;
- *WPA Enterprise* – режим подключения к точке доступа с использованием авторизации и аутентификации на вышестоящем RADIUS-сервере. При выборе данного режима для редактирования будут доступны следующие настройки:

- *WPA Versions* – версия используемого протокола безопасности: WPA-TKIP, WPA2-AES;
- *MFP* – настройка режима защиты клиентских фреймов:
  - *Not Required* – не использовать защиту;
  - *Capable* – использовать защиту при наличии возможности;
  - *Required* – использовать защиту обязательно, все клиенты должны поддерживать CCX5.
- *EAP Method* – выбор протокола аутентификации (peap или tls);
- *Username* – имя пользователя, используемое при авторизации на RADIUS-сервере;
- *Password* – пароль пользователя, используемый при авторизации на RADIUS-сервере;
- *Connection Status* – статус подключения к точке доступа.

**Downstream Interface** – настройка интерфейса, выступающего в качестве точки доступа.

*Status* – включение/выключение downstream-интерфейса:

- *Up* – интерфейс включен;
- *Down* – интерфейс выключен.
- *VLAN ID* – номер VLAN, в котором будет передаваться сетевой трафик для данной точки доступа;
- *SSID* – имя беспроводной сети;
- *Broadcast SSID* – включить/выключить вещание беспроводной сети:
  - *On* – вещание включено;
  - *Off* – вещание выключено.
- *Security* – режим безопасности создаваемой беспроводной сети:
  - *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:

- *WPA Versions* – 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. Параметр принимает значения от 0 до 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. Параметр принимает значения от 0 до 86400.
- *MFP* – настройка режима защиты клиентских фреймов:
  - *Not Required* – не использовать защиту;
  - *Capable* – использовать защиту при наличии возможности;
  - *Required* – использовать защиту обязательно, все клиенты должны поддерживать CCX5.

*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.

Для вступления в силу новой конфигурации и внесения настроек в энергонезависимую память нажмите кнопку «Update».

Для обновления информации на странице нажмите кнопку «Refresh».

#### 4.12.2 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.

<i>View transmit and receive statistics for this access point</i>			
Click "Refresh" button to refresh the page.			
<input type="button" value="Refresh"/>			
<b>Interface</b>	<b>Status</b>	<b>VLAN ID</b>	<b>Name (SSID)</b>
wlan0upstrm	Associated to AP a8:f9:4b:b7:8b:c0	1	Test_AP
wlan0dwstrm	up	1	Test_Clients
Transmit			
<b>Interface</b>	<b>Total packets</b>	<b>Total bytes</b>	
wlan0upstrm	275	323895	
wlan0dwstrm	0	0	
Receive			
<b>Interface</b>	<b>Total packets</b>	<b>Total bytes</b>	
wlan0upstrm	351	36370	
wlan0dwstrm	0	0	

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.

Чтобы перейти к расширенному списку параметров, нажмите кнопку с изображением символа «+» напротив «Advanced settings»:

## 5 Управление устройством с помощью командной строки

В данном разделе описаны различные способы подключения к интерфейсу командной строки (CLI) точки доступа, а также основные команды управления устройством посредством CLI.

Для подключения к точке доступа используется три способа:

- Serial port: последовательный порт или COM-порт;
- Telnet, небезопасное подключение;
- SSH, безопасное подключение.

### 5.1 Подключение к CLI через COM-порт

Для использования этого типа подключения персональный компьютер либо должен иметь встроенный COM-порт, либо должен комплектоваться кабелем-переходником USB-to-COM. На компьютере также должна быть установлена терминальная программа, например, Hyperterminal, PuTTY, SecureCRT.

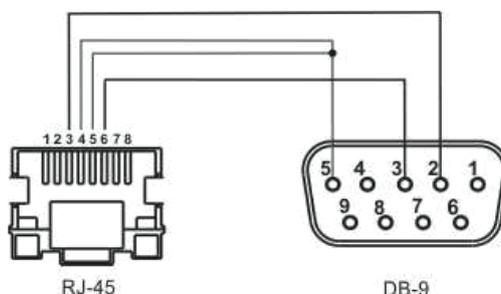
Точка доступа (порт «Console») напрямую соединяется с компьютером с помощью консольного кабеля. Для доступа к командой консоли устройства используется терминальная программа.

Для подключения к точке доступа через COM-порт Вам понадобится консольный кабель RJ45-DB9 (не входит в комплект поставки устройства).

#### Распайка консольного кабеля RJ45-DB9

Serial Port (RJ-45 Connector) Pin	Adapter (DB-9) Pin
3 (TXD)	2 (RXD)
4 (Signaling Ground)	5 (Signaling Ground)
5 (Signaling Ground)	5 (Signaling Ground)
6 (RXD)	3 (TXD)

Пример исполнения приведен на следующем рисунке:



**Шаг 1.** При помощи консольного кабеля соедините порт **CONSOLE** точки доступа с COM-портом компьютера. Для работы консольного кабеля могут потребоваться драйвера в зависимости от операционной системы компьютера.

**Шаг 2.** Запустите терминальную программу и создайте новое подключение. В выпадающем списке «Подключаться через» выберите нужный COM-порт. COM-порт (номер порта) определяется диспетчером устройств, например, COM4. Задайте параметры порта согласно таблице 6. Нажмите кнопку **ОК**.

Таблица 6 – Параметры COM-порта

Параметры	Значение
Скорость COM-порта (Baud rate)	115200
Биты данных (Data bits)	8
Четность (Parity)	нет
Стоповые биты (Stop bits)	1
Управление потоком (Flow control)	отсутствует

**Шаг 3.** Нажмите кнопку «Соединение». Произведите вход в CLI устройства.

Данные для входа По умолчанию –

- User name: **admin**
- Password: **password**

После успешной авторизации на экране будет отображаться (*Имя точки доступа*)#, например, *WEP-2ac#* или *Eltex WLAN AP#* – это означает, что включен режим конфигурирования настроек точки доступа.

- ✓ По умолчанию скорость COM-порта точки доступа равна 115200 бит/с. С помощью web-интерфейса в разделе «Serial Settings» вкладки «Status» можно изменить скорость на 9600, 19200, 38400 и 57600 бит/с. В интерфейсе CLI для изменения скорости используется команда: *set serial baud-rate <RATE>* (например, *set serial baud-rate 115200*). После применения данной команды необходимо изменить скорость в настройках подключения терминальной программы вашего ПК.

## 5.2 Подключение по протоколу Telnet

Подключение по протоколу *Telnet* является более универсальным по сравнению с подключением через COM-порт. Недостаток такого подключения, по сравнению с подключением через COM-порт, заключается в отсутствии сообщений инициализации точки доступа. Подключение к CLI можно выполнить как непосредственно в месте установки устройства, так и с удаленного рабочего места через IP-сеть. Для подключения к точке доступа персональный компьютер должен иметь сетевую карту. Дополнительно потребуется сетевая кабель (Patching Cord RJ-45) необходимой длины (не входит в комплект поставки устройства).

Для подключения по Telnet можно использовать такие программы, как PuTTY, HyperTerminal, SecureCRT.

**Шаг 1.** Подключите сетевую кабель от PoE-порта инжектора к Ethernet-порту точки доступа (для WEP-2ac – это порт **GE (PoE)**), а сетевую кабель от Data-порта инжектора – к сетевой карте компьютера.

**Шаг 2.** Запустите, например, программу PuTTY. Укажите IP-адрес узла доступа. На рисунке 10 в качестве примера указан 192.168.10.10.

- IP-адрес точки доступа, по умолчанию установлен – **192.168.1.10**;
- Порт, по умолчанию – **23**;
- Тип соединения – **Telnet**.

Нажмите кнопку «Соединиться».

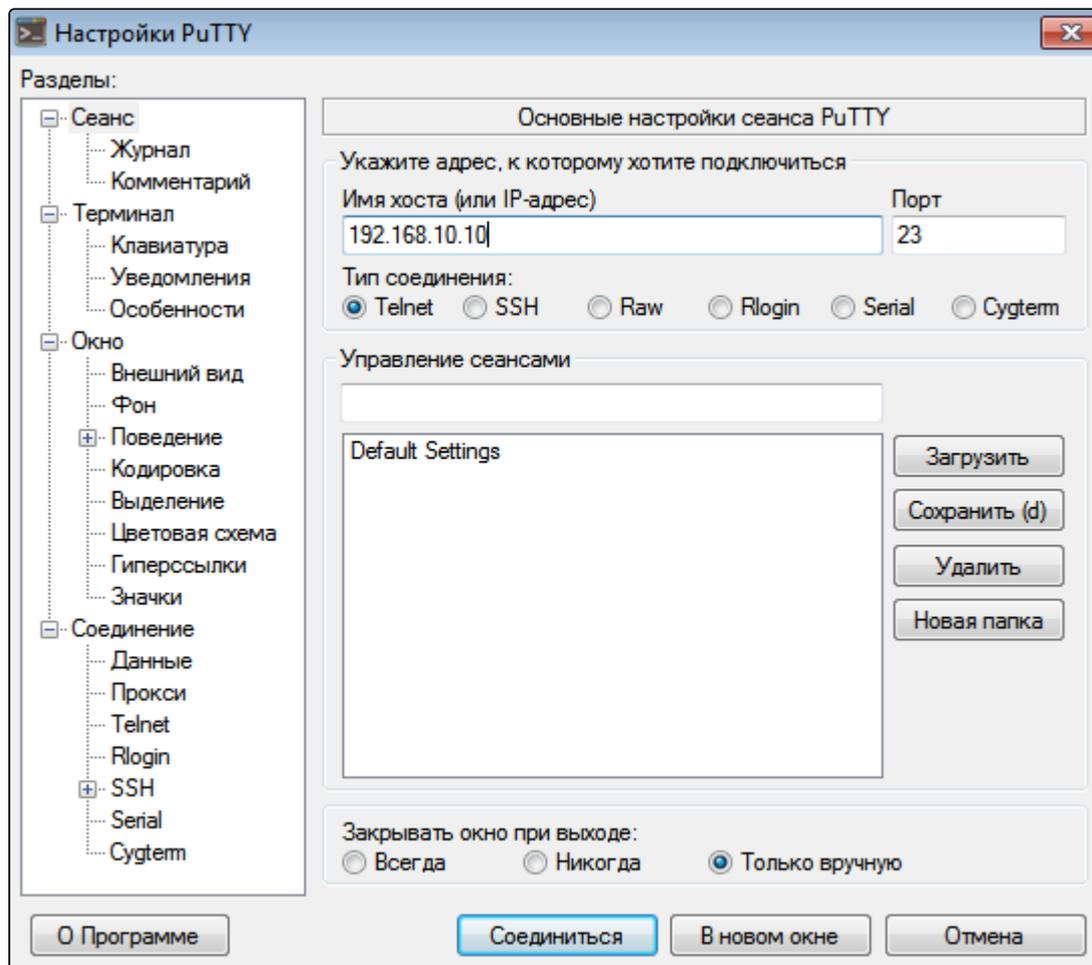


Рисунок 10 – Telnet-подключение в программе PuTTY

**Шаг 3.** Произведите вход в CLI устройства.

Данные для входа По умолчанию –

- login: **admin**
- password: **password**

После успешной авторизации на экране будет отображаться (*Имя точки доступа*)#, например, *WEP-2ac#* или *Eltex WLAN AP#* – это означает, что включен режим конфигурирования настроек точки доступа.

### 5.3 Подключение по протоколу Secure Shell

Подключение по протоколу *Secure Shell (SSH)* схоже по функциональности с подключением по протоколу Telnet. В отличие от Telnet, Secure Shell шифрует весь трафик, включая пароли. Таким образом обеспечивается возможность безопасного удаленного подключения по публичным IP-сетям.

Для подключения к узлу доступа персональный компьютер должен иметь сетевую карту. На компьютере должна быть установлена программа SSH-клиент, например, PuTTY, HyperTerminal, SecureCRT.

Дополнительно потребуется сетевая кабель (Patch Cord RJ-45) необходимой длины (не входит в комплект поставки устройства).

**Шаг 1.** Подключите сетевой кабель от PoE-порта инжектора к Ethernet-порту точки доступа (для WEP-2ac это порт **GE (PoE)**), а сетевой кабель от Data-порта инжектора – к сетевой карте компьютера.

**Шаг 2.** Запустите, например, программу PuTTY. Укажите IP-адрес узла доступа. На рисунке 11 в качестве примера указан 192.168.10.10.

- IP-адрес точки доступа, по умолчанию установлен – **192.168.1.10**;
- Порт, по умолчанию – **22**;
- Тип соединения – **SSH**.

Нажмите кнопку «**Соединиться**».

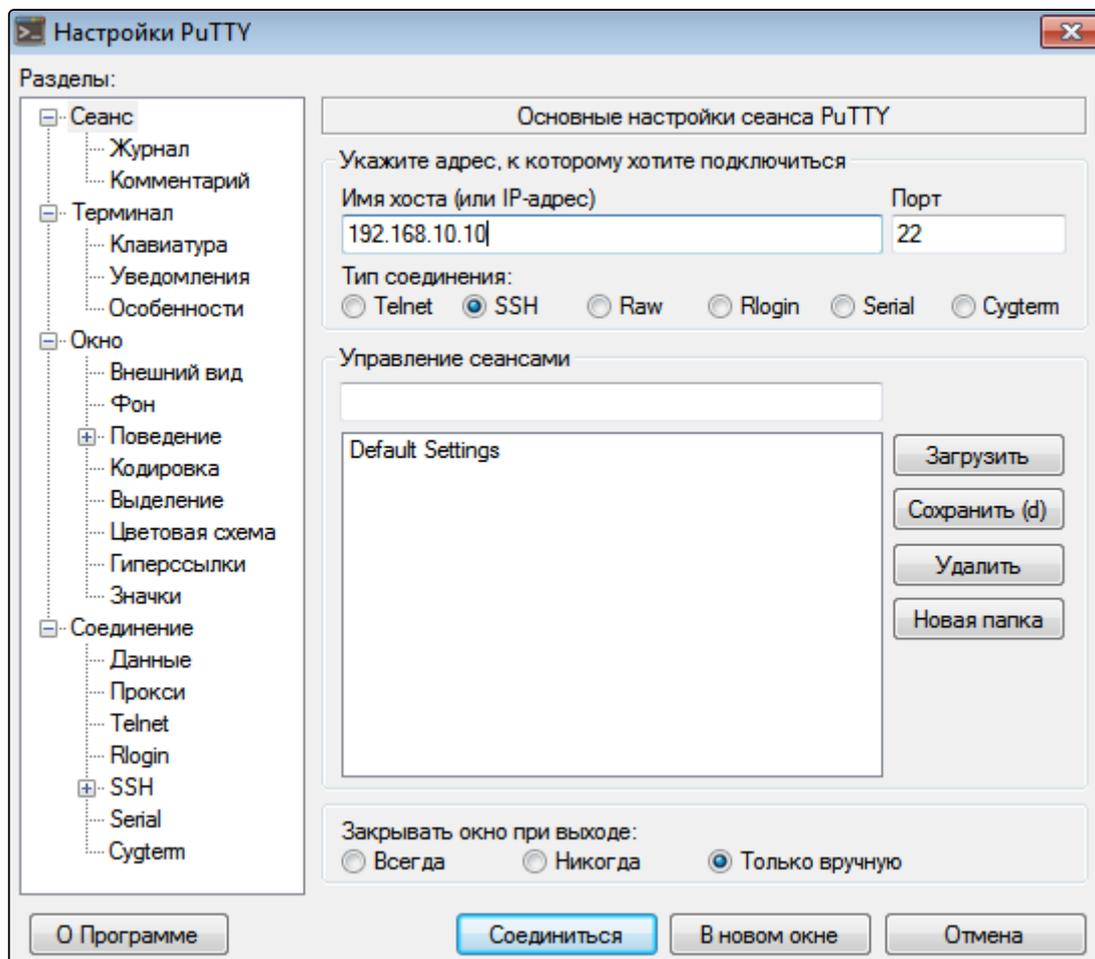


Рисунок 11 – Запуск SSH-клиента

**Шаг 3.** Произведите вход в CLI точки доступа.

Данные для входа По умолчанию –

- login: **admin**
- password: **password**

После успешной авторизации на экране будет отображаться *(Имя точки доступа)#*, например, *WEP-2ac#* или *Eltex WLAN AP#* – это означает, что включен режим конфигурирования настроек точки доступа.

## 5.4 Начало работы в CLI точки доступа

CLI является дополнительным к web-конфигуратору способом взаимодействия специалиста с устройством. В этом разделе рассматриваются общие правила работы в CLI.

Конфигурация точки доступа представлена набором классов (продолжение команды) и объектов (начало команды).

Консоль точки доступа предоставляет доступ к использованию таких объектов:

- get
- set
- add
- remove

 При использовании команд `set`, `add` и `remove` изменяется текущая конфигурация точки доступа, а не загрузочная. Для сохранения текущей конфигурации в загрузочную нужно использовать команду **save-running**.

### 5.4.1 Правила пользования командной строкой

Для упрощения использования командной строки интерфейс поддерживает функцию автоматического дополнения команд. Эта функция активизируется при неполно набранной команде и нажатии клавиши <Tab>.

Другая функция, помогающая пользоваться командной строкой – контекстная подсказка. На любом этапе ввода команды можно получить подсказку о следующих элементах команды путем двойного нажатия клавиши <Tab>.

Для удобства использования командной строки реализована поддержка горячих клавиш. Список горячих клавиш представлен в таблице 7.

Таблица 7 – Описание горячих клавиш командной строки CLI

Сочетание клавиш	Действие в CLI
CTRL+a	Перемещение курсора в начало строки
CTRL+e	Перемещение курсора в конец строки
CTRL+b	Перемещение курсора влево
CTRL+f	Перемещение курсора вправо
CTRL+c	Прерывает выполнение команды
CTRL+h	Удаляет один символ слева (backspace)
CTRL+w	Удаляет слово слева от курсора
CTRL+k	Удаляет все после курсора
CTRL+u	Удаляет все перед курсором
CTRL+p	Показывает предыдущую команду
CTRL+n	Показывает следующую команду
CTRL+d	Выход из CLI (exit)

#### 5.4.2 Условные обозначения интерфейсов

В данном разделе описано именование интерфейсов, используемое при конфигурировании устройства.

Для получения описания в CLI можно выполнить команду **get interface all description**. Для получения более подробной информации обо всех интерфейсах используйте команду **get interface all**. В таблице 8 приведено описание интерфейсов.

Таблица 8 – Обозначения интерфейсов

Интерфейс	Описание
brtrunk	Bridge - Trunk
brtrunk-user	Bridge - Trunk
eth0	Ethernet
lo	Loopback
isatap0	ISATAP Tunnel
wlan0	Wireless - Virtual Access Point 0
wlan1	Wireless - Virtual Access Point 0 - Radio 2
wlan0vapX	Wireless - Virtual Access Point X
wlan1vapX	Wireless - Virtual Access Point X - Radio 2
wlan0bssvapX	Virtual Access Point X
wlan1bssvapX	Virtual Access Point X - Radio 2
wlan0wdsX	Wireless Distribution System - Link X

### 5.4.3 Сохранение изменений в конфигурации

В системе существует несколько экземпляров конфигураций:

- *Заводская конфигурация.* Конфигурация включает настройки по умолчанию. Вернуться к заводской конфигурации можно командой **factory-reset** или при помощи функциональной кнопки «F» на корпусе устройства. Для этого удерживайте кнопку «F», пока не начнет мигать индикатор «Power»;
- *Загрузочная конфигурация.* В загрузочной конфигурации хранятся настройки, которые будут использованы при следующей загрузке точки доступа (например, после перезагрузки). Для сохранения изменений, выполненных в CLI, в загрузочную конфигурацию необходимо выполнить команду **save-running** или **set config startup running** – текущая конфигурация будет скопирована в загрузочную;
- *Текущая конфигурация.* Конфигурация точки доступа, которая применена на данный момент. При использовании команд **get**, **set**, **add**, **remove** происходит просмотр и изменение значений только текущей конфигурации. Если данные изменения не сохранены, то после перезагрузки точки доступа они будут потеряны.

## 5.5 Описание команд CLI

### 5.5.1 Команда *get*

Команда **get** позволяет просматривать установленные значения полей в классах. Классы разделяются на классы без имени (unnamed-class) и с именем (named-class).

#### Синтаксис

```
get unnamed-class <ЗНАЧЕНИЕ> |detail
get named-class [<ПОДКЛАСС> |all| [<ЗНАЧЕНИЕ > ... | имя | detail]]
```

#### Пример

1. Пример использования команды «get» в классе без имени с одним набором значений:

```
get log
```

Точка доступа имеет только один набор параметров для log-файлов, данная команда выводит информацию о параметрах log-файлов.

2. Пример использования команды «get» в классе без имени с множеством значений:

```
get log-entry
```

В файле хранится последовательность логов без разбиения на файлы, команда выводит всю последовательность данных, которая находится в log-файле.

3. Пример использования команды «get» в классе с именем с множеством значений:

```
get bss wlan1bssvap3
```

Существует набор значений класса bss, которые набираются в данной команде. Данная команда выводит информацию о наборе базовых услуг, называемом wlan1bssvap3.

4. Пример использования команды «get» в классе с именем для получения всех значений:

```
get interface all mac
get interface all
get radio all detail
```

### 5.5.2 Команда *set*

Команда **set** устанавливает значения полей в классах.

#### Синтаксис

```
set unnamed-class [<ПОДКЛАСС> <ЗНАЧЕНИЕ> ...] <ЗНАЧЕНИЕ> ...
set named-class <ПОДКЛАСС> | all [<ПОДКЛАСС> <ЗНАЧЕНИЕ> ...] <ЗНАЧЕНИЕ> ...
```

#### Пример

Пример настройки SSID, параметров Radio-интерфейса и установки статического IP-адреса:

```
set interface wlan0 ssid "Eltex"
set vap vap2 with radio wlan0 to vlan-id 123
set radio all beacon-interval 200
set tx-queue wlan0 with queue data0 to aifs 3
set management static-ip 192.168.10.10
set management static-mask 255.255.255.0
set management dhcp-status down
```

### 5.5.3 Команды *add*

Команда **add** добавляет новый подкласс или группу подклассов, содержащих определенный набор значений, для упрощения конфигурации оборудования.

#### Синтаксис

```
add unique-named-class <ПОДКЛАСС> [<ЗНАЧЕНИЕ> ...]
add group-named-class <ПОДКЛАСС> [<ЗНАЧЕНИЕ> ...]
add anonymous-named-class <ПОДКЛАСС> [<ЗНАЧЕНИЕ> ...]
```

#### Пример

Пример настройки базовой канальной скорости на Radio-интерфейсе:

```
add basic-rate wlan1 rate 1
```

### 5.5.4 Команда *remove*

Команда **remove** удаляет созданные подклассы.

#### Синтаксис

```
add unnamed-class [<ЗНАЧЕНИЕ> ...]
add named-class <ПОДКЛАСС> | all [<ЗНАЧЕНИЕ> ...]
```

**Пример**

Пример удаления настройки базовой канальной скорости на Radio-интерфейсе:

```
remove basic-rate wlan1 rate 1
```

**5.5.5 Дополнительные команды**

Интерфейс командной строки точки доступа также включает следующие команды, таблица 9.

Таблица 9 – Дополнительные команды

Команда	Описание
config	Загрузка/Выгрузка конфигурации точки доступа
copy	Загрузка/Выгрузка/Сохранение конфигурации точки доступа
delete	Удаление файлов конфигурации
dot1x-cert	Выгрузка DOT1X-сертификата подключения к точке доступа
factory-reset	Сброс устройства к заводской конфигурации и перезагрузка
factory-reset-partial	Сброс устройства к заводской конфигурации с сохранением параметров доступа
firmware-switch	Смена образа ПО: текущей версии ПО на альтернативную
firmware-upgrade	Обновление прошивки
packet-capture	Формирование и выгрузка дампа трафика с интерфейса
reboot	Перезагрузка точки доступа
save-running	Сохранение текущей конфигурации в загрузочную
show	Отображение списка файлов конфигурации
wgbridge-cert	Выгрузка WGB-сертификата подключения к точке доступа

## 5.6 Настройка точки доступа через CLI

В данном разделе приведен пример настройки точки доступа WEP-2ac с использованием интерфейса командной строки.

После подключения к точке доступа (описание приведено в разделе [Управление устройством с помощью командной строки](#)) необходимо настроить сетевые параметры, если они не были настроены ранее.

### 5.6.1 Настройка сетевых параметров

#### Настройка статических сетевых параметров точки доступа

WEP-2ac# **set management dhcp-status down** (**down** – выключить получение сетевых параметров по DHCP, использовать сетевые параметры настроенные статически. **up** – включить получение сетевых параметров по DHCP)

WEP-2ac# **set management static-ip 192.168.1.15** (где 192.168.1.15 – статический IP-адрес устройства)

WEP-2ac# **set management static-mask 255.255.255.0** (где 255.255.255.0 – маска подсети)

WEP-2ac# **set static-ip-route gateway 192.168.1.1** (где 192.168.1.1 – IP-адрес шлюза по умолчанию)

#### Настройка VLAN для управления точкой доступа

WEP-2ac# **set management vlan-id 1510** (где 1510 – номер VLAN для управления точкой доступа)

#### Настройка статических IP-адресов DNS

WEP-2ac# **set host dns-via-dhcp down** (**down** – использовать DNS-сервера установленные статически. **up** – использовать DNS-сервера, полученные по DHCP)

WEP-2ac# **set host static-dns-1 8.8.8.8** (где 8.8.8.8 – IP-адрес DNS-сервера 1)

WEP-2ac# **set host static-dns-2 192.168.1.253** (где 192.168.1.253 – IP-адрес DNS-сервера 2)

## 5.6.2 Настройка беспроводных интерфейсов

На радиоинтерфейсах по умолчанию используется автоматический выбор рабочего канала, для того чтобы установить канал вручную или сменить мощность, используйте следующие команды:

### Настройка радиоканала, ширины полосы и мощности радиоинтерфейса

#### Настройка для Radio 1 (5 ГГц):

WEP-2ac# **set radio wlan0 status up** (**up** – включение радиоинтерфейса Radio 1, **down** – выключение радиоинтерфейса Radio 1)

WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – установка режима работы радиоинтерфейса Radio 1. Для Radio 1 доступны следующие режимы работы: **a** – 802.11a, **a-n-ac** – 802.11a/n/ac, **n-ac** – 802.11n/ac)

WEP-2ac# **set radio wlan0 channel-policy static** (**static** – выключение функционала автоматического выбора канала. **best** – включение автоматического выбора рабочего канала)

WEP-2ac# **set radio wlan0 static-channel 36** (**36** – номер статического канала, на котором будет работать точка доступа)

WEP-2ac# **set radio wlan0 n-bandwidth 80** (**80** – ширина канала. Для Radio 1 доступны следующие значения ширины канала: **20** – 20 МГц, **40** – 40 МГц, **80** – 80 МГц)

WEP-2ac# **set radio wlan0 tx-power-dbm 19** (**19** – значение мощности передатчика для интерфейса Radio 1. Доступные значения для Radio 1: **от 1 до 21** дБм)

#### Настройка для Radio 2 (2.4 ГГц):

WEP-2ac# **set radio wlan1 status up** (**up** – включение радиоинтерфейса Radio 2, **down** – выключение радиоинтерфейса Radio 2)

WEP-2ac# **set radio wlan1 mode bg-n** (**bg-n** – установка режима работы радиоинтерфейса Radio 2. Для Radio 2 доступны следующие режимы работы: **bg** – 802.11b/g, **bg-n** – 802.11b/g/n, **n-only-g** – 2.4 GHz 802.11n)

WEP-2ac# **set radio wlan1 channel-policy static** (**static** – выключение функционала автоматического выбора канала. **best** – включение автоматического выбора рабочего канала)

WEP-2ac# **set radio wlan1 static-channel 6** (**6** – номер статического канала, на котором будет работать точка доступа)

WEP-2ac# **set radio wlan1 n-bandwidth 20** (**20** – ширина канала. Для Radio 2 доступны следующие значения ширины канала: **20** – 20 МГц, **40** – 40 МГц)

WEP-2ac# **set radio wlan1 tx-power-dbm 16** (**16** – значение мощности передатчика для интерфейса Radio 2. Доступные значения для Radio 2: **от 5 до 18** дБм)

### ✓ Списки доступных каналов

#### Для Radio 1 для выбора доступны следующие каналы:

- при ширине канала 20 МГц: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161, 165.
- при ширине канала 40 МГц:
  - если "n-primary-channel" = lower: 36, 44, 52, 60, 132, 140, 149, 157.
  - если "n-primary-channel" = upper: 40, 48, 56, 64, 136, 144, 153, 161.
- при ширине канала 80 МГц: 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161.

#### Для Radio 2 для выбора доступны следующие каналы:

- при ширине канала 20 МГц: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.
- при ширине канала 40 МГц:
  - если "n-primary-channel" = lower: 1, 2, 3, 4, 5, 6, 7, 8, 9.
  - если "n-primary-channel" = upper: 5, 6, 7, 8, 9, 10, 11, 12, 13.

### 5.6.2.1 Дополнительные настройки беспроводных интерфейсов

#### Изменение режима работы радиointерфейса

##### Настройка для Radio 1 (5 ГГц):

WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – установка режима работы радиointерфейса Radio 1. Для Radio 1 доступны следующие режимы работы: **a** – 802.11a, **a-n-ac** – 802.11a/n/ac, **n-ac** – 802.11n/ac)

##### Настройка для Radio 2 (2.4 ГГц):

WEP-2ac# **set radio wlan1 mode bg-n** (**bg-n** – установка режима работы радиointерфейса Radio 2. Для Radio 2 доступны следующие режимы работы: **bg** – 802.11b/g, **bg-n** – 802.11b/g/n, **n-only-g** – 2.4 GHz 802.11n)

#### Настройка ограниченного списка каналов

##### Настройка для Radio 1 (5 ГГц):

WEP-2ac# **set radio wlan0 limit-channels '36 40 44 48'** (**36 40 44 48** – номера каналов, которые будут использоваться при автовыборе рабочего канала на точке доступа)

##### Настройка для Radio 2 (2.4 ГГц):

WEP-2ac# **set radio wlan1 limit-channels '1 6 11'** (**1 6 11** – номера каналов, которые будут использоваться при автовыборе рабочего канала на точке доступа)

#### Изменение основного канала

##### Настройка для Radio 1 (5 ГГц):

WEP-2ac# **set radio wlan0 n-primary-channel upper** (параметр может принимать значения: **upper**, **lower**)

##### Настройка для Radio 2 (2.4 ГГц):

WEP-2ac# **set radio wlan1 n-primary-channel upper** (параметр может принимать значения: **upper**, **lower**)

#### Изменение списка VLAN

##### Настройка для Radio 1 (5 ГГц):

WEP-2ac# **set radio wlan0 vlan-list '10;4033'** (**10** и **4033** – номера VLAN. Максимальное возможное количество VLAN в списке: 20)

##### Настройка для Radio 2 (2.4 ГГц):

WEP-2ac# **set radio wlan1 vlan-list '10;4033'** (**10** и **4033** – номера VLAN. Максимальное возможное количество VLAN в списке: 20)

**Включение использования короткого защитного интервала****Настройка для Radio 1 (5 ГГц):**

WEP-2ac# **set radio wlan0 short-guard-interval-supported yes** (параметр может принимать значения: **yes, no**)

**Настройка для Radio 2 (2.4 ГГц):**

WEP-2ac# **set radio wlan1 short-guard-interval-supported yes** (параметр может принимать значения: **yes, no**)

**Включение STBC****Настройка для Radio 1 (5 ГГц):**

WEP-2ac# **set radio wlan0 stbc-mode auto** (параметр может принимать значения: **auto, on, off**. По умолчанию – **auto**)

**Настройка для Radio 2 (2.4 ГГц):**

WEP-2ac# **set radio wlan1 stbc-mode auto** (параметр может принимать значения: **auto, on, off**. По умолчанию – **auto**)

**Включение механизма DFS****Настройка для Radio 1 (5 ГГц):**

WEP-2ac# **set radio wlan0 dot11h on** (параметр может принимать значения: **on, off**. По умолчанию – **on**)

**Включение режима автоматической смены ширины канала****Настройка для Radio 1 (5 ГГц):**

WEP-2ac# **set radio wlan0 coex-mode on** (параметр может принимать значения: **on, off**. По умолчанию – **on**)

**Настройка для Radio 2 (2.4 ГГц):**

WEP-2ac# **set radio wlan1 coex-mode on** (параметр может принимать значения: **on, off**. По умолчанию – **on**)

**Ограничение количества клиентов, одновременно подключенных к радиointерфейсу****Настройка для Radio 1 (5 ГГц):**

WEP-2ac# **set radio wlan0 max-stations 150** (**150** – ограничение по количеству клиентов. Параметр может принимать значения: **от 0 до 200**, где 0 – ограничение выключено. По умолчанию – **0**)

**Настройка для Radio 2 (2.4 ГГц):**

WEP-2ac# **set radio wlan1 max-stations 150** (**150** – ограничение по количеству клиентов. Параметр может принимать значения: **от 0 до 200**, где 0 – ограничение выключено. По умолчанию – **0**)

## Настройка политики обработки DHCP Option 82

- ✓ Для одновременной настройки политики обработки 82 опции DHCP на всех радиоинтерфейсах точки доступа после слова **radio** введите **all**. Если необходимо произвести настройку для каждого радиоинтерфейса в отдельности, вместо **all** введите имя радиоинтерфейса: **wlan0** – Radio 5 ГГц, **wlan1** – Radio 2.4 ГГц.

WEP-2ac# **set radio all dhcp-snooping replace** (**replace** – точка доступа подставляет или заменяет значение опции 82. Параметр может принимать значения: **ignore** – обработка опции 82 отключена; **remove** – точка доступа удаляет значение опции 82. По умолчанию – **ignore**)

Если на радиоинтерфейсе настроена политика обработки опции 82 **replace**, то для конфигурирования становятся доступны следующие параметры:

WEP-2ac# **set radio all dhcp-option-82-CID-format string** (**string** – менять содержимое CID на значение, указанное в **dhcp-option-82-string**. Параметр может принимать значения: **APMAC-SSID** – менять содержимое CID на <MAC-адрес точки доступа>;<имя SSID>. **SSID** – менять содержимое CID на имя SSID, к которому подключен клиент. По умолчанию – **APMAC-SSID**)

WEP-2ac# **set radio all dhcp-option-82-string longstring** (**longstring** – значение от 1 до 52 символов, которое будет передаваться в CID. Допускаются только латинские буквы и цифры, знаки «.», «-», «\_», «#», «\$», «%». Допустимые плейсхолдеры в формате wildcard приведены в таблице 10. Если значение параметра **dhcp-option-82-string** не задано, точка будет менять CID на значение по умолчанию – <MAC-адрес точки доступа>;<имя SSID>)

WEP-2ac# **set radio all dhcp-option-82-RID-format string2** (**string2** – менять содержимое RID на значение, указанное в **dhcp-option-82-string2**. Параметр может принимать значения: **ClientMAC** – менять содержимое RID на MAC-адрес клиентского устройства; **APMAC** – менять содержимое RID на MAC-адрес точки доступа; **APdomain** – менять содержимое RID на имя последнего по дереву домена из параметра "AP location". По умолчанию – **ClientMAC**)

WEP-2ac# **set radio all dhcp-option-82-string2 longstring** (**longstring** – значение от 1 до 63 символов, которое будет передаваться в RID. Допускаются только латинские буквы и цифры, знаки «.», «-», «\_», «#», «\$», «%». Допустимые плейсхолдеры в формате wildcard приведены в таблице 10. Если значение параметра **dhcp-option-82-string2** не задано, точка будет менять RID на значение по умолчанию – MAC-адрес клиентского устройства)

WEP-2ac# **set radio all dhcp-option-82-MAC-format radius** (**radius** – MAC-адрес передается в RADIUS-формате; **default** – MAC-адрес передается в обычном формате, таком же, как в опции "Client-Ethernet-Address" DHCP-пакета)

- ✓ В случае использования символа «%» в **longstring** требуется экранирование символа знаком «\», либо экранирование **longstring** знаками «'» с обеих сторон: **set radio all dhcp-option-82-string \$ap-mac\$-\%ssid\%**, либо **set radio all dhcp-option-82-string '\$ap-mac\$-%ssid%'**.

Таблица 10 – Настройка шаблона подопций DHCP Option 82

Подопция	Параметр	Описание
CID	%ap-mac%	MAC-адрес точки доступа в формате ASCII
	%ssid%	SSID в формате ASCII
	%ap-hostname%	Hostname точки доступа в формате ASCII
	%vlan-id%	VLAN ID в формате ASCII
	%interface%	Имя интерфейса в формате ASCII
	\$ap-mac\$	MAC-адрес точки доступа в hex
	\$vlan-id\$	VLAN ID в hex
RID	%ap-mac%	MAC-адрес точки доступа в формате ASCII
	%ssid%	SSID в формате ASCII
	%ap-location%	Домен точки доступа в формате ASCII
	%client-mac%	MAC-адрес клиента в формате ASCII
	\$ap-mac\$	MAC-адрес точки доступа в hex
	\$client-mac\$	MAC-адрес клиента в hex

### 5.6.3 Настройка виртуальных точек доступа Wi-Fi (VAP)

#### 5.6.3.1 Настройка VAP без шифрования

##### Создание VAP без шифрования

###### **Настройка VAP0 на Radio 1 (5 ГГц):**

```
WEP-2ac# set bss wlan0bssvap0 status up (up – включение VAP0, down – выключение VAP0)
WEP-2ac# set interface wlan0 ssid Test_open_vap0 (Test_open_vap0 – название беспроводной сети)
WEP-2ac# set interface wlan0 security plain-text (plain-text – режим шифрования – без пароля)
```

###### **Настройка VAP1 на Radio 1 (5 ГГц):**

```
WEP-2ac# set bss wlan0bssvap1 status up (up – включение VAP0, down – выключение VAP0)
WEP-2ac# set interface wlan0vap1 ssid Test_open_vap1 (Test_open_vap1 – название беспроводной сети)
WEP-2ac# set interface wlan0vap1 security plain-text (plain-text – режим шифрования – без пароля)
```

###### **Настройка VAP0 на Radio 2 (2.4 ГГц):**

```
WEP-2ac# set bss wlan1bssvap0 status up (up – включение VAP0, down – выключение VAP0)
WEP-2ac# set interface wlan1 ssid Test_open_vap0 (Test_open_vap0 – название беспроводной сети)
WEP-2ac# set interface wlan1 security plain-text (plain-text – режим шифрования – без пароля)
```

###### **Настройка VAP1 на Radio 2 (2.4 ГГц):**

```
WEP-2ac# set bss wlan1bssvap1 status up (up – включение VAP0, down – выключение VAP0)
WEP-2ac# set interface wlan1vap1 ssid Test_open_vap1 (Test_open_vap1 – название беспроводной сети)
WEP-2ac# set interface wlan1vap1 security plain-text (plain-text – режим шифрования – без пароля)
```

## 5.6.3.2 Настройка VAP с режимом безопасности WPA-Personal

**Создание VAP с режимом безопасности WPA-Personal****Настройка VAP0 на Radio 1 (5 ГГц):**

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan0 ssid Test\_personal\_vap0** (**Test\_personal\_vap0** – название беспроводной сети)  
 WEP-2ac# **set interface wlan0 security wpa-personal** (**wpa-personal** – режим шифрования)  
 WEP-2ac# **set interface wlan0 wpa-personal-key 12345678** (**123456789** – пароль для подключения к беспроводной сети. Должен содержать от 8 до 64 символов)

**Настройка VAP1 на Radio 1 (5 ГГц):**

WEP-2ac# **set bss wlan0bssvap1 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan0vap1 ssid Test\_personal\_vap1** (**Test\_personal\_vap1** – название беспроводной сети)  
 WEP-2ac# **set interface wlan0vap1 security wpa-personal** (**wpa-personal** – режим шифрования)  
 WEP-2ac# **set interface wlan0vap1 wpa-personal-key 12345678** (**123456789** – пароль для подключения к беспроводной сети. Должен содержать от 8 до 64 символов)

**Настройка VAP0 на Radio 2 (2.4 ГГц):**

WEP-2ac# **set bss wlan1bssvap0 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan1 ssid Test\_personal\_vap0** (**Test\_personal\_vap0** – название беспроводной сети)  
 WEP-2ac# **set interface wlan1 security wpa-personal** (**wpa-personal** – режим шифрования)  
 WEP-2ac# **set interface wlan1 wpa-personal-key 12345678** (**123456789** – пароль для подключения к беспроводной сети. Должен содержать от 8 до 64 символов)

**Настройка VAP1 на Radio 2 (2.4 ГГц):**

WEP-2ac# **set bss wlan1bssvap1 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan1vap1 ssid Test\_personal\_vap1** (**Test\_personal\_vap1** – название беспроводной сети)  
 WEP-2ac# **set interface wlan1vap1 security wpa-personal** (**wpa-personal** – режим шифрования)  
 WEP-2ac# **set interface wlan1vap1 wpa-personal-key 12345678** (**123456789** – пароль для подключения к беспроводной сети. Должен содержать от 8 до 64 символов)

### 5.6.3.3 Настройка VAP с Enterprise-авторизацией

#### Создание VAP с режимом безопасности WPA2-Enterprise

##### Настройка VAP0 на Radio 1 (5 ГГц):

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan0 ssid Test\_enterprise\_vap0** (**Test\_enterprise\_vap0** – название беспроводной сети)  
 WEP-2ac# **set interface wlan0 security wpa-enterprise** (**wpa-enterprise** – режим шифрования)  
 WEP-2ac# **set bss wlan0bssvap0 global-radius on** (**on** – использование глобальных настроек RADIUS-сервера. Параметр может принимать значения: **on**, **off**. По умолчанию – **on**)

##### Настройка VAP1 на Radio 1 (5 ГГц):

WEP-2ac# **set bss wlan0bssvap1 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan0vap1 ssid Test\_enterprise\_vap1** (**Test\_enterprise\_vap1** – название беспроводной сети)  
 WEP-2ac# **set interface wlan0vap1 security wpa-enterprise** (**wpa-enterprise** – режим шифрования)  
 WEP-2ac# **set bss wlan0bssvap1 global-radius on** (**on** – использование глобальных настроек RADIUS-сервера. Параметр может принимать значения: **on**, **off**. По умолчанию – **on**)

##### Настройка VAP0 на Radio 2 (2.4 ГГц):

WEP-2ac# **set bss wlan1bssvap0 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan1 ssid Test\_enterprise\_vap0** (**Test\_enterprise\_vap0** – название беспроводной сети)  
 WEP-2ac# **set interface wlan1 security wpa-enterprise** (**wpa-enterprise** – режим шифрования)  
 WEP-2ac# **set bss wlan1bssvap0 global-radius on** (**on** – использование глобальных настроек RADIUS-сервера. Параметр может принимать значения: **on**, **off**. По умолчанию – **on**)

##### Настройка VAP1 на Radio 2 (2.4 ГГц):

WEP-2ac# **set bss wlan1bssvap1 status up** (**up** – включение VAP0, **down** – выключение VAP0)  
 WEP-2ac# **set interface wlan1vap1 ssid Test\_enterprise\_vap1** (**Test\_enterprise\_vap1** – название беспроводной сети)  
 WEP-2ac# **set interface wlan1vap1 security wpa-enterprise** (**wpa-enterprise** – режим шифрования)  
 WEP-2ac# **set bss wlan1bssvap1 global-radius on** (**on** – использование глобальных настроек RADIUS-сервера. Параметр может принимать значения: **on**, **off**. По умолчанию – **on**)

## 5.6.3.3.1 Настройка параметров Global RADIUS

**Настройка параметров Global RADIUS**

WEP-2ac# **set bss wlan0bssvap0 global-radius on** (**on** – использование глобальных настроек RADIUS-сервера на VAP0 Radio1. Параметр может принимать значения: **on, off**. По умолчанию – **on**)

WEP-2ac# **set global-radius-server radius-domain enterprise.service.root** (**enterprise.service.root** – домен пользователя)

WEP-2ac# **set global-radius-server radius-ip 192.168.1.100** (**192.168.1.100** – IP-адрес основного RADIUS-сервера)

WEP-2ac# **set global-radius-server radius-key eltex** (**eltex** – ключ для подключения к основному RADIUS-серверу)

WEP-2ac# **set global-radius-server radius-port 1812** (**1812** – порт RADIUS-сервера, который используется для аутентификации и авторизации. По умолчанию – **1812**)

WEP-2ac# **set global-radius-server radius-accounting-port 1813** (**1813** – порт RADIUS-сервера, который используется для учета аккаунтинга пользователей. По умолчанию – **1813**)

WEP-2ac# **set global-radius-server radius-acct-periodic on**(**on** – включение периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию – **off**)

WEP-2ac# **set global-radius-server radius-acct-period 60** (**60** – интервал периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию – **30**)

WEP-2ac# **set global-radius-server radius-accounting on** (**on** – включение отправки сообщений "Accounting" на RADIUS-сервер. По умолчанию – **off**)

**Настройка отдельного RADIUS-сервера для аккаунтинга:**

WEP-2ac# **set global-radius-server radius-separate-auth-acct on** (**on** – использование отдельного RADIUS-сервера для аккаунтинга. Параметр может принимать значения: **on, off**. По умолчанию – **off**)

WEP-2ac# **set global-radius-server radius-acct-ip 192.168.1.200** (**192.168.1.200** – IP-адрес RADIUS-сервера для аккаунтинга)

WEP-2ac# **set global-radius-server radius-acct-key secret** (**secret** – ключ подключения к RADIUS-серверу для аккаунтинга)

**Настройка резервных RADIUS-серверов:**

WEP-2ac# **set global-radius-server radius-backupone-ip 192.168.1.101** (**192.168.1.101** – IP-адрес резервного RADIUS-сервера-1)

WEP-2ac# **set global-radius-server radius-backupone-key eltex1** (**eltex1** – ключ для подключения к резервному RADIUS-серверу-1)

WEP-2ac# **set global-radius-server radius-backupone-acct-ip 192.168.1.201** (**192.168.1.201** – IP-адрес резервного RADIUS-сервера-1 для аккаунтинга)

WEP-2ac# **set global-radius-server radius-backupone-acct-key secret1** (**secret1** – ключ подключения к резервному RADIUS-серверу-1 для аккаунтинга)

WEP-2ac# **set global-radius-server radius-backuptwo-ip 192.168.1.102** (**192.168.1.102** – IP-адрес резервного RADIUS-сервера-2)

WEP-2ac# **set global-radius-server radius-backuptwo-key eltex2** (**eltex2** – ключ для подключения к резервному RADIUS-серверу-2)

WEP-2ac# **set global-radius-server radius-backuptwo-acct-ip 192.168.1.202** (**192.168.1.202** – IP-адрес резервного RADIUS-сервера-2 для аккаунтинга)

WEP-2ac# **set global-radius-server radius-backuptwo-acct-key secret2** (**secret2** – ключ подключения к резервному RADIUS-серверу-2 для аккаунтинга)

```

WEP-2ac# set global-radius-server radius-backupthree-ip 192.168.1.103 (192.168.1.103 – IP-адрес
резервного RADIUS-сервера-3)
WEP-2ac# set global-radius-server radius-backupthree-key eltex3 (eltex3 – ключ для подключения к
резервному RADIUS-серверу-3)
WEP-2ac# set global-radius-server radius-backupthree-acct-ip 192.168.1.203 (192.168.1.203 – IP-адрес
резервного RADIUS-сервера-3 для аккаунтинга)
WEP-2ac# set global-radius-server radius-backupthree-acct-key secret3 (secret3 – ключ подключения к
резервному RADIUS-серверу-3 для аккаунтинга)

```

### 5.6.3.3.2 Настройка параметров RADIUS-сервера для конкретного VAP

Для примера рассмотрим настройку параметров RADIUS-сервера для VAP0 Radio1 (5 ГГц).

#### Настройка параметров RADIUS-сервера для VAP0 на Radio1

```

WEP-2ac# set bss wlan0bssvap0 global-radius on (on – использование глобальных настроек RADIUS-
сервера на VAP0 Radio1. Параметр может принимать значения: on, off. По умолчанию – on)
WEP-2ac# set bss wlan0bssvap0 radius-domain enterprise.service.root (enterprise.service.root – домен
пользователя)
WEP-2ac# set bss wlan0bssvap0 radius-ip 192.168.1.100 (192.168.1.100 – IP-адрес основного RADIUS-
сервера)
WEP-2ac# set bss wlan0bssvap0 radius-key eltex (eltex – ключ для подключения к основному RADIUS-
серверу)
WEP-2ac# set bss wlan0bssvap0 radius-port 1812 (1812 – порт RADIUS-сервера, который используется
для аутентификации и авторизации. По умолчанию – 1812)
WEP-2ac# set bss wlan0bssvap0 radius-current primary (primary – использование основного RADIUS-
сервера. Параметр может принимать значения: primary, backuptwo, backupone, backupthree. По
умолчанию – primary)
WEP-2ac# set bss wlan0bssvap0 radius-accounting-port 1813 (1813 – порт RADIUS-сервера, который
используется для учета аккаунтинга пользователей. По умолчанию – 1813)
WEP-2ac# set bss wlan0bssvap0 radius-acct-periodic on (on – включение периодической отправки
сообщений «Accounting» на RADIUS-сервер. По умолчанию – on)
WEP-2ac# set bss wlan0bssvap0 radius-acct-period 60 (60 – интервал периодической отправки
сообщений «Accounting» на RADIUS-сервер. По умолчанию – 30)
WEP-2ac# set bss wlan0bssvap0 radius-accounting on (on – включение отправки сообщений "Accounting"
на RADIUS-сервер. По умолчанию – off)

```

#### Настройка отдельного RADIUS-сервера для аккаунтинга:

```

WEP-2ac# set bss wlan0bssvap0 radius-separate-auth-acct on (on – использование отдельного RADIUS-
сервера для аккаунтинга. Параметр может принимать значения: on, off. По умолчанию – off)
WEP-2ac# set bss wlan0bssvap0 radius-acct-ip 192.168.1.200 (192.168.1.200 – IP-адрес RADIUS-сервера
для аккаунтинга)
WEP-2ac# set bss wlan0bssvap0 radius-acct-key secret (secret – ключ подключения к RADIUS-серверу для
аккаунтинга)

```

**Настройка резервных RADIUS-серверов:**

WEP-2ac# **set bss wlan0bssvap0 radius-backupone-ip 192.168.1.101 (192.168.1.101** – IP-адрес резервного RADIUS-сервера-1)

WEP-2ac# **set bss wlan0bssvap0 radius-backupone-key eltex1 (eltex1** – ключ для подключения к резервному RADIUS-серверу-1)

WEP-2ac# **set bss wlan0bssvap0 radius-backupone-acct-ip 192.168.1.201 (192.168.1.201** – IP-адрес резервного RADIUS-сервера-1 для аккаунтинга)

WEP-2ac# **set bss wlan0bssvap0 radius-backupone-acct-key secret1 (secret1** – ключ подключения к резервному RADIUS-серверу-1 для аккаунтинга)

WEP-2ac# **set bss wlan0bssvap0 radius-backuptwo-ip 192.168.1.102 (192.168.1.102** – IP-адрес резервного RADIUS-сервера-2)

WEP-2ac# **set bss wlan0bssvap0 radius-backuptwo-key eltex2 (eltex2** – ключ для подключения к резервному RADIUS-серверу-2)

WEP-2ac# **set bss wlan0bssvap0 radius-backuptwo-acct-ip 192.168.1.202 (192.168.1.202** – IP-адрес резервного RADIUS-сервера-2 для аккаунтинга)

WEP-2ac# **set bss wlan0bssvap0 radius-backuptwo-acct-key secret2 (secret2** – ключ подключения к резервному RADIUS-серверу-2 для аккаунтинга)

WEP-2ac# **set bss wlan0bssvap0 radius-backupthree-ip 192.168.1.103 (192.168.1.103** – IP-адрес резервного RADIUS-сервера-3)

WEP-2ac# **set bss wlan0bssvap0 radius-backupthree-key eltex3 (eltex3** – ключ для подключения к резервному RADIUS-серверу-3)

WEP-2ac# **set bss wlan0bssvap0 radius-backupthree-acct-ip 192.168.1.203 (192.168.1.203** – IP-адрес резервного RADIUS-сервера-3 для аккаунтинга)

WEP-2ac# **set bss wlan0bssvap0 radius-backupthree-acct-key secret3 (radius-key eltex** – ключ подключения к резервному RADIUS-серверу-3 для аккаунтинга)

**5.6.3.4 Настройка VAP с порталной авторизацией**

Для того, чтобы настроить VAP с порталной авторизацией, необходимо:

1. Создать VAP без шифрования (подробно описано в блоке [Настройка VAP без шифрования](#));
2. Настроить портал на точке доступа;
3. Назначить портал на настроенный ранее VAP.

**5.6.3.4.1 Настройка портала**

Для настройки Captive Portal на VAP0 на Radio 1 необходимо вносить изменения в ранее созданный шаблон портала – `sr-instance wlan0bssvap0`. Если требуется настроить портал, например, для VAP12 на Radio 2, то редактировать необходимо шаблон портала под именем **wlan1bssvap12**.

В примере рассмотрим настройку портала для VAP0 на Radio 1.

**Пример настройки портала wlan0bssvap0**

WEP-2ac# **set captive-portal mode up** (**up** – включение Captive Portal. Параметр может принимать значения: **down, up**. По умолчанию – **down**)

WEP-2ac# **set cp-instance wlan0bssvap0 global-radius off** (**off** – выключение использования настроек Global RADIUS для данного портала. Параметр может принимать значения: **off, on**. По умолчанию – **off**)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-ip 192.168.1.100** (**192.168.1.100** – IP-адрес основного RADIUS-сервера)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-key eltex** (**eltex** – ключ для подключения к основному RADIUS-серверу)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-domain portal.service.root** (**enterprise.service.root** – домен пользователя)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-accounting on** (**on** – включение отправки сообщений "Accounting" на RADIUS-сервер. Параметр может принимать значения: **off, on**. По умолчанию – **on**)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-acct-periodic on** (**on** – включение периодической отправки сообщений «Accounting» на RADIUS-сервер. Параметр может принимать значения: **off, on**. По умолчанию – **on**)

WEP-2ac# **set cp-instance wlan0bssvap0 radius-acct-period 60** (**60** – интервал периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию – **30**)

WEP-2ac# **set cp-instance wlan0bssvap0 external up** (**up** – включение перенаправления пользователя на внешний виртуальный портал. Параметр может принимать значения: **up, down**. По умолчанию – **up**)

WEP-2ac# **set cp-instance wlan0bssvap0 external-url http://192.168.1.100:8080/eltex\_portal/** (URL виртуального портала, на который будет перенаправлен пользователь при подключении к беспроводной сети)

WEP-2ac# **set cp-instance wlan0bssvap0 apb-mac-auth up** (включить MAC-авторизацию порталных пользователей через APB сервис (доступно только с SoftWLC 1.34.1 и выше). По умолчанию: **down**)

WEP-2ac# **set cp-instance wlan0bssvap0 admin-mode up** (**up** – включение работы виртуального портала. Параметр может принимать значения: **up, down**. По умолчанию – **down**)

**5.6.3.4.2 Привязка портала к VAP**

По умолчанию портал с именем конкретного VAP привязан к данному VAP, но можно привязать портал к нескольким VAP. Ниже представлен пример привязки портала с именем **wlan0bssvap0** к VAP3 на Radio 2.

```
WEP-2ac# set cp-vap vap3 with radio wlan1 cp-instance-name wlan0bssvap0 (привязка портала с именем wlan0bssvap0 к VAP3 на Radio 2)
```

Также можно привязать портал одновременно к двум одноименным VAP, расположенным на всех радиointерфейсах точки доступа.

```
WEP-2ac# set cp-vap vap1 cp-instance-name wlan0bssvap0 (одновременная привязка портала с именем wlan0bssvap0 к VAP1 на Radio 1 и VAP1 на Radio 2)
```

### 5.6.3.5 Дополнительные настройки VAP

#### Назначение VLAN ID на VAP

WEP-2ac# **set vap vap0 with radio wlan0 vlan-id 15** (15 – номер VLAN, назначенный на VAP0 Radio1)  
 WEP-2ac# **set vap vap0 vlan-id 15** (15 – номер VLAN, назначенный одновременно на VAP0 Radio1 и на VAP0 Radio2)

#### Ограничение количества клиентов, одновременно подключенных к VAP

WEP-2ac# **set bss wlan0bssvap0 max-stations 150** (150 – ограничение по количеству клиентов. Параметр может принимать значения: от 0 до 200, где 0 – ограничение выключено. По умолчанию – 0)

#### Включение Minimal Signal и Roaming Signal

WEP-2ac# **set bss wlan0bssvap0 min-signal-enable on** (on – включение функционала minimal signal. Для выключения введите off. По умолчанию – off)

WEP-2ac# **set bss wlan0bssvap0 min-signal -75** (-75 – пороговое значение RSSI, при достижении которого точка доступа будет отключать клиента от VAP. Параметр принимает значения от -100 до -1 дБм)

WEP-2ac# **set bss wlan0bssvap0 check-signal-timeout 10** (10 – период времени в секундах, по истечении которого принимается решение об отключении клиентского оборудования от виртуальной сети. По умолчанию – 10)

WEP-2ac# **set bss wlan0bssvap0 roaming-signal-limit -70** (-70 – пороговое значение RSSI, при достижении которого происходит переключение клиентского оборудования на другую точку доступа. Параметр принимает значения от -100 до -1 дБм)

Параметр **roaming-signal-limit** должен быть ниже, чем **min-signal**: если **min-signal** = -75 дБм, то **roaming-signal-limit** должен быть равен, например, -70 дБм)

#### Включение VLAN Trunk на VAP

WEP-2ac# **set bss wlan0bssvap0 tagged-sta-mode on** (on – включение VLAN Trunk на VAP0 Radio 1. Для отключения введите – off)

Для того, чтобы тегированный трафик передавался в сторону клиента необходимо на радиоинтерфейсе обозначить номера VLAN, которые могут проходить через радиоинтерфейс. Номера VLAN нужно указать в параметре **vlan-list**.

Пример настройки **vlan-list** на Radio 1:

WEP-2ac# **set radio wlan0 vlan-list '10;4033'** (10 и 4033 – номера VLAN. Максимальное возможное количество VLAN в списке: 20)

#### Включение General VLAN на VAP

WEP-2ac# **set bss wlan0bssvap0 general-vlan-mode on** (on – включение General VLAN на VAP0 Radio 1. Для отключения введите off)

WEP-2ac# **set bss wlan0bssvap0 general-vlan-id 12** (12 – номер General VLAN)

**Включение скрытого SSID**

WEP-2ac# **set bss wlan0bssvap0 ignore-broadcast-ssid on** (**on** – включение скрытого SSID на VAP0 Radio 1. Для отключения введите **off**)

**Включение Band Steer**

WEP-2ac# **set vap vap0 with radio wlan0 band-steer-mode up** (**up** – включение Band Steer на VAP0 Radio1. Для отключения введите **down**)

WEP-2ac# **set vap vap0 band-steer-mode up** (**up** – включение Band Steer одновременно на VAP0 Radio1 и на VAP0 Radio2. Для отключения введите **down**)

**Включение изоляции клиентов на VAP**

WEP-2ac# **set bss wlan0bssvap0 station-isolation on** (**on** – включение изоляции клиентов на VAP0 Radio 1. Для отключения введите **off**)

**Настройка VLAN Priority на VAP**

WEP-2ac# **set vap vap0 with radio wlan0 vlan-prio 6** (**6** – приоритет DSCP, который будет присваиваться трафику, полученному от клиента, подключенного к VAP0 Radio 1. По умолчанию – **0**)

WEP-2ac# **set vap vap0 vlan-prio 6** (**6** – приоритет DSCP, который будет присваиваться трафику, полученному от клиента, подключенного к VAP0 Radio 1 или к VAP0 Radio 2. По умолчанию – **0**)

**Настройка DSCP Priority на VAP**

WEP-2ac# **set bss wlan0bssvap0 dscp-prio 0** (**0** – анализ приоритета из поля CoS (протокол 802.1p) тегированных пакетов на VAP0 Radio1. Для анализа приоритета из поля DSCP заголовка IP-пакета введите **1**)

**Настройка таймаута неактивности STA на VAP**

WEP-2ac# **set bss wlan0bssvap0 scb-timeout 30** (**30** – период времени в секундах, по истечении которого принимается решение об отключении клиентского оборудования от VAP. **0** – не использовать таймаут на VAP. По умолчанию – **0**)

## 5.6.4 Настройка Cluster

**Настройка Cluster**

WEP-2ac# **set cluster cluster-name test** (**test** – имя кластера. По умолчанию – **default**)

WEP-2ac# **set cluster location floor-2** (**floor-2** – физическое местоположение точки доступа. По умолчанию – **not set** – не задано)

WEP-2ac# **set cluster priority 255** (**255** – приоритет точки доступа в кластере. Если приоритет у всех точек в кластере одинаковый, то Master-точка выбирается по признаку меньшего MAC-адреса. Параметр принимает значения: **от 0 до 255**. По умолчанию – **0**)

WEP-2ac# **set cluster clustered 1** (**1** – включение режима Cluster. Параметр принимает значения: **0** – Cluster выключен; **softwlc** – Cluster выключен, режим для работы с SoftWLC; **1** – Cluster включен. По умолчанию – **1**)

**Настройка Single IP Management**

WEP-2ac# **set cluster cluster-ipaddr 192.168.1.222** (**192.168.1.222** – IP-адрес, по которому будет доступна Master-точка кластера. По умолчанию – **0.0.0.0**)

**Настройка параметров безопасности Cluster**

WEP-2ac# **set cluster cluster secure-mode 1** (**1** – включение безопасности кластера – в кластер смогут добавиться только те точки доступа, у которых совпадает пароль указанный в параметре **pass-phrase**. Для выключения введите – **0**. По умолчанию – **0**)

WEP-2ac# **set cluster pass-phrase 12345678** (**12345678** – пароль безопасности кластера. Должен содержать от 8 до 63 символов)

**Обновление программного обеспечения точек, входящих в кластер**

WEP-2ac# **set cluster-firmware-upgrade upgrade-method selective** (**selective** – режим, при котором будет обновляться программное обеспечение только выбранной точки доступа. Если необходимо обновить все точки доступа в кластере введите – **all**)

WEP-2ac# **set cluster-firmware-upgrade upgrade-members 192.168.0.58** (**192.168.0.58** – IP-адрес точки, входящей в кластер, которую необходимо обновить. Если был выбран **upgrade-method = all**, IP-адрес точек указывать не нужно)

WEP-2ac# **set cluster-firmware-upgrade upgrade-url tftp://<IP-адрес TFTP-сервера>/<Имя файла ПО>.tar.gz** (путь до файла ПО точки доступа, который лежит на TFTP-сервере. Пример: **set cluster-firmware-upgrade upgrade-url tftp://192.168.1.7/WEP-2ac-1.22.X.X.tar.gz**)

WEP-2ac# **set cluster-firmware-upgrade upgrade start** (**start** – запуск процесса обновления программного обеспечения на выбранных точках доступа. Для остановки процесса обновления введите – **stop**)

### 5.6.5 Настройка WDS

Пример настройки WDS на Radio 1 (5 ГГц).

Перед непосредственной настройкой WDS на точках доступа необходимо: выключить Cluster, настроить радиointерфейс и VAP.

#### Предварительная настройка

```
WEP-2ac# set cluster clustered 0 (0 – выключение режима Cluster)
WEP-2ac# set bss wlan0bssvap0 status up (up – включение VAP0 на Radio1)
WEP-2ac# set radio wlan0 mode a-n-ac (a-n-ac – установка режима работы радиointерфейса,
посредством которого устройство будет подключаться к точке доступа в режиме клиента. Режим
работы должен совпадать с режимом работы на точке доступа)
WEP-2ac# set radio wlan0 channel-policy static (static – выключение функционала автоматического
выбора канала)
WEP-2ac# set radio wlan0 static-channel 144 (144 – номер статического канала, на котором работает
точка доступа, к которой будет подключаться данное устройство в режиме клиента)
WEP-2ac# set radio wlan0 n-bandwidth 20 (20 – ширина канала, на котором работает точка доступа, к
которой будет подключаться данное устройство в режиме клиента)
WEP-2ac# set interface wlan0 ssid WDS (WDS – название беспроводной сети на VAP0 Radio 1)
WEP-2ac# set interface wlan0 security wpa-personal (wpa-personal – режим шифрования)
WEP-2ac# set interface wlan0 wpa-personal-key 12345678 (123456789 – пароль беспроводной сети.
Должен содержать от 8 до 64 символов)
```

Всего на точке можно настроить 8 WDS-соединений. WDS-интерфейсы на точке именуются следующим образом: wlan0wdsX, где X – число от 0 до 7.

Ниже представлен пример настройки WDS без шифрования и с типом шифрования wpa-personal на интерфейсе wlan0wds0.

#### Настройка WDS без шифрования

```
WEP-2ac# set interface wlan0wds0 radio wlan0 (wlan0 – выбор интерфейса устройства, который будет
использоваться для построения WDS. Параметр принимает значения: wlan0 (Radio 1 – 5 ГГц), wlan1
(Radio 2 – 2.4 ГГц))
WEP-2ac# set interface wlan0wds0 remote-mac A8:F9:4B:B7:8B:C0 (A8:F9:4B:B7:8B:C0 – MAC-адрес
радиointерфейса точки доступа, с которой предусматривается совместная работа. MAC-адрес
радиointерфейса указан в выводе команды get interface wlanX, где X – номер беспроводного
интерфейса: 0 – Radio 1 (5 ГГц); 1 – Radio 2 (2.4 ГГц))
WEP-2ac# set interface wlan0wds0 status up (up – включение WDS на точке доступа. Для выключения
введите – down)
```

### Настройка WDS с wpa-personal

WEP-2ac# **set interface wlan0wds0 radio wlan0** (**wlan0** – выбор интерфейса устройства, который будет использоваться для построения WDS. Параметр принимает значения: **wlan0** (Radio 1 – 5 ГГц), **wlan1** (Radio 2 – 2.4 ГГц))

WEP-2ac# **set interface wlan0wds0 remote-mac A8:F9:4B:B7:8B:C0** (**A8:F9:4B:B7:8B:C0** – MAC-адрес радиointерфейса точки доступа, с которой предусматривается совместная работа. MAC-адрес радиointерфейса указан в выводе команды *get interface wlanX*, где X – номер беспроводного интерфейса: 0 – Radio 1 (5 ГГц); 1 – Radio 2 (2.4 ГГц))

WEP-2ac# **set interface wlan0wds0 wds-ssid WDS** (**WDS** – имя SSID для построения шифрованного WDS)

WEP-2ac# **set interface wlan0wds0 wds-security-policy wpa-personal** (**wpa-personal** – режим шифрования)

WEP-2ac# **set interface wlan0wds0 wds-wpa-psk-key 12345678** (**12345678** – WPA-ключ. Длина ключа составляет от 8 до 63 символов)

WEP-2ac# **set interface wlan0wds0 status up** (**up** -включение WDS на точке доступа. Для выключения введите – **down**)

### 5.6.6 Настройка WGB

Пример настройки WGB на Radio 1 (5 ГГц).

Перед непосредственной настройкой WGB на точке доступа необходимо: выключить на точке доступа Cluster, настроить радиointерфейс точки и VAP.

#### Предварительная настройка

WEP-2ac# **set cluster clustered 0** (**0** – выключение режима Cluster)

WEP-2ac# **set bss wlan0bssvap0 status up** (**up** – включение VAP0 на Radio1)

WEP-2ac# **set radio wlan0 mode a-n-ac** (**a-n-ac** – установка режима работы радиointерфейса, посредством которого устройство будет подключаться к точке доступа в режиме клиента. Режим работы должен совпадать с режимом работы на точке доступа)

WEP-2ac# **set radio wlan0 channel-policy static** (**static** – выключение функционала автоматического выбора канала)

WEP-2ac# **set radio wlan0 static-channel 144** (**144** – номер статического канала, на котором работает точка доступа, к которой будет подключаться данное устройство в режиме клиента)

WEP-2ac# **set radio wlan0 n-bandwidth 20** (**20** – ширина канала, на котором работает точка доступа, к которой будет подключаться данное устройство в режиме клиента)

WEP-2ac# **set interface wlan0 ssid WGB** (**WGB** – название беспроводной сети на VAP0 Radio 1)

WEP-2ac# **set interface wlan0 security wpa-personal** (**wpa-personal** – режим шифрования)

WEP-2ac# **set interface wlan0 wpa-personal-key 12345678** (**123456789** – пароль беспроводной сети. Должен содержать от 8 до 64 символов)

После проведения предварительной настройки необходимо настроить параметры "Upstream Interface" – интерфейс для подключения к точке доступа в режиме клиента. Ниже рассмотрены примеры настройки "Upstream Interface" WGB с различными типами шифрования.

### 5.6.6.1 Настройка Upstream Interface

#### Настройка WGB без шифрования

WEP-2ac# **set wgb-bridge radio wlan0** (**wlan0** – выбор интерфейса устройства, который будет использоваться для подключения к точке доступа. Параметр принимает значения: **wlan0** (Radio 1 – 5 ГГц), **wlan1** (Radio 2 – 2.4 ГГц))

WEP-2ac# **set wgb-bridge-upstrm ssid AP-ssid** (**AP-ssid** – имя беспроводной сети, к которой необходимо подключиться устройством в режиме клиента)

WEP-2ac# **set wgb-bridge wgb-bridge-mode up** (**up** – включение режима WGB на точке доступа. Для выключения введите – **down**)

WEP-2ac# **set wgb-bridge-upstrm security plain-text** (**plain-text** – режим шифрования. Параметр принимает значения: **wpa-personal**, **wpa-enterprise**, **plain-text**)

WEP-2ac# **set wgb-bridge-upstrm roam-threshold -85** (**-85** – минимальный уровень сигнала от точки доступа, при котором происходит подключение к точке)

WEP-2ac# **set wgb-bridge-upstrm vlan-id 15** (**15** – номер VLAN, используемый на точке доступа. По умолчанию – **1**)

#### Настройка WGB с wpa-personal

WEP-2ac# **set wgb-bridge radio wlan0** (**wlan0** – выбор интерфейса устройства, который будет использоваться для подключения к точке доступа. Параметр принимает значения: **wlan0** (Radio 1 – 5 ГГц), **wlan1** (Radio 2 – 2.4 ГГц))

WEP-2ac# **set wgb-bridge-upstrm ssid AP-ssid** (**AP-ssid** – имя беспроводной сети, к которой необходимо подключиться устройством в режиме клиента)

WEP-2ac# **set wgb-bridge wgb-bridge-mode up** (**up** – включение режима WGB на точке доступа. Для выключения введите – **down**)

WEP-2ac# **set wgb-bridge-upstrm wpa-personal-key 12345678** (**12345678** – пароль, необходимый для авторизации на точке доступа.. Должен содержать от 8 до 64 символов)

WEP-2ac# **set wgb-bridge-upstrm security wpa-personal** (**wpa-personal** – режим шифрования. Параметр принимает значения: **wpa-personal**, **wpa-enterprise**, **plain-text**)

WEP-2ac# **set wgb-bridge-upstrm roam-threshold -85** (**-85** – минимальный уровень сигнала от точки доступа, при котором происходит подключение к точке)

WEP-2ac# **set wgb-bridge-upstrm vlan-id 15** (**15** – номер VLAN, используемый на точке доступа. По умолчанию – **1**)

### Настройка WGB с wpa-enterprise

WEP-2ac# **set wgb-bridge radio wlan0** (**wlan0** – выбор интерфейса устройства, который будет использоваться для подключения к точке доступа. Параметр принимает значения: **wlan0** (Radio 1 – 5 ГГц), **wlan1** (Radio 2 – 2.4 ГГц))

WEP-2ac# **set wgb-bridge-upstrm ssid AP-ssid** (**AP-ssid** – имя беспроводной сети, к которой необходимо подключиться устройством в режиме клиента)

WEP-2ac# **set wgb-bridge wgb-bridge-mode up** (**up** – включение режима WGB на точке доступа. Для выключения введите – **down**)

WEP-2ac# **set wgb-bridge-upstrm security wpa-enterprise** (**wpa-enterprise** – режим шифрования. Параметр принимает значения: **wpa-personal**, **wpa-enterprise**, **plain-text**)

WEP-2ac# **set wgb-bridge-upstrm eap-user client** (**client** – имя пользователя, используемое при авторизации на RADIUS-сервере)

WEP-2ac# **set wgb-bridge-upstrm eap-password clientspassword** (**clientspassword** – пароль пользователя, используемый при авторизации на RADIUS-сервере)

WEP-2ac# **set wgb-bridge-upstrm roam-threshold -85** (**-85** – минимальный уровень сигнала от точки доступа, при котором происходит подключение к точке)

WEP-2ac# **set wgb-bridge-upstrm eap-method peap** (**peap** – выбор протокола аутентификации. Параметр принимает значения: **peap**, **tls**)

WEP-2ac# **set wgb-bridge-upstrm vlan-id 15** (**15** – номер VLAN, используемый на точке доступа. По умолчанию – **1**)

При необходимости можно произвести настройку интерфейса "Downstream Interface", выступающего в качестве точки доступа для подключения клиентских устройств.

#### 5.6.6.2 Настройка Downstream Interface

### Настройка "Downstream Interface" с wpa-personal

WEP-2ac# **set wgb-bridge-dwstrm ssid Client-ssid** (**Client-ssid** – имя беспроводной сети, к которой необходимо подключиться устройством в режиме клиента)

WEP-2ac# **set wgb-bridge-dwstrm wpa-personal-key 12345678** (**12345678** – пароль для подключения к беспроводной сети)

WEP-2ac# **set wgb-bridge-dwstrm security wpa-personal** (**wpa-personal** – режим шифрования. Для создания SSID без режима шифрования введите – **plain-text**. Параметр принимает значения: **wpa-personal**, **plain-text**)

WEP-2ac# **set wgb-bridge-dwstrm ignore-broadcast-ssid off** (**off** – выключение режима скрытого SSID. Для включения режима введите – **on**)

WEP-2ac# **set wgb-bridge-dwstrm vlan-id 15** (**15** – номер VLAN, в котором будет передаваться сетевой трафик для данной точки доступа. По умолчанию – **1**)

WEP-2ac# **set wgb-bridge-dwstrm status up** (**up** – включение Downstream Interface. Для выключения введите – **down**)

#### 5.6.6.3 Настройка WGB-ARP-Timeout

### Настройка WGB-ARP-Timeout

WOP-2ac# **set wgb-bridge wgb-arp-timeout 5** (**5** – время жизни записи в ARP-таблице режима WGB. Параметр принимает значение от **1** до **1440** минут. По умолчанию – **5** минут)

## 5.6.7 Настройка Radar

Radar обеспечивает сбор MAC-адресов всех пользовательских устройств, попадающих в зону действия точки доступа, работающей в режиме Radar.

При включении режима active точка доступа не может предоставлять услугу Wi-Fi. В данном режиме точка доступа весь ресурс времени занимает сканированием на всех доступных каналах.

При включении режима passive сервис Wi-Fi доступен. В данном режиме сканирование происходит только на рабочих каналах, которые настроены на Radio1/2, переключения на другие каналы не происходит.

### Настройка Radar

```

WEP-2ac# set radar radar-service up (up – статус режима Radar. По умолчанию – down)
WEP-2ac# set radar radar-service-url http://<host>:<port>/ (http://<host>:<port>/ – URL коллектора сбора
MAC-адресов. Может быть задан через протокол MQTT – mqtt://<host>:<port>/)
WEP-2ac# set radar mqtt-username username (username – имя пользователя. По умолчанию –
username)
WEP-2ac# set radar mqtt-password password (password – пароль. По умолчанию – password)
WEP-2ac# set radar mqtt-topic eltex-radar (eltex-radar – канал отправки и получения сообщений между
устройствами. По умолчанию – eltex-radar)
WEP-2ac# set radar radar-mode passive (passive – режим пассивного сбора MAC-адресов. По
умолчанию – active)
WEP-2ac# set radar scan-interface wlan_2g (wlan_2g – перечень интерфейсов, на которых запущен
режим Radar. Параметр принимает значения: wlan_2g/wlan_5g/all. По умолчанию – all)
WEP-2ac# set radar send-interval 1 (1 – интервал отправки данных на коллектор. Параметр принимает
значение от 1 до 3600. По умолчанию – 5)
WEP-2ac# set radar list-size 255 (255 – размер буфера для накопления записей о MAC-адресах
клиентов. Параметр принимает значение от 255 до 65535. По умолчанию – 1000)
WEP-2ac# set radar mgmt-probe on (on – получение информации от пакетов probe request. По
умолчанию – on)
WEP-2ac# set radar mgmt-assoc off (off – получение информации от пакетов assoc/disassoc, auth/deauth.
По умолчанию – off)
WEP-2ac# set radar data off (off – получение информации из пользовательского трафика в эфире. По
умолчанию – off)
WEP-2ac# set radar scan-channel-timeout 100 (100 – время на сканирование одного канала. Параметр
принимает значение от 100 до 60000. По умолчанию – 200)
WEP-2ac# set radar scan-channel-2g 1 (1 – канал для сканирования в диапазоне 2.4 ГГц, если 0, то
сканируются все доступные каналы. По умолчанию – 0)
WEP-2ac# set radar scan-channel-5g 36 (36 – канал для сканирования в диапазоне 5 ГГц, если 0, то
сканируются все доступные каналы. По умолчанию – 0)
WEP-2ac# set radar scan-channel-list-2g "1 2 3" ("1 2 3" – список каналов для сканирования в
диапазоне 2.4 ГГц. Параметр принимает значение от 1 до 13. Для работы списка необходимо, чтобы
параметр scan-channel-2g был равен 0)
WEP-2ac# set radar scan-channel-list-5g "36 40 44" ("36 40 44" – список каналов для сканирования в
диапазоне 5 ГГц. Параметр принимает значение от 36 до 165. Для работы списка необходимо, чтобы
параметр scan-channel-5g был равен 0)
WEP-2ac# set radar scan-min-signal -65 (-65 – минимальный порог уровня RSSI. По умолчанию – 0)

```

## 5.6.8 Системные настройки

### 5.6.8.1 Обновление ПО устройства

**✘** Не отключайте питание устройства и не выполняйте перезагрузку устройства в процессе обновления ПО.

Для обновления ПО по протоколу TFTP загрузите на TFTP-сервер файл прошивки WEP-2ac-1.22.X.X.tar.gz и выполните команду:

#### Обновление ПО точки доступа по TFTP

WEP-2ac# **firmware-upgrade tftp://<IP-адрес tftp-сервера>/<Название файла ПО>** (пример: firmware-upgrade tftp://192.168.1.100/WEP-2ac-1.22.X.X.tar.gz)

Для обновления ПО по протоколу HTTP загрузите на HTTP-сервер файл прошивки WEP-2ac-1.22.X.X.tar.gz и выполните команды:

#### Обновление ПО точки доступа по HTTP

WEP-2ac# **set firmware-upgrade upgrade-url http://<IP-адрес http-сервера>:[порт]/<Название файла ПО>** (пример: set firmware-upgrade upgrade-url http://192.168.1.100:8080/WEP-2ac-1.22.X.X.tar.gz)  
WEP-2ac# **set firmware-upgrade start yes** (команда для начала обновления ПО)

#### Переключение на резервную версию ПО точки доступа

WEP-2ac# **firmware-switch**

### 5.6.8.2 Управление конфигурацией устройства

#### Сброс конфигурации устройства в дефолтное состояние

WEP-2ac# **factory-reset**

#### Скачать конфигурационный файл устройства на TFTP-сервер

WEP-2ac# **config download tftp://<IP-адрес tftp-сервера>/<Название файла>.xml** (пример: config download tftp://192.168.1.100/WEP-2ac.xml)

#### Загрузить конфигурационный файл на устройство с tftp сервера

WEP-2ac# **config upload tftp://<IP-адрес tftp-сервера>/<Название файла>.xml** (пример: config upload tftp://192.168.1.100/WEP-2ac.xml)

### 5.6.8.3 Перезагрузка устройства

#### Команда для перезагрузки устройства

WEP-2ac# **reboot**

### 5.6.8.4 Настройка режима аутентификации

#### Настройка аутентификации через RADIUS

WEP-2ac# **set authentication radius-auth-status on** (on – включение аутентификации через RADIUS. Параметр принимает значения: **on**, **off**. По умолчанию – **off**)

WEP-2ac# **set authentication radius-auth-address <IP-адрес RADIUS-сервера>** (пример: set authentication radius-auth-address 192.168.1.1)

WEP-2ac# **set authentication radius-auth-port <порт RADIUS-сервера>** (пример: set authentication radius-auth-port 1234. По умолчанию – **1812**)

WEP-2ac# **set authentication radius-auth-password <ключ для RADIUS-сервера>** (пример: set authentication radius-auth-password secret. По умолчанию – **password**)

- ✓ Аутентифицировать можно только пользователя с именем, заданным в `get system username` (По умолчанию – **admin**).  
В случае, если RADIUS-сервер окажется недоступен, аутентификация пройдет по локальной учетной записи.

### 5.6.8.5 Настройка даты и времени

#### Команды для настройки синхронизации времени с сервером NTP

WEP-2ac# **set ntp status up** (**up** – включение синхронизации времени с NTP-сервером. Параметр принимает значения: **down**, **up**. По умолчанию – **up**)

WEP-2ac# **set ntp server 192.168.1.100** (**192.168.1.100** – IP-адрес основного NTP-сервера)

WEP-2ac# **set ntp alternative-server ntp1.stratum2.ru** (**ntp1.stratum2.ru** – доменное имя резервного NTP-сервера-1)

WEP-2ac# **set ntp alternative-server2 192.168.1.102** (**192.168.1.102** – IP-адрес резервного NTP-сервера-2)

WEP-2ac# **set ntp interval 3600** (**3600** – значение параметра управления периодом синхронизации в секундах. Параметр принимает значения: **1-86400**. По умолчанию – **3600**)

WEP-2ac# **set system time-zone 'Russian Fed. Zone 6 (Novosibirsk; Krasnoyarsk)'** (**Russian Fed. Zone 6 (Novosibirsk; Krasnoyarsk)** – установка тайм-зоны. По умолчанию – 'Russia (Moscow)')

### 5.6.8.6 Настройка отправки SNMP-трапов

#### Настройка отправки SNMP-трапов

WEP-2ac# **set snmp source-status up** (**up** – включение принятия SNMP-запросов только с указанных в параметре **snmp source** адресов. Параметр принимает значения: **down, up**. По умолчанию – **down**)  
WEP-2ac# **set snmp source 192.168.1.100 (192.168.1.100** – IP-адрес хоста, от которого разрешено принимать SNMP-запросы)  
WEP-2ac# **add traphost host 192.168.1.100 community public host-type ipv4 trap\_version snmpV2**  
(настройка отправки SNMP-трапов версии **snmpV2**, на хост **ipv4** с ip-адресом **192.168.1.100**, для группы **public**)

### 5.6.9 Настройка сервиса APB

#### Команды для настройки сервиса APB

WEP-2ac# **set captive-portal mode up** (**up** – активировать подключение к сервису APB. Параметр принимает значения: **up, down**. По умолчанию – **up**)  
WEP-2ac# **set captive-portal roaming-service-url ws://<Адрес сервиса APB>:8090/apb/broadcast**  
(пример: **set captive-portal roaming-service-url ws://192.168.1.100:8090/apb/broadcast**)  
WEP-2ac# **get captive-portal apb-operation-status** (команда для вывода статуса сервиса APB: **connected, not\_connected** или **not\_running**)

## 5.6.10 Мониторинг

## 5.6.10.1 Wi-Fi клиенты

## WEP-2ac# get association detail

Property	Value
<b>interface</b>	wlan0vap1
station	62:3b:f9:4d:ac:27
authenticated	Yes
associated	Yes
authorized	Yes
ip-address	10.24.80.74
hostname	HUAWEI_P40_Pro-81afe9c34a
fw-version	
board-type	
rx-packets	318
tx-packets	293
rx-bytes	64360
tx-bytes	158746
tx-rate	156
rx-rate	156
tx-actual-rate	0
rx-actual-rate	0
tx-modulation	VHT LDPC MCS8 NSS2 20MHz
rx-modulation	VHT LDPC MCS8 NSS2 20MHz
listen-interval	10
last-rssi	-48
last-snr	44 dB
noise	-92 dBm
tx-link-quality	100%
tx-rate-quality	100%
tx-link-capacity	100% (not changed)
tx-drop-bytes	0
rx-drop-bytes	0
tx-drop-packets	0
rx-drop-packets	0
client-qos-enabled	Disabled
bw-limit-up	0
bw-limit-down	0
acl-type-up	None
acl-up	
acl-type-down	None
acl-down	
policy-up	
policy-down	
ts-violate-rx-packets	
ts-violate-tx-packets	
uptime	00:00:00
identity	tutu
domain	enterprise.service.root
supported-channels	36-64,132-140,149-165
using-802.11r	No
using-802.11k	No

```
mode                802.11ac
aid                 1
ps-mode             0
vlan-id             10
auth-mode            WPA2
encryption           AES-CCMP
eltex-serial-number
assoc-duration      0.001337
auth-duration        2.525727
dhcp-start-duration 0.000000
dhcp-end-duration    0.019971
count-dhcp-dis       0
count-dhcp-off       0
count-dhcp-req       1
count-dhcp-ack       1
```

## 5.6.10.2 Информация об устройстве

## WEP-2ac# get system detail

Property	Value
username	admin
model	Eltex WEP-2ac
version	1.22.X.X
altversion	1.22.X.X
build-year	2021
build-date	2021.03.18 13:42 +07
loader-version	1.22.X.X
platform	bcm947452acnrm
uptime	0 days, 0 hours, 5 minutes
system-time	Tue Apr 27 2021 06:02:52 MST
time-zone	Russia (Moscow)
enable-dst	off
dst-start	March.Second.Sunday/02:00
dst-end	November.First.Sunday/02:00
dst-offset	60
country	RU
country-mode	on
full-isolation	on
tunneling-over-wds	off
force-allow-eth	off
power-source	
nmode-supported	Y
forty-mhz-supported-g	Y
forty-mhz-supported-a	Y
eighty-mhz-supported-a	Y
base-mac	e8:28:c1:c1:27:60
base-mac-status	on
serial-number	WP12034181
country-code-is-configurable	on
system-name	
system-contact	admin@example.com
system-location	Default
band-plan	
lastboot	success
wpa-personal-key-min-complexity-support	off
wpa-personal-key-min-character-class	3
wpa-personal-key-min-length	8
wpa-personal-key-max-length	63
wpa-personal-key-different-from-current	no
password-min-complexity-support	off
password-min-character-class	3
password-min-length	8
password-max-length	64
password-aging-support	off
password-aging-time	180
password-different-from-current	yes

## 5.6.10.3 Сетевая информация

WEP-2ac# **get management detail**

Property	Value
vlan-id	1
mtu	1500
<b>interface</b>	brtrunk
tunnel-ip	
<b>static-ip</b>	192.168.1.10
<b>static-mask</b>	255.255.255.0
ip	100.110.0.242
mask	255.255.254.0
mac	E8:28:C1:C1:27:60
ap-location	eltex.root
dhcp-status	up
<b>static-ipv6</b>	::
<b>static-ipv6-mask</b>	
ipv6	
ipv6-mask	
sw-ratelimit-enable	up
sw-ratelimit-timer	100
ucast-prom-ratelimit	150000
ucast-sw-ratelimit-mode	auto
ucast-sw-ratelimit	120000
ucast-sw-gre-ratelimit	10500
mcast-sw-ratelimit	10000
bcast-sw-ratelimit	1000
arp-req-sw-ratelimit	500
vlan-lock	up
ipv6-status	down
ipv6-autoconfig-status	down
<b>static-ipv6</b>	::
<b>static-ipv6-prefix-length</b>	0
<b>static-ipv6-addr-status</b>	
dhcp6-status	up
autoconfig-link-local	
autoconfig-ipv6-global-all	

WEP-2ac# **get ip-route**

Property	Value
destination	0.0.0.0
mask	0.0.0.0
gateway	100.110.0.1
table	254

WEP-2ac# **get ntp detail**

Property	Value
status	up
server	100.110.1.253
alternative-server	100.110.0.22
alternative-server2	0.ru.pool.ntp.org
dhcp_server	100.110.1.252
dhcp_alt_server	
dhcp_alt_server2	
manual-daily-drift-secs	0
interval	3600

## 5.6.10.4 Беспроводные интерфейсы

## WEP-2ac# get radio wlan0 detail

Property	Value
status	up
description	IEEE 802.11a
<b>static</b> -mac	
channel-policy	best
channel-update	1440
mode	a-n-ac
tpc	off
scb-timeout	120
atf	on
ampdu_atf_us	4000
ampdu_atf_min_us	1000
dot11h	off
dot11d	up
<b>static</b> -channel	36
channel	56
tx-power-dbm	19
tx-power-dbm-max	19
tx-power-dbm-min	1
tx-power-output	0.00
tx-chain	3
beacon-interval	100
rts-threshold	2347
fragmentation-threshold	2346
arp-suppression	on
ap-detection	on
limit-channels	36 40 44 48 52 56 60 64
operational-bandwidth	20
n-bandwidth	20
n-primary-channel	lower
protection	auto
edca-template	custom
<b>short</b> -guard-interval-supported	no
stbc-mode	auto
ldpc-mode	auto
dhcp-snooping-mode	ignore
dhcp-option-82-string	
coex-mode	on
vlan-list	
wme	on
wme-noack	off
wme-apsd	on
rate-limit-enable	off
rate-limit	50
rate-limit-burst	75
stp-block-enable	on
wlan-util	8
num-stations	0
wds-status	down
fixed-multicast-rate	auto
fixed-tx-modulation	auto

```

max-stations                200
dtim-period                 2
reinit-period               0
scheduler-profile-name
operational-mode            up
scheduler-operational-mode
vht-mode                    on
vht-features                 off
rsdb-mode                   off
frame-burst                 off
spectrum-analyser-start
spectrum-analyser-status    Not ready
spectrum-analyser-results   Not ready
rrm-block-tpc
rrm-block-dca
ampdu                        up
amsdu                        up
olpc-cal-period              300
olpc-channel                 yes

```

### WEP-2ac# **get radio wlan1 detail**

```

Property                    Value
-----
status                      up
description                  IEEE 802.11g
static-mac
channel-policy               best
channel-update               1440
mode                         bg-n
tpc                          off
scb-timeout                  120
atf                           on
ampdu_atf_us                 4000
ampdu_atf_min_us             1000
dot11h                       off
dot11d                       up
static-channel                6
channel                      11
tx-power-dbm                 16
tx-power-dbm-max             16
tx-power-dbm-min             5
tx-power-output               15.25
tx-chain                      3
beacon-interval              100
rts-threshold                 1025
fragmentation-threshold      1024
arp-suppression               on
ap-detection                  on
limit-channels                1 6 11
operational-bandwidth         20
n-bandwidth                   20
n-primary-channel             lower
protection                    auto
edca-template                 custom
short-guard-interval-supported no

```

stbc-mode	auto
ldpc-mode	auto
dhcp-snooping-mode	ignore
dhcp-option-82-string	
coex-mode	on
vlan-list	
wme	on
wme-noack	off
wme-apsd	on
rate-limit-enable	off
rate-limit	50
rate-limit-burst	75
stp-block-enable	on
wlan-util	88
num-stations	0
wds-status	down
fixed-multicast-rate	auto
fixed-tx-modulation	auto
max-stations	200
dtim-period	2
reinit-period	0
scheduler-profile-name	
operational-mode	up
scheduler-operational-mode	
vht-mode	
vht-features	off
rsdb-mode	
frame-burst	off
spectrum-analyser-start	
spectrum-analyser-status	Not ready
spectrum-analyser-results	Not ready
rrm-block-tpc	
rrm-block-dca	
ampdu	up
amsdu	down
olpc-cal-period	300
olpc-channel	no

## 5.6.10.5 WDS

## WEP-2ac# get interface wlan0wds0 detail

Property	Value
type	wds
status	up
description	Wireless Distribution System - Link 1
mac	E8:28:C1:C1:27:60
ip	
mask	
static-ip	
static-mask	
rx-bytes	8235818
rx-packets	38800
rx-errors	0
tx-bytes	172159433
tx-packets	263429
tx-errors	0
tx-drop-bytes	0
rx-drop-bytes	0
tx-drop-packets	0
rx-drop-packets	0
ts-vo-rx-packets	0
ts-vo-tx-packets	0
ts-vo-rx-bytes	0
ts-vo-tx-bytes	0
ts-vi-rx-packets	0
ts-vi-tx-packets	0
ts-vi-rx-bytes	0
ts-vi-tx-bytes	0
ts-be-rx-packets	0
ts-be-tx-packets	0
ts-be-rx-bytes	0
ts-be-tx-bytes	0
ts-bk-rx-packets	0
ts-bk-tx-packets	0
ts-bk-rx-bytes	0
ts-bk-tx-bytes	0
priority	128
port-isolation	
auto-negotiation	
speed	
duplex	
link-status	
link-uptime	
intf-speed	
duplex-mode	
green-ethernet-mode	
ssid	
bss	
security	
wep-key-ascii	no
wep-key-length	104
wep-default-key	

```
wep-key-mapping-length
vlan-interface
vlan-id
radio wlan0
remote-mac A8:F9:4B:B7:8B:C0
remote-rssi -16
wep-key
operational-status up
wds-link-uptime 00:00:46
wds-ssid WDS
wds-security-policy wpa-personal
wds-wpa-psk-key 12345678
```

## 5.6.10.6 WGB

## WEP-2ac# get wgbriidge detail

Property	Value
wgbridge-mode	up
radio	wlan0
debug	

## WEP-2ac# get wg-bridge-upstrm detail

Property	Value
ssid	AP-ssid
security	wpa-personal
wep-key-ascii	no
wep-key-length	104
wep- <b>default</b> -key	1
wpa-allowed	off
wpa2-allowed	on
upstream-bssid	
vlan-id	1
connection-status	Associated to AP a8:f9:4b:b7:8b:c0
rx-bytes	8337952
rx-packets	50212
rx-errors	0
tx-bytes	306207
tx-packets	913
tx-errors	0
iface	wlan0upstrm
eap-user	
eap-method	peap
debug	
cert-present	no
cert-exp-date	Not Present
mfp	mfp-not-reqd
roam-threshold	-75
roam-delta	10

## WEP-2ac# get wg-bridge-dwstrm detail

Property	Value
ssid	Client-ssid
security	wpa-personal
wep-key-ascii	no
wep-key-length	104
wep- <b>default</b> -key	1
wep-key-mapping-length	
status	up
ignore-broadcast-ssid	off

```
open-system-authentication on
shared-key-authentication off
wpa-cipher-tkip on
wpa-cipher-ccmp on
wpa-allowed on
wpa2-allowed on
broadcast-key-refresh-rate 0
vlan-id 1
rx-bytes 6522
rx-packets 40
rx-errors 0
tx-bytes 8439
tx-packets 34
tx-errors 0
iface wlan0dwstrm
mfp mfp-not-reqd
```

## 5.6.10.7 Cluster

WEP-2ac# **get cluster detail**

Property	Value
clustered	1
location	floor-2
cluster-name	test
ipversion	ipv4
member-count	2
clustering-allowed	true
compat	WEP-2ac
operational-mode	1
cluster-ipaddr	192.168.0.222
priority	255
reauth-timeout	300
secure-mode	1
pass-set	1
secure-mode-status	Enabled
trace-debug	0

WEP-2ac# **get cluster-member detail**

Property	Value
mac	A8:F9:4B:B7:8B:C0
ip	192.168.0.58
compat	WEP-2ac
location	floor-1
uptime	120
is-dominant	true
priority	0
firmware-version	1.22.X.X
cluster-controller	no

Property	Value
mac	E8:28:C1:C1:27:60
ip	192.168.0.135
compat	WEP-2ac
location	floor-2
uptime	124
is-dominant	false
priority	255
firmware-version	1.22.X.X
cluster-controller	yes

WEP-2ac# **get cluster-fw-member detail**

Property	Value
upgrade	
upgrade-url	tftp://192.168.1.7/WEP-2ac-1.22.X.X.tar.gz
upgrade-method	selective
upgrade-status	Completed
upgrade-members	192.168.0.58

WEP-2ac# **get cluster-fw-member**

ip	mac	fw-download-status
192.168.0.58	A8:F9:4B:B7:8B:C0	Success
192.168.0.135	E8:28:C1:C1:27:60	None

## 5.6.10.8 Журнал событий

## WEP-2ac# get log-entry

Property	Value
----------	-------

---

number	1
priority	debug
time	Apr 27 2021 05:32:50
daemon	hostapd[17753]
message	Station 62:3b:f9:4d:ac:27 associated, time = 0.001337

Property	Value
----------	-------

---

number	2
priority	debug
time	Apr 27 2021 05:32:50
daemon	hostapd[17753]
message	station: 62:3b:f9:4d:ac:27 associated rssi -49(-49)

Property	Value
----------	-------

---

number	3
priority	info
time	Apr 27 2021 05:32:50
daemon	hostapd[17753]
message	STA 62:3b:f9:4d:ac:27 associated with BSSID e8:28:c1:c1:27:61

Property	Value
----------	-------

---

number	4
priority	info
time	Apr 27 2021 05:32:50
daemon	hostapd[17753]
message	Assoc request from 62:3b:f9:4d:ac:27 BSSID e8:28:c1:c1:27:61 SSID Test_Enterprise

### 5.6.10.9 Сканирование эфира

Сканирование эфира предоставляет информацию обо всех беспроводных точках доступа, которые устройство детектирует вокруг себя.

WEP-2ac# **get detected-ap**

mac	type	privacy	ssid	channel	signal
e0:d9:e3:50:71:e0	AP	On	i-OTT-ent-06	56	-61
e0:d9:e3:50:71:e1	AP	Off	i-OTT-06-portal	56	-61
e8:28:c1:d7:3c:24	AP	Off	i-200	11	-45
a8:f9:4b:17:02:20	AP	Off	(Non Broadcasting)	11	-56
e8:28:c1:cf:d9:14	AP	On	RT-WiFi-5278	11	-61
e0:d9:e3:8a:38:50	AP	Off	GPB_Free	11	-53

### 5.6.10.10 Спектроанализатор

Спектроанализатор предоставляет информацию о загруженности каналов в диапазонах 2.4 и 5 ГГц. Спектроанализатор сканирует каналы указанные в параметре **limit-channels** в настройках радиоинтерфейса. Результат выводится в процентах.

- ✔ После запуска сканирования для получения результатов необходимо подождать несколько минут. На время сканирования у подключенных клиентов будет наблюдаться прерывание работы сервисов.

WEP-2ac# **set radio all spectrum-analyser-start yes** (запуск спектроанализатора на всех радиоинтерфейсах одновременно. Для запуска спектроанализатора на конкретном радиоинтерфейсе вместо **all** введите название интерфейса: **wlan0** - Radio1, **wlan1** - Radio2)

WEP-2ac# **get radio all spectrum-analyser-results** (вывод результата работы спектроанализатора)

```
Property                               Value
-----
name                                    wlan0
spectrum-analyser-results
 36:   52 | *****
 40:   52 | *****
 44:   15 | ****
 48:   13 | ***
 52:    9 | **
 56:    4 | *
 60:    5 | **
 64:   10 | ***
Optimal 20MHz channel: 56
Optimal 40MHz channel: 52l
Optimal 80MHz channel: 56/80
```

```
Property                               Value
-----
name                                    wlan1
spectrum-analyser-results
  1:   92 | *****
  6:   84 | *****
 11:   88 | *****
Optimal 20MHz channel: 11
```

## 6 Приложение. Список основных классов и подклассов команд

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
debug Отладочные команды	level	Уровень отладочной информации	get, set	get debug level set debug level <value>	WEP-2ac# get debug level 0
	timestamp	Добавить метку времени к отладочной информации	get, set	get debug timestamp set debug timestamp <value>	WEP-2ac# get debug timestamp
	klevel	Уровень отладочной информации ядра	get, set	get debug klevel set debug klevel <value>	WEP-2ac# set debug klevel 1 WEP-2ac# get debug klevel 1
system Настройки системы	password	Пароль доступа к пользовательскому web-интерфейсу и CLI	set	set system password <value>	WEP-2ac# set system password password
	model	Модель устройства	get	get system model	WEP-2ac# get system model Eltex WEP-2ac
	version	Версия ПО	get	get system version	WEP-2ac# get system version 1.14.0.89
	platform	Аппаратная платформа	get	get system platform	WEP-2ac# get system platform bcm953012er
	encrypted-password	Зашифрованный пароль	get, set	get system encrypted-password set system encrypted-password <value>	WEP-2ac# set system encrypted-password "\$1\$G6G6G6G6\$Dh39pxWqjp3nBRrBPBL7o1" WEP-2ac# WEP-2ac# get system encrypted-password\$1\$G6G6G6G6\$Dh39pxWqjp3nBRrBPBL7o1

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	uptime	Время работы системы с момента загрузки	get	get system uptime	WEP-2ac# get system uptime  6 days, 17 hours, 25 minutes
	system-time	Текущее время системы	get	get system system-time	WEP-2ac# get system system-time  Thu May 31 2018 06:59:46 MST
	time-zone	Часовой пояс	get, set	get system time-zone  set system time-zone <value>	WEP-2ac# set system time-zone "Russia (Moscow)"  WEP-2ac# get system time-zone  Russia (Moscow)  WEP-2ac#
	enable-dst	Включить переход на летнее время	get, set	get system enable-dst  set system enable-dst <value>	WEP-2ac# set system enable-dst on  WEP-2ac# get system enable-dst on
	summer-time		get, set	get system summer-time  set system summer-time <value>	WEP-2ac# set system summer-time enabled  WEP-2ac# get system summer-time enabled
	dst-start	Время перехода на летнее время	get, set	get system dst-start  set system dst-start <value>	WEP-2ac# set system dst-start "March.Second.Sunday/02:00"  WEP-2ac# get system dst-start  March.Second.Sunday/02:00

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	dst-end	Время перехода на зимнее время	get, set	<pre>get system dst-end set system dst-end &lt;value&gt;</pre>	<pre>WEP-2ac# set system dst-start "November.First.Sunday/02:00" WEP-2ac# get system dst-end November.First.Sunday/02:00</pre>
	dst-offset		get, set	<pre>get system dst-offset set system dst-offset &lt;value&gt;</pre>	<pre>WEP-2ac# set system dst-offset 60 WEP-2ac# get system dst-offset 60</pre>
	reboot	Перезагрузить точку доступа	set	<pre>set system reboot</pre>	<pre>WEP-2ac# set system reboot</pre>
	country	Страна	get, set	<pre>get system country set system country &lt;value&gt;</pre>	<pre>WEP-2ac# set system country RU WEP-2ac# get system country RU</pre>
	country-mode	Возможные значения: on, off	get, set	<pre>get system country-mode set system country-mode &lt;value&gt;</pre>	<pre>WEP-2ac# set system country-mode off WEP-2ac# get system country-mode off</pre>
	full-isolation	Полная изоляция. Возможные значения: on – функция активна, off – функция неактивна	get, set	<pre>get system full-isolation set system full-isolation &lt;value&gt;</pre>	<pre>WEP-2ac# set system full-isolation off WEP-2ac# get system full-isolation off</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	nmode-supported	Поддержка стандарта IEEE 802.11n. Возможные значения: Y – поддерживает, N – не поддерживает	get	get system nmode-supported	WEP-2ac# get system nmode-supported Y
	forty-mhz-supported	Поддержка полосы пропускания шириной 40 МГц в 5 ГГц диапазоне	get	get system forty-mhz-supported	
	base-mac		get, set	get system base-mac  set system base-mac <value>	WEP-2ac# set system base-mac "a8:f9:4b:b0:21:60"  WEP-2ac# get system base-mac a8:f9:4b:b0:21:60
	serial-number	Серийный номер изделия	get, set	get system base-mac  set system base-mac <value>	WEP-2ac# set system serial-number WP01000167  WEP-2ac# get system serial-number WP01000167
	country-code-is-configurable	Настройка кода страны. Возможные значения: on – функция активна, off – функция неактивна.	get, set	get system country-code-is-configurable  set system country-code-is-configurable <value>	WEP-2ac# set system country-code-is-configurable on  WEP-2ac# get system country-code-is-configurable on
	system-name	Имя системы	get, set	get system system-name  set system system-name <value>	WEP-2ac# set system system-name "WEP-2ac"  WEP-2ac# get system system-name WEP-2ac

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	system-contact	Контакты системы	get, set	get system system-contact  set system system-contact <value>	
	system-location	Местоположение системы	get, set	get system system-location  set system system-location <value>	WEP-2ac# get system system- location Default
host Настройки хоста	id	ID хоста	get, set	get host id  set host id <value>	WEP-2ac# set host id "WEP-2ac"  WEP-2ac# get host id WEP-2ac
	dns-1	IP-адрес DNS-сервера (1)	get	get host dns-1	WEP-2ac# get host dns-1 172.16.0.250
	dns-2	IP-адрес DNS-сервера (2)	get	get host dns-2	WEP-2ac# get host dns-2 172.16.0.100
	domain	Имя домена	get	get host domain	WEP-2ac# get host domain eltex.loc
	static-dns-1	DNS-сервер (1), который будет использован, если адрес не получен по DHCP	get, set	get host static-dns-1  set host static-dns-1 <value>	WEP-2ac# get host static-dns-1
	static-dns-2	DNS-сервер (2), который будет использован, если адрес не получен по DHCP	get, set	get host static-dns-2  set host static-dns-2 <value>	WEP-2ac# get host static-dns-1

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	static-domain	Имя домена, используемого, если не получено имя домена по DHCP	get, set	get host static-domain set host static-domain <value>	WEP-2ac# set host static-domain "example.com" WEP-2ac# get host static-domain example.com
	dns-via-dhcp	Получать параметры DNS-сервера по DHCP. Возможные значения: up – получать по DHCP, down – использовать статические параметры	get, set	get host dns-via-dhcp set host dns-via-dhcp <value>	WEP-2ac# set host dns-via-dhcp up WEP-2ac# get host dns-via-dhcp up
config Настройки конфигурации	startup	Настройка во время загрузки	set	set config startup <value>	
	version	Версия файла конфигурации	get	get config version	WEP-2ac# get config version 1.02
	backup-file-format	Формат файла конфигурации. Возможные значения: plain – незашифрованный, encrypted – зашифрованный	get, set	get config backup-file-format set config backup-file-format <value>	WEP-2ac# set config backup-file-format plain WEP-2ac# get config backup-file-format plain
interface Настройки сетевого интерфейса	type	Тип сетевого интерфейса	add, get	add interface <interface_name> type <value> get interface <interface_name> type	WEP-2ac# add interface wlan1vap1 type service-set WEP-2ac# get interface wlan1vap1 type service-set

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	status	Состояние интерфейса	add, get, set	<pre>add interface &lt;interface_name&gt; status &lt;value&gt;  get interface &lt;interface_name&gt; status  set interface &lt;interface_name&gt; status &lt;value&gt;</pre>	<pre>WEP-2ac# add interface wlan1vap1 status up  WEP-2ac# set interface wlan1vap1 status up  WEP-2ac# get interface wlan1vap1 status up</pre>
	description	Описание интерфейса	get, set	<pre>get interface &lt;interface_name&gt; description  set interface &lt;interface_name&gt; description &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 description "Wireless - Virtual Access Point 1 - Radio 2"  WEP-2ac# get interface wlan1vap1 description Wireless - Virtual Access Point 1 - Radio 2</pre>
	ip	IP-адрес интерфейса	add, get	<pre>add interface &lt;interface_name&gt; ip &lt;value&gt;  get interface &lt;interface_name&gt; ip</pre>	<pre>WEP-2ac# get interface wlan1vap1 ip</pre>
	mask	Маска сети	add, get, set	<pre>add interface &lt;interface_name&gt; mask &lt;value&gt;  get interface &lt;interface_name&gt; mask  set interface &lt;interface_name&gt; mask &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 mask</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	static-ip	Статический IP-адрес, используемый, когда DHCP-сервер не активен	add, get, set	<pre>add interface &lt;interface_name&gt; static-ip  get interface &lt;interface_name&gt; static-ip  set interface &lt;interface_name&gt; static-ip &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 static- ip</pre>
	static-mask	Маска сети, используемая, когда DHCP-сервер не активен	add, get, set	<pre>add interface &lt;interface_name&gt; static-mask  get interface &lt;interface_name&gt; static-mask  set interface &lt;interface_name&gt; static-mask &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 static- mask</pre>
	rx-bytes	Количество полученных байтов	get	<pre>get interface &lt;interface_name&gt; rx-bytes</pre>	<pre>WEP-2ac# get interface wlan1vap1 rx-bytes 0</pre>
	rx-packets	Количество полученных пакетов	get	<pre>get interface &lt;interface_name&gt; rx-packets</pre>	<pre>WEP-2ac# get interface wlan1vap1 rx- packets 0</pre>
	rx-errors	Количество полученных пакетов с ошибками	get	<pre>get interface &lt;interface_name&gt; rx-errors</pre>	<pre>WEP-2ac# get interface wlan1vap1 rx- errors 0</pre>
	rx-drop	Количество полученных пакетов, которые были отброшены	get	<pre>get interface &lt;interface_name&gt; rx-drop</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	rx-fifo	Количество пакетов, полученное при переполнении буфера	get	get interface <interface_name> rx-fifo	WEP-2ac# get interface wlan1vap1 rx-fifo 0
	rx-frame	Количество пакетов, полученных с ошибкой кадра	get	get interface <interface_name> rx-frame	WEP-2ac# get interface wlan1vap1 rx-frame 0
	rx-compressed	Количество полученных сжатых пакетов	get	get interface <interface_name> rx-compressed	WEP-2ac# get interface wlan1vap1 rx-compressed 0
	rx-multicast	Количество полученных пакетов multicast	get	get interface <interface_name> rx-multicast	WEP-2ac# get interface wlan1vap1 rx-multicast 0
	tx-bytes	Количество отправленных байт	get	get interface <interface_name> tx-bytes	WEP-2ac# get interface wlan1vap1 tx-bytes 0
	tx-packets	Количество отправленных пакетов	get	get interface <interface_name> tx-packets	WEP-2ac# get interface wlan1vap1 tx-packets 0
	tx-errors	Количество отправленных пакетов с ошибками	get	get interface <interface_name> tx-errors	WEP-2ac# get interface wlan1vap1 tx-errors 0
	tx-fifo	Количество пакетов, отправленных при переполнении буфера	get	get interface <interface_name> tx-fifo	WEP-2ac# get interface wlan1vap1 tx-fifo 0
	tx-colls	Количество отправленных пакетов с коллизиями	get	get interface <interface_name> tx-colls	WEP-2ac# get interface wlan1vap1 tx-colls

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	tx-carrier	Количество отправленных пакетов с ошибками несущей	get	get interface <interface_name> tx-carrier	WEP-2ac# get interface wlan1vap1 tx- carrier
	tx-compressed	Количество отправленных сжатых пакетов	get	get interface <interface_name> tx-compressed	WEP-2ac# get interface wlan1vap1 tx- compressed
	tx-drop-bytes	Количество отброшенных Tx-байт	get	get interface <interface_name> tx-drop-bytes	WEP-2ac# get interface wlan1vap1 tx-drop- bytes
	rx-drop-bytes	Количество отброшенных Rx-байт	get	get interface <interface_name> rx-drop-bytes	WEP-2ac# get interface wlan1vap1 rx-drop- bytes
	tx-drop-packets	Количество отброшенных Tx-пакетов	get	get interface <interface_name> tx-drop-packets	WEP-2ac# get interface wlan1vap1 tx-drop- packets
	rx-drop-packets	Количество отброшенных Rx-пакетов	get	get interface <interface_name> rx-drop-packets	WEP-2ac# get interface wlan1vap1 rx-drop- packets
	stp	Spanning Tree Protocol	add, get, set	add interface <interface_name> stp <value>  get interface <interface_name> stp  set interface <interface_name> stp <value>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	fd	Задержка отправки	add, get, set	<pre>add interface &lt;interface_name&gt; fd &lt;value&gt;  get interface &lt;interface_name&gt; fd  set interface &lt;interface_name&gt; fd &lt;value&gt;</pre>	
	hello	Интервал hello	add, get, set	<pre>add interface &lt;interface_name&gt; hello &lt;value&gt;  get interface &lt;interface_name&gt; hello  set interface &lt;interface_name&gt; hello &lt;value&gt;</pre>	
	priority	Приоритет моста	add, get, set	<pre>add interface &lt;interface_name&gt; priority &lt;value&gt;  get interface &lt;interface_name&gt; priority  set interface &lt;interface_name&gt; priority &lt;value&gt;</pre>	
	port-isolation	Изоляция беспроводных портов друг от друга	add, get, set	<pre>add interface &lt;interface_name&gt; port-isolation &lt;value&gt;  get interface &lt;interface_name&gt; port-isolation  set interface &lt;interface_name&gt; port-isolation &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ssid	Имя сети	add, get, set	<pre>add interface &lt;interface_name&gt; ssid &lt;value&gt;  get interface &lt;interface_name&gt; ssid  set interface &lt;interface_name&gt; ssid &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan0vap1 ssid ___wep12_15-105</pre>
	bss	BSS, к которому принадлежит интерфейс	add, get, set	<pre>add interface &lt;interface_name&gt; bss &lt;value&gt;  get interface &lt;interface_name&gt; bss  set interface &lt;interface_name&gt; bss &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 bss wlan1bssvap1</pre>
	security	Режим безопасности	add, get, set	<pre>add interface &lt;interface_name&gt; security &lt;value&gt;  get interface &lt;interface_name&gt; security  set interface &lt;interface_name&gt; security &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 security plain-text</pre>
	wpa-personal-key	Персональный ключ WPA (совместное использование)	add, set	<pre>add interface &lt;interface_name&gt; wpa-personal-key &lt;value&gt;  get interface &lt;interface_name&gt; wpa-personal-key  set interface &lt;interface_name&gt; wpa-personal-key &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wep-key-ascii	Формат WEP-ключа: ascii или hex	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-ascii &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-ascii  set interface &lt;interface_name&gt; wep-key-ascii &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wep-key- ascii no</pre>
	wep-key-length	Длина WEP-ключа	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-length &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-length  set interface &lt;interface_name&gt; wep-key-length &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wep-key- length 104</pre>
	wep-default-key	WEP-ключ, используемый для передачи	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-length &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-length  set interface &lt;interface_name&gt; wep-key-length &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wep- default-key 1</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wep-key-1	WEP-ключ (1)	add, set	<pre>add interface &lt;interface_name&gt; wep-key-1 &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-1  set interface &lt;interface_name&gt; wep-key-1 &lt;value&gt;</pre>	
	wep-key-2	WEP-ключ (2)	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-2 &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-2  set interface &lt;interface_name&gt; wep-key-2 &lt;value&gt;</pre>	
	wep-key-3	WEP-ключ (3)	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-3 &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-3  set interface &lt;interface_name&gt; wep-key-3 &lt;value&gt;</pre>	
	wep-key-4	WEP-ключ (4)	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key-4 &lt;value&gt;  get interface &lt;interface_name&gt; wep-key-4  set interface &lt;interface_name&gt; wep-key-4 &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wep-key-mapping-length		get	get interface <interface_name> wep-key-mapping-length	WEP-2ac# get interface wlan1vap1 wep-key-mapping-length 400
	multicast-received-frame-count	Количество полученных кадров multicast	get	get interface <interface_name> multicast-received-frame-count	WEP-2ac# get interface wlan1vap1 multicast-received-frame-count
	vlan-id	ID, используемый в тегах	add, get	add interface <interface_name> vlan-id <value>  get interface <interface_name> vlan-id	WEP-2ac# get interface wlan1vap1 vlan-id
	radio	Радиоинтерфейс для WDS	add, get, set	add interface <interface_name> radio <value>  get interface <interface_name> radio  set interface <interface_name> radio <value>	WEP-2ac# get interface wlan1vap1 radio
	remote-mac	MAC-адрес конечной точки соединения WDS	add, get, set	add interface <interface_name> remote-mac <value>  get interface <interface_name> remote-mac  set interface <interface_name> remote-mac <value>	WEP-2ac# get interface wlan1vap1 remote-mac

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wep-key	WEP-ключ для соединения WDS	add, get, set	<pre>add interface &lt;interface_name&gt; wep-key &lt;value&gt;  get interface &lt;interface_name&gt; wep-key  set interface &lt;interface_name&gt; wep-key &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wep-key</pre>
	wds-ssid	SSID WDS-соединения	add, get, set	<pre>add interface &lt;interface_name&gt; wds-ssid &lt;value&gt;  get interface &lt;interface_name&gt; wds-ssid  set interface &lt;interface_name&gt; wds-ssid &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wds-ssid</pre>
	wds-security-policy	Политика безопасности для WDS-соединения	add, get, set	<pre>add interface &lt;interface_name&gt; wds-security-policy &lt;value&gt;  get interface &lt;interface_name&gt; wds-security-policy  set interface &lt;interface_name&gt; wds-security-policy &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wds-security-policy</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wds-wpa-psk-key	WPA PSK-ключ для WDS соединения	add, get, set	<pre>add interface &lt;interface_name&gt; wds-wpa-psk-key &lt;value&gt;  get interface &lt;interface_name&gt; wds-wpa-psk-key  set interface &lt;interface_name&gt; wds-wpa-psk-key &lt;value&gt;</pre>	<pre>WEP-2ac# get interface wlan1vap1 wds-wpa- psk-key</pre>
	interface	Интерфейс управления	get	<pre>get management interface</pre>	<pre>WEP-2ac# get management interface brtrunk</pre>
	static-ip	Статический IP-адрес интерфейса управления	get, set	<pre>get management static-ip  set management static-ip &lt;value&gt;</pre>	<pre>WEP-2ac# set management static- ip "192.168.1.10"  WEP-2ac# get management static- ip  192.168.1.10</pre>
	static-mask	Статическая маска интерфейса управления	get, set	<pre>get management static-mask  set management static-mask &lt;value&gt;</pre>	<pre>WEP-2ac# set management static- mask "255.255.255.0"  WEP-2ac# get management static- mask  255.255.255.0</pre>
	ip	IP-адрес интерфейса управления	get	<pre>get management ip</pre>	<pre>WEP-2ac# get management ip  192.168.15.105</pre>
	mask	Маска IP-адреса интерфейса управления	get	<pre>get management mask</pre>	<pre>WEP-2ac# get management mask  255.255.255.0</pre>
	mac	MAC-адрес интерфейса управления	get	<pre>get management mac</pre>	<pre>WEP-2ac# get management mac  A8:F9:4B:B0:21:60</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	dhcp-status	Включен ли DHCP на интерфейсе управления	get	get management dhcp-status	WEP-2ac# get management dhcp- status up
vap Настройка виртуальных точек доступа	radio	Радиоинтерфейс виртуальной точки доступа	get, set	get vap <vap> radio  set vap <vap> radio <value>	WEP-2ac# get vap vap1 radio radio ----- wlan0 wlan1
	status	Статус	get, set	get vap <vap> status  set vap <vap> status <value>	WEP-2ac# get vap vap1 status status ----- down down
	vlan-id	VLAN ID	add, get, set	add vap <vap> vlan-id <value>  get vap <vap> vlan-id  set vap <vap> vlan-id <value>	WEP-2ac# get vap vap1 vlan-id vlan-id ----- 1 1
	global-radius	Использование глобальных настроек RADIUS	get, set	get vap <vap> global radius  set vap <vap> global radius <value>	
	description	Описание виртуальной точки доступа	get, set	get vap <vap> description  set vap <vap> description <value>	WEP-2ac# get vap vap1 description description ----- ----- Virtual Access Point 1 Virtual Access Point 1 - Radio 2

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	qos-mode	Режим администрирования QoS	get, set	<pre>get vap &lt;vap&gt; qos-mode  set vap &lt;vap&gt; qos-mode &lt;value&gt;</pre>	<pre>WEP-2ac# get vap vap1 qos-mode qos-mode ----- up up</pre>
	def-bwmax-up	Максимальная пропускная способность в направлении upstream по умолчанию (0-4294967295)	get, set	<pre>get vap &lt;vap&gt; def-bwmax-up  set vap &lt;vap&gt; def-bwmax-up &lt;value&gt;</pre>	<pre>WEP-2ac# get vap vap1 def-bwmax-up def-bwmax-up ----- 0 0</pre>
	def-bwmax-down	Максимальная пропускная способность в направлении downstream по умолчанию (0-4294967295)	get, set	<pre>get vap &lt;vap&gt; def-bwmax-down  set vap &lt;vap&gt; def-bwmax-down &lt;value&gt;</pre>	<pre>WEP-2ac# get vap vap1 def-bwmax- down def-bwmax-down ----- 0 0</pre>
	def-acltype-up	Тип ACL для исходящих соединений по умолчанию (none/ipv4, Currently Unsupported:ipv6/mac)	get, set	<pre>get vap &lt;vap&gt; def-acltype-up  set vap &lt;vap&gt; def-acltype-up &lt;value&gt;</pre>	
	def-acltype-down	Тип ACL для входящих соединений по умолчанию (none/ipv4, Currently Unsupported:ipv6/mac)	get, set	<pre>get vap &lt;vap&gt; def-acltype-down  set vap &lt;vap&gt; def-acltype-down &lt;value&gt;</pre>	<pre>WEP-2ac# get vap vap1 def-acltype- up def-acltype-up ----- none none</pre>
	def-acl-up	ACL для исходящих соединений по умолчанию	get, set	<pre>get vap &lt;vap&gt; def-acl-up  set vap &lt;vap&gt; def-acl-up &lt;value&gt;</pre>	
	def-acl-down	ACL для входящих соединений по умолчанию	get, set	<pre>get vap &lt;vap&gt; def-acl-down  set vap &lt;vap&gt; def-acl-down &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	def-policy-up	Default Policy Up	get, set	get vap <vap> def-policy-up  set vap <vap> def-policy-up <value>	
	def-policy-down	Default Policy Down	get, set	get vap <vap> def-policy-down  set vap <vap> def-policy-down <value>	
global-radius-server  Глобальные настройки RADIUS-сервера	radius-accounting	Активация RADIUS Accounting	get, set	get global-radius-server radius-accounting  set global-radius-server radius-accounting <value>	WEP-2ac# set global-radius-server radius-accounting off  WEP-2ac# get global-radius-server radius-accounting off
	radius-ip	IP-адрес RADIUS-сервера	get, set	get global-radius-server radius-ip  set global-radius-server radius-ip <value>	WEP-2ac# set global-radius-server radius-ip "192.168.1.1"  WEP-2ac# get global-radius-server radius-ip 192.168.1.1
	radius-ip-network	IP-сеть RADIUS-сервера	get, set	get global-radius-server radius-ip-network  set global-radius-server radius-ip-network <value>	WEP-2ac# set global-radius-server radius-ip-network ipv4  WEP-2ac# get global-radius-server radius-ip-network ipv4

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	radius-key	Ключ подключения к RADIUS-серверу	set	<pre>get global- radius-server radius-key  set global- radius-server radius-key &lt;value&gt;</pre>	
	radius-nas-identifier	Опциональный идентификатор NAS для RADIUS Клиента	get, set	<pre>get global- radius-server radius-nas- identifier  set global- radius-server radius-nas- identifier &lt;value&gt;</pre>	
	description	Описание	get, set	<pre>get global- radius-server description  set global- radius-server description &lt;value&gt;</pre>	<pre>WEP-2ac# set global-radius- server description "Global radius server settings"  WEP-2ac# get global-radius- server description Global radius server settings</pre>
dot11 Поддержка стандартов IEEE 802.11	status	Статус	get, set	<pre>get dot11 status  set dot11 status &lt;value&gt;</pre>	<pre>WEP-2ac# set dot11 status up  WEP-2ac# get dot11 status up</pre>
radio Настройки радиointерфейсов	status	Статус	get, set	<pre>get radio &lt;radio_interface_n ame&gt; status  set radio &lt;radio_interface_n ame&gt; status &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 status up  WEP-2ac# get radio wlan0 status up</pre>
	description	Описание	get	<pre>get radio &lt;radio_interface_n ame&gt; description</pre>	<pre>WEP-2ac# get radio wlan0 description IEEE 802.11g</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	mac	MAC-адрес радиointерфейса (начальный)	get	get radio <radio_interface_name> mac	WEP-2ac# get radio wlan1 mac A8:F9:4B:B0:21:70
	static-mac	Статический MAC-адрес радиointерфейса (начальный)	get	get radio <radio_interface_name> static-mac	WEP-2ac# get radio wlan0 static-mac
	max-bss	Максимальное количество BSS/MAC-адресов	get	get radio <radio_interface_name> max-bss	WEP-2ac# set radio wlan0 max-bss 16  WEP-2ac# get radio wlan0 max-bss 16
	channel-policy	Политика выбора канала	get, set	get radio <radio_interface_name> channel-policy  set radio <radio_interface_name> channel-policy <value>	WEP-2ac# set radio wlan0 channel-policy best  WEP-2ac# get radio wlan0 channel-policy best
	mode	Режим беспроводного интерфейса	get, set	get radio <radio_interface_name> mode  set radio <radio_interface_name> mode <value>	WEP-2ac# set radio wlan1 mode "a-n-ac"  WEP-2ac# get radio wlan1 mode a-n-ac
	dot11h	Поддержка стандарта IEEE 802.11h	get, set	get radio <radio_interface_name> dot11h  set radio <radio_interface_name> dot11h <value>	WEP-2ac# set radio wlan0 dot11h off  WEP-2ac# get radio wlan0 dot11h off

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	dot11d	Поддержка стандарта IEEE 802.11d	get, set	<pre>get radio &lt;radio_interface_name&gt; dot11d  set radio &lt;radio_interface_name&gt; dot11d &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 dot11d off  WEP-2ac# get radio wlan0 dot11d off</pre>
	block-time	Время, в течение которого канал будет заблокирован после обнаружения радаром	get, set	<pre>get radio &lt;radio_interface_name&gt; block-time  set radio &lt;radio_interface_name&gt; block-time &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 block-time 31  WEP-2ac# get radio wlan1 block-time 31</pre>
	quiet-duration	Длительность quiet-интервала в TU	get, set	<pre>get radio &lt;radio_interface_name&gt; quiet-duration  set radio &lt;radio_interface_name&gt; quiet-duration &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 quiet-duration 0  WEP-2ac# get radio wlan0 quiet-duration 0</pre>
	quiet-period	Beacon-интервал между регулярными quiet-интервалами	get, set	<pre>get radio &lt;radio_interface_name&gt; quiet-period  set radio &lt;radio_interface_name&gt; quiet-period &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 quiet-period 0  WEP-2ac# get radio wlan1 quiet-period 0</pre>
	tx-mitigation	Снижать мощность передачи для станций (Transmit Power mitigation for stations)	get, set	<pre>get radio &lt;radio_interface_name&gt; tx-mitigation  set radio &lt;radio_interface_name&gt; tx-mitigation &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 tx-mitigation 3  WEP-2ac# get radio wlan0 tx-mitigation 3</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	static-channel	Канал, который будет использоваться при статической политике каналов (channel policy)	get, set	<pre>get radio &lt;radio_interface_name&gt; static-channel set radio &lt;radio_interface_name&gt; static-channel &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 static-channel 1  WEP-2ac# get radio wlan0 static-channel 1</pre>
	channel	Используемый канал	get	<pre>get radio &lt;radio_interface_name&gt; channel</pre>	<pre>WEP-2ac# get radio wlan0 channel 11</pre>
	tx-power-dbm	Мощность передачи	get, set	<pre>get radio &lt;radio_interface_name&gt; tx-power-dbm set radio &lt;radio_interface_name&gt; tx-power-dbm &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 tx-power-dbm 5  WEP-2ac# get radio wlan0 tx-power-dbm 5</pre>
	tx-power-dbm-max	Максимальная мощность передачи	get	<pre>get radio &lt;radio_interface_name&gt; tx-power-dbm-max</pre>	<pre>WEP-2ac# get radio wlan0 tx-power-dbm-max 19</pre>
	tx-power-output	Последняя установленная мощность (Last est. power from wl_curpower)	get	<pre>get radio &lt;radio_interface_name&gt; tx-power-output</pre>	<pre>WEP-2ac# get radio wlan0 tx-power-output 5.00</pre>
	tpc	IEEE 802.11h TPC	get, set	<pre>get radio &lt;radio_interface_name&gt; tpc set radio &lt;radio_interface_name&gt; tpc &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 tpc off  WEP-2ac# get radio wlan0 tpc off</pre>
	atf	Airtime Fairness	get, set	<pre>get radio &lt;radio_interface_name&gt; atf set radio &lt;radio_interface_name&gt; atf &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 atf on  WEP-2ac# get radio wlan1 atf on</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ampdu_atf_us	ampdu_atf_us	get, set	<pre>get radio &lt;radio_interface_name&gt; ampdu_atf_us  set radio &lt;radio_interface_name&gt; ampdu_atf_us &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 ampdu_atf_us 4000  WEP-2ac# get radio wlan1 ampdu_atf_us 4000</pre>
	ampdu_atf_min_us	ampdu_atf_min_us	get, set	<pre>get radio &lt;radio_interface_name&gt; ampdu_atf_min_us  set radio &lt;radio_interface_name&gt; ampdu_atf_min_us &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 ampdu_atf_min_us 1000  WEP-2ac# get radio wlan1 ampdu_atf_min_us 1000</pre>
	tx-chain	Конфигурация антенны	get, set	<pre>get radio &lt;radio_interface_name&gt; tx-chain  set radio &lt;radio_interface_name&gt; tx-chain &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan1 tx-chain 7  WEP-2ac# get radio wlan1 tx-chain 7</pre>
	antenna	Использовать антенну	get, set	<pre>get radio &lt;radio_interface_name&gt; antenna  set radio &lt;radio_interface_name&gt; antenna &lt;value&gt;</pre>	
	tx-rx-status	Статус приема и передачи на радиointерфейсе	get, set	<pre>get radio &lt;radio_interface_name&gt; tx-rx-status  set radio &lt;radio_interface_name&gt; tx-rx-status &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 tx-rx-status up  WEP-2ac# get radio wlan0 tx-rx-status up</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	beacon-interval	Beacon-интервал	get, set	<pre>get radio &lt;radio_interface_name&gt; beacon-interval  set radio &lt;radio_interface_name&gt; beacon-interval &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 beacon-interval 100  WEP-2ac# get radio wlan0 beacon-interval 100</pre>
	rts-threshold	Минимальный размер пакета, при котором будет использован Request-To-Send	get, set	<pre>get radio &lt;radio_interface_name&gt; rts-threshold  set radio &lt;radio_interface_name&gt; rts-threshold &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 rts- threshold 2347  WEP-2ac# get radio wlan0 rts- threshold 2347</pre>
	fragmentation-threshold	Минимальный размер пакета, при котором будет использована фрагментация	get, set	<pre>get radio &lt;radio_interface_name&gt; fragmentation- threshold  set radio &lt;radio_interface_name&gt; fragmentation- threshold &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 fragmentation- threshold 2346  WEP-2ac# get radio wlan0 fragmentation- threshold 2346</pre>
	load-balance-no-association-utilization	Utilization required to prevent new associations	get, set	<pre>get radio &lt;radio_interface_name&gt; load-balance- no-association- utilization  set radio &lt;radio_interface_name&gt; load-balance- no-association- utilization &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 load- balance-no- association- utilization 0  WEP-2ac# get radio wlan0 load- balance-no- association- utilization 0</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ap-detection	Включение детектора точек доступа	get, set	<pre>get radio &lt;radio_interface_name&gt; ap-detection  set radio &lt;radio_interface_name&gt; ap-detection &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 ap- detection on  WEP-2ac# get radio wlan0 ap- detection on</pre>
	sentry-mode	Включение режима sentry	get, set	<pre>get radio &lt;radio_interface_name&gt; sentry-mode  set radio &lt;radio_interface_name&gt; sentry-mode &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 sentry-mode off  WEP-2ac# get radio wlan0 sentry-mode off</pre>
	dedicated-spectrum-mode	Включение режима Dedicated Spectrum	get, set	<pre>get radio &lt;radio_interface_name&gt; dedicated- spectrum-mode  set radio &lt;radio_interface_name&gt; dedicated- spectrum-mode &lt;value&gt;</pre>	
	channel-hopping	Переключение каналов	get, set	<pre>get radio &lt;radio_interface_name&gt; channel- hopping  set radio &lt;radio_interface_name&gt; channel- hopping &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 channel-hopping on  WEP-2ac# get radio wlan0 channel-hopping on</pre>
	passive-scan-mode	Сканирование в одной полосе или в обеих полосах в режиме sentry	get, set	<pre>get radio &lt;radio_interface_name&gt; passive-scan- mode  set radio &lt;radio_interface_name&gt; passive-scan- mode &lt;value&gt;</pre>	<pre>WEP-2ac# get radio wlan0 passive-scan-mode</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	scan-leave-time	Интервалы между сканированиями	get, set	<pre>get radio &lt;radio_interface_name&gt; scan-leave-time  set radio &lt;radio_interface_name&gt; scan-leave-time &lt;value&gt;</pre>	<pre>WEP-2ac# get radio wlan0 scan-leave-time</pre>
	scan-duration	Длительность сканирования радиочастот в канале, в мс	get, set	<pre>get radio &lt;radio_interface_name&gt; scan-duration  set radio &lt;radio_interface_name&gt; scan-duration &lt;value&gt;</pre>	<pre>WEP-2ac# get radio wlan0 scan-duration</pre>
	limit-channel-selection	Ограничение каналов 802.11a	get, set	<pre>get radio &lt;radio_interface_name&gt; limit-channel-selection  set radio &lt;radio_interface_name&gt; limit-channel-selection &lt;value&gt;</pre>	<pre>WEP-2ac# get radio wlan0 limit-channel-selection</pre>
	data-snooping	Активировать snooping	get, set	<pre>get radio &lt;radio_interface_name&gt; data-snooping  set radio &lt;radio_interface_name&gt; data-snooping &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 data-snooping off  WEP-2ac# get radio wlan0 data-snooping off</pre>
	n-bandwidth	Пропускная способность каналов 802.11n (20/40)	get, set	<pre>get radio &lt;radio_interface_name&gt; n-bandwidth  set radio &lt;radio_interface_name&gt; n-bandwidth &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 n-bandwidth 20  WEP-2ac# get radio wlan0 n-bandwidth 20</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	n-primary-channel	Расположение основного канала 802.11n (lower/upper)	get, set	<pre>get radio &lt;radio_interface_name&gt; n-primary-channel  set radio &lt;radio_interface_name&gt; n-primary-channel &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 n- primary-channel lower  WEP-2ac# get radio wlan0 n- primary-channel lower</pre>
	protection	Режим защиты для 802.11g и 802.11n (auto/off)	get, set	<pre>get radio &lt;radio_interface_name&gt; protection  set radio &lt;radio_interface_name&gt; protection &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 protection auto  WEP-2ac# get radio wlan0 protection auto</pre>
	frequency	Используемая частота в МГц	get	<pre>get radio &lt;radio_interface_name&gt; frequency</pre>	<pre>WEP-2ac# get radio wlan0 frequency 2462</pre>
	wme	Включить WME	get, set	<pre>get radio &lt;radio_interface_name&gt; wme  set radio &lt;radio_interface_name&gt; wme &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 wme on  WEP-2ac# get radio wlan0 wme on</pre>
	wme-noack	Включить WME "No Acknowledgement"	get, set	<pre>get radio &lt;radio_interface_name&gt; wme-noack  set radio &lt;radio_interface_name&gt; wme-noack &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 wme- noack off  WEP-2ac# get radio wlan0 wme- noack off</pre>
	wme-apsd	Включить WME APSD	get, set	<pre>get radio &lt;radio_interface_name&gt; wme-apsd  set radio &lt;radio_interface_name&gt; wme-apsd &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 wme- apsd on  WEP-2ac# get radio wlan0 wme- apsd on</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	rate-limit-enable	Включить ограничение скорости broadcast/multicast трафика	get, set	<pre>get radio &lt;radio_interface_name&gt; rate-limit-enable set radio &lt;radio_interface_name&gt; rate-limit-enable &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 rate-limit-enable off WEP-2ac# get radio wlan0 rate-limit-enable off</pre>
	rate-limit	Ограничение скорости broadcast/multicast-трафика (пакетов в секунду)	get, set	<pre>get radio &lt;radio_interface_name&gt; rate-limit set radio &lt;radio_interface_name&gt; rate-limit &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 rate-limit 50 WEP-2ac# get radio wlan0 rate-limit 50</pre>
	rate-limit-burst	Значение burst для broadcast/multicast-трафика (пакеты в секунду)	get, set	<pre>get radio &lt;radio_interface_name&gt; rate-limit-burst set radio &lt;radio_interface_name&gt; rate-limit-burst &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 rate-limit-burst 75 WEP-2ac# get radio wlan0 rate-limit-burst 75</pre>
	stp-block-enable	Блокировать все STP-пакеты на радиоинтерфейсе	get, set	<pre>get radio &lt;radio_interface_name&gt; stp-block-enable set radio &lt;radio_interface_name&gt; stp-block-enable &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 stp-block-enable on WEP-2ac# get radio wlan0 stp-block-enable on</pre>
	wlan-util	Использование беспроводной LAN	get	<pre>get radio &lt;radio_interface_name&gt; wlan-util</pre>	<pre>WEP-2ac# get radio wlan0 wlan-util 74</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	fixed-multicast-rate	Фиксированная скорость для Multicast-трафика для полосы	get, set	<pre>get radio &lt;radio_interface_name&gt; fixed-multicast-rate  set radio &lt;radio_interface_name&gt; fixed-multicast-rate &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 fixed-multicast-rate auto  WEP-2ac# get radio wlan0 fixed-multicast-rate auto</pre>
	fixed-tx-modulation	Фиксированная модуляция для полосы	get, set	<pre>get radio &lt;radio_interface_name&gt; fixed-tx-modulation  set radio &lt;radio_interface_name&gt; fixed-tx-modulation &lt;value&gt;</pre>	<pre>WEP-2ac# set radio wlan0 fixed-tx-modulation auto  WEP-2ac# get radio wlan0 fixed-tx-modulation auto</pre>
	antenna-diversity	Разнесение антенн	get, set	<pre>get radio &lt;radio_interface_name&gt; antenna-diversity  set radio &lt;radio_interface_name&gt; antenna-diversity &lt;value&gt;</pre>	
	antenna-selection	Номер используемой антенны	get, set	<pre>get radio &lt;radio_interface_name&gt; antenna-selection  set radio &lt;radio_interface_name&gt; antenna-selection &lt;value&gt;</pre>	
bss Базовая зона обслуживания (BSS)	status	Статус	add, get, set	<pre>add bss &lt;bss_id&gt; status &lt;value&gt;  get bss &lt;bss_id&gt; status  set bss &lt;bss_id&gt; status &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 status up  WEP-2ac# get bss wlan0bssvap1 status  up</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	description	Описание	get, set	<pre>get bss &lt;bss_id&gt; description set bss &lt;bss_id&gt; description &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 description Virtual Access Point 1  WEP-2ac# get bss wlan0bssvap1 description Virtual Access Point 1</pre>
	radio	Радиоинтерфейс данного BSS	add, get, set	<pre>add bss &lt;bss_id&gt; radio &lt;value&gt;  get bss &lt;bss_id&gt; radio  set bss &lt;bss_id&gt; radio &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radio wlan0  WEP-2ac# get bss wlan0bssvap1 radio wlan0</pre>
	beacon-interface	Интерфейс BSS, используемый для beacon	add, get, set	<pre>add bss &lt;bss_id&gt; beacon-interface &lt;value&gt;  get bss &lt;bss_id&gt; beacon-interface  set bss &lt;bss_id&gt; beacon-interface &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 beacon-interface wlan0vap1  WEP-2ac# get bss wlan0bssvap1 beacon-interface wlan0vap1</pre>
	mac	MAC-адрес	add, get	<pre>add bss &lt;bss_id&gt; mac &lt;value&gt;  get bss &lt;bss_id&gt; mac</pre>	<pre>WEP-2ac# get bss wlan0bssvap1 mac  A8:F9:4B:B0:21:61</pre>
	dtim-period	Интервал DTIM	add, get, set	<pre>add bss &lt;bss_id&gt; dtim-period &lt;value&gt;  get bss &lt;bss_id&gt; dtim-period  set bss &lt;bss_id&gt; dtim-period &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	max-stations	Максимальное число станций	add, get, set	<pre>add bss &lt;bss_id&gt; max-stations &lt;value&gt;  get bss &lt;bss_id&gt; max-stations  set bss &lt;bss_id&gt; max-stations &lt;value&gt;</pre>	
	ignore-broadcast-ssid	Не отправлять SSID в beacon и игнорировать пробные запросы	add, get, set	<pre>add bss &lt;bss_id&gt; max-stations &lt;value&gt;  get bss &lt;bss_id&gt; max-stations  set bss &lt;bss_id&gt; max-stations &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 ignore-broadcast- ssid off  WEP-2ac# get bss wlan0bssvap1 ignore-broadcast- ssid off</pre>
	station-isolation	Изоляция станции	add, get, set	<pre>add bss &lt;bss_id&gt; max-stations &lt;value&gt;  get bss &lt;bss_id&gt; max-stations  set bss &lt;bss_id&gt; max-stations &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 station-isolation off  WEP-2ac# get bss wlan0bssvap1 station-isolation off</pre>
	tagged-sta-mode	Включить/выключить тегирование трафика от/к STA	add, get, set	<pre>add bss &lt;bss_id&gt; tagged-sta-mode &lt;value&gt;  get bss &lt;bss_id&gt; tagged-sta-mode  set bss &lt;bss_id&gt; tagged-sta-mode &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 tagged-sta-mode off  WEP-2ac# get bss wlan0bssvap1 tagged-sta-mode off</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	mac-acl-mode	Список MAC-адресов	add, get, set	<pre>add bss &lt;bss_id&gt; mac-acl-mode &lt;value&gt;  get bss &lt;bss_id&gt; mac-acl-mode  set bss &lt;bss_id&gt; mac-acl-mode &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 mac- acl-mode deny-list  WEP-2ac# get bss wlan0bssvap1 mac- acl-mode deny-list</pre>
	mac-acl-name	Имя списка MAC-адресов	add, get, set	<pre>add bss &lt;bss_id&gt; mac-acl-name &lt;value&gt;  get bss &lt;bss_id&gt; mac-acl-name  set bss &lt;bss_id&gt; mac-acl-name &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 mac- acl-name default  WEP-2ac# get bss wlan0bssvap1 mac- acl-name default</pre>
	mac-acl-auth-type	Тип аутентификации MAC-адресов	add, get, set	<pre>add bss &lt;bss_id&gt; mac-acl-auth-type &lt;value&gt;  get bss &lt;bss_id&gt; mac-acl-auth-type  set bss &lt;bss_id&gt; mac-acl-auth-type &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 mac- acl-auth-type disable  WEP-2ac# get bss wlan0bssvap1 mac- acl-auth-type disable</pre>
	radius-accounting	Авторизация на RADIUS-сервере	add, get, set	<pre>add bss &lt;bss_id&gt; radius-accounting &lt;value&gt;  get bss &lt;bss_id&gt; radius-accounting  set bss &lt;bss_id&gt; radius-accounting &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radius-accounting on  WEP-2ac# get bss wlan0bssvap1 radius-accounting on</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	radius-ip	IP-адрес RADIUS-сервера	add, get, set	<pre>add bss &lt;bss_id&gt; radius-ip &lt;value&gt;  get bss &lt;bss_id&gt; radius-ip  set bss &lt;bss_id&gt; radius-ip &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radius-ip "192.168.42.220"  WEP-2ac# get bss wlan0bssvap1 radius-ip 192.168.42.220</pre>
	radius-ip-network	IP-сеть RADIUS-сервера	add, get, set	<pre>add bss &lt;bss_id&gt; radius-ip-network &lt;value&gt;  get bss &lt;bss_id&gt; radius-ip-network  set bss &lt;bss_id&gt; radius-ip-network &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radius-ip-network ipv4  WEP-2ac# get bss wlan0bssvap1 radius-ip-network ipv4</pre>
	radius-key	Ключ для связи с RADIUS-сервером	add, set	<pre>add bss &lt;bss_id&gt; radius-key &lt;value&gt;  get bss &lt;bss_id&gt; radius-key  set bss &lt;bss_id&gt; radius-key &lt;value&gt;</pre>	
	radius-port	Порт для аутентификации на сервере RADIUS	add, get, set	<pre>add bss &lt;bss_id&gt; radius-port &lt;value&gt;  get bss &lt;bss_id&gt; radius-port  set bss &lt;bss_id&gt; radius-port &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radius-port 1812port  WEP-2ac# get bss wlan0bssvap1 radius-port 1812port</pre>
	radius-accounting-port	Порт для аккаунтинга на RADIUS-сервере	add, get, set	<pre>add bss &lt;bss_id&gt; radius-accounting- port &lt;value&gt;  get bss &lt;bss_id&gt; radius-accounting- port  set bss &lt;bss_id&gt; radius-accounting- port &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 radius-accounting- port 1813  WEP-2ac# get bss wlan0bssvap1 radius-accounting- port 1813</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	vlan-tagged-interface	Добавить динамические VLAN на интерфейс	add, get, set	<pre>add bss &lt;bss_id&gt; vlan-tagged-interface &lt;value&gt;  get bss &lt;bss_id&gt; vlan-tagged-interface  set bss &lt;bss_id&gt; vlan-tagged-interface &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 vlan- tagged-interface brtrunk  WEP-2ac# get bss wlan0bssvap1 vlan- tagged-interface brtrunk</pre>
	open-system-authentication	Разрешена ли аутентификация Open System	add, get, set	<pre>add bss &lt;bss_id&gt; open-system-authentication &lt;value&gt;  get bss &lt;bss_id&gt; open-system-authentication  set bss &lt;bss_id&gt; open-system-authentication &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 open- system- authentication on  WEP-2ac# get bss wlan0bssvap1 open- system- authentication on</pre>
	shared-key-authentication	Разрешена ли аутентификация Shared key	add, get, set	<pre>add bss &lt;bss_id&gt; shared-key-authentication &lt;value&gt;  get bss &lt;bss_id&gt; shared-key-authentication  set bss &lt;bss_id&gt; open-system-authentication &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 shared-key- authentication off  WEP-2ac# get bss wlan0bssvap1 shared-key- authentication off</pre>
	wpa-cipher-tkip	Использование TKIP как метода шифрования WPA	add, get, set	<pre>add bss &lt;bss_id&gt; wpa-cipher-tkip &lt;value&gt;  get bss &lt;bss_id&gt; wpa-cipher-tkip  set bss &lt;bss_id&gt; wpa-cipher-tkip &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 wpa- cipher-tkip on  WEP-2ac# get bss wlan0bssvap1 wpa- cipher-tkip on</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wpa-cipher-ccmp	Использование ССМР как метода шифрования WPA	add, get, set	<pre>add bss &lt;bss_id&gt; wpa-cipher-ccmp &lt;value&gt;  get bss &lt;bss_id&gt; wpa-cipher-ccmp  set bss &lt;bss_id&gt; wpa-cipher-ccmp &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 wpa- cipher-ccmp on  WEP-2ac# get bss wlan0bssvap1 wpa- cipher-ccmp on</pre>
	wpa-allowed	Разрешить WPA	add, get, set	<pre>add bss &lt;bss_id&gt; wpa-allowed &lt;value&gt;  get bss &lt;bss_id&gt; wpa-allowed  set bss &lt;bss_id&gt; wpa-allowed &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 wpa- allowed on  WEP-2ac# get bss wlan0bssvap1 wpa- allowed on</pre>
	wpa2-allowed	Разрешить WPA2	add, get, set	<pre>add bss &lt;bss_id&gt; wpa2-allowed &lt;value&gt;  get bss &lt;bss_id&gt; wpa2-allowed  set bss &lt;bss_id&gt; wpa2-allowed &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 wpa2- allowed on  WEP-2ac# get bss wlan0bssvap1 wpa2- allowed on</pre>
	rsn-preauthentication	Разрешить предварительную аутентификацию RSN	add, get, set	<pre>add bss &lt;bss_id&gt; rsn- preauthentication &lt;value&gt;  get bss &lt;bss_id&gt; rsn- preauthentication  set bss &lt;bss_id&gt; rsn- preauthentication &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 rsn- preauthentication off  WEP-2ac# get bss wlan0bssvap1 rsn- preauthentication off</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	broadcast-key-refresh-rate	Команда устанавливает интервал, через который происходит смена паролей доступа у пользователей (broadcasting key)	add, get, set	<pre>add bss &lt;bss_id&gt; rsn- preauthentication &lt;value&gt;  get bss &lt;bss_id&gt; rsn- preauthentication  set bss &lt;bss_id&gt; rsn- preauthentication &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 broadcast-key- refresh-rate 0  WEP-2ac# get bss wlan0bssvap1 broadcast-key- refresh-rate 0</pre>
	check-signal-timeout	Timeout check min signal (sec)	add, get, set	<pre>add bss &lt;bss_id&gt; check-signal- timeout &lt;value&gt;  get bss &lt;bss_id&gt; check-signal- timeout  set bss &lt;bss_id&gt; check-signal- timeout &lt;value&gt;</pre>	<pre>WEP-2ac# set bss wlan0bssvap1 check-signal- timeout 10  WEP-2ac# get bss wlan0bssvap1 check-signal- timeout 10</pre>
	wlan-util	Использование беспроводной LAN	add, get, set	<pre>add bss &lt;bss_id&gt; wlan-util &lt;value&gt;  get bss &lt;bss_id&gt; wlan-util  set bss &lt;bss_id&gt; wlan-util &lt;value&gt;</pre>	
	fixed-multicast-rate	Фиксированная скорость полосы для Multicast-трафика	add, get, set	<pre>add bss &lt;bss_id&gt; fixed-multicast- rate &lt;value&gt;  get bss &lt;bss_id&gt; fixed-multicast- rate  set bss &lt;bss_id&gt; fixed-multicast- rate &lt;value&gt;</pre>	
bridge-port Порт моста		Введите команду "get bridge-port" и получите все доступные для просмотра характеристики интерфейса моста или используйте команды, представленные ниже			

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	interface	Интерфейс моста	add, get	<pre>add bridge-port &lt;all brtrunk&gt; interface &lt;value&gt;  get bridge-port &lt;all brtrunk&gt; interface</pre>	<pre>WEP-2ac# get bridge-port brtrunk interface interface ----- eth0 wlan0wds0 wlan0wds1 wlan0wds2 wlan0wds3 wlan0wds4 wlan0wds5 wlan0wds6 wlan0wds7 wlan0 wlan0vap1 wlan0vap2</pre>
	path-cost	Стоимость интерфейса	add, get, set	<pre>add bridge-port &lt;all brtrunk&gt; path-cost &lt;value&gt;  get bridge-port &lt;all brtrunk&gt; path-cost  set bridge-port &lt;all brtrunk&gt; path-cost &lt;value&gt;</pre>	
	priority	Приоритет порта	add, get, set	<pre>add bridge-port &lt;all brtrunk&gt; priority &lt;value&gt;  get bridge-port &lt;all brtrunk&gt; priority  set bridge-port &lt;all brtrunk&gt; priority &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	stp-state	Состояние связующего дерева	get	get bridge-port <all brtrunk> stp-state	WEP-2ac# get bridge-port brtrunk stp-state stp-state ----- forwarding  forwarding forwarding forwarding forwarding forwarding
mac-acl Элементы таблицы MAC- адресов	mac	Разрешить/ запретить MAC- адрес	add, get, set	add mac-acl <value>  get mac-acl  set mac-acl <value>	
tx-queue Передача параметров очередей		Введите команду "get tx-queue <interface_name all>" и получите все доступные для просмотра характеристики интерфейса моста или используйте команды, представленные ниже		get tx-queue <interface_name  all>	WEP-2ac# get tx- queue all name queue aifs cwmin cwmax burst ----- ----- ----- wlan0 data0 1 3 7 1.5 wlan0 data1 1 7 15 3.0 wlan0 data2 3 15 63 0 wlan0 data3 7 15 1023 0 wlan1 data0 1 3 7 1.5 wlan1 data1 1 7 15 3.0 wlan1 data2 3 15 63 0 wlan1 data3 7 15 1023 0

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	queue	Имя очереди	get	<pre>get tx-queue &lt;interface_name  all&gt; queue</pre>	<pre>WEP-2ac# get tx- queue all queue name queue ----- wlan0 data0 wlan0 data1 wlan0 data2 wlan0 data3 wlan1 data0 wlan1 data1 wlan1 data2 wlan1 data3</pre>
	aifs	Адаптивный межкадровый интервал	get, set	<pre>get tx-queue &lt;interface_name  all&gt; aifs  set tx-queue &lt;interface_name  all&gt; aifs &lt;value&gt;</pre>	<pre>WEP-2ac# get tx- queue wlan0 aifs aifs ---- 1 1 3 7</pre>
	cwmin	Минимальное значение конкурентного окна	get, set	<pre>get tx-queue &lt;interface_name  all&gt; cwmin  set tx-queue &lt;interface_name  all&gt; cwmin &lt;value&gt;</pre>	<pre>WEP-2ac# get tx- queue wlan0 cwmin cwmin ----- 3 7 15 15</pre>
	cwmax	Максимальное значение конкурентного окна	get, set	<pre>get tx-queue &lt;interface_name  all&gt; cwmax  set tx-queue &lt;interface_name  all&gt; cwmax &lt;value&gt;</pre>	<pre>WEP-2ac# get tx- queue wlan0 cwmax cwmax ----- 7 15 63 1023</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	burst	Максимальная длина очереди	get, set	<pre>get tx-queue &lt;interface_name  all&gt; burst  set tx-queue &lt;interface_name  all&gt; burst &lt;value&gt;</pre>	<pre>WEP-2ac# get tx- queue wlan0 burst burst ----- 1.5 3.0 0 0</pre>
wme-queue Передача параметров очередей станциям		Введите команду "get wme-queue <interface_name  all>" и получите все доступные для просмотра характеристики интерфейса моста или используйте команды, представленные ниже		<pre>get wme-queue &lt;interface_name  all&gt;</pre>	<pre>WEP-2ac# get wme- queue all name queue aifs cwmn cwmmax txop- limit ----- ----- ----- wlan0 vo 2 3 7 47 wlan0 vi 2 7 15 94 wlan0 be 3 15 1023 0 wlan0 bk 7 15 1023 0 wlan1 vo 2 3 7 47 wlan1 vi 2 7 15 94 wlan1 be 3 15 1023 0 wlan1 bk 7 15 1023 0</pre>
	queue	Имя очереди	get	<pre>get wme-queue &lt;interface_name  all&gt; queue</pre>	<pre>WEP-2ac# get wme- queue all queue name queue ----- wlan0 vo wlan0 vi wlan0 be wlan0 bk wlan1 vo wlan1 vi wlan1 be wlan1 bk</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	aifs	Адаптивный межкадровый интервал	get, set	<pre>get wme-queue &lt;interface_name  all&gt; aifs  get wme-queue &lt;interface_name  all&gt; aifs &lt;value&gt;</pre>	<pre>WEP-2ac# get wme- queue wlan0 aifs aifs ---- 2 2 3 7</pre>
	cwmin	Минимальное значение конкурентного окна	get, set	<pre>get wme-queue &lt;interface_name  all&gt; cwmin  get wme-queue &lt;interface_name  all&gt; cwmin &lt;value&gt;</pre>	<pre>WEP-2ac# get wme- queue wlan0 cwmin cwmin ----- 3 7 15 15</pre>
	cwmax	Максимальное значение конкурентного окна	get, set	<pre>get wme-queue &lt;interface_name  all&gt; cwmax  get wme-queue &lt;interface_name  all&gt; cwmax &lt;value&gt;</pre>	<pre>WEP-2ac# get wme- queue wlan0 cwmax cwmax ----- 7 15 1023 1023</pre>
	burst	Максимальная длина очереди	get, set		
	txop-limit	Ограничение возможности передачи	get, set	<pre>get wme-queue &lt;interface_name  all&gt; txop-limit  set wme-queue &lt;interface_name  all&gt; txop-limit &lt;value&gt;</pre>	<pre>WEP-2ac# get wme- queue wlan0 txop- limit txop-limit ----- 47 94 0 0</pre>
static-ip-route Static IP route entry	destination	Префикс IP-адреса назначения	get	<pre>get static-ip- route destination</pre>	<pre>WEP-2ac# get static-ip-route destination 0.0.0.0</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	mask	Маска подсети	get	get static-ip-route mask	WEP-2ac# get static-ip-route mask 0.0.0.0
	gateway	IP-адрес маршрута	get	get static-ip-route gateway	WEP-2ac# get static-ip-route gateway 192.168.1.254
	table	Номер в таблице маршрутизации	get	get static-ip-route table	WEP-2ac# get static-ip-route table 254
ip-route IP route entry	destination	Префикс IP-адреса назначения	get	get ip-route destination	WEP-2ac# get ip-route destination 0.0.0.0
	mask	Маска подсети	get	get ip-route mask	WEP-2ac# get ip-route mask 0.0.0.0
	gateway	IP-адрес маршрута	get	get ip-route gateway	WEP-2ac# get ip-route gateway 192.168.15.1
	table	Номер в таблице маршрутизации	get	get ip-route table	WEP-2ac# get ip-route table 254
log Настройка логирования	depth	Количество записей, которое может быть внесено в журнал	get, set	get log depth set log depth <value>	WEP-2ac# set log depth 512 WEP-2ac# get log depth 512
	persistence	Сохранять журнал в энергонезависимую память	get, set	get log persistence set log persistence <value>	WEP-2ac# set log persistence no WEP-2ac# get log persistence no

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	severity	Установить уровень важности сохраненной записи	get, set	get log severity set log severity <value>	WEP-2ac# set log severity 7 WEP-2ac# get log severity 7
	remove	Удалить все записи в журнале	set	set log remove	
	relay-enabled	Активировать передачу системного журнала (syslog)	get, set	get log relay-enabled set log relay-enabled <value>	WEP-2ac# set log relay-enabled 0 WEP-2ac# get log relay-enabled 0
	relay-host	Хост, на который будет передаваться системный журнал	get, set	get log relay-host set log relay-host <value>	
	relay-port	Порт, на который будет передаваться системный журнал	get, set	get log relay-port set log relay-port <value>	WEP-2ac# set log relay-port 514 WEP-2ac# get log relay-port 514
log-entry Запись в журнале	number	Номер записи	get	get log-entry number	WEP-2ac# get log-entry number ----- 1 2 3 4 5
	priority	Приоритет записи	get	get log-entry priority	WEP-2ac# get log-entry priority ----- err info info err err info

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	time	Время записи	get	get log-entry time	WEP-2ac# get log- entry time time ----- --- Oct 11 2018 00:00:19 Oct 11 2018 00:00:18 Oct 11 2018 00:00:16 Oct 11 2018 00:00:12
	daemon	daemon	get	get log-entry daemon	WEP-2ac# get log- entry daemon daemon ----- dnzd[28523] dman[1239] dman[1239] dnzd[28410] dnzd[18233]
	message	Сообщение	get	get log-entry message	WEP-2ac# get log- entry message Property Value ----- ----- ----- message accepting UDP packets on 0.0.0.0:4553
association Связанные станции	interface	Интерфейс станции связан с (Interface station is associated with)	get	get association interface	
	station	MAC-адрес станции	get	get association station	
	authenticated	Пройдена ли аутентификация	get	get association authenticated	
	associated	Associated	get	get association associated	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	rx-packets	Получено от станции (пакеты)	get	get association rx-packets	
	tx-packets	Передано станции (пакеты)	get	get association tx-packets	
	rx-bytes	Получено от станции (байт)	get	get association rx-bytes	
	tx-bytes	Передано станции (байт)	get	get association tx-bytes	
	tx-rate	Скорость передачи	get	get association tx-rate	
	rx-rate	Скорость приема	get	get association rx-rate	
	listen-interval	Listen-интервал	get	get association listen-interval	
	last-rssi	Полученный в последнем кадре RSSI	get	get association last-rssi	
	tx-drop-bytes	Количество отброшенных байт при передаче станции	get	get association tx-drop-bytes	
	rx-drop-bytes	Количество отброшенных байт при приеме от станции	get	get association rx-drop-bytes	
	tx-drop-packets	Количество отброшенных пакетов при передаче станции	get	get association tx-drop-packets	
	rx-drop-packets	Количество отброшенных пакетов при приеме от станции	get	get association rx-drop-packets	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
basic-rate Основные скорости радиointерфейсов	rate	Скорость 0.5 Мбит/с	add, get, remove	<pre>add basic-rate &lt;interface_id all&gt; rate &lt;value&gt;  get basic-rate &lt;interface_id all&gt; rate  remove basic-rate &lt;interface_id all&gt; rate &lt;value&gt;</pre>	<pre>WEP-2ac# get basic-rate all rate name rate ----- wlan1 24 wlan1 12 wlan1 6 wlan0 11 wlan0 5.5 wlan0 2 wlan0 1</pre>
supported-rate Поддерживаемые скорости радиointерфейсов	rate	Скорость 0.5 Мбит/с	add, get, remove	<pre>add supported- rate &lt;interface_id all&gt; rate &lt;value&gt;  get supported- rate &lt;interface_id all&gt; rate  remove supported- rate &lt;interface_id all&gt; rate &lt;value&gt;</pre>	<pre>WEP-2ac# get supported-rate wlan0 rate rate ---- 54 48 36 24 18 12 11 9 6 5.5 2 1</pre>
detected-ap Обнаружение точек доступа	mac	MAC-адрес	get	get detected-ap mac	
	radio	Используемый радиointерфейс	get	get detected-ap radio	
	beacon-interval	Beacon-интервал	get	get detected-ap beacon-interval	
	capability	Возможности IEEE 802.11	get	get detected-ap capability	
	type	Тип (AP, Ad hoc, or Other)	get	get detected-ap type	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	privacy	WEP or WPA enabled	get	get detected-ap privacy	
	ssid	Имя сети	get	get detected-ap ssid	
	wpa	Безопасность посредством WPA	get	get detected-ap wpa	
	phy-type	Определение PHY режима	get	get detected-ap phy-type	
	band	Полоса частот	get	get detected-ap band	
	channel	Канал	get	get detected-ap channel	
	rate	Скорость	get	get detected-ap rate	
	signal	Мощность сигнала	get	get detected-ap signal	
	erp	ERP	get	get detected-ap erp	
	beacons	Количество полученных beacon	get	get detected-ap beacons	
	last-beacon	Время приема последнего beacon	get	get detected-ap last-beacon	
	supported-rates	Список поддерживаемых скоростей	get	get detected-ap supported-rates	
	security	Безопасность	get	get detected-ap security	
	hi-rate	Максимально возможная поддерживаемая скорость	get	get detected-ap hi-rate	
	noise	Уровень шума	get	get detected-ap noise	
	nmode	Поддержка 802.11n	get	get detected-ap nmode	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	wired	Точка доступа подключена к проводной сети	get	get detected-ap wired	
	wds	Точка доступа – часть wds-сети	get	get detected-ap wds	
	rsssi	RSSI точки доступа	get	get detected-ap rsssi	
portal Настройки Captive portal	status	Административный статус	get, set	get portal status	
	welcome-screen	Отображается ли экран для гостей	get, set	get portal welcome-screen  set portal welcome-screen <value>	
	welcome-screen-text	Текст, который будет отображаться в окне приветствия	get, set	get portal welcome-screen-text  set portal welcome-screen-text <value>	
snmpv1 Доступ по SNMPv1 и SNMPv2 протоколу	status	Административный статус	get, set	get snmpv1 status  set snmpv1 status <value>	
snmp-view SNMP MIB view	type	Тип поддеревы OID (included или excluded)	add, get, set	add snmp-view <view-all view-none all> type <value>  get snmp-view <view-all view-none all> type  set snmp-view <view-all view-none all> type <value>	WEP-2ac# get snmp-view all type name type ----- -- view-all included view-none excluded

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	oid	Поддерево OID (строка)	add, get, set	<pre>add snmp-view &lt;view-all view- none all&gt; oid &lt;value&gt;  get snmp-view &lt;view-all view- none all&gt; oid  set snmp-view &lt;view-all view- none all&gt; oid &lt;value&gt;</pre>	<pre>WEP-2ac# get snmp-view all oid name type ----- -- view-all included view-none excluded</pre>
	mask	<p>Маска OID – список октетов в hex-формате, разделенных знаком .</p> <p>Оставьте пустую строку, если маска не нужна.</p>	add, get, set	<pre>add snmp-view &lt;view-all view- none all&gt; mask &lt;value&gt;  get snmp-view &lt;view-all view- none all&gt; mask  set snmp-view &lt;view-all view- none all&gt; mask &lt;value&gt;</pre>	<pre>WEP-2ac# get snmp-view all mask name mask ----- view-all view-none</pre>
snmp-group Группа пользователей SNMP	secur-level	Уровень безопасности (noAuthNoPriv, authNoPriv или authPriv)	add, get, set	<pre>add snmp-group &lt;R0 RW all&gt; secur- level &lt;value&gt;  get snmp-group &lt;R0 RW all&gt; secur- level  set snmp-group &lt;R0 RW all&gt; secur- level &lt;value&gt;</pre>	<pre>WEP-2ac# set snmp-group R0 secur-level authPriv  WEP-2ac# get snmp-group R0 secur-level authPriv</pre>
	write-view	SNMP-имя для доступа к записи	add, get, set	<pre>add snmp-group &lt;R0 RW all&gt; write- view &lt;value&gt;  get snmp-group &lt;R0 RW all&gt; write- view  set snmp-group &lt;R0 RW all&gt; write- view &lt;value&gt;</pre>	<pre>WEP-2ac# set snmp-group R0 write-view view- none  WEP-2ac# get snmp-group R0 write-view view-none</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	read-view	SNMP-имя для доступа к чтению (view name for read access)	add, get, set	<pre>add snmp-group &lt;RO RW all&gt; read-view &lt;value&gt;  get snmp-group &lt;RO RW all&gt; read-view  set snmp-group &lt;RO RW all&gt; read-view &lt;value&gt;</pre>	<pre>WEP-2ac# set snmp-group R0 read-view view-all  WEP-2ac# get snmp-group R0 read-view view-all</pre>
snmp-user SNMPv3 пользователи	group	Имя SNMP-группы	add, get, set	<pre>add snmp-user group &lt;value&gt;  get snmp-user group  set snmp-user group &lt;value&gt;</pre>	
	auth-type	Протокол аутентификации ('md5' или 'none')	add, get, set	<pre>add snmp-user auth-type &lt;value&gt;  get snmp-user auth-type  set snmp-user auth-type &lt;value&gt;</pre>	
	auth-pass	Пароль для аутентификации	add, get, set	<pre>add snmp-user auth-pass &lt;value&gt;  get snmp-user auth-pass  set snmp-user auth-pass &lt;value&gt;</pre>	
	priv-type	Установить тип шифрования ('des' – использовать тип шифрования DES, 'none' – не использовать шифрование)	add, get, set	<pre>add snmp-user priv-type &lt;value&gt;  get snmp-user priv-type  set snmp-user priv-type &lt;value&gt;</pre>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	priv-pass	Ключ шифрования	add, get, set	<pre>add snmp-user priv-pass &lt;value&gt;  get snmp-user priv-pass  set snmp-user priv-pass &lt;value&gt;</pre>	
snmp-target SNMPv3-таргеты для получения SNMP traps	host	IP-адрес, на который будут отправлены трапы	add, get, set	<pre>add snmp-target host &lt;value&gt;  get snmp-target host  set snmp-target host &lt;value&gt;</pre>	
	port	Номер порта, на который будут отправляться SNMP-трапы	add, get, set	<pre>add snmp-target port &lt;value&gt;  get snmp-target port  set snmp-target port &lt;value&gt;</pre>	
	user-name	Имя пользователя SNMPv3	add, get, set	<pre>add snmp-target user-name &lt;value&gt;  get snmp-target user-name  set snmp-target user-name &lt;value&gt;</pre>	
serial Последовательный доступ к CLI	status	Статус	get, set	<pre>get serial status  set serial status &lt;value&gt;</pre>	<pre>WEP-2ac# set serial status up  WEP-2ac# get serial status up</pre>
	baud-rate	Скорость передачи данных (Serial baudrate)	get, set	<pre>get serial baud- rate  set serial baud- rate &lt;value&gt;</pre>	<pre>WEP-2ac# set serial baud-rate 115200  WEP-2ac# get serial baud-rate 115200</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
telnet Доступ к CLI по протоколу Telnet	status	Статус	get, set	get telnet status  set telnet status <value>	WEP-2ac# set telnet status up  WEP-2ac# get telnet status up
ftp-server FTP-сервер	status	Статус	get, set	get ftp-server status  set ftp-server status <value>	WEP-2ac# set ftp-server status down  WEP-2ac# get ftp-server status down
firmware-upgrade Обновление ПО точки доступа по HTTP	upgrade-url	http://<server IP>[:<server port>]/filename	get, set	get firmware-upgrade upgrade-url  set firmware-upgrade upgrade-url <value>	WEP-2ac# get firmware-upgrade upgrade-url
	progress	Отображение статуса процесса обновления ПО	get	get firmware-upgrade progress	WEP-2ac# get firmware-upgrade progress
	validate	Установите 'yes' для подтверждения файла	set	set firmware-upgrade validate	
	start	Установите 'yes' для начала обновления ПО	set	set firmware-upgrade start	
untagged-vlan Настройка нетегированных VLAN	vlan-id	VLAN ID для использования нетегированных VLAN	get, set	get untagged-vlan vlan-id  set untagged-vlan vlan-id <value>	WEP-2ac# set untagged-vlan vlan-id 1  WEP-2ac# get untagged-vlan vlan-id 1
	status	Статус	get, set	get untagged-vlan status  set untagged-vlan status <value>	WEP-2ac# set untagged-vlan status up  WEP-2ac# get untagged-vlan status up

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
managed-ap Управляемая точка доступа	mode	Режим	get, set	get managed-ap mode set managed-ap mode <value>	WEP-2ac# set managed-ap mode down WEP-2ac# get managed-ap mode down
	ap-state	Статус точки доступа	get	get managed-ap ap-state	WEP-2ac# set managed-ap ap-state down WEP-2ac# get managed-ap ap-state down
	switch-address-1	IP-адрес коммутатора 1	get, set	get managed-ap switch-address-1 set managed-ap switch-address-1 <value>	WEP-2ac# get managed-ap switch-address-1
	switch-address-2	IP-адрес коммутатора 2	get, set	get managed-ap switch-address-2 set managed-ap switch-address-2 <value>	
	switch-address-3	IP-адрес коммутатора 3	get, set	get managed-ap switch-address-3 set managed-ap switch-address-3 <value>	
	switch-address-4	IP-адрес коммутатора 4	get, set	get managed-ap switch-address-4 set managed-ap switch-address-4 <value>	
	pass-phrase	Пароль коммутатора	set	set managed-ap pass-phrase <value>	

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	dhcp-switch-address-1	IP-адрес коммутатора DHCP 1	get	get managed-ap dhcp-switch-address-1	WEP-2ac# get managed-ap dhcp-switch-address-1 104.116.116.112.5 8.47.47.49.57.50.4 6.49.54.56.46.49.5 4.46.49.54.48.58.5 7.53.57.53
	dhcp-switch-address-2	IP-адрес коммутатора DHCP 2	get	get managed-ap dhcp-switch-address-2	WEP-2ac# get managed-ap dhcp-switch-address-2 2
	dhcp-switch-address-3	IP-адрес коммутатора DHCP 3	get	get managed-ap dhcp-switch-address-3	WEP-2ac# get managed-ap dhcp-switch-address-3
	dhcp-switch-address-4	IP-адрес коммутатора DHCP 4	get	get managed-ap dhcp-switch-address-4	WEP-2ac# get managed-ap dhcp-switch-address-4
	managed-mode-watchdog	Время, через которое сторожевой таймер (watchdog) перезагрузит систему при необходимости (в минутах) (0-1440)	get, set	get managed-ap managed-mode-watchdog  set managed-ap managed-mode-watchdog <value>	WEP-2ac# set managed-ap managed-mode-watchdog 0  WEP-2ac# get managed-ap managed-mode-watchdog 0
	dhcp-ip-base-port	DHCP Base IP порт	get, set	get managed-ap dhcp-ip-base-port  set managed-ap dhcp-ip-base-port <value>	WEP-2ac# get managed-ap dhcp-ip-base-port
	cfg-ip-base-port	Настроить Base IP порт (1-65000)	get, set	get managed-ap cfg-ip-base-port  set managed-ap cfg-ip-base-port <value>	WEP-2ac# set managed-ap cfg-ip-base-port 57775  WEP-2ac# get managed-ap cfg-ip-base-port 57775

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ip-base-port	Base IP порт	get, set	<pre>get managed-ap ip-base-port set managed-ap ip-base-port &lt;value&gt;</pre>	<pre>WEP-2ac# set managed-ap ip-base-port 25459 WEP-2ac# get managed-ap ip-base-port 25459</pre>
	ip-tnl-udp-port	Tunnel UDP IP порт	get, set	<pre>get managed-ap ip-tnl-udp-port set managed-ap ip-tnl-udp-port &lt;value&gt;</pre>	<pre>WEP-2ac# set managed-ap ip-tnl-udp-port 25459 WEP-2ac# get managed-ap ip-tnl-udp-port 25459</pre>
	ip-udp-port	UDP IP порт	get, set	<pre>get managed-ap ip-udp-port set managed-ap ip-udp-port &lt;value&gt;</pre>	<pre>WEP-2ac# set managed-ap ip-udp-port 25460 WEP-2ac# get managed-ap ip-udp-port 25460</pre>
	ip-ssl-port	Secure SSL IP порт	get, set	<pre>get managed-ap ip-ssl-port set managed-ap ip-ssl-port &lt;value&gt;</pre>	<pre>WEP-2ac# set managed-ap ip-ssl-port 25461 WEP-2ac# get managed-ap ip-ssl-port 25461</pre>
	ip-capwap-src-port	CAPWAP Src IP порт	get, set	<pre>get managed-ap ip-capwap-src-port set managed-ap ip-capwap-src-port &lt;value&gt;</pre>	<pre>WEP-2ac# set managed-ap ip-capwap-src-port 25462 WEP-2ac# get managed-ap ip-capwap-src-port 25462</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ip-capwap-dst-port	CAPWAP Dst IP порт	get, set	get managed-ap ip-capwap-dst-port set managed-ap ip-capwap-dst-port <value>	WEP-2ac# set managed-ap ip-capwap-dst-port 25463 WEP-2ac# get managed-ap ip-capwap-dst-port 25463
dot1x-suppliant 802.1X суппликант	status	Статус	get, set	get dot1x-suppliant status set dot1x-suppliant status <value>	WEP-2ac# set dot1x-suppliant status down WEP-2ac# get dot1x-suppliant status down
	user	802.1X пользователь-суппликант	get, set	get dot1x-suppliant user set dot1x-suppliant user <value>	WEP-2ac# get dot1x-suppliant user
	password	802.1X пароль пользователя	set	set dot1x-suppliant password <value>	
mgmt-acl Список адресов, разрешенных для управления	mode	Режим	get, set	get mgmt-acl mode set mgmt-acl mode <value>	WEP-2ac# set mgmt-acl mode down WEP-2ac# get mgmt-acl mode down
	mgmt-address-1	IP-адрес управления 1	get, set	get mgmt-acl mgmt-address-1 set mgmt-acl mgmt-address-1 <value>	WEP-2ac# get mgmt-acl mgmt-address-1
	mgmt-address-2	IP-адрес управления 2	get, set	get mgmt-acl mgmt-address-2 set mgmt-acl mgmt-address-2 <value>	WEP-2ac# get mgmt-acl mgmt-address-2

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	mgmt-address-3	IP-адрес управления 3	get, set	get mgmt-acl mgmt-address-3  set mgmt-acl mgmt-address-3 <value>	WEP-2ac# get mgmt-acl mgmt- address-3
	mgmt-address-4	IP-адрес управления 4	get, set	get mgmt-acl mgmt-address-4  set mgmt-acl mgmt-address-4 <value>	WEP-2ac# get mgmt-acl mgmt- address-4
	mgmt-address-5	IP-адрес управления 5	get, set	get mgmt-acl mgmt-address-5  set mgmt-acl mgmt-address-5 <value>	WEP-2ac# get mgmt-acl mgmt- address-5
cluster Настройки кластера	clustered	Активировать/ Отключить режим кластера для данного узла	get, set	get cluster clustered  set cluster clustered <value>	WEP-2ac# get cluster clustered  softwlc  WEP-2ac# set cluster clustered 0
	location	Расположение кластера	get, set	get cluster location  set cluster location <value>	WEP-2ac# set cluster location Moscow  WEP-2ac# get cluster location Moscow
	cluster-name	Имя кластера для присоединения к нему	get, set	get cluster cluster-name  set cluster cluster-name <value>	WEP-2ac# set cluster cluster- name root  WEP-2ac# get cluster cluster- name root

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	ipversion	Выберите версию IP протокола: IPv4 или IPv6	add, get, set	add cluster ipversion <value> get cluster ipversion set cluster ipversion <value>	WEP-2ac# set cluster ipversion ipv4 WEP-2ac# get cluster ipversion ipv4
	member-count	Число устройств в кластере	get	get cluster member-count	WEP-2ac# get cluster member- count 2
	clustering-allowed	Разрешен ли режим кластера для данного узла	get	get cluster clustering-allowed	WEP-2ac# get cluster clustering-allowed true
	compat	Модель устройства, входящего в кластер	get	get cluster compat	WEP-2ac# get cluster compat WEP-2ac
	operational-mode	Режим работы	get	get cluster operational-mode	WEP-2ac# get cluster operational-mode 1
	cluster-ipaddr	IP-адрес устройства, управляющего кластером	get, set	get cluster cluster-ipaddr set cluster cluster-ipaddr <value>	WEP-2ac# set cluster cluster- ipaddr 192.168.1.1 WEP-2ac# get cluster cluster- ipaddr 192.168.1.1
	priority	Приоритет	get, set	get cluster priority set cluster priority <value>	WEP-2ac# set cluster priority 1 WEP-2ac# get cluster priority 1

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	reauth-timeout	Интервал времени до повторной аутентификации	get, set	get cluster reauth-timeout set cluster reauth-timeout <value>	WEP-2ac# set cluster reauth-timeout 300 WEP-2ac# get cluster reauth-timeout 300
	secure-mode	Режим безопасного объединения	get, set	get cluster secure-mode set cluster secure-mode <value>	WEP-2ac# set cluster secure-mode 1 WEP-2ac# get cluster secure-mode 1
	pass-set	Значение параметра 1, если пароль сконфигурирован	get	get cluster pass-set	WEP-2ac# get cluster pass-set
	secure-mode-status	Состояние работы безопасного режима	get	get cluster secure-mode-status	WEP-2ac# get cluster secure-mode-status Disabled

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
cluster-member Состояние устройств кластера	mac	MAC-адрес устройства, входящего в кластер	get	get cluster-member mac	WEP-2ac# get cluster-member mac  E0:D9:E3:50:06:C0  A8:F9:4B:B5:FB:A0
	ip	IP-адрес устройства, входящего в кластер	get	get cluster-member ip	WEP-2ac# get cluster-member ip  100.110.0.200  100.110.0.249
	compat	Модель устройства, входящего в кластер	get	get cluster-member compat	WEP-2ac# get cluster-member compat  WEP-2ac  WEP-2ac
	location	Расположение устройства	get	get cluster-member location	WEP-2ac# get cluster-member location  Moscow  Moscow
	uptime	Время с момента включения устройства	get	get cluster-member uptime	WEP-2ac# get cluster-member uptime  2923  1260
	is-dominant	Доминирующее устройство	get	get cluster-member is-dominant	WEP-2ac# get cluster-member is-dominant  true  false
	priority	Приоритет	get	get cluster-member priority	WEP-2ac# get cluster-member priority  0  0

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	firmware-version	Версия ПО	get	get cluster-member firmware-version	WEP-2ac# get cluster-member firmware-version  1.21.1.14
	cluster-controller	Контроллер кластера	get	get cluster-member cluster-controller	WEP-2ac# get cluster-member cluster-controller  no  yes
cluster-fw-member  Статус загрузки ПО на устройство в кластере	ip	IP-адрес устройства, входящего в кластер	get	get cluster-fw-member ip	
	mac	MAC-адрес устройства, входящего в кластер	get	get cluster-fw-member mac	
	fw-download-status	Состояние загрузки ПО	get	get cluster-fw-member fw-download-status	
cluster-firmware-upgrade  Настройки кластера	upgrade	(Start/stop) начать/остановить процесс загрузки	get, set	get cluster-firmware-upgrade  set cluster-firmware-upgrade <value>	WEP-2ac# set cluster-firmware-upgrade upgrade Start  WEP-2ac# get cluster-firmware-upgrade upgrade

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	upgrade-url	заполнить url в формате tftp://<ip>/<image_name>	get, set	<pre>get cluster-firmware-upgrade upgrade-url set cluster-firmware-upgrade upgrade-url &lt;value&gt;</pre>	<pre>WEP-2ac# set cluster-firmware-upgrade upgrade-url tftp://192.168.1.2/Wep-2ac_1.21.0.244.tar.gz WEP-2ac# get cluster-firmware-upgrade upgrade-url tftp://192.168.1.2/Wep-2ac_1.21.0.244.tar.gz</pre>
	upgrade-method	all/selective/< >, метод обновления	get, set	<pre>get cluster-firmware-upgrade upgrade-method set cluster-firmware-upgrade upgrade-method &lt;value&gt;</pre>	<pre>WEP-2ac# set cluster-firmware-upgrade upgrade-method all WEP-2ac# get cluster-firmware-upgrade upgrade-method all</pre>
	upgrade-status	Текущий статус обновлений	get	<pre>get cluster-firmware-upgrade upgrade-status</pre>	<pre>WEP-2ac# get cluster-firmware-upgrade upgrade-status Not Initialized</pre>

Класс	Подкласс	Функция	Возможные команды	Синтаксис	Примеры
	upgrade-members	Список IP-адресов устройств в кластере, разделенных запятой	get, set	<pre>get cluster-firmware-upgrade-upgrade-members set cluster-firmware-upgrade-upgrade-members &lt;value&gt;</pre>	<pre>WEP-2ac# set cluster-firmware-upgrade upgrade-members 192.168.1.1,192.168.1.3 WEP-2ac# get cluster-firmware-upgrade upgrade-members 192.168.1.1,192.168.1.3</pre>

## 7 Список изменений

Версия документа	Дата выпуска	Содержание изменений
Версия 1.23	27.02.2026	Синхронизация с версией ПО 1.25.7 Корректировка: <ul style="list-style-type: none"> <li>• 5.6.2.1 Дополнительные настройки беспроводных интерфейсов</li> </ul>
Версия 1.22	21.06.2024	Синхронизация с версией ПО 1.25.0 Корректировка: <ul style="list-style-type: none"> <li>• 4.5.8 Подменю «VAP»</li> <li>• 4.6.3 Подменю «SSH»</li> <li>• 4.6.4 Подменю «Telnet»</li> <li>• 4.6.8 Подменю «SNMP»</li> <li>• 4.8.1 Подменю «Configuration»</li> <li>• 5.5.5 Дополнительные команды</li> <li>• 5.6.3 Настройка виртуальных точек доступа Wi-Fi (VAP)</li> </ul>
Версия 1.21	08.09.2023	Синхронизация с версией ПО 1.24.0 Корректировка: <ul style="list-style-type: none"> <li>• 4.6.9 Подменю «Time Settings (NTP)»</li> </ul> Добавлено: <ul style="list-style-type: none"> <li>• 5.6.7 Настройка Radar</li> </ul>
Версия 1.20	21.04.2023	Синхронизация с версией ПО 1.23.0 Корректировка: <ul style="list-style-type: none"> <li>• 5.6.3 Настройка виртуальных точек доступа Wi-Fi (VAP)</li> <li>• 5.6.8 Системные настройки</li> </ul>
Версия 1.19	09.09.2022	Синхронизация с версией ПО 1.22.4 Добавлено: <ul style="list-style-type: none"> <li>• 5.5.6.3 Настройка WGB-ARP-Timeout</li> </ul> Корректировка: <ul style="list-style-type: none"> <li>• 4.12 Меню «Workgroup Bridge»</li> </ul>
Версия 1.18	03.06.2022	Синхронизация с версией ПО 1.22.2
Версия 1.17	22.04.2022	Синхронизация с версией ПО 1.22.1 Корректировка: <ul style="list-style-type: none"> <li>• 4.5.5 Подменю «Radio»</li> <li>• 5.6.2.1 Дополнительные настройки беспроводных интерфейсов</li> <li>• 5.6.8 Настройка сервиса APB</li> </ul>
Версия 1.16	03.12.2021	Синхронизация с версией ПО 1.21.1
Версия 1.15	30.09.2021	Синхронизация с версией ПО 1.21.0
Версия 1.14	07.12.2020	Синхронизация с версией ПО 1.20.0 Объединение предыдущих версий руководства в единый документ
Версия 1.13	09.04.2020	Синхронизация с версией ПО 1.19.3
Версия 1.12	24.02.2020	Синхронизация с версией ПО 1.19.0

Версия документа	Дата выпуска	Содержание изменений
Версия 1.11	01.10.2019	Синхронизация с версией ПО 1.18.1
Версия 1.10	05.06.2019	Синхронизация с версией ПО 1.17.0
Версия 1.9	12.02.2018	Синхронизация с версией ПО 1.16.0
Версия 1.8	30.11.2018	Синхронизация с версией ПО 1.15.0
Версия 1.7	10.08.2018	Синхронизация с версией ПО 1.14.0
Версия 1.6	8.05.2018	Синхронизация с версией ПО 1.12.2 Корректировка: <ul style="list-style-type: none"> <li>• Характеристика устройства</li> </ul>
Версия 1.5	26.12.2017	Синхронизация с версией 1.11.4
Версия 1.4	30.10.2017	Синхронизация с версией 1.11.2
Версия 1.3	02.08.2017	Синхронизация с версией 1.10.0
Версия 1.2	01.02.2017	Синхронизация с версией 1.9.0
Версия 1.1	16.12.2016	Синхронизация с версией 1.8.0
Версия 1.0	20.07.2016	Первая публикация.
Версия программного обеспечения 1.25.7		

## 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 или оставить интерактивную заявку:

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

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

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