Беспроводная точка доступа

WEP-500K

Руководство по эксплуатации

Версия ПО 1.3.1

IP-адрес: 192.168.1.10

Username: admin

Password: password

Содержание

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 они за короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей ШПД, сопоставимых по скорости с проводными сетями и обладающих высокими критериями к качеству предоставления услуг.

Основное предназначение WEP-500K — установка внутри зданий в качестве точек 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 устройства, а также рекомендации по его установке и настройке.

1.2 Условные обозначения

Примечания и предупреждения

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

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

2 Описание изделия

2.1 Назначение

Для возможности предоставления доступа пользователей к высокоскоростной и безопасной сети разработаны беспроводные точки доступа WEP-500K.

Основным назначением устройства является создание беспроводной сети передачи данных L2-уровня на стыке с проводной сетью. WEP-500K подключается к проводной сети через 10/100/1000/2500M Ethernet-интерфейс и с помощью радиоинтерфейсов создает беспроводной высокоскоростной доступ для устройств, поддерживающих технологию Wi-Fi в диапазоне 2.4/5/6 ГГц.

Устройство содержит 3 радиоинтерфейса для организации трех физических беспроводных сетей.

WEP-500K поддерживает современные требования к качеству сервисов и позволяет передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Приоритизация обеспечивается следующими технологиями QoS: CoS (теги в заголовке VLAN-кадра) и ToS (метки в заголовке IP-пакета).

WEP-500K подходит для оснащения офисов, государственных учреждений, гостиниц, конференц-залов, лабораторий и учебных аудиторий.

2.2 Характеристики устройства

Интерфейсы:

- 1 порт 10/100/1000/2500BASE-T (RJ-45) с поддержкой PoE;
- 1 порт 10/100/1000BASE-T (RJ-45);
- Wi-Fi 2.4 ГГц IEEE 802.11b/g/n/ax/be;
- Wi-Fi 5 ГГц IEEE 802.11a/n/ac/ax/be;
- Wi-Fi 6 ГГц IEEE 802.11ax/be.

Функции:

Возможности WLAN:

- поддержка стандартов IEEE 802.11a/b/g/n/ac/ax/be;
- роуминг пользователей IEEE 802.11r/k/v;
- агрегация данных, включая A-MPDU и A-MSDU;
- приоритеты и планирование пакетов на основе WMM;
- динамический выбор частоты (DFS);
- поддержка скрытого SSID;
- автовыбор канала;
- 48 виртуальных точек доступа.

Сетевые функции:

- автоматическое согласование скорости, дуплексного режима и переключения между режимами MDI и MDI-X;
- поддержка VLAN;
- поддержка C-VLAN;
- DHCP-клиент;
- поддержка GRE;
- передача абонентского трафика вне туннелей;
- поддержка NTP;
- поддержка Syslog;
- поддержка LLDP.

Безопасность:

- централизованная авторизация через RADIUS-сервер (802.1X WPA/WPA2/WPA3 Enterprise);
- шифрование WPA/WPA2/WPA3/OWE;
- поддержка внешнего портала авторизации.

На рисунке 1 приведена схема применения оборудования WEP-500K.

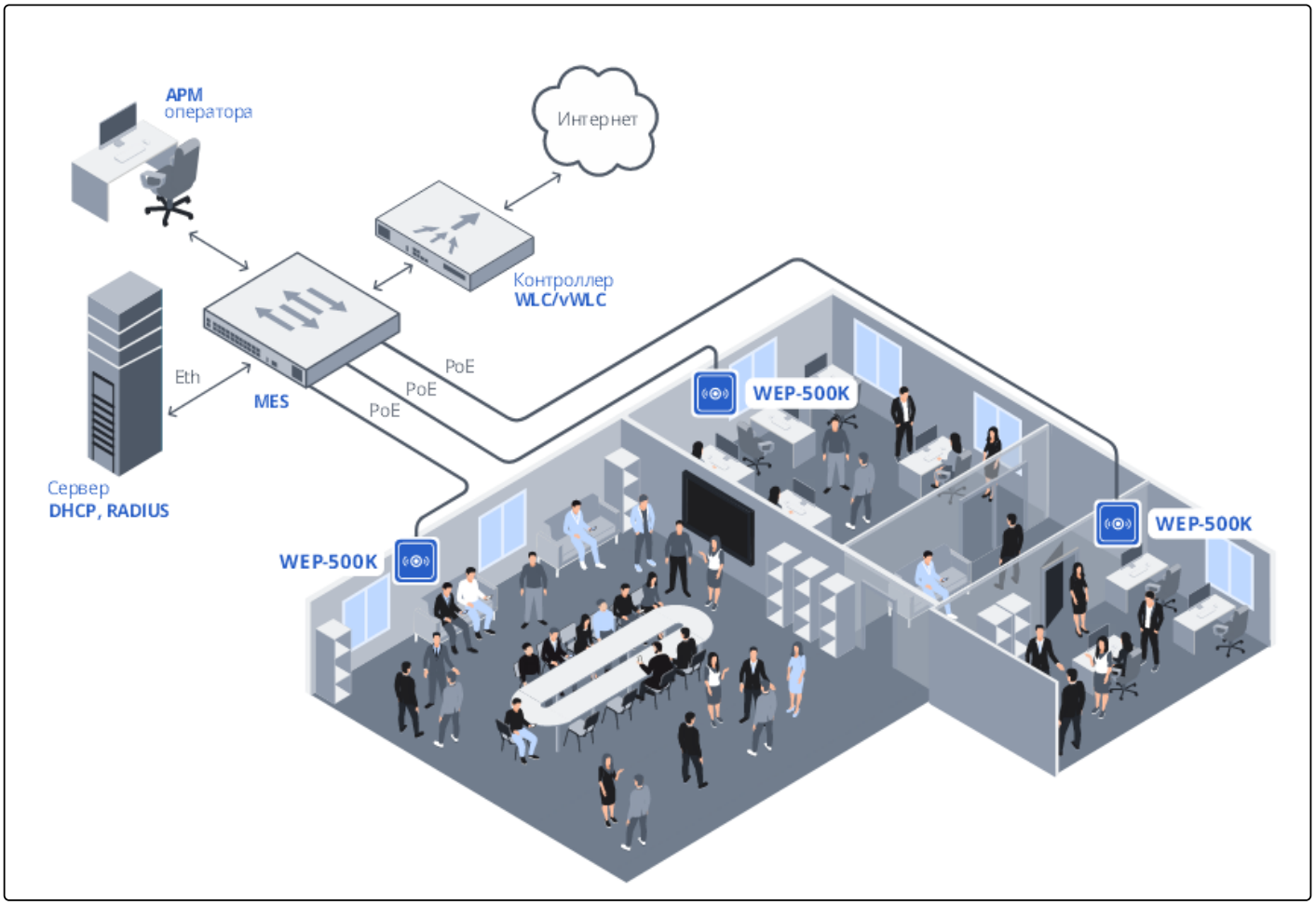


Рисунок 1 — Функциональная схема использования WEP-500K

2.3 Технические параметры устройства

Таблица 1 — Основные технические параметры

Параметры WAN-интерфейса Ethernet	
Количество портов	2
Электрический разъем	RJ-45
Скорость передачи	10/100/1000/2500 Мбит/с, автоопределение 10/100/1000 Мбит/с, автоопределение
Поддержка стандартов	BASE-T
Параметры беспроводного интерфейса	
Стандарты	802.11a/b/g/n/ac/ax/be
Частотный диапазон	2400–2483.5 МГц; 5150–5350 МГц, 5470–5850 МГц, 5935–7125 МГц
Модуляция	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM, 4096QAM
Рабочие каналы	802.11b/g/n/ax/be: 1–13 (2401–2483 МГц) 802.11a/n/ac/ax/be: • 36–64 (5170–5330 МГц) • 100–144 (5490–5730 МГц) • 149–165 (5735–5835 МГц) 802.11ax/be: 1–233 (5935–7125 МГц)
Скорость передачи данных	2.4 ГГц, 802.11be: 688 Мбит/с 5 ГГц, 802.11be: 4324 Мбит/с 6 ГГц, 802.11be: 8647 Мбит/с
Максимальное количество одновременных подключений	1024
Максимальная мощность передатчика	2.4 ГГц: 21 дБм 5 ГГц: 21 дБм 6 ГГц: 21 дБм
Коэффициент усиления встроенных антенн	2.4 ГГц: ~4 дБи 5 ГГц: ~6 дБи 6 ГГц: ~3 дБи
Чувствительность приемника	2.4 ГГц: до -95 дБм 5 ГГц: до -94 дБм 6 ГГц: до -95 дБм
Безопасность	централизованная авторизация через RADIUS-сервер (802.1X WPA/WPA2/WPA3 Enterprise) шифрование данных WPA/WPA2/WPA3/OWE поддержка внешнего портала авторизации
Поддержка MU-MIMO 2×2 для 2.4 ГГц; MU-MIMO 3×3 для 5 и 6 ГГц Поддержка OFDMA и MLO (Multi-Link Operation)	
Управление	
Удаленное управление	web-интерфейс, Telnet, SSH, CLI, NETCONF
Ограничение доступа	по паролю

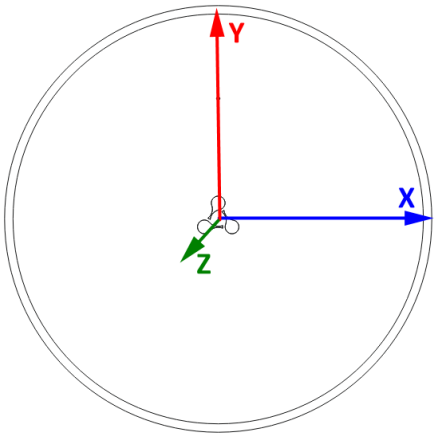
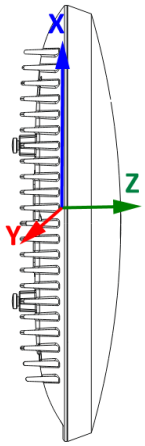
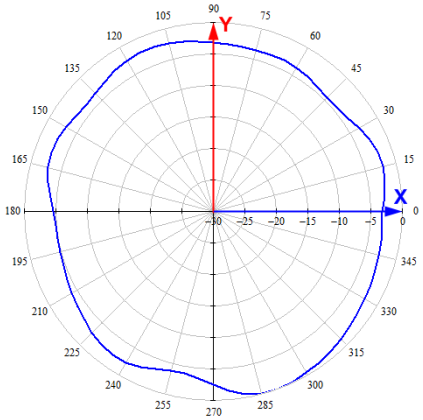
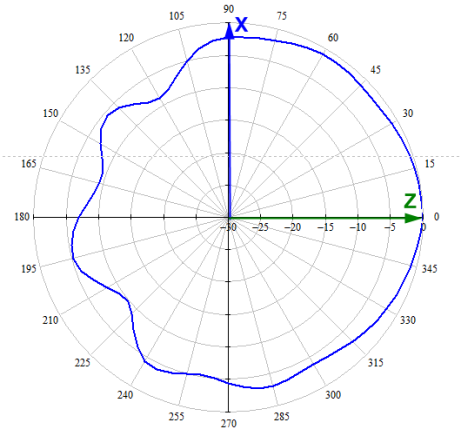
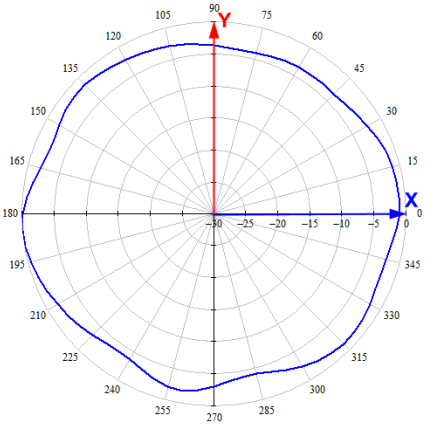
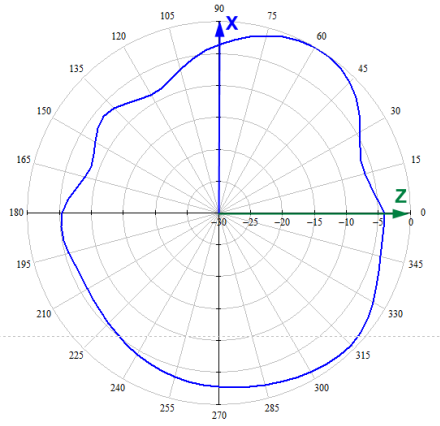
Общие параметры	
Flash-память	256 МБ SPI-NAND Flash
RAM	1 ГБ DDR4 RAM
Питание	PoE+ 48 В/56 В (IEEE 802.3at-2009)
Потребляемая мощность	не более 24,5 Вт
Рабочий диапазон температур	от +5 до +40 °C
Относительная влажность при температуре 25 °C	до 80 %
Габариты (диаметр × высота)	280 × 64,5 мм
Масса	1,8 кг
Срок службы	не менее 15 лет

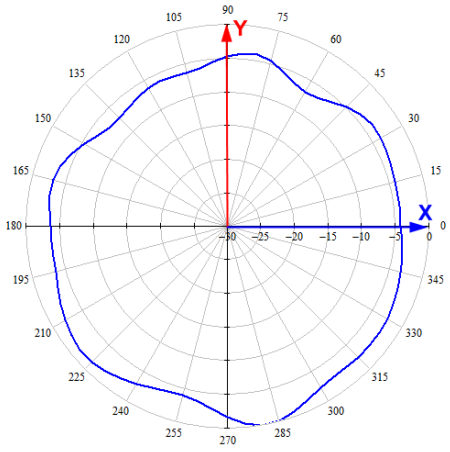
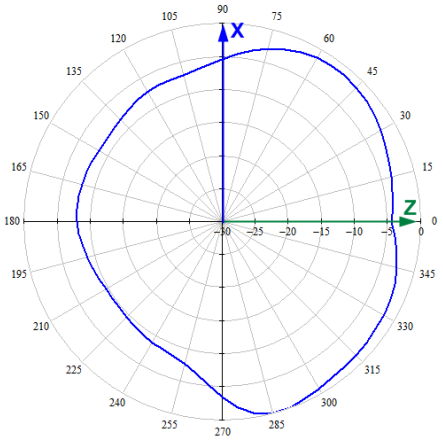
Таблица 2 — Таблица совместимости скоростей сетевого подключения и категорий кабелей Ethernet

Скорость	**Категория кабеля**
2.5G	CAT5e
1G	CAT5e
100M	CAT5

2.4 Диаграммы направленности

На рисунках ниже представлены диаграммы направленности устройства.

Положение при измерении	
AZIMUTH (XY)	**ELEVATION (XZ)**
	
Диапазон 2.4 ГГц	
	
Диапазон 5 ГГц	
	

Диапазон 6 ГГц	
	

2.5 Конструктивное исполнение

Устройства WEP-500K выполнены в пластиковом корпусе.

2.5.1 Основная панель устройства

Внешний вид основной панели устройства приведен на рисунке 2.

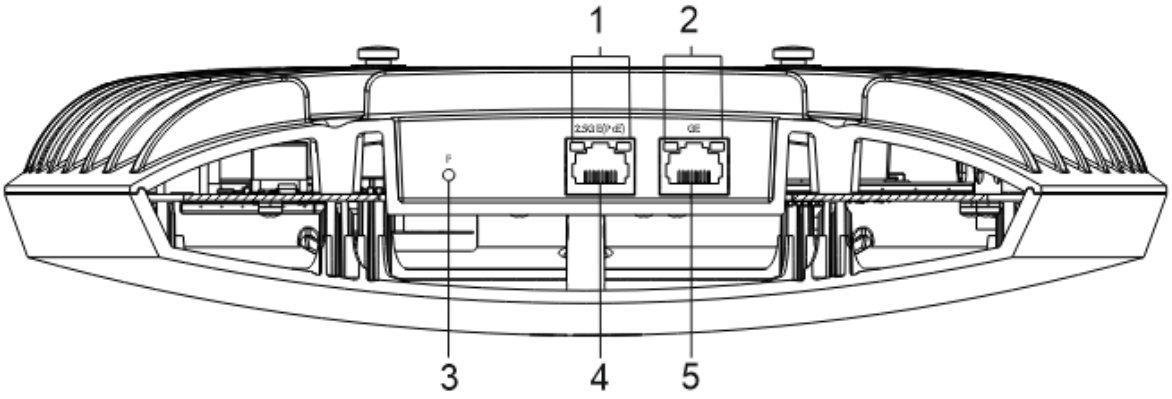


Рисунок 2 — Внешний вид основной панели WEP-500K

На основной панели устройств WEP-500K расположены следующие световые индикаторы, разъемы и органы управления (таблица 3).

Таблица 3 — Описание индикаторов, портов и органов управления

Элемент панели		Описание
1	LAN_1	Световая индикация состояния порта 2.5GE (PoE)
2	LAN_2	Световая индикация состояния порта GE
3	F	Кнопка сброса к заводским настройкам
4	2.5GE	Порт 2.5GE для подключения Ethernet-кабеля и подачи питания PoE+
5	GE	Порт GE для подключения Ethernet-кабеля

2.5.2 Верхняя панель устройства

Внешний вид верхней панели устройства приведен на рисунке 3.

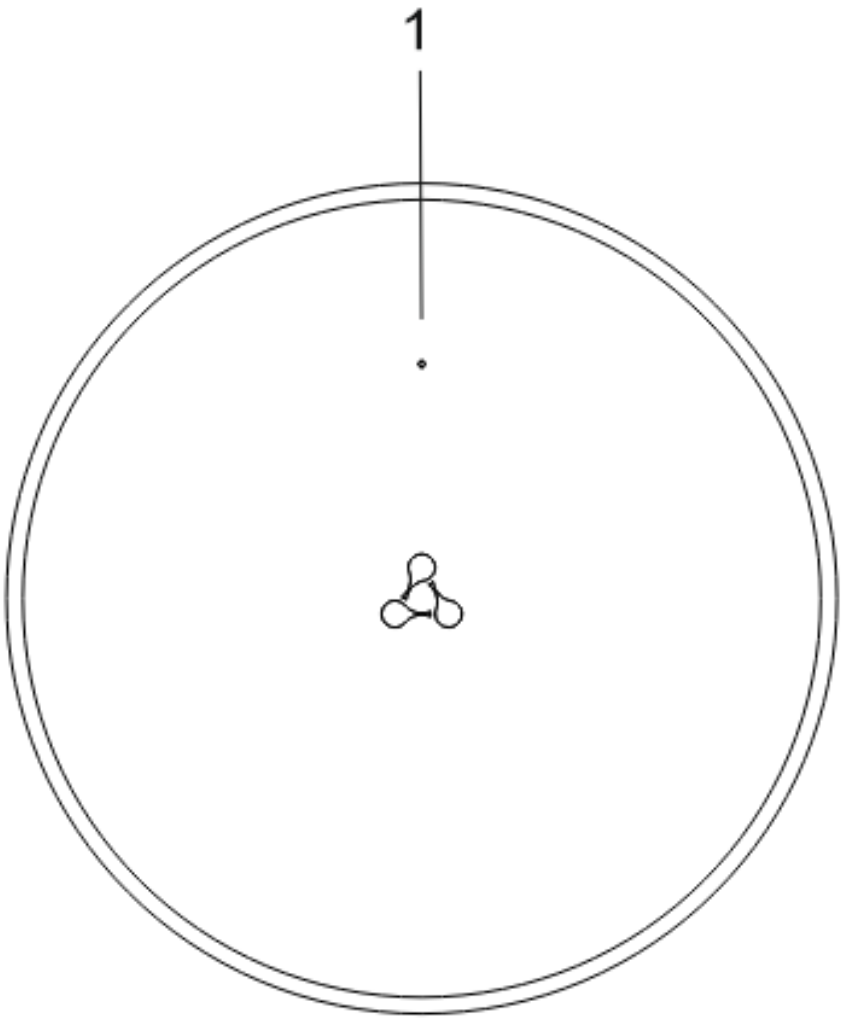


Рисунок 3 — Внешний вид верхней панели WEP-500K

Таблица 4 — Описание индикаторов верхней панели

Элемент панели		**Описание**
1	Power	Индикатор статуса работы устройства

2.6 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов **LAN, Power**. Перечень состояний индикаторов приведен в таблице 5.

Таблица 5 — Световая индикация состояния устройства

Индикатор	Состояние индикатора	Состояние устройства
LAN_1	Горит зеленый светодиод (10, 100 Мбит/с); Горит зеленый и оранжевый светодиод (1000, 2500 Мбит/с)	Установлено соединение с подключенным сетевым устройством
	Зеленый, мигает	Процесс пакетной передачи данных по LAN-интерфейсу
LAN_2	Горит зеленый светодиод (10, 100 Мбит/с); Горит зеленый и оранжевый светодиод (1000 Мбит/с)	Установлено соединение с подключенным сетевым устройством
	Зеленый, мигает	Процесс пакетной передачи данных по LAN-интерфейсу
Power	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 к заводским настройкам необходимо в загруженном состоянии устройства нажать и удерживать кнопку «F» в течение 10–15 секунд, пока индикатор «Power» не начнет мигать. 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:

- оборудование радиодоступа WEP-500K;
- 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 °C или выше 40 °C.
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 его на наличие видимых механических повреждений. В случае обнаружения повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.
3. Если устройство длительное время находилось 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:
    - Устанавливайте устройство в центре беспроводной сети.
    - Минимизируйте число преград (стены, потолки, мебель и др.) между точкой доступа и другими беспроводными сетевыми устройствами.
    - Не устанавливайте устройство вблизи (порядка 2 м) электрических и радиоустройств.
    - Не рекомендуется использовать радиотелефоны и другое оборудование, работающее на частоте 2.4, 5 или 6 ГГц, в радиусе действия беспроводной сети Wi-Fi.
    - 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 его 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-500K при монтаже на потолке в типовых офисных помещениях: 2.4 ГГц — 40–50 м, 5 ГГц/6 ГГц — 20–30 м. При полном отсутствии препятствий радиус охвата: 2.4 ГГц — до 100 м, 5 ГГц/6 ГГц — до 60 м.
В таблице 6 приведены приблизительные значения затухания.

Таблица 6 — Значения затухания

Материал	**Изменение уровня сигнала, дБ**		
	2.4 ГГц	**5 ГГц**	**6 ГГц**
Гипсокартон	3	3,2	3,5
Кирпич (стена 9 см)	5	7	8
Бетон (стена 20 см)	12	15	18
Армированный бетон (стена 30 см)	20	25	30
Обычное стекло (окно)	1	1,5	2
Мебель	1	1,5	2
Дерево (пустотелое/дверь)	3	4	5
Дерево (массив/стена)	10	15	20
Металл	25	30	35

3.4 Выбор каналов соседствующих точек

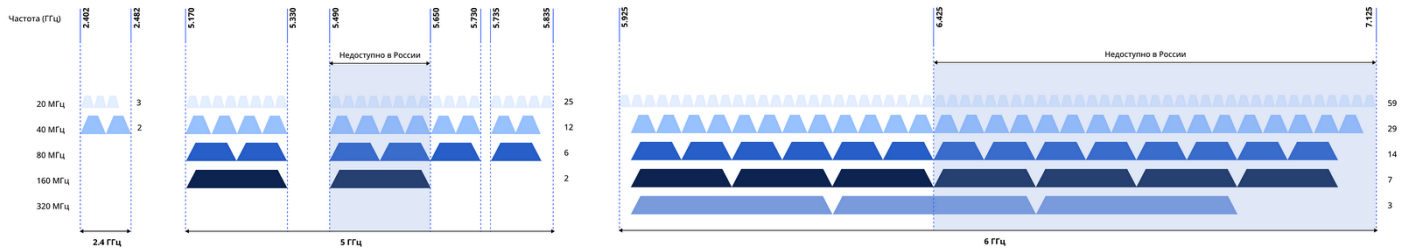


Рисунок 4 — Полный частотный спектр Wi-Fi

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

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

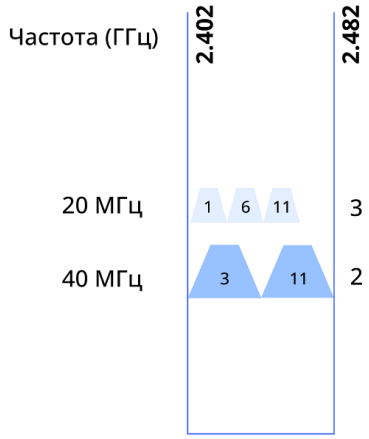


Рисунок 5 — Каналы, используемые в диапазоне в 2.4 ГГц при ширине канала 20, 40 МГц

Пример схемы распределения каналов между соседними точками в диапазоне 2.4 ГГц при ширине канала в 20 МГц приведен на рисунке 6.

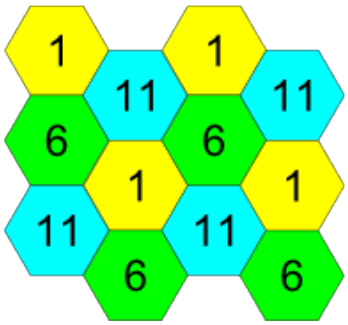


Рисунок 6 — Схема распределения каналов между соседними точками доступа в диапазоне 2.4 ГГц при ширине канала в 20 МГц

Аналогично рекомендуется сохранять данный механизм распределения каналов при расположении точек между этажами (рисунок 7).

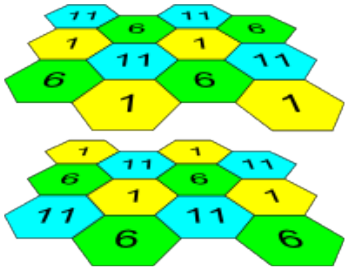


Рисунок 7 — Схема распределения каналов между соседними точками доступа, расположенными между этажами

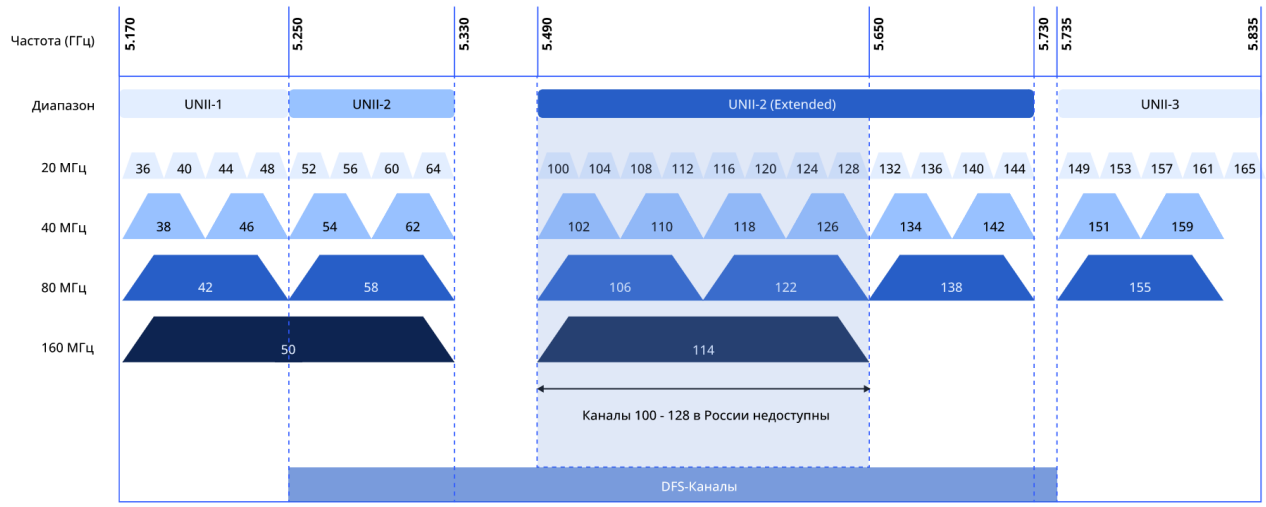


Рисунок 8 — Каналы, используемые в диапазоне 5 ГГц при ширине канала 20, 40, 80, 160 МГц

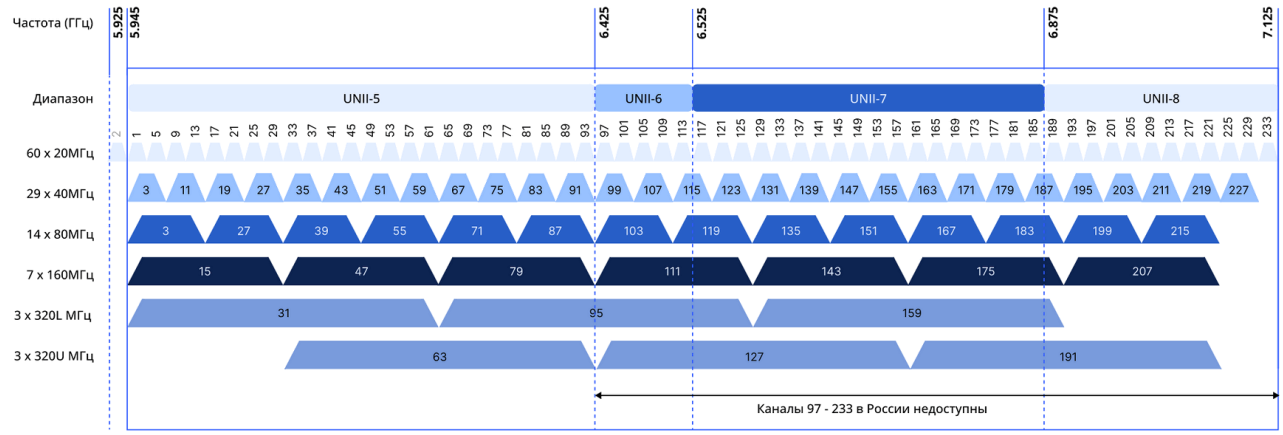


Рисунок 9 — Каналы, используемые в диапазоне 6 ГГц при ширине канала 20, 40, 80, 160, 320 МГц

4 Установка устройства

Устройство может быть установлено на потолочный профиль, шпильку, плоскую поверхность, кронштейн VESA100 при соблюдении инструкций по технике безопасности и рекомендаций, приведенных выше.
В комплект поставки входит крепеж для установки устройства на потолочный профиль, шпильку, плоскую поверхность.

4.1 Установка устройства на плоскую поверхность

Отверстия для крепления монтажной пластины к плоской поверхности отмечены на рисунке 10.

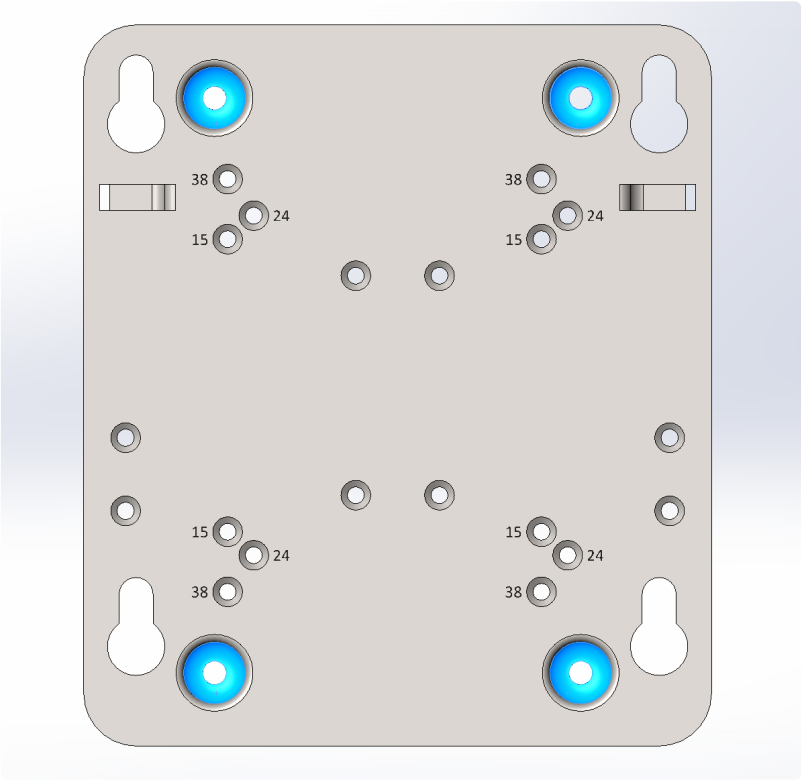


Рисунок 10 — Отверстия для крепления монтажной пластины к стене/потолку

1. Закрепите монтажную пластину на поверхности, используя крепёж из комплекта поставки. Выпуклые края на отверстиях должны быть направлены в сторону установочной поверхности (рисунок 11).

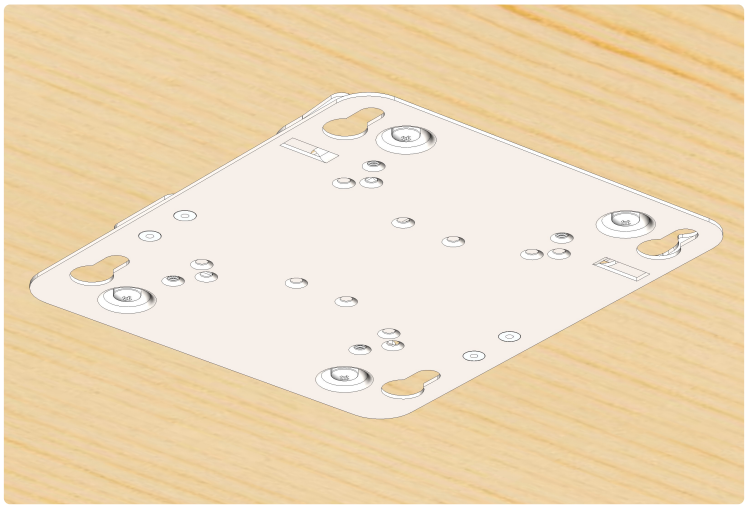


Рисунок 11 — Крепление монтажной пластины на поверхность

2. Подключите кабели к соответствующим разъемам устройства. Описание разъемов приведено в разделе Конструктивное исполнение. Установите устройство на монтажную пластину, совместив резиновые ножки с отверстиями на пластине, рисунки 12 (а) и 12 (б).

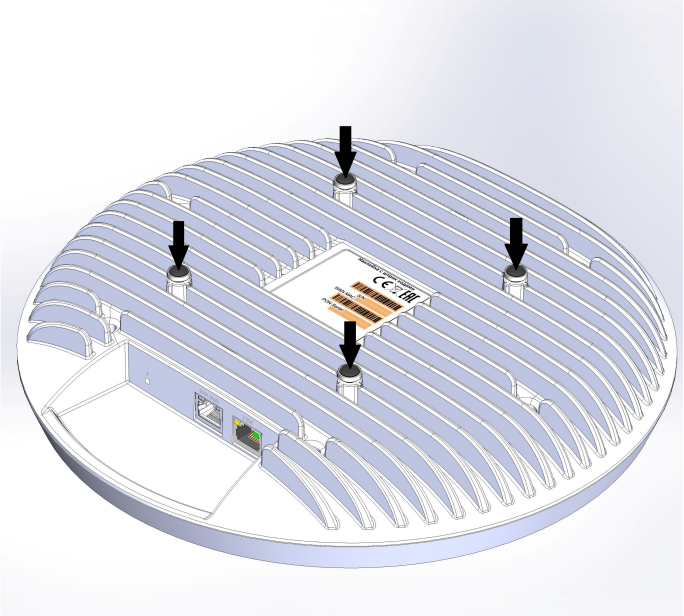


Рисунок 12 (а)

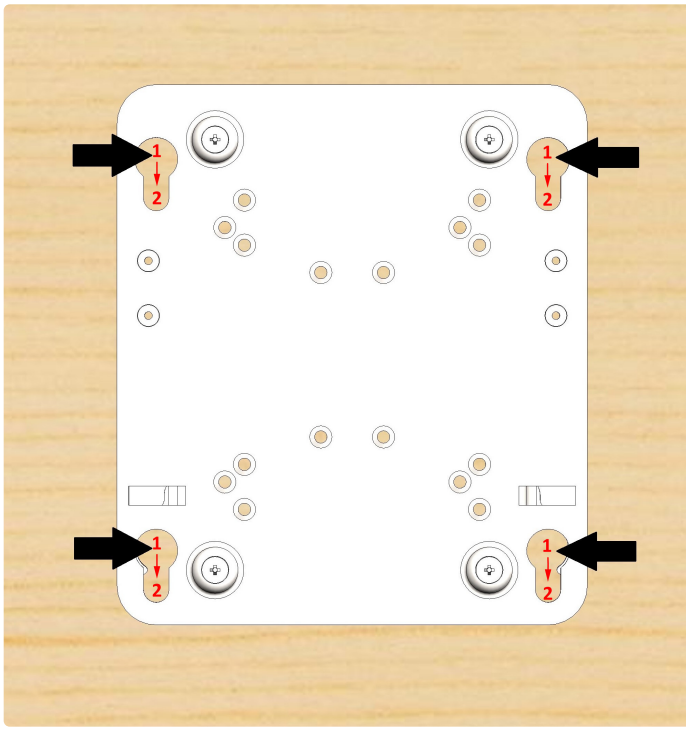


Рисунок 12 (б)

3. Зафиксируйте устройство на монтажной пластине, сдвинув его из положения 1 в положение 2 (рисунок 12 (б)).

4.2 Установка устройства на Армстронг

1. Для установки устройства на потолочный профиль используйте потолочный зажим, изображённый на рисунке 13.

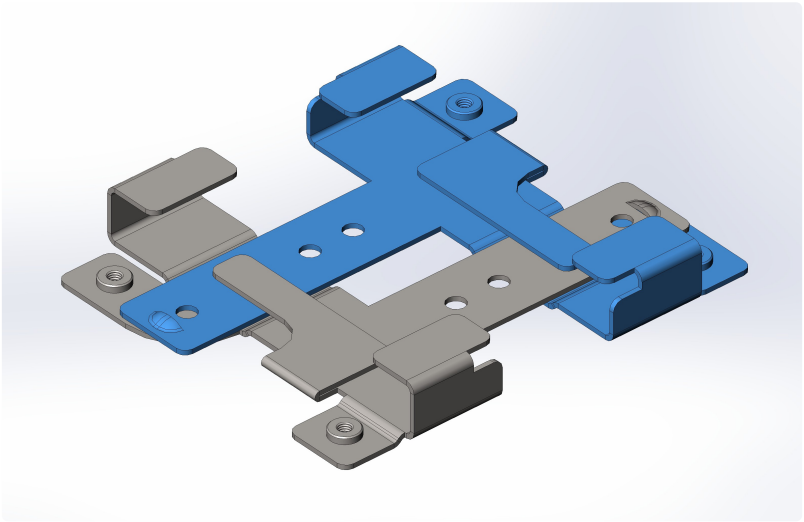


Рисунок 13 — Потолочный зажим

2. Раздвиньте зажим в крайнее положение и защёлкните на профиле потолка (рисунок 14). Предлагаемый вариант крепежа предназначен для трёх типов профилей с шириной 15, 24 и 38 мм (см. рисунок 10).

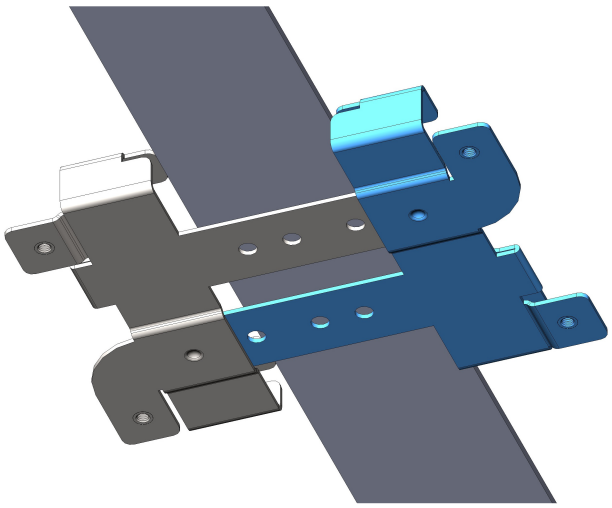


Рисунок 14 — Крепление зажима на потолочном профиле

3. Закрепите монтажную пластину на потолочном зажиме, используя винты М3×5 из комплекта поставки, рисунок 15.

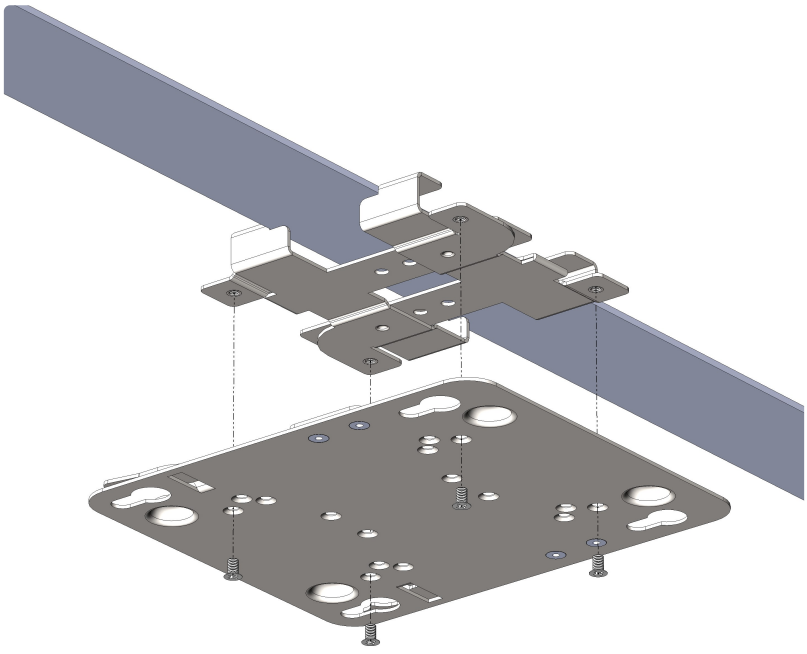


Рисунок 15 — Крепление монтажной пластины к зажиму

4. Подключите кабели к соответствующим разъемам устройства. Описание разъемов приведено в разделе Конструктивное исполнение. Установите устройство на монтажную пластину, совместив резиновые ножки с отверстиями на пластине, рисунок 16.

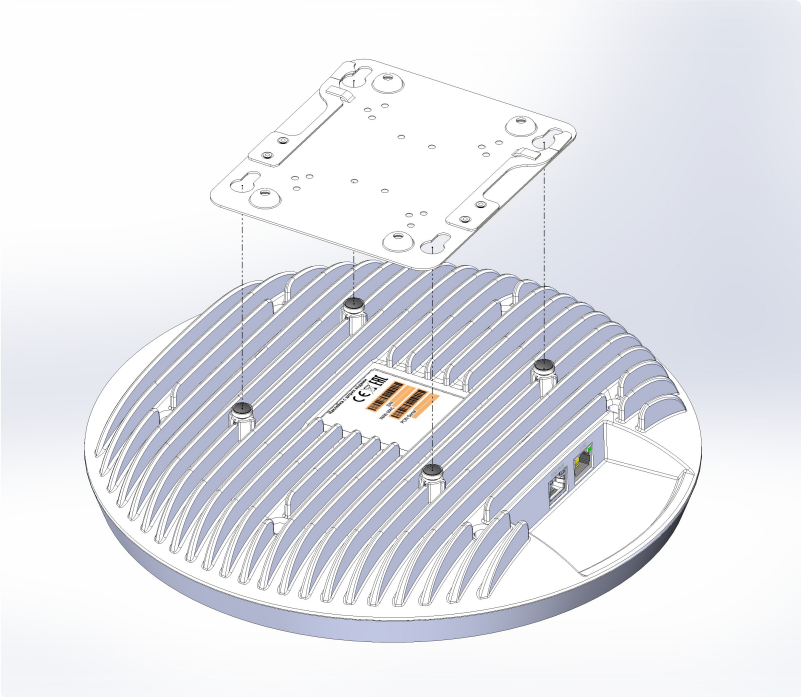


Рисунок 16 — Установка устройства на монтажную пластину

5. Зафиксируйте устройство на монтажной пластине, сдвинув его в сторону по направлению стрелки 1, рисунок 17 (а). Обратите внимание на положение индикации (направление стрелки 2) и разъёмов, они должны быть расположены вдоль направления профиля, рисунок 17 (б).

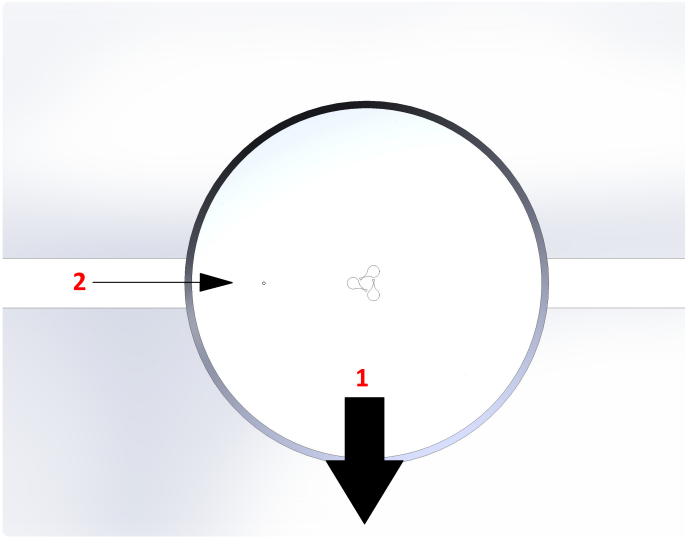


Рисунок 17 (а) — Фиксация устройства на монтажной пластине

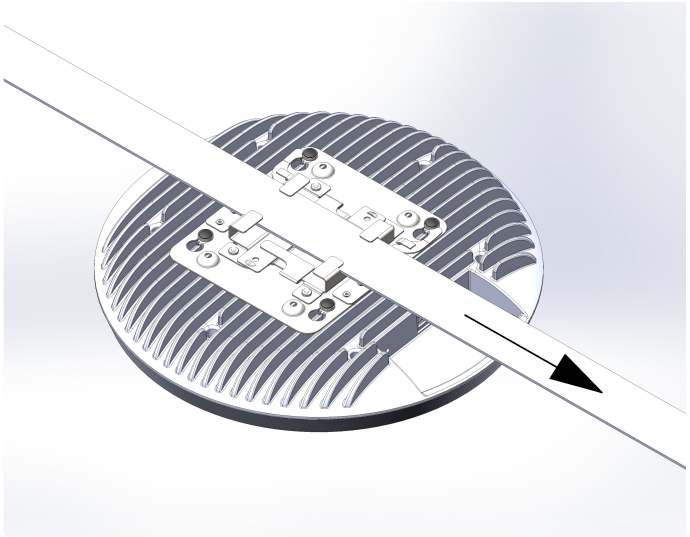


Рисунок 17 (б) — Расположение разъёмов

4.3 Установка устройства на шпильку

1. Установите скобу из комплекта поставки на монтажную пластину с помощью винтов M3×5, рисунок 18.

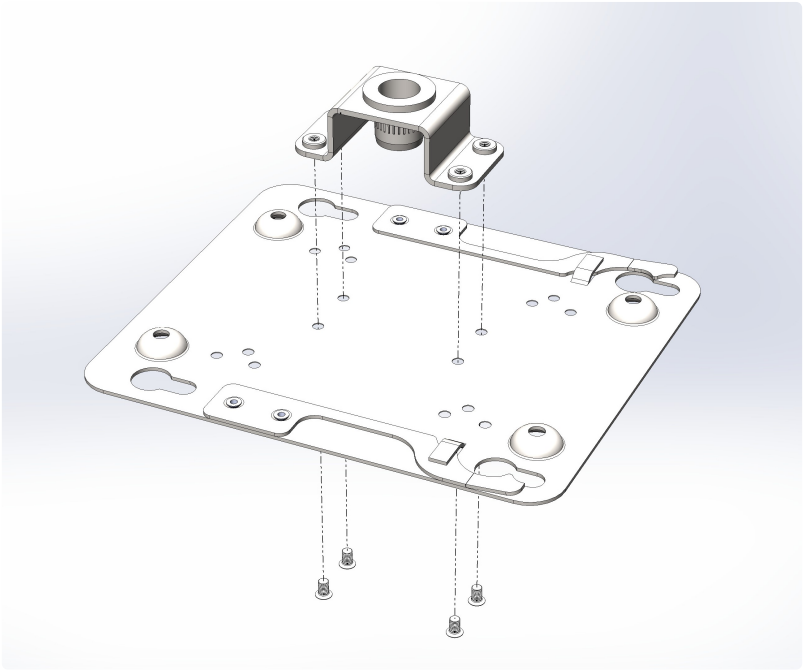


Рисунок 18 — Установка скобы на монтажную пластину

2. Накрутите монтажную пластину на шпильку M10 до упора, рисунок 19.

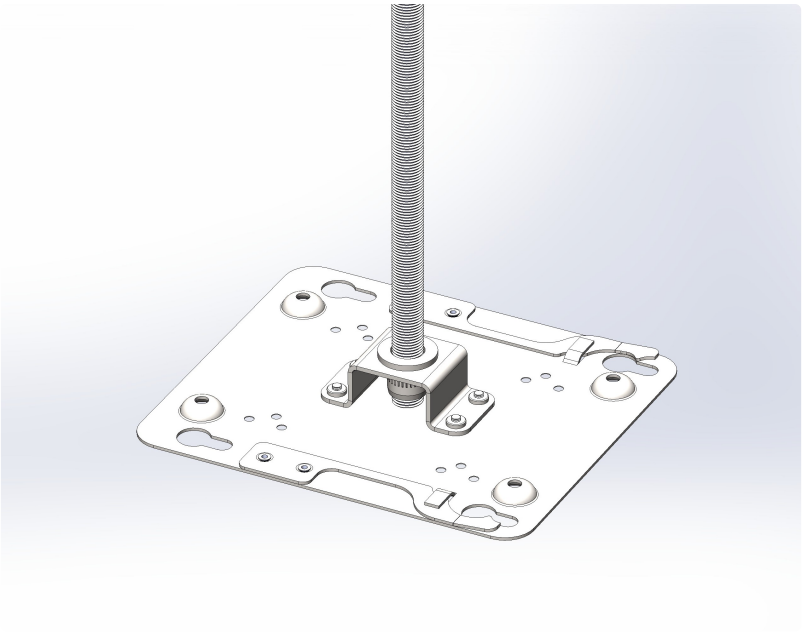


Рисунок 19 — Установка монтажной пластины на шпильку

3. Подключите кабели к соответствующим разъемам устройства. Описание разъемов приведено в разделе Конструктивное исполнение. Установите устройство на монтажную пластину, совместив резиновые ножки с отверстиями на пластине, рисунок 20.

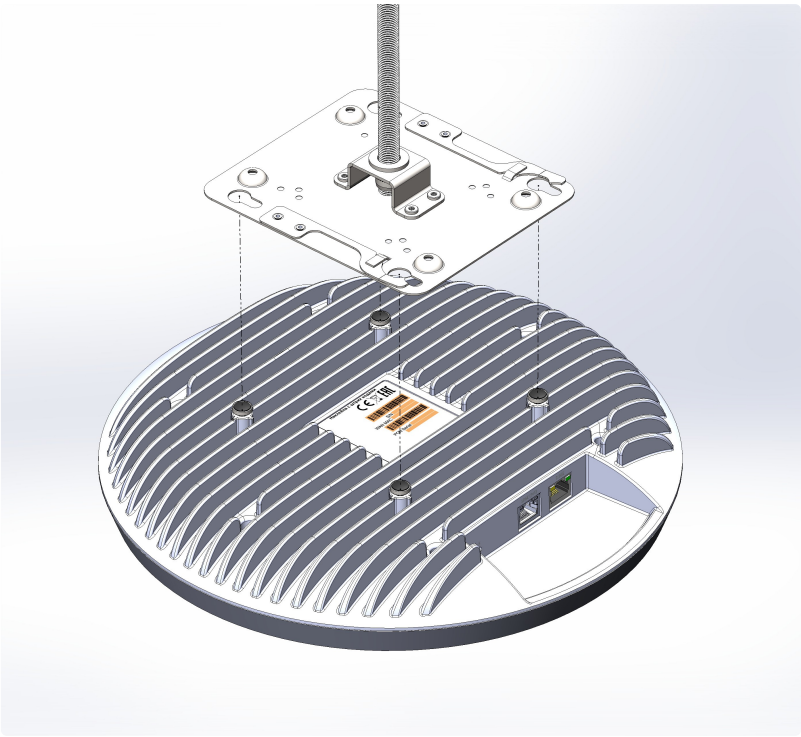


Рисунок 20 — Установка устройства на монтажную пластину

4. Зафиксируйте устройство на пластине, сдвинув его в сторону, рисунок 21.

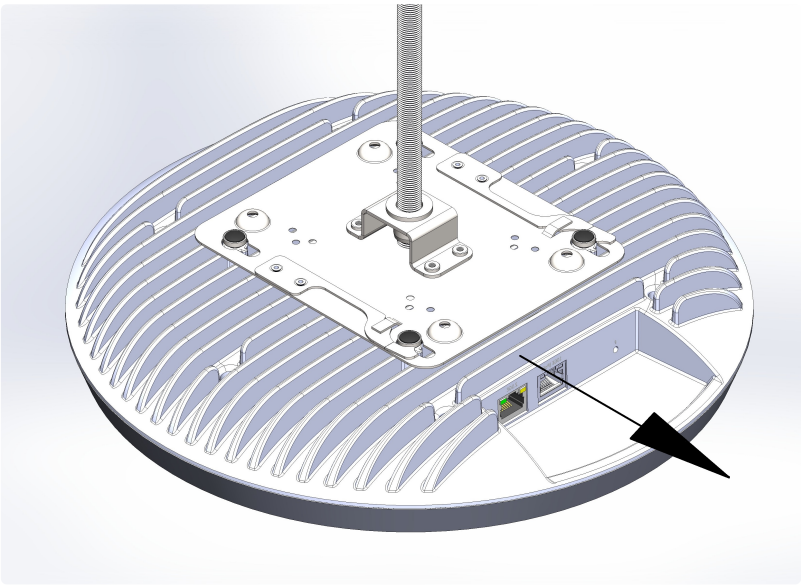


Рисунок 21 — Фиксация устройства на монтажной пластине

4.4 Установка устройства на кронштейн VESA100

Конструкция данного устройства предусматривает крепление с использованием кронштейнов VESA100.

1. Выкрутите резиновые ножки, расположенные на радиаторе устройства (рисунок 12 (a)).
2. Прикрепите крепление к устройству.

> Перед установкой на кронштейн VESA100 убедитесь, что крепление способно выдержать массу устройства.

5 Управление устройством через web-интерфейс

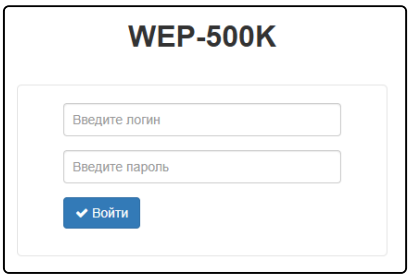
5.1 Начало работы

Для начала работы подключитесь к устройству по интерфейсу WAN 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.

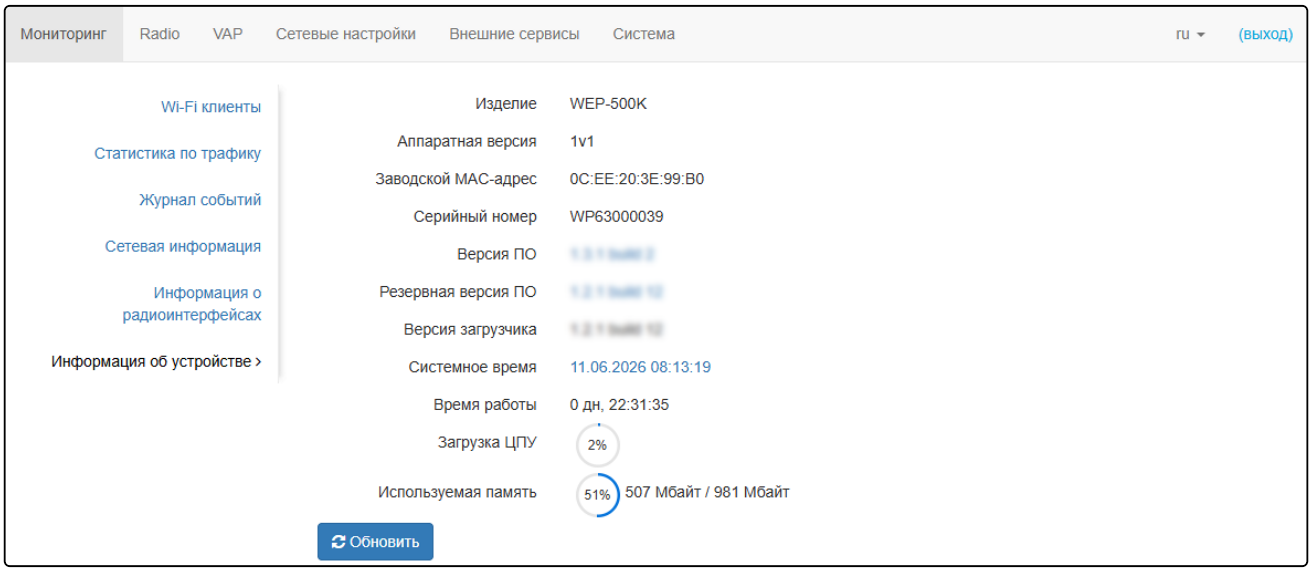
При успешном обнаружении устройства в окне браузера отобразится страница с запросом имени пользователя и пароля.



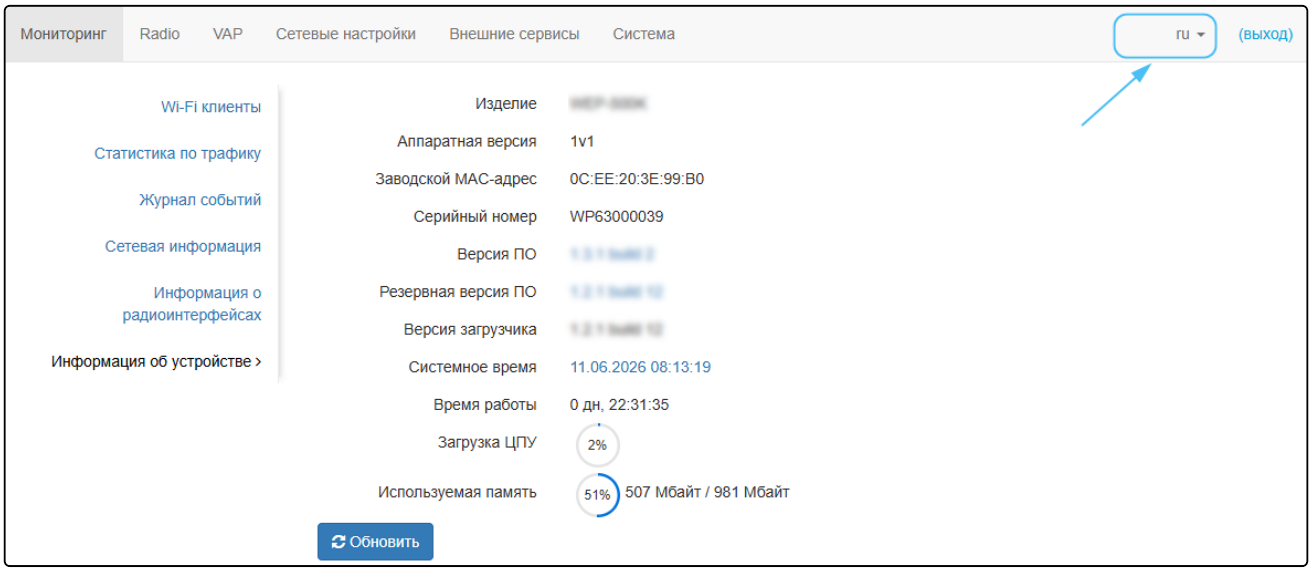
3. Введите имя пользователя в строке «Введите логин» и пароль в строке «Введите пароль».

> Заводские установки: логин — *admin*, пароль — *password*.

4. Нажмите кнопку «Войти». В окне браузера откроется меню мониторинга состояния устройства.



5. При необходимости можно переключить язык отображения информации. Для устройств WEP-500K доступны русская и английская версии web-интерфейса.



5.2 Применение конфигурации и отмена изменений

1. Применение конфигурации

При нажатии кнопки Применить запускается процесс сохранения конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

В web-интерфейсе WEP-500K реализована визуальная индикация текущего состояния процесса применения настроек (таблица 7).

Таблица 7 – Визуальная индикация текущего состояния процесса применения настроек

Внешний вид	Описание состояния
Применить	После нажатия на кнопку «Применить» происходит процесс применения и записи настроек в память устройства. Об этом информирует значок в названии вкладки и на кнопке «Применить».
Применить	Об успешном сохранении и применении настроек информирует значок в названии вкладки.

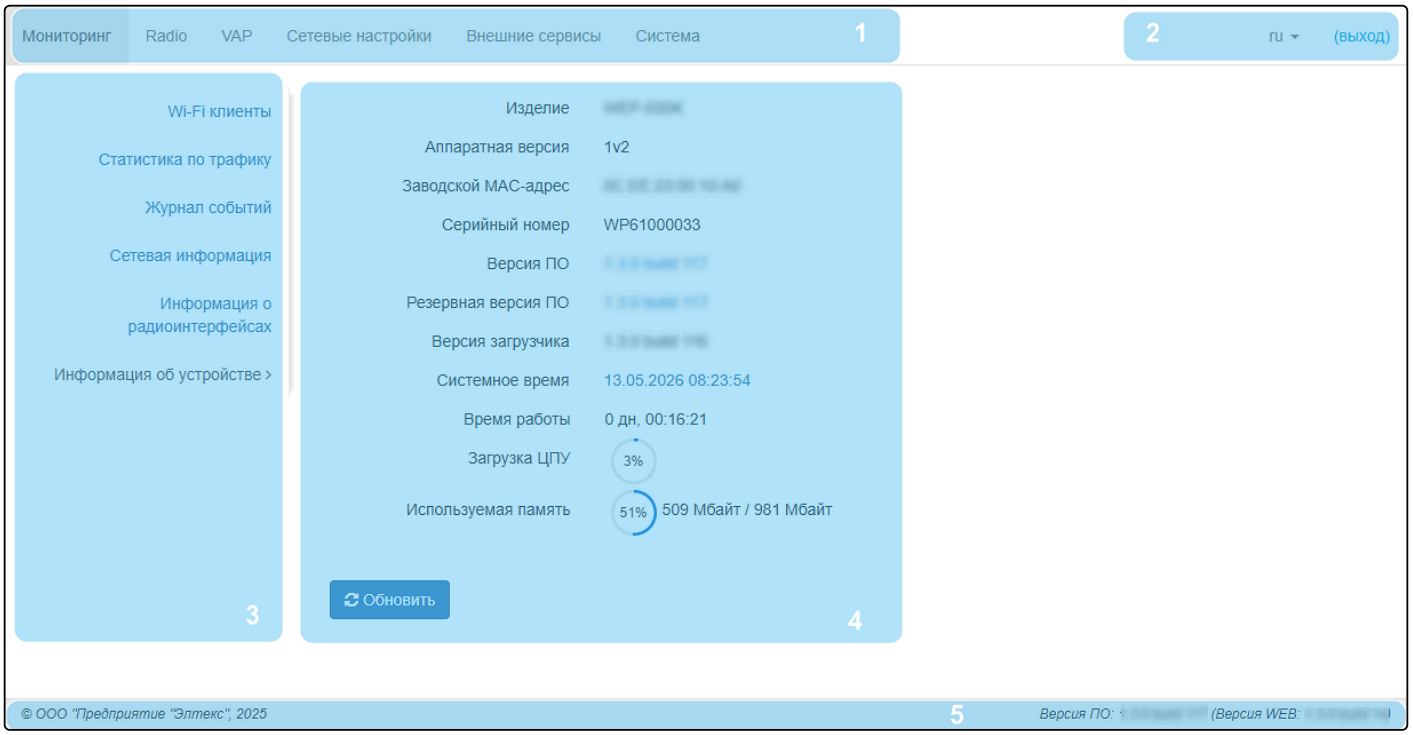
2. Отмена изменений

Отмена изменений производится только до нажатия на кнопку «Применить». При нажатии на кнопку «Применить» изменённые на странице параметры будут обновлены на текущие значения, записанные в памяти устройства. После нажатия на кнопку «Применить» возврат к предыдущим настройкам будет невозможен.

Кнопка отмены изменений имеет следующий вид: Отмена .

5.3 Основные элементы web-интерфейса

На рисунке ниже представлены элементы навигации web-интерфейса.



Окно пользовательского интерфейса разделено на пять областей:

1. Вкладки меню – для группировки подменю по категориям: **Мониторинг, Radio, VAP, Сетевые настройки, Внешние сервисы, Система**.
2. Выбор языка интерфейса и кнопка «(выход)», предназначенная для завершения сеанса работы в web-интерфейсе под данным пользователем.
3. Вкладки подменю – для управления полем настроек.
4. Поле настроек устройства – для просмотра данных и конфигурации.
5. Информационное поле, отображающее версию ПО, установленную на устройстве.

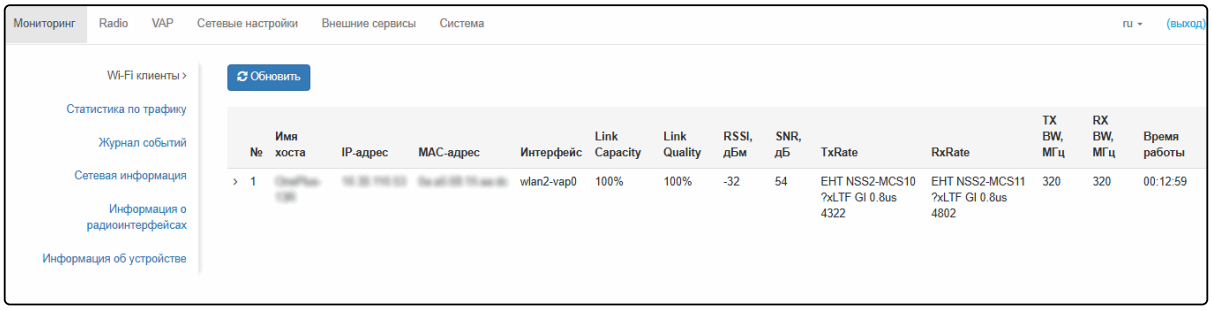
5.4 Меню «Мониторинг»

В меню **«Мониторинг»** отображается текущее состояние системы.

5.4.1 Подменю «Wi-Fi клиенты»

В подменю **«Wi-Fi клиенты»** отображается информация о состоянии подключенных Wi-Fi клиентов.

Информация по подключенным клиентам не отображается в реальном времени. Для того чтобы обновить информацию на странице, необходимо нажать на кнопку «Обновить».



- *№* — номер подключенного устройства в списке;
- *Имя хоста* — сетевое имя устройства;
- *IP-адрес* — IP-адрес подключенного устройства;
- *MAC-адрес* — MAC-адрес подключенного устройства;
- *Интерфейс* — интерфейс взаимодействия WEP-500K с подключенным устройством;
- *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 3×3). Значение параметра рассчитывается за последние 10 секунд;
- *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). Значение параметра рассчитывается за последние 10 с;
- *RSSI* — уровень принимаемого сигнала, дБм;
- *SNR* — отношение сигнал/шум, дБ;
- *TxRate* — канальная скорость передачи, Мбит/с;
- *RxRate* — канальная скорость приема, Мбит/с;
- *Tx BW* — полоса пропускания на передаче, МГц;
- *Rx BW* — полоса пропускания на приеме, МГц;
- *Время работы* — время соединения с Wi-Fi клиентом.

Для вывода более развернутой информации по определенному клиенту выберите его в списке.

Подробное описание включает в себя следующие параметры:

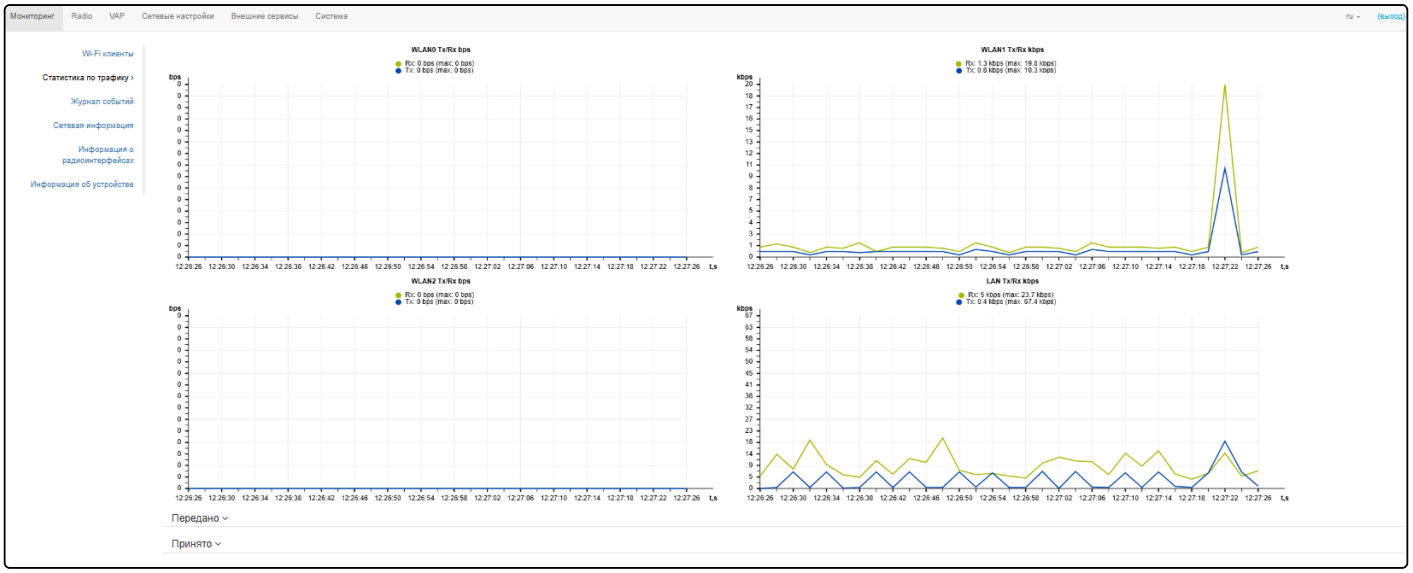
- *Передано/принято всего, байт* — количество переданных/принятых на подключенное устройство байт;
- *Передано/принято всего, пакетов* — количество переданных/принятых на подключенное устройство пакетов;
- *Передано с ошибками, пакетов* — количество пакетов, переданных с ошибками на подключенное устройство.

5.4.2 Подменю «Статистика по трафику»

В подменю «**Статистика по трафику**» отображаются графики скорости переданного/полученного трафика за последние 2 минуты, а также статистика о количестве переданного/полученного трафика с момента включения точки доступа.

График LAN Tx/Rx показывает скорость переданного/полученного трафика через Ethernet-интерфейс (ETH0) точки доступа за последние 2 минуты. График автоматически обновляется каждые 6 секунд.

Графики WLAN0, WLAN1 и WLAN2 Tx/Rx показывают скорость переданного/полученного трафика через интерфейсы Radio 2.4 ГГц, Radio 5 ГГц и Radio 6 ГГц за последние 2 минуты. График автоматически обновляется каждые 6 секунд.



Описание таблицы «*Передано*»:

- *Интерфейс* — имя интерфейса;
- *Всего пакетов* — количество успешно отправленных пакетов;
- *Всего байт* — количество успешно отправленных байт;
- *Отброшено пакетов* — количество пакетов, отброшенных при отправке;
- *Ошибки* — количество ошибок.

Передано

Интерфейс	Всего пакетов	Всего байт	Отброшено пакетов	Ошибки
LAN	1385095	1947952084	0	0
WLAN0	0	0	0	0
WLAN1	3436942	4765613248	18569	18569
erspan0	0	0	0	0
eth1	0	0	0	0
ip6gre0	0	0	0	0
ip6tnl0	0	0	0	0
wlan0-apcli0	0	0	0	0
wlan1-apcli0	0	0	0	0
wlan2	0	0	0	0
wlan2-apcli0	0	0	0	0

Описание таблицы «*Принято*»:

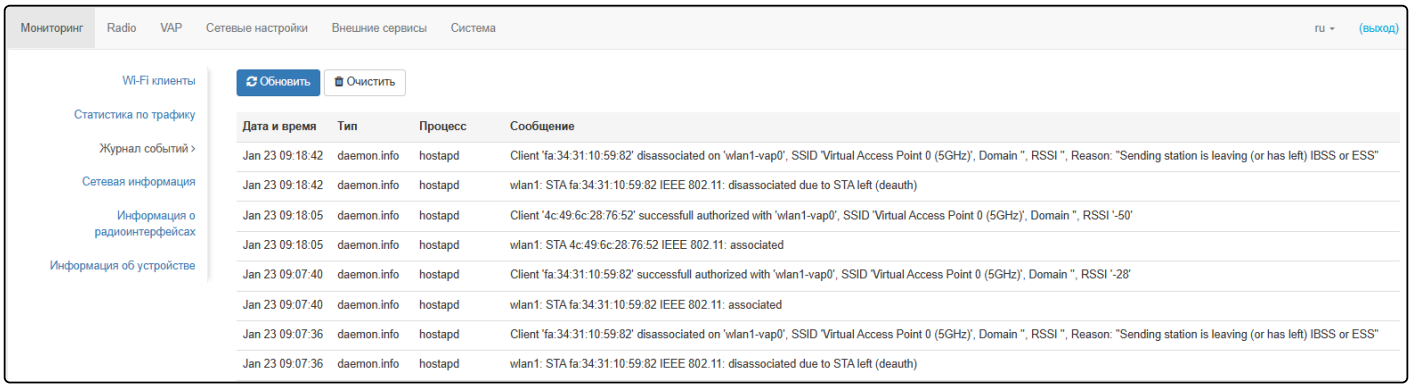
- *Интерфейс* – имя интерфейса;
- *Всего пакетов* – количество успешно принятых пакетов;
- *Всего байт* – количество успешно принятых байт;
- *Отброшено пакетов* – количество пакетов, отброшенных при получении;
- *Ошибки* – количество ошибок.

Принято

Интерфейс	Всего пакетов	Всего байт	Отброшено пакетов	Ошибки
LAN	9856185	14495002366	33	0
WLAN0	0	0	0	0
WLAN1	1382677	1941183584	4281	4281
erspan0	0	0	0	0
eth1	0	0	0	0
ip6gre0	0	0	0	0
ip6tnl0	0	0	0	0
wlan0-apcli0	0	0	0	0
wlan1-apcli0	0	0	0	0
wlan2	0	0	0	0
wlan2-apcli0	0	0	0	0

5.4.3 Подменю «Журнал событий»

В подменю «**Журнал событий**» можно просмотреть список информационных сообщений в реальном времени, содержащий следующую информацию:



- *Дата и время* — дата и время, когда событие было сгенерировано;
- *Тип* — категория и уровень важности события;
- *Процесс* — имя процесса, сгенерировавшего сообщение;
- *Сообщение* — описание события.

Таблица 8 — Описание категорий важности событий

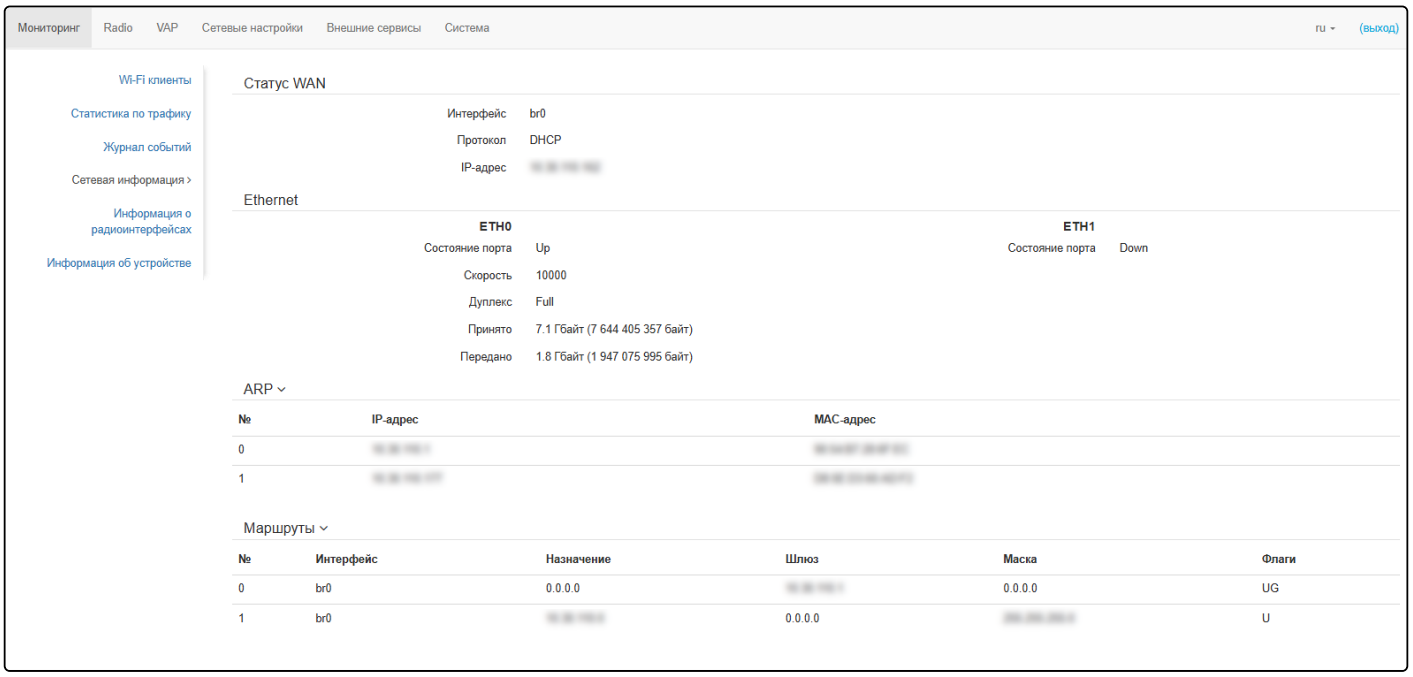
Уровень	Тип важности сообщений	Описание
0	Чрезвычайные (emergency)	В системе произошла критическая ошибка, система может работать неправильно
1	Сигналы тревоги (alert)	Необходимо немедленное вмешательство в систему
2	Критические (critical)	В системе произошла критическая ошибка
3	Ошибочные (error)	В 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

Для получения новых сообщений в журнале событий необходимо нажать на кнопку «Обновить».

При необходимости все старые сообщения из журнала можно удалить, нажав на кнопку «Очистить».

5.4.4 Подменю «Сетевая информация»

В подменю «**Сетевая информация**» осуществляется просмотр основных сетевых настроек устройства.



Статус WAN:

- *Интерфейс* — имя bridge-интерфейса;
- *Протокол* — протокол, используемый для доступа к сети WAN;
- *IP-адрес* — IP-адрес устройства во внешней сети;

Ethernet:

- *Состояние порта* — состояние Ethernet-порта;
- *Скорость* — скорость подключения по порту Ethernet;
- *Дуплекс* — режим передачи данных:
  - *Full* — полный дуплекс;
  - *Half* — полудуплекс.
- *Принято* — количество принятых на ETH байт;
- *Передано* — количество переданных с ETH байт.

ARP:

В ARP-таблице содержится информация о соответствии IP- и MAC-адресов соседних сетевых устройств:

- *IP-адрес* — IP-адрес устройства;
- *MAC-адрес* — MAC-адрес устройства.

Маршруты:

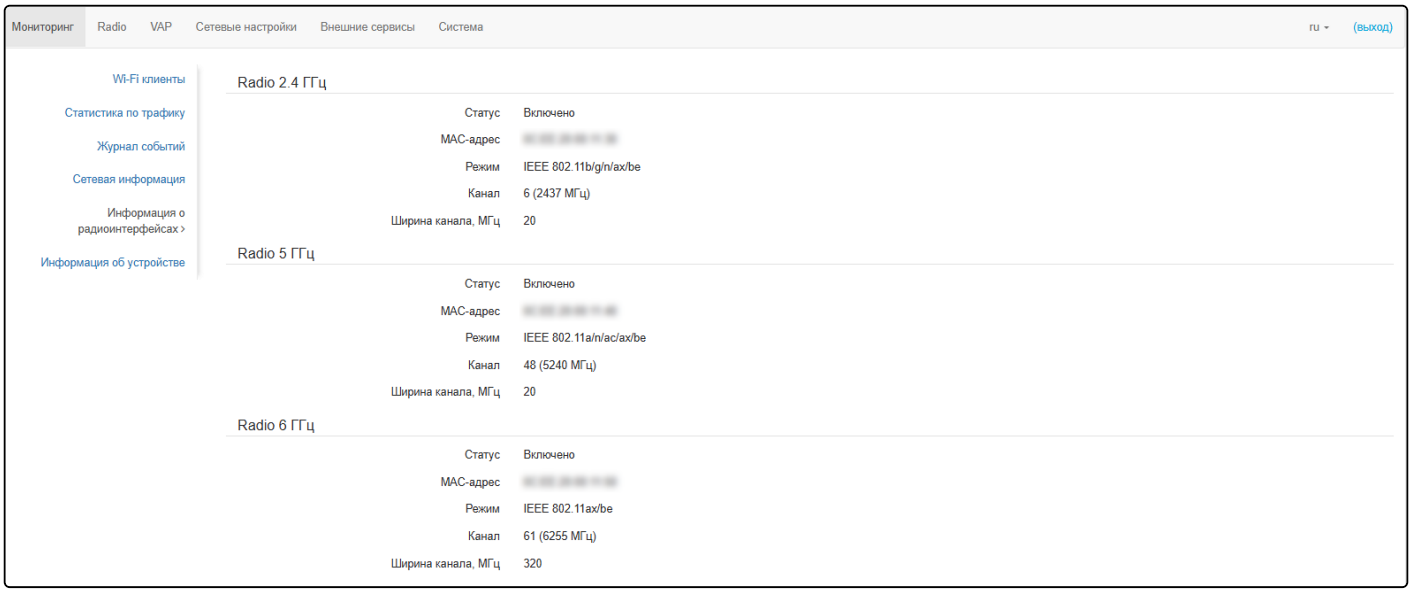
- *Интерфейс* — имя bridge-интерфейса;
- *Назначение* — IP-адрес хоста или подсети назначения, до которых установлен маршрут;
- *Шлюз* — IP-адрес шлюза, через который осуществляется выход на адресата;
- *Маска* — маска подсети;
- *Флаги* — определенные характеристики данного маршрута.

Существуют следующие значения флагов:

- **U** – указывает, что маршрут создан и является проходимым.
- **H** – указывает на маршрут к определенном узлу.
- **G** – указывает, что маршрут пролегает через внешний шлюз. Сетевой интерфейс системы предоставляет маршруты в сети с прямым подключением. Все прочие маршруты проходят через внешние шлюзы. Флагом G отмечаются все маршруты, кроме маршрутов в сети с прямым подключением.
- **R** – указывает, что маршрут, скорее всего, был создан динамическим протоколом маршрутизации, работающим на локальной системе, посредством параметра reinstate.
- **D** – указывает, что маршрут был добавлен в результате получения сообщения перенаправления ICMP (ICMP Redirect Message). Когда система узнает о маршруте из сообщения ICMP Redirect, маршрут включается в таблицу маршрутизации, чтобы исключить перенаправление для последующих пакетов, предназначенных тому же адресату.
- **M** – указывает, что маршрут подвергся изменению, вероятно, в результате работы динамического протокола маршрутизации на локальной системе и применения параметра mod.
- **A** – указывает на буферизованный маршрут, которому соответствует запись в таблице ARP.
- **C** – указывает, что источником маршрута является буфер маршрутизации ядра.
- **L** – указывает, что пунктом назначения маршрута является один из адресов данного компьютера. Такие «локальные маршруты» существуют только в буфере маршрутизации.
- **B** – указывает, что конечным пунктом маршрута является широковещательный адрес. Такие «широковещательные маршруты» существуют только в буфере маршрутизации.
- **I** – указывает, что маршрут связан с кольцевым (loopback) интерфейсом с целью иной, нежели обращение к кольцевой сети. Такие «внутренние маршруты» существуют только в буфере маршрутизации.
- **!** – указывает, что дейтаграммы, направляемые по этому адресу, будут отвергаться системой.

5.4.5 Подменю «Информация о радиоинтерфейсах»

В подменю «**Информация о радиоинтерфейсах**» отображено текущее состояние радиоинтерфейсов WEP-500K.



Радиоинтерфейсы точки доступа могут находиться в двух состояниях: «Включено» и «Выключено». Статус каждого из радиоинтерфейсов отражается в одноименном параметре «Статус».
Статус Radio зависит от того, есть ли на данном радиоинтерфейсе включенные виртуальные точки доступа (VAP). В случае если на радиоинтерфейсе имеется хотя бы одна активная VAP, Radio будет находиться в статусе «Включено», иначе — «Выключено».

В зависимости от статуса Radio для мониторинга доступна следующая информация:

«Выключено»:

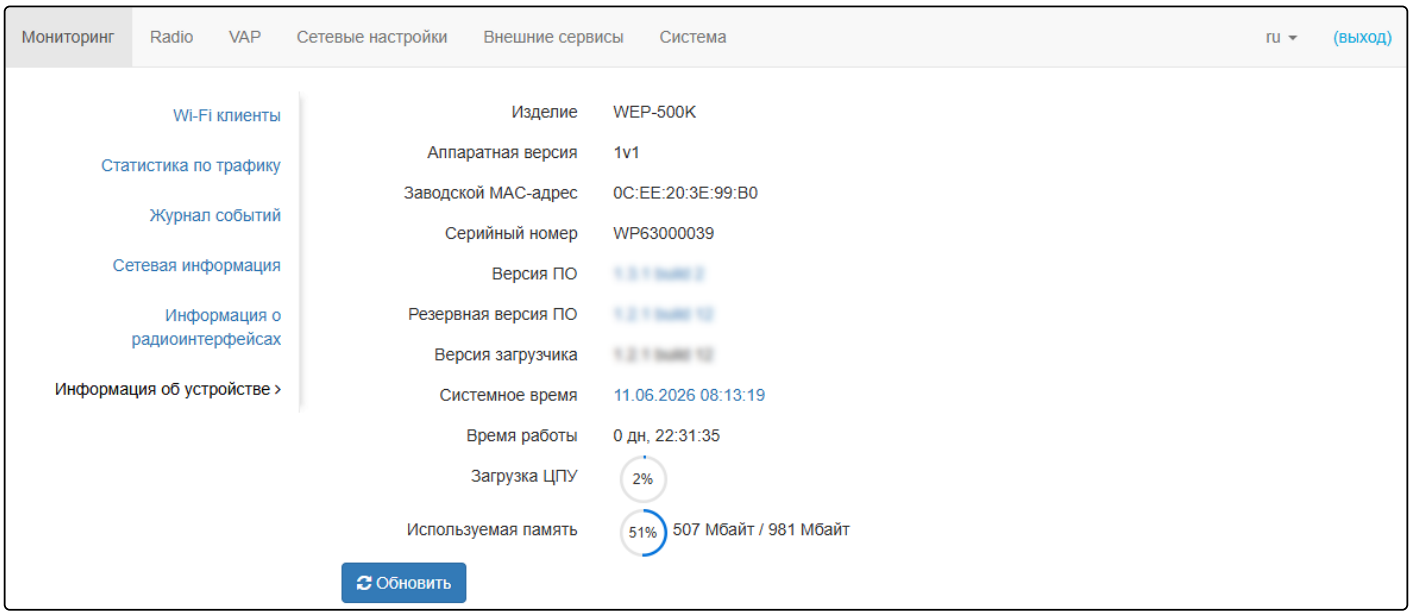
- *Статус* — состояние радиоинтерфейса;
- *MAC-адрес* — MAC-адрес радиоинтерфейса;
- *Режим* — режим работы радиоинтерфейса согласно стандартам IEEE 802.11.

«Включено»:

- *Статус* — состояние радиоинтерфейса;
- *MAC-адрес* — MAC-адрес радиоинтерфейса;
- *Режим* — режим работы радиоинтерфейса согласно стандартам IEEE 802.11;
- *Канал* — номер беспроводного канала, на котором работает радиоинтерфейс;
- *Ширина канала* — ширина полосы частот канала, на котором работает радиоинтерфейс.

5.4.6 Подменю «Информация об устройстве»

В подменю «**Информация об устройстве**» отображены основные характеристики WEP-500K.



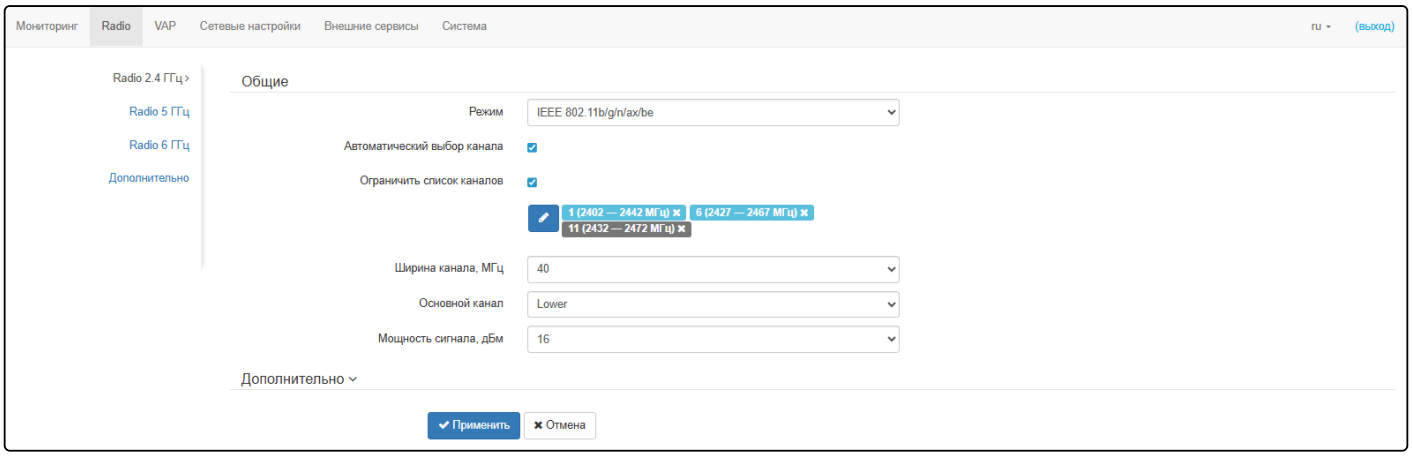
- *Изделие* – наименование модели устройства;
- *Аппаратная версия* – версия аппаратного обеспечения устройства;
- *Заводской MAC-адрес* – MAC-адрес WAN-интерфейса устройства, установленный заводом-изготовителем;
- *Серийный номер* – серийный номер устройства, установленный заводом-изготовителем;
- *Версия ПО* – версия программного обеспечения устройства;
- *Резервная версия ПО* – предыдущая установленная версия ПО;
- *Версия загрузчика* – версия программного обеспечения загрузчика устройства;
- *Системное время* – текущие время и дата, установленные в системе;
- *Время работы* – время работы с момента последнего включения или перезагрузки устройства;
- *Загрузка ЦПУ* – средний процент загрузки процессора за последние 5 секунд;
- *Используемая память* – процент использования оперативной памяти устройства.

5.5 Меню «Radio»

В меню «**Radio**» производится настройка радиоинтерфейсов устройства.

5.5.1 Подменю «Radio 2.4 ГГц»

В подменю «**Radio 2.4 ГГц**» осуществляются настройки основных параметров радиоинтерфейса устройства, работающего в диапазоне 2.4 ГГц.



Для подключения устройств в стандарте IEEE 802.11be (Wi-Fi 7) рекомендуется настройка режима безопасности WPA2/WPA3, WPA3 или OWE.

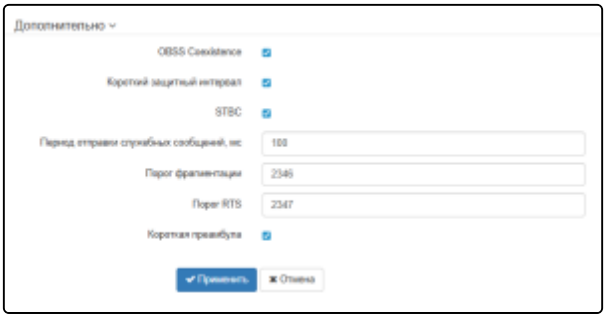
- *Режим* — режим работы интерфейса согласно следующим стандартам:
  - *IEEE 802.11b/g/n;*
  - *IEEE 802.11b/g/n/ax;*
  - *IEEE 802.11b/g/n/ax/be.*
- *Автоматический выбор канала* — при установленном флаге точка будет автоматически выбирать наименее загруженный радиоканал для работы Wi-Fi-интерфейса. При снятом флаге открывается доступ для установки статического рабочего канала;
- *Канал* — выбор канала передачи данных;
- *Ограничить список каналов* — при установленном флаге точка доступа будет использовать ограниченный пользователем список каналов для работы в автоматическом режиме выбора канала. Если флаг напротив «Ограничить список каналов» не установлен или в списке отсутствуют каналы, то точка доступа будет выбирать рабочий канал из всех доступных каналов данного диапазона частот. Каналы диапазона 2.4 ГГц: 1–13;
- *Ширина канала, МГц* — ширина полосы частот канала, на котором работает точка доступа, принимает значения 20 и 40 МГц;
- *Основной канал* — параметр может быть изменен только при пропускной способности статически заданного канала, равной 40 МГц. Канал 40 МГц можно считать состоящим из двух каналов по 20 МГц, которые граничат в частотной области. Эти два канала
  20 МГц называют первичным и вторичным каналами. Первичный канал используется клиентами, которые поддерживают только полосу пропускания канала 20 МГц:
  - *Upper* — первичным каналом будет верхний канал 20 МГц в полосе 40 МГц;
  - *Lower* — первичным каналом будет нижний канал 20 МГц в полосе 40 МГц.
- *Мощность сигнала, дБм* — регулировка мощности сигнала передатчика Wi-Fi в дБм. Принимает значение от 0 до 16 дБм.

В случае, если в списке «Ограничить список каналов» указан недоступный для выбора канал, то он будет отмечен серым цветом. Для того чтобы новая конфигурация была применена на точке доступа, в списке «Ограничить список каналов» должны быть указаны только доступные (выделенные синим цветом) каналы.
Пример. На точке доступа еще не производилось никаких настроек, по умолчанию на Radio 2.4 ГГц установлена «Ширина канала» 20 МГц, а в списке «Ограничить список каналов» указаны каналы: 1, 6, 11.
Допустим, необходимо установить параметр «Ширина канала», равный 40 МГц. При изменении данного параметра с 20 МГц на 40 МГц происходит следующее:

- для редактирования открывается параметр «Основной канал», принимающий значение по умолчанию «Lower»,
- канал 11 в списке «Ограничить список каналов» меняет свой цвет с синего на серый.

Если изменить параметр «Ширина канала» на 40 МГц и не удалить серые каналы из списка, то при нажатии на кнопку «Применить» в браузере появится ошибка «Введенные данные содержат ошибки. Изменения не были применены». Соответственно, конфигурация точки доступа изменена не будет. Это происходит по причине того, что каналы, выделенные серым цветом в списке «Ограничить список каналов», не подходят под определение «Основной канал» = Lower.

В разделе «Дополнительно» осуществляется настройка дополнительных параметров радиоинтерфейса устройства.

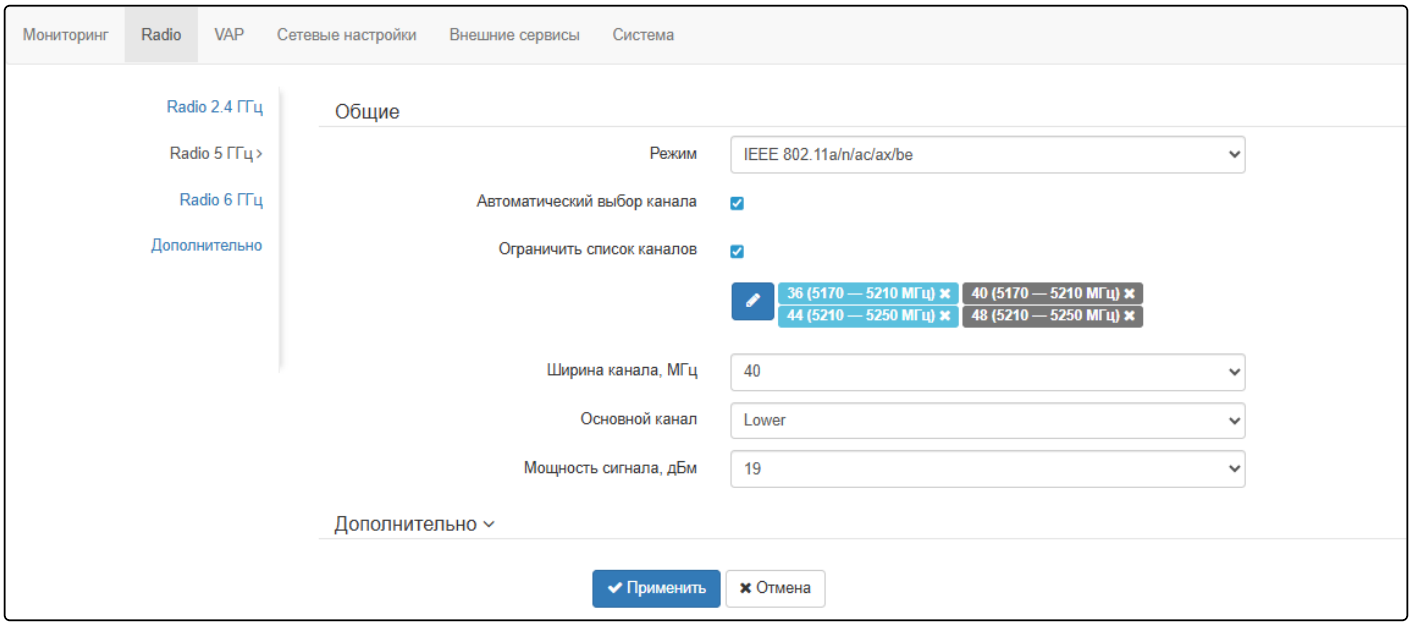


- *OBSS Coexistence* — режим автоматического уменьшения ширины канала при загруженном радиоэфире. При установленном флаге режим включен;
- *Короткий защитный интервал* — поддержка укороченного защитного интервала. Точка доступа передает данные, используя защитный интервал в 400 нс (вместо 800 нс) при общении с клиентами, которые также поддерживают короткий защитный интервал;
- *STBC* — метод пространственно-временного блочного кодирования, направленный на повышение надежности передачи данных. При установленном флаге устройство передает один поток данных через несколько антенн. Если флаг не установлен, устройство не передает один и тот же поток данных через несколько антенн;
- *Период отправки служебных сообщений* — период посылки Beacon-фреймов. Фреймы передаются для обнаружения точки доступа в эфире. Параметр принимает значения 20–2000 мс, по умолчанию — 100 мс;
- *Порог фрагментации* — порог фрагментации фрейма в байтах. Принимает значения 256–2346, по умолчанию — 2346;
- *Порог RTS* — указывает число байт, через которое посылается запрос на передачу (Request to Send). Уменьшение данного значения может улучшить работу точки доступа при большом количестве подключенных клиентов, однако это уменьшает общую пропускную способность беспроводной сети. Принимает значения 0–2347, по умолчанию — 2347;
- *Короткая преамбула* — использование короткой преамбулы пакета.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.5.2 Подменю «Radio 5 ГГц»

В подменю «**Radio 5 ГГц**» осуществляются настройки основных параметров радиоинтерфейса устройства, работающего в диапазоне 5 ГГц.



Для подключения устройств в стандарте IEEE 802.11be (Wi-Fi 7) рекомендуется настройка режима безопасности WPA2/WPA3, WPA3 или OWE.

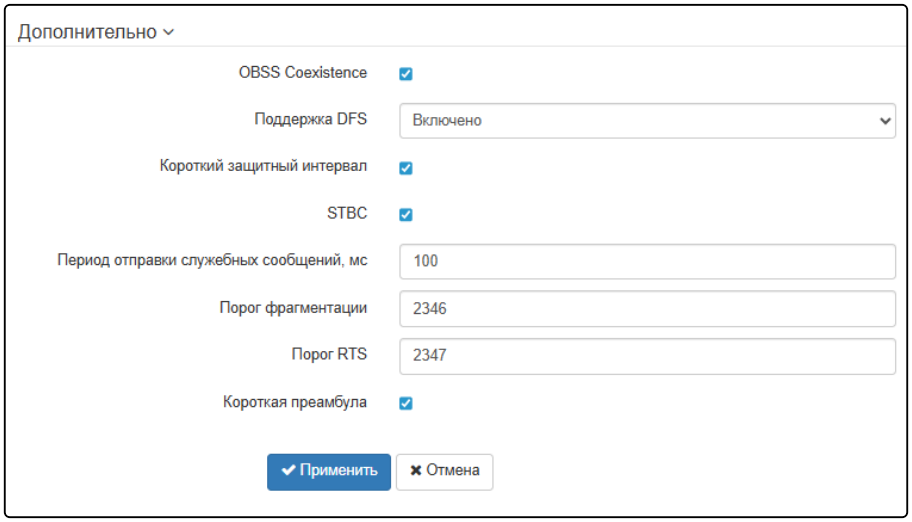
- *Режим* — режим работы интерфейса согласно стандартам:
  - *IEEE 802.11 a/n/ac;*
  - *IEEE 802.11a/n/ac/ax;*
  - *IEEE 802.11a/n/ac/ax/be.*
- *Автоматический выбор канала* — при установленном флаге точка будет автоматически выбирать наименее загруженный радиоканал для работы Wi-Fi интерфейса. При снятом флаге открывается доступ для установки статического рабочего канала;
- *Канал* — выбор канала передачи данных;
- *Ограничить список каналов* — при установленном флаге точка доступа будет использовать ограниченный пользователем список каналов для работы в автоматическом режиме выбора канала. Если флаг напротив «Ограничить список каналов» не установлен или в списке отсутствуют каналы, то точка доступа будет выбирать рабочий канал из всех доступных каналов данного диапазона частот. Каналы диапазона 5 ГГц: 36–64, 132–144, 149–165;
- *Ширина канала, МГц* — ширина полосы частот канала, на котором работает точка доступа, принимает значения 20, 40, 80 и 160 МГц;
- *Основной канал* — параметр может быть изменен только при пропускной способности статически заданного канала, равной 40 МГц. Канал 40 МГц можно считать состоящим из двух каналов по 20 МГц, которые граничат в частотной области. Эти два канала 20 МГц называют первичным и вторичным каналами. Первичный канал используется клиентами, которые поддерживают только полосу пропускания канала 20 МГц:
  - *Upper* — первичным каналом будет верхний канал 20 МГц в полосе 40 МГц;
  - *Lower* — первичным каналом будет нижний канал 20 МГц в полосе 40 МГц.
- *Мощность сигнала, дБм* — регулировка мощности сигнала передатчика Wi-Fi в дБм. Принимает значение от 0 до 19 дБм.

В случае, если в списке «Ограничить список каналов» указан недоступный для выбора канал, то он будет отмечен серым цветом. Для того чтобы новая конфигурация была применена на точке доступа, в списке «Ограничить список каналов» должны быть указаны только доступные (выделенные синим цветом) каналы.
Пример. На точке доступа еще не производилось никаких настроек, по умолчанию на Radio 5 ГГц установлена «Ширина канала» 20 МГц, а в списке «Ограничить список каналов» указаны каналы: 36, 40, 44, 48.
Допустим, необходимо установить параметр «Ширина канала», равный 40 МГц. При изменении данного параметра с 20 МГц на 40 МГц происходит следующее:

- для редактирования открывается параметр «Основной канал», принимающий значение по умолчанию «Upper»,
- каналы 36 и 44 в списке «Ограничить список каналов» меняют свой цвет с синего на серый.

Если изменить параметр «Ширина канала» на 40 МГц и не удалить серые каналы из списка, то при нажатии на кнопку «Применить» в браузере появится ошибка «Введенные данные содержат ошибки. Изменения не были применены». Соответственно, конфигурация точки доступа изменена не будет. Это происходит по причине того, что каналы, выделенные серым цветом в списке «Ограничить список каналов», не подходят под определение «Основной канал» = Upper.

В разделе «Дополнительно» осуществляется настройка дополнительных параметров радиоинтерфейса устройства.



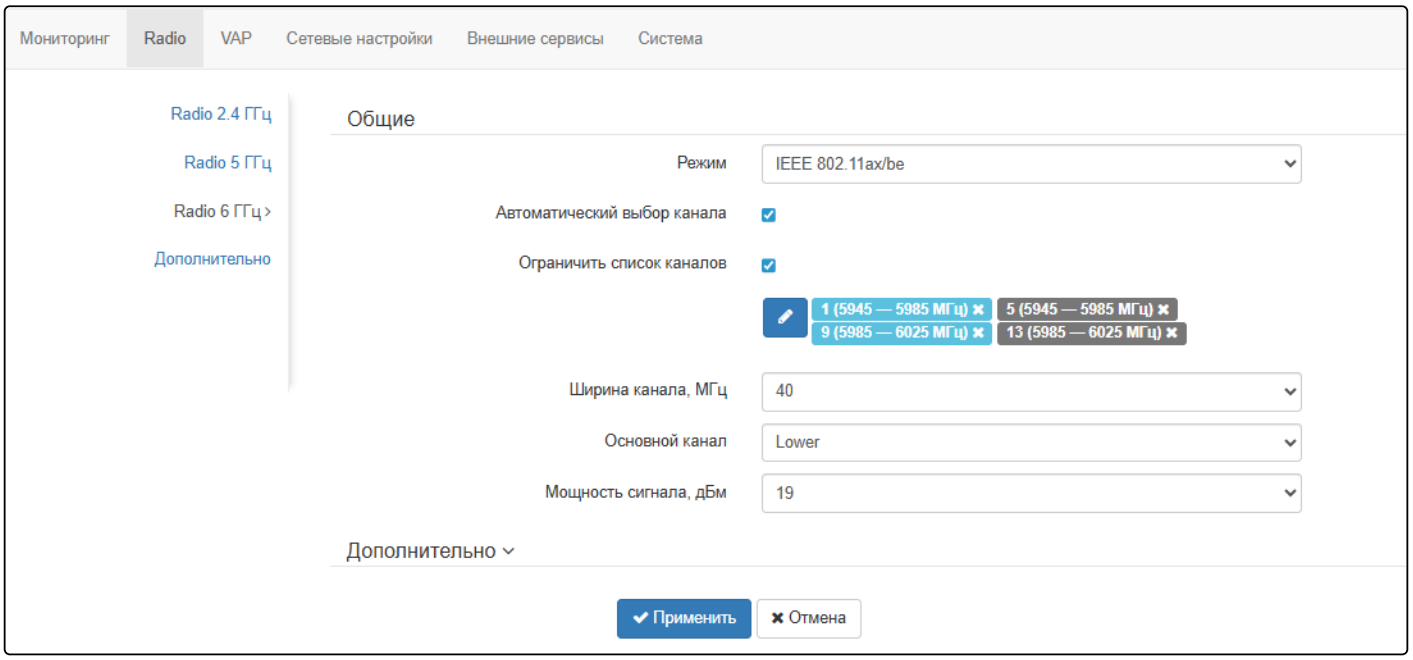
- *OBSS Coexistence* — режим автоматического уменьшения ширины канала при загруженном радиоэфире. При установленном флаге режим включен;
- *Поддержка DFS* — механизм динамического выбора частоты. Требует от беспроводных устройств сканировать радиоэфир и избегать использования каналов, совпадающих с каналами, на которых работают радиолокационные системы в 5 ГГц диапазоне:
  - *Выключено* — механизм выключен. DFS-каналы не доступны для выбора;
  - *Включено* — механизм включен;
  - *Принудительно* — механизм выключен. DFS-каналы доступны для выбора.
- *Короткий защитный интервал* — поддержка укороченного защитного интервала. Точка доступа передает данные, используя защитный интервал в 400 нс (вместо 800 нс) при общении с клиентами, которые также поддерживают короткий защитный интервал;
- *STBC* — метод пространственно-временного блочного кодирования, направленный на повышение надежности передачи данных. При установленном флаге устройство передает один поток данных через несколько антенн. Если флаг не установлен, устройство не передает один и тот же поток данных через несколько антенн;

- *Период отправки служебных сообщений* — период посылки Beacon-фреймов. Фреймы передаются для обнаружения точки доступа в эфире, принимает значения 20–2000 мс, по умолчанию — 100 мс;
- *Порог фрагментации* — порог фрагментации фрейма в байтах. Принимает значения 256–2346, по умолчанию — 2346;
- *Порог RTS* — указывает число байт, через которое посылается запрос на передачу (Request to Send). Уменьшение данного значения может улучшить работу точки доступа при большом количестве подключенных клиентов, однако это уменьшает общую пропускную способность беспроводной сети. Принимает значения 0–2347, по умолчанию — 2347;
- *Короткая преамбула* — использование короткой преамбулы пакета.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.5.3 Подменю «Radio 6 ГГц»

В подменю «**Radio 6 ГГц**» осуществляются настройки основных параметров радиоинтерфейса устройства, работающего в диапазоне 6 ГГц.



Для 6 ГГц доступны режимы безопасности только OWE, WPA3, WPA3-Enterprise.

- *Режим* — режим работы интерфейса согласно стандартам:
  - *IEEE 802.11ax;*
  - *IEEE 802.11ax/be.*
- *Автоматический выбор канала* — при установленном флаге точка будет автоматически выбирать наименее загруженный радиоканал для работы Wi-Fi интерфейса. При снятом флаге открывается доступ для установки статического рабочего канала;
- *Канал* — выбор канала передачи данных;
- *Ограничить список каналов* — при установленном флаге точка доступа будет использовать ограниченный пользователем список каналов для работы в автоматическом режиме выбора канала. Если флаг напротив «Ограничить список каналов» не установлен или в списке отсутствуют каналы, то точка доступа будет выбирать рабочий канал из всех доступных каналов данного диапазона частот. Каналы диапазона 6 ГГц: 1–93;

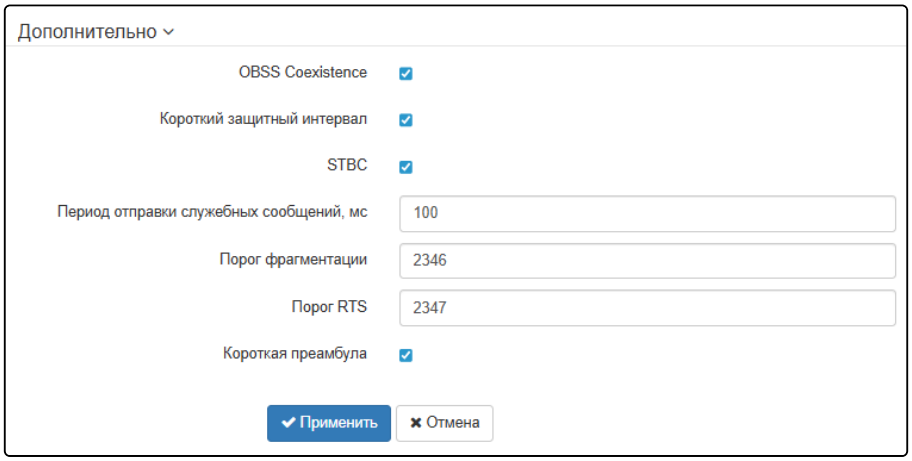
- *Ширина канала, МГц* — ширина полосы частот канала, на котором работает точка доступа, принимает значения 20, 40, 80, 160 и 320 МГц;
- *Основной канал* — параметр может быть изменен только при пропускных способностях статически заданных каналов, равных 40 МГц и 320 МГц.
    - Канал 40 МГц можно считать состоящим из двух каналов по 20 МГц, которые граничат в частотной области. Эти два канала 20 МГц называют первичным и вторичным каналами. Первичный канал используется клиентами, которые поддерживают только полосу пропускания канала 20 МГц:
        - *Upper* — первичным каналом будет верхний канал 20 МГц в полосе 40 МГц;
        - *Lower* — первичным каналом будет нижний канал 20 МГц в полосе 40 МГц.
    - Канал 320 МГц можно считать состоящим из двух полос по 160 МГц, которые граничат в частотной области. Канал, используемый клиентами, которые поддерживают только полосу пропускания 20 МГц, может размещаться в одной из этих полос:
        - *Upper* — канал передачи данных 20 МГц будет размещен в верхней полосе 160 МГц;
        - *Lower* — канал передачи данных 20 МГц будет размещен в нижней полосе 160 МГц.
- *Мощность сигнала, дБм* — регулировка мощности сигнала передатчика Wi-Fi в дБм. Принимает значение от 0 до 19 дБм.

В случае, если в списке «Ограничить список каналов» указан недоступный для выбора канал, то он будет отмечен серым цветом. Для того чтобы новая конфигурация была применена на точке доступа, в списке «Ограничить список каналов» должны быть указаны только доступные (выделенные синим цветом) каналы.
Пример. На точке доступа еще не производилось никаких настроек, по умолчанию на Radio 5 ГГц установлена «Ширина канала» 20 МГц, а в списке «Ограничить список каналов» указаны каналы: 1, 5, 9, 13.
Допустим, необходимо установить параметр «Ширина канала», равный 40 МГц. При изменении данного параметра с 20 МГц на 40 МГц происходит следующее:

- для редактирования открывается параметр «Основной канал», принимающий значение по умолчанию «Upper»,
- каналы 1 и 9 в списке «Ограничить список каналов» меняют свой цвет с синего на серый.

Если изменить параметр «Ширина канала» на 40 МГц и не удалить серые каналы из списка, то при нажатии на кнопку «Применить» в браузере появится ошибка «Введенные данные содержат ошибки. Изменения не были применены». Соответственно, конфигурация точки доступа изменена не будет. Это происходит по причине того, что каналы, выделенные серым цветом в списке «Ограничить список каналов», не подходят под определение «Основной канал» = Upper.

В разделе «Дополнительно» осуществляется настройка дополнительных параметров радиоинтерфейса устройства.



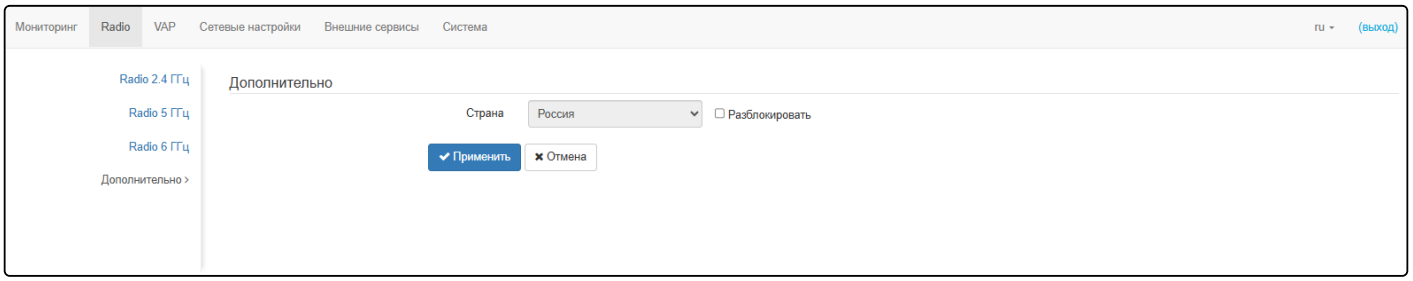
- *OBSS Coexistence* — режим автоматического уменьшения ширины канала при загруженном радиоэфире. При установленном флаге режим включен;

- *Короткий защитный интервал* — поддержка укороченного защитного интервала. Точка доступа передает данные, используя защитный интервал в 400 нс (вместо 800 нс) при общении с клиентами, которые также поддерживают короткий защитный интервал;
- *STBC* — метод пространственно-временного блочного кодирования, направленный на повышение надежности передачи данных. При установленном флаге устройство передает один поток данных через несколько антенн. Если флаг не установлен, устройство не передает один и тот же поток данных через несколько антенн;
- *Период отправки служебных сообщений* — период посылки Beacon-фреймов. Фреймы передаются для обнаружения точки доступа в эфире, принимает значения 20–2000 мс, по умолчанию — 100 мс;
- *Порог фрагментации* — порог фрагментации фрейма в байтах. Принимает значения 256–2346, по умолчанию — 2346;
- *Порог RTS* — указывает число байт, через которое посылается запрос на передачу (Request to Send). Уменьшение данного значения может улучшить работу точки доступа при большом количестве подключенных клиентов, однако это уменьшает общую пропускную способность беспроводной сети. Принимает значения 0–2347, по умолчанию — 2347;
- *Короткая преамбула* — использование короткой преамбулы пакета.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.5.4 Подменю «Дополнительно»

В подменю «**Дополнительно**» осуществляется настройка дополнительных параметров радиоинтерфейсов устройства.



- *Страна* — название страны, в которой работает точка доступа. Для выбора страны нужно выставить флаг «Разблокировать». 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.

> Настройка локальных (региональных) ограничений, включая работу на разрешенных частотных каналах и выходной мощности, является ответственностью инсталляторов.

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

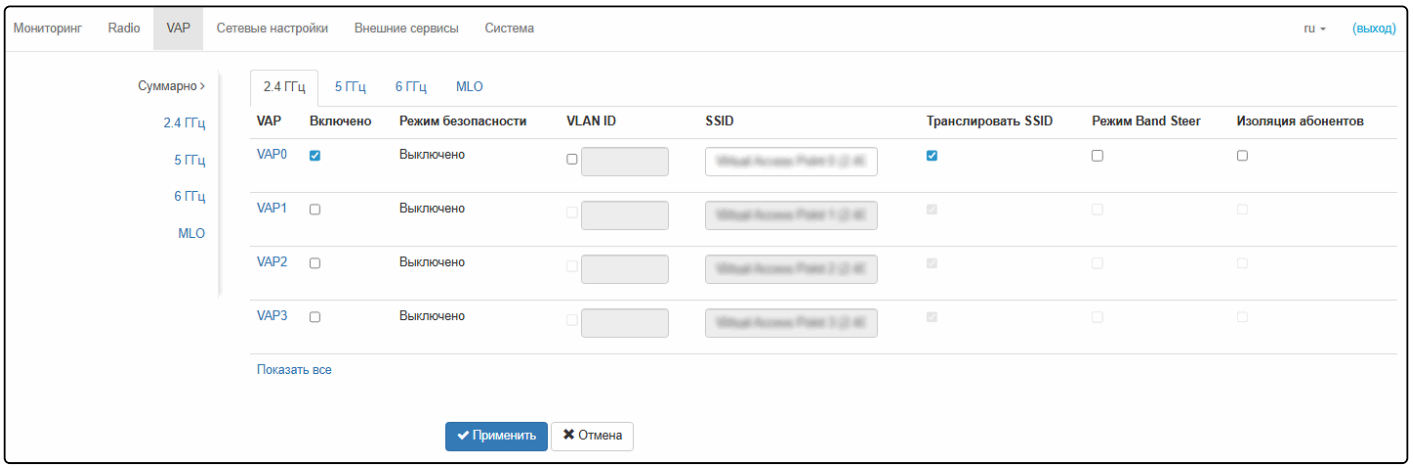
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.6 Меню «VAP»

В меню **«VAP»** выполняется настройка виртуальных точек доступа Wi-Fi (VAP) и групп Multi-link Operation (MLO) .

5.6.1 Подменю «Суммарно»

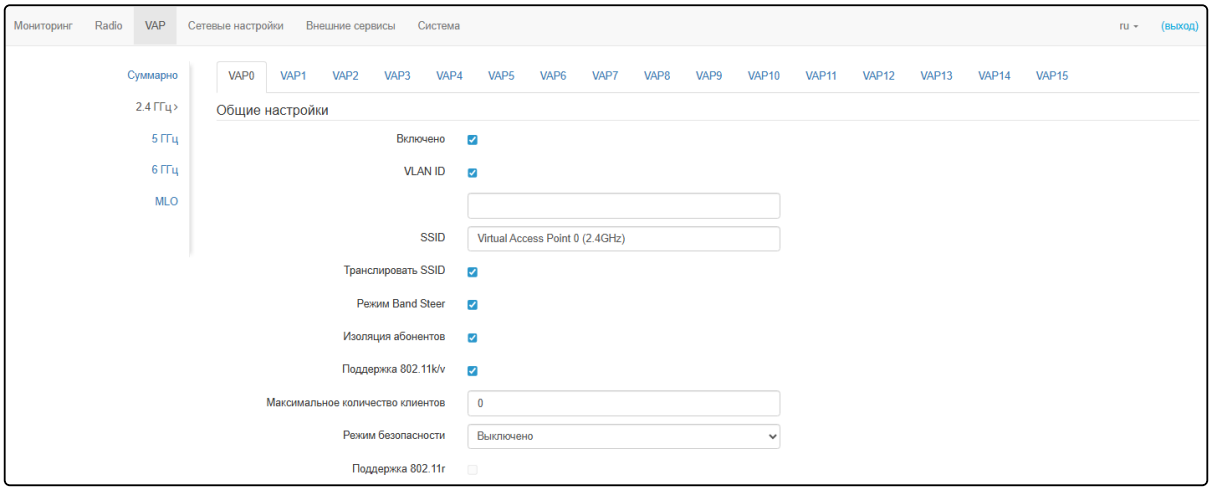
В подменю «**Суммарно**» отображаются настройки всех VAP на радиоинтерфейсах Radio 2.4 ГГц, Radio 5 ГГц и Radio 6 ГГц, а также настройки MLO-групп. Можно посмотреть настройки каждой виртуальной точки в разделах VAP0–VAP15, MLO-групп 1–16.



- *VAP0–VAP15* — порядковый номер виртуальной точки доступа;
- *1-16* — порядковый номер группы MLO;
- *Включено* — при установленном флаге виртуальная точка доступа включена, иначе — выключена;
- *Режим безопасности* — тип шифрования данных, используемый на виртуальной точке доступа;
- *VLAN ID* — номер VLAN, с которого будет сниматься тег при передаче трафика Wi-Fi клиентам, подключенным к данной VAP. При прохождении трафика в обратную сторону на нетегированный трафик от клиентов будет навешиваться тег VLAN ID;
- *SSID* — имя виртуальной беспроводной сети;
- *Транслировать SSID* — при установленном флаге включено вещание в эфир SSID, иначе — выключено;
- *Режим Band Steer* — при установленном флаге активно приоритетное подключение клиента к 5 ГГц сети. Для работы функции нужно создать VAP с одинаковым SSID как минимум на двух радиоинтерфейсах и активировать на них параметр «Режим Band Steer»;
- *Изоляция абонентов* — при установленном флаге включена изоляция трафика между клиентами в пределах одной VAP.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.6.2 Подменю «VAP»



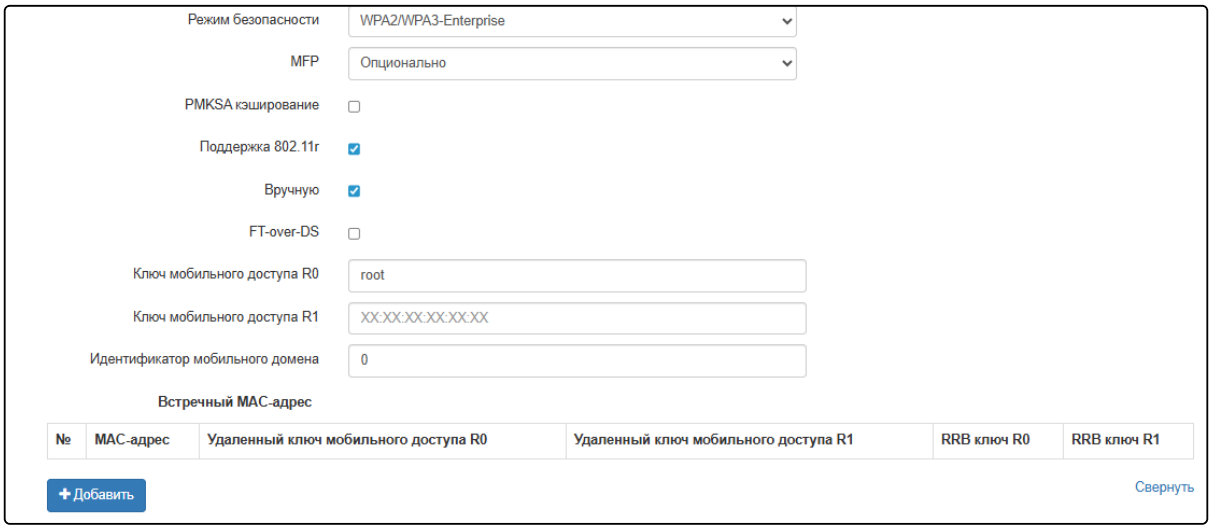
Общие настройки:

- *Включено* — при установленном флаге виртуальная точка доступа включена, иначе — выключена;
- *VLAN ID* — номер VLAN, с которого будет сниматься тег при передаче трафика Wi-Fi клиентам, подключенным к данной VAP. При прохождении трафика в обратную сторону на нетегированный трафик от клиентов будет навешиваться тег VLAN ID;
- *SSID* — имя виртуальной беспроводной сети;
- *Транслировать SSID* — при установленном флаге включено вещание в эфир SSID, иначе — выключено;
- *Режим Band Steer* — при установленном флаге активно приоритетное подключение клиента к 5 ГГц сети. Для работы функции нужно создать VAP с одинаковым SSID как минимум на двух радиоинтерфейсах и активировать на них параметр «Режим Band Steer»;
- *Изоляция абонентов* — при установленном флаге включена изоляция трафика между клиентами в пределах одной VAP;
- *Поддержка 802.11k/v* — включить поддержку стандартов 802.11k/v на виртуальной точке доступа;
- *Максимальное количество клиентов* — максимально допустимое число подключаемых к виртуальной сети клиентов;
- *Режим безопасности* — режим безопасности доступа к беспроводной сети:

Для подключения устройств в стандарте IEEE 802.11be (Wi-Fi 7), рекомендуется настройка режима безопасности WPA2/WPA3, WPA3 или OWE.

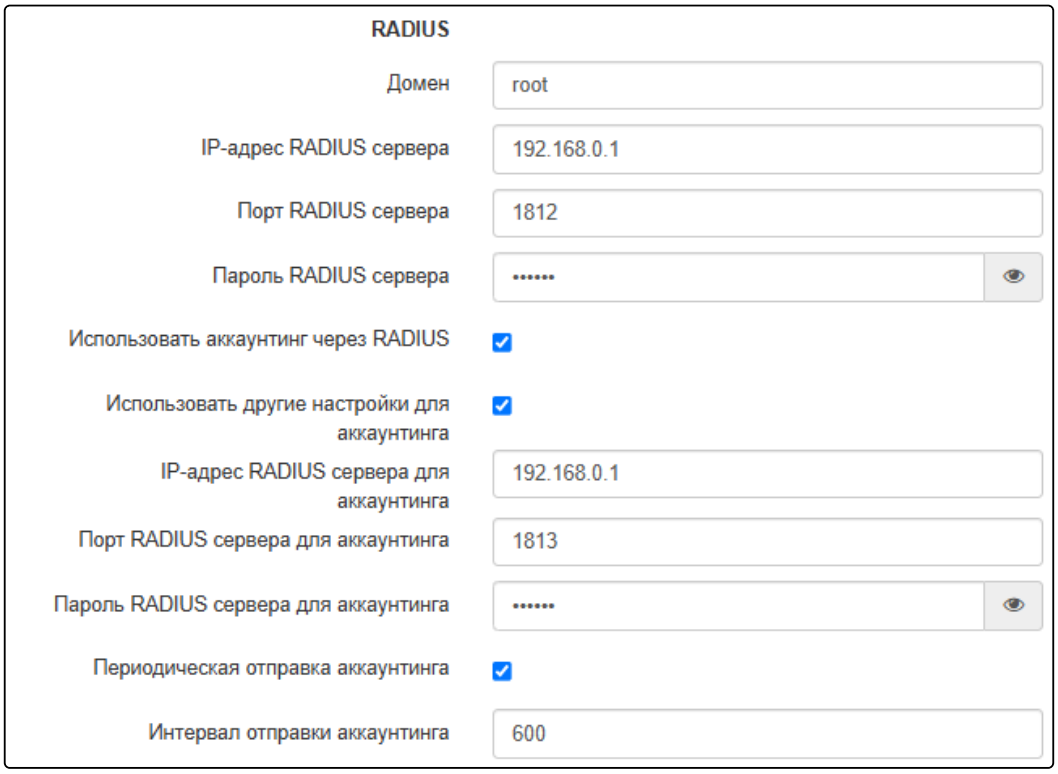
  - *Выключено* — не использовать шифрование для передачи данных. Точка доступна для подключения любого клиента;
  - *OWE (Opportunistic Wireless Encryption)* — метод шифрования, обеспечивающий безопасность данных, передаваемых по незащищенной сети.
    При этом от пользователей не требуется каких-то дополнительных действий и ввода пароля для подключения к сети;
  - *WPA, WPA2, WPA/WPA2, WPA2/WPA3, WPA3* — способы шифрования, при выборе одного из способов будет доступна следующая настройка:
    - *Ключ WPA* — ключ/пароль, необходимый для подключения к виртуальной точке доступа. Длина ключа составляет от 8 до 63 символов.
  - *WPA-Enterprise, WPA2-Enterprise, WPA/WPA2-Enterprise, WPA2/WPA3-Enterprise, WPA3-Enterprise* — режим шифрования канала беспроводной связи, при котором клиент авторизуется на централизованном RADIUS-сервере. Для настройки данного режима безопасности требуется указать параметры RADIUS-сервера. Также требуется указать ключ

для RADIUS-сервера. При выборе определенного режима безопасности будут доступны следующие настройки.



- *MFP* — защита management-кадров (доступно при режиме безопасности WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise и WPA3-Enterprise, при выборе других режимов безопасности MFP переводится в состояние *Отключено*, при выборе режима безопасности WPA3, WPA3-Enterprise, MFP переводится в состояние *Включено*):
  - *Отключено* — защита management-кадров отключена;
  - *Опционально* — защита работает, если клиент поддерживает MFP. Клиенты без поддержки MFP могут подключиться к данной VAP;
  - *Включено* — защита включена, клиенты, не поддерживающие MFP, подключиться не могут.
- *PMKSA кэширование* — флаг управляет включением кэширования информации о подключении Enterprise-клиента. При включении данной функции точка доступа запоминает клиентское устройство после авторизации на 12 часов и не требует повторной аутентификации на RADIUS-сервере при подключении в течение этого времени. Включение данной функции сокращает время роуминга при возвращении клиента на точку в режиме WPA Enterprise. Настройка доступна только при режимах безопасности Enterprise;
- *802.11r* — функционал быстрого роуминга, работает только с клиентами, которые поддерживают стандарт IEEE 802.11r. Роуминг 802.11r возможен только между VAP с режимами безопасности WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA2/WPA3-Enterprise.
  - *Поддержка 802.11r* — включить поддержку стандарта 802.11r на виртуальной точке доступа;
  - *Вручную* — при установленном флаге появляется возможность ручной настройки параметров роуминга;
  - *FT-over-DS* — включение режима «Over the DS»;
  - *Ключ мобильного доступа R0* — уникальный ключ для данной VAP, например, серийный номер;
  - *Ключ мобильного доступа R1* — MAC-адрес VAP (можно посмотреть в выводе команды ifconfig);
  - *Идентификатор мобильного домена* — номер группы, в рамках которой может быть совершен роуминг. Принимает значения от 0 до 65535;
  - *Встречный MAC-адрес:*
    - *MAC-адрес* — MAC-адрес VAP-интерфейса встречной точки доступа. Максимальное количество — 256;
    - *Удаленный ключ мобильного доступа R0* — уникальный ключ, должен совпадать с «Ключ мобильного доступа R0» на VAP встречной ТД;
    - *Удаленный ключ мобильного доступа R1* — MAC-адрес VAP на встречной ТД;
    - *RRB ключ R0* — случайный ключ. Не должен совпадать с «RRB ключ R1», но обязательно должен совпадать с «RRB ключ R1» встречной ТД. Длина ключа — 16 символов;
    - *RRB ключ R1* — случайный ключ. Не должен совпадать с «RRB ключ R0», но обязательно должен совпадать с «RRB ключ R0» встречной ТД. Длина ключа — 16 символов.

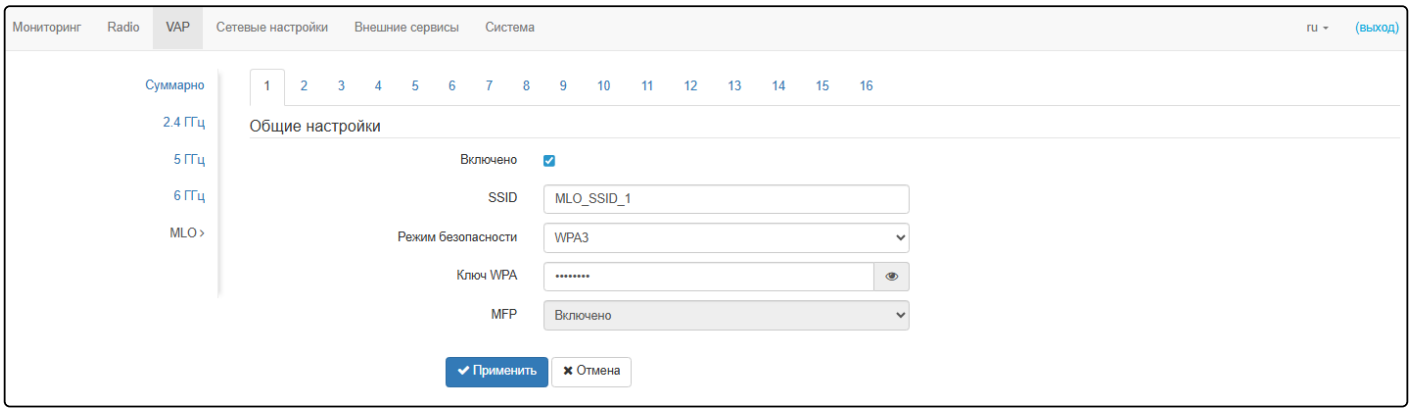
RADIUS:



- *Домен* — домен пользователя;
- *IP-адрес RADIUS сервера* — адрес RADIUS-сервера;
- *Порт RADIUS сервера* — порт RADIUS-сервера, который используется для аутентификации и авторизации;
- *Пароль RADIUS сервера* — пароль для RADIUS-сервера, используемого для аутентификации и авторизации;
- *Использовать аккаунтинг через RADIUS* — при установленном флаге будут отправляться сообщения «Accounting» на RADIUS-сервер;
- *Использовать другие настройки для аккаунтинга:*
  - *IP-адрес RADIUS сервера для аккаунтинга* — адрес RADIUS-сервера, используемого для аккаунтинга;
  - *Пароль RADIUS сервера для аккаунтинга* — пароль для RADIUS-сервера, используемого для аккаунтинга;
- *Порт RADIUS сервера для аккаунтинга* — порт, который будет использован для сбора аккаунтинга на RADIUS-сервере;
- *Пароль RADIUS сервера* — пароль для RADIUS-сервера, используемого для аутентификации и авторизации;
- *Периодическая отправка аккаунтинга* — включить периодическую отправку сообщений «Accounting» на RADIUS-сервер. Задать интервал отправки сообщений можно в поле «Интервал отправки аккаунтинга».

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.6.3 Подменю «MLO»



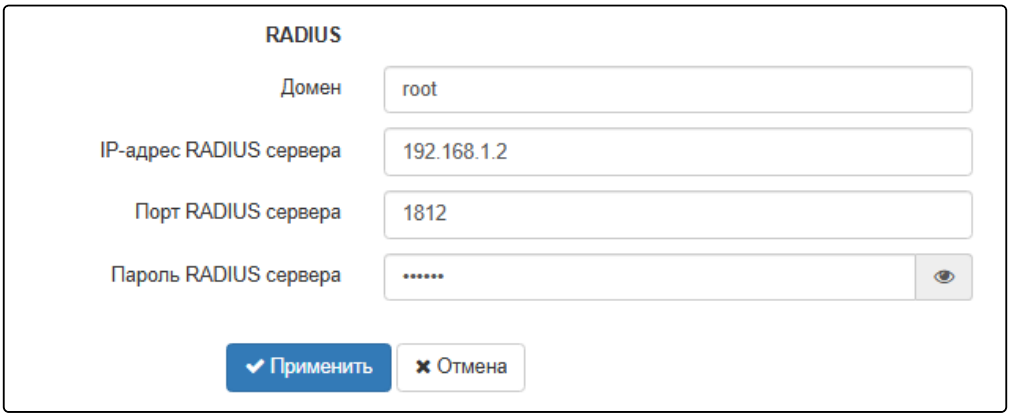
MLO (Multi-Link Operation) представляет из себя ключевую функцию стандарта Wi-Fi 7, которая позволяет устройству (например, смартфону) подключаться к точке доступа одновременно по нескольким диапазонам (2.4 ГГц, 5 ГГц и 6 ГГц).

MLO-группа под номером N использует VAP'ы под номером N-1 на всех радиодиапазонах, что приводит к тому, что настройки соответствующих VAP становятся недоступны при включении MLO-группы.

Общие настройки:

- *Включено* — при установленном флаге виртуальная точка доступа включена, иначе — выключена;
- *SSID* — имя виртуальной беспроводной сети;
- *Режим безопасности* — режим безопасности доступа к беспроводной сети:
  - *OWE (Opportunistic Wireless Encryption)* — метод шифрования, обеспечивающий безопасность данных, передаваемых по незащищенной сети.
    При этом от пользователей не требуется каких-то дополнительных действий и ввода пароля для подключения к сети.
  - *WPA3* — способы шифрования, при выборе одного из способов будет доступна следующая настройка:
    - *Ключ WPA* — ключ/пароль, необходимый для подключения к виртуальной точке доступа. Длина ключа составляет от 8 до 63 символов.
  - *WPA3-Enterprise* — режим шифрования канала беспроводной связи, при котором клиент авторизуется на централизованном RADIUS-сервере. Для настройки данного режима безопасности требуется указать параметры RADIUS-сервера (см. скрин ниже).
- *MFP* — защита management-кадров (доступно при режиме безопасности WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA2/WPA3-Enterprise и WPA3-Enterprise, при выборе других режимов безопасности MFP переводится в состояние *Отключено*, при выборе режима безопасности WPA3, WPA3-Enterprise, MFP переводится в состояние *Включено*):
  - *Включено* — защита включена, клиенты, не поддерживающие MFP, подключиться не могут (значение опции установлено по умолчанию, а иные варианты в данном режиме не предусмотрены).

RADIUS:

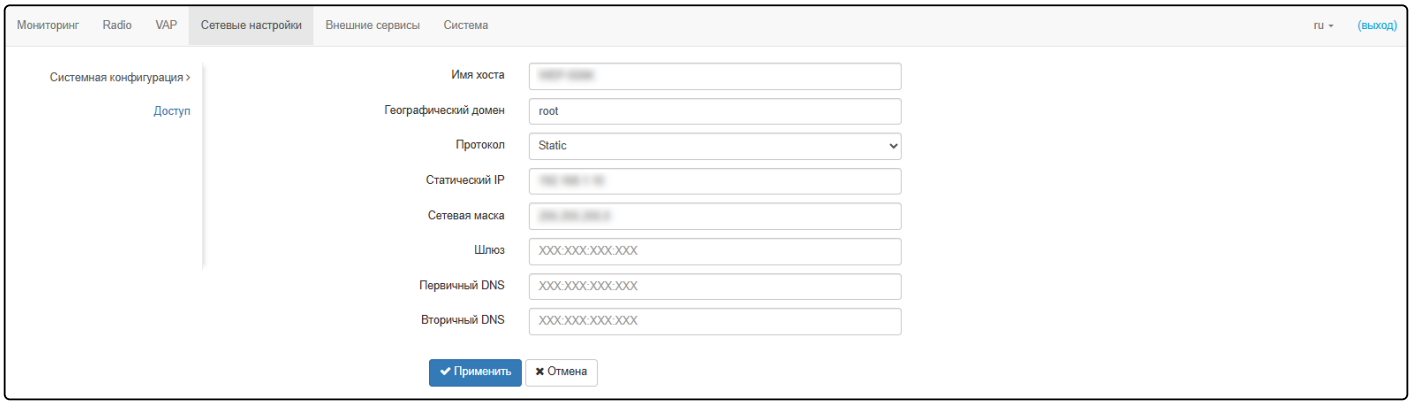


- *Домен* – домен пользователя;
- *IP-адрес RADIUS сервера* – адрес RADIUS-сервера;
- *Порт RADIUS сервера* – порт RADIUS-сервера, который используется для аутентификации и авторизации;
- *Пароль RADIUS сервера* – пароль для RADIUS-сервера, используемого для аутентификации и авторизации;

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.7 Меню «Сетевые настройки»

5.7.1 Подменю «Системная конфигурация»



- *Имя хоста* — сетевое имя устройства, задается строка 1–63 символов: латинские заглавные и строчные буквы, цифры, знак дефис «-» (дефис не может быть последним символом в имени);
- *Географический домен* — домен узла дерева устройств системы управления EMS, в котором располагается точка доступа;
- *Протокол* — выбор протокола, по которому будет осуществляться подключение по Ethernet-интерфейсу 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* — режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *Статический IP* — IP-адрес WAN-интерфейса устройства в сети провайдера;
    - *Сетевая маска* — маска внешней подсети;
    - *Шлюз* — адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации.
- *Первичный DNS, Вторичный DNS* — IP-адреса DNS-серверов. Если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, задайте их вручную.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

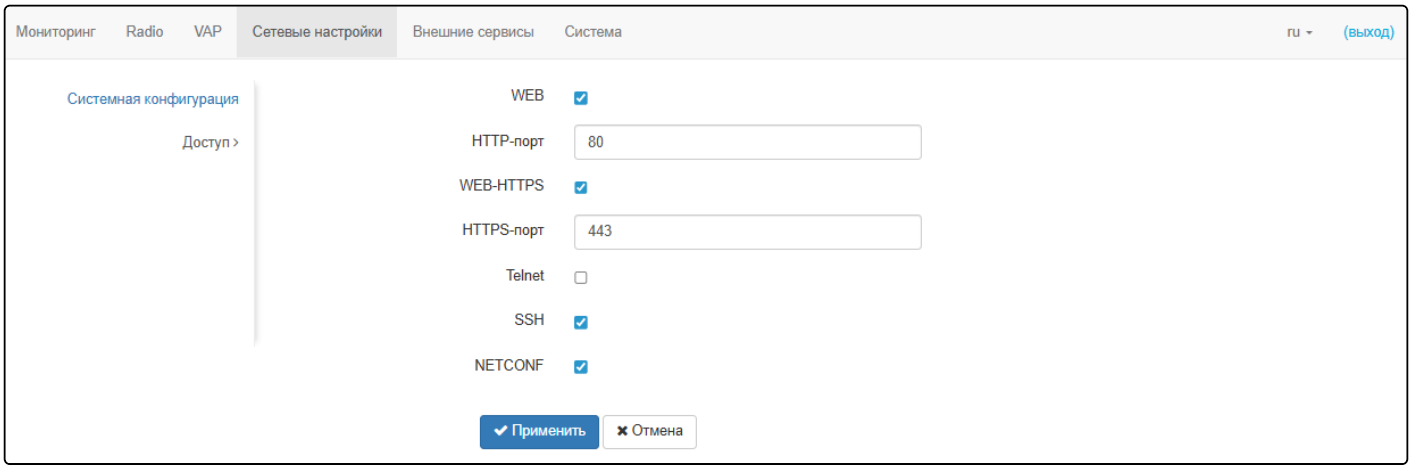
5.7.2 Подменю «Доступ»

В подменю «**Доступ**» производится настройка доступа к устройству посредством web-интерфейса, Telnet, SSH, NETCONF.

- Для включения доступа к устройству через web-интерфейс по протоколу HTTP установите флаг напротив «WEB». В появившемся окне есть возможность поменять HTTP-порт (по умолчанию — 80). Диапазон допустимых значений портов, помимо установленного по умолчанию, с 1025 по 65535 включительно;
- Для включения доступа к устройству через web-интерфейс по протоколу HTTPS установите флаг напротив «WEB-HTTPS». В появившемся окне есть возможность поменять HTTPS-порт (по умолчанию — 443). Диапазон допустимых значений портов, помимо установленного по умолчанию, с 1025 по 65535 включительно;

> Порты для протоколов HTTP и HTTPS не должны иметь одинаковое значение.

- Для включения доступа к устройству через Telnet установите флаг напротив «Telnet»;
- Для включения доступа к устройству через SSH установите флаг напротив «SSH»;
- Для включения доступа к устройству через NETCONF установите флаг напротив «NETCONF».



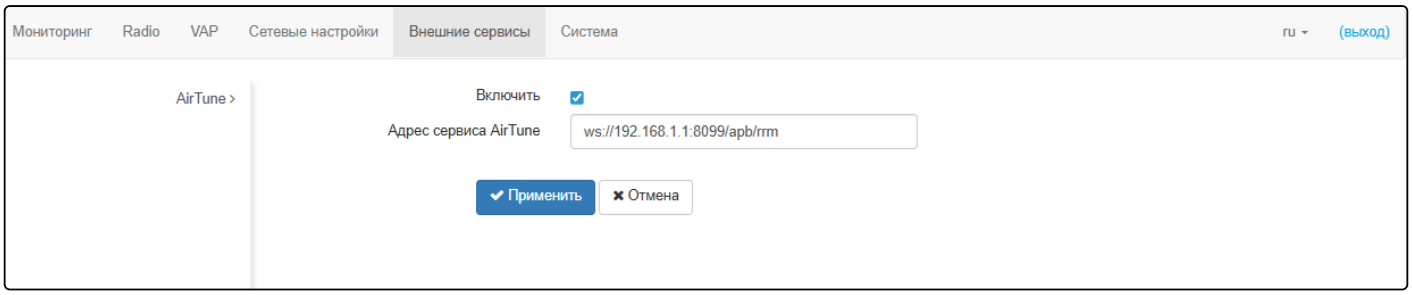
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.8 Меню «Внешние сервисы»

5.8.1 Подменю «AirTune»

Подменю «**AirTune**» предназначено для включения и настройки сервиса AirTune на точке доступа.

Сервис AirTune используется для оптимизации радиоресурсов (Radio Resource Management) и автоматической настройки бесшовного роуминга 802.11 k/r.



- *Включить* — при установленном флаге точка будет подключаться к сервису AirTune, адрес которого указан в поле «Адрес сервиса AirTune», для обеспечения функций Radio Resource Management и/или роуминга 802.11 k/r;
- *Адрес сервиса AirTune* — адрес сервиса AirTune. Задается в формате: «ws://<host>:<port>/apb/rrm».

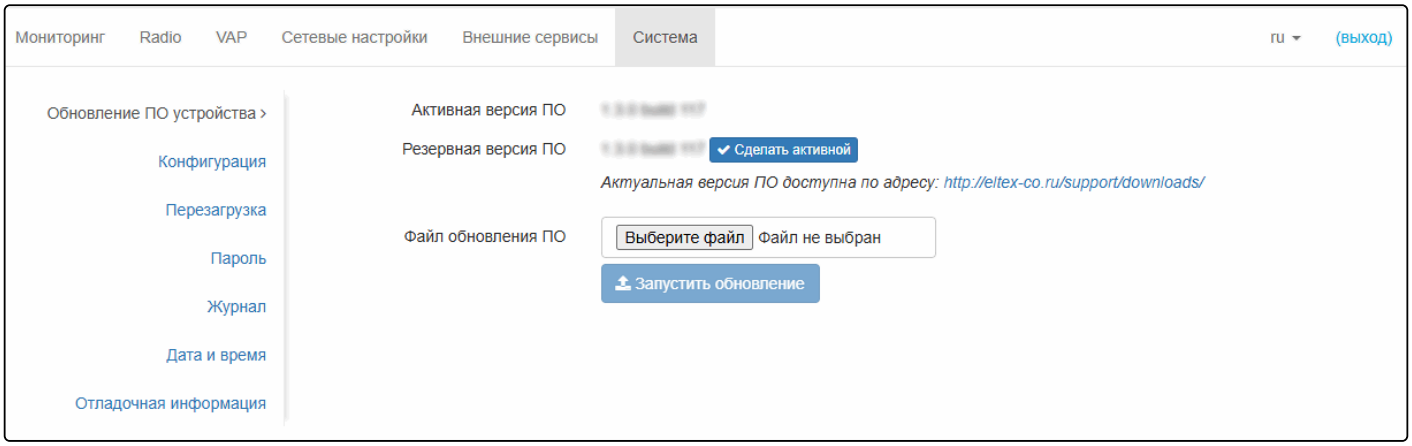
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.9 Меню «Система»

В меню «**Система**» выполняются настройки системы, времени, доступа к устройству по различным протоколам, производится смена пароля и обновление программного обеспечения устройства.

5.9.1 Подменю «Обновление ПО устройства»

Подменю «**Обновление ПО устройства**» предназначено для обновления программного обеспечения устройства.



- *Активная версия ПО* — версия программного обеспечения, установленного на устройстве, работающая в данный момент;
- *Резервная версия ПО* — версия программного обеспечения, установленного на устройстве, на которую можно переключиться без загрузки файла ПО.
  - *Сделать активной* — кнопка, позволяющая сделать резервную версию ПО активной, для этого потребуется перезагрузка устройства. Активная версия ПО в этом случае станет резервной.

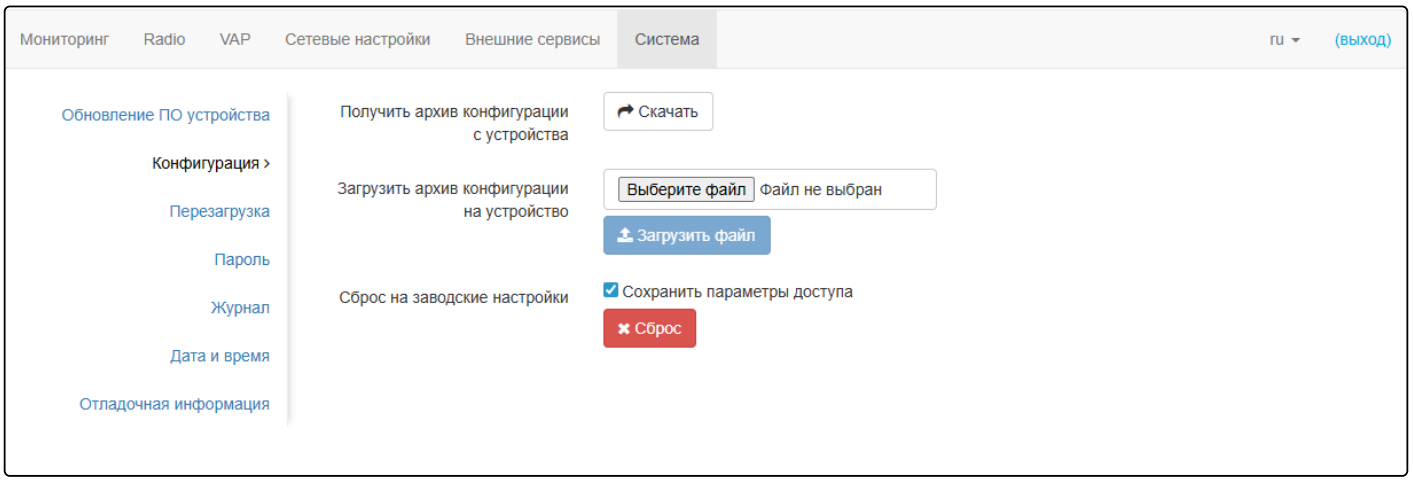
Обновление программного обеспечения

Загрузите файл ПО с сайта https://eltex.ru/download, выбрав WEP-500K в списке устройств и сохраните его на компьютере. После этого нажмите кнопку «Выберите файл» в поле *Файл обновления ПО* и укажите путь к файлу ПО в формате .tar.gz.
Для запуска процесса обновления необходимо нажать кнопку «Запустить обновление». Процесс обновления займет несколько минут (о его текущем статусе будет указано на странице), после чего устройство автоматически перезагрузится.

Не отключайте питание устройства и не выполняйте его перезагрузку в процессе обновления ПО.

5.9.2 Подменю «Конфигурация»

В подменю «**Конфигурация**» выполняется сохранение и обновление текущей конфигурации.



Получение конфигурации

Чтобы сохранить текущую конфигурацию устройства на локальный компьютер, нажмите кнопку «Скачать».

Обновление конфигурации

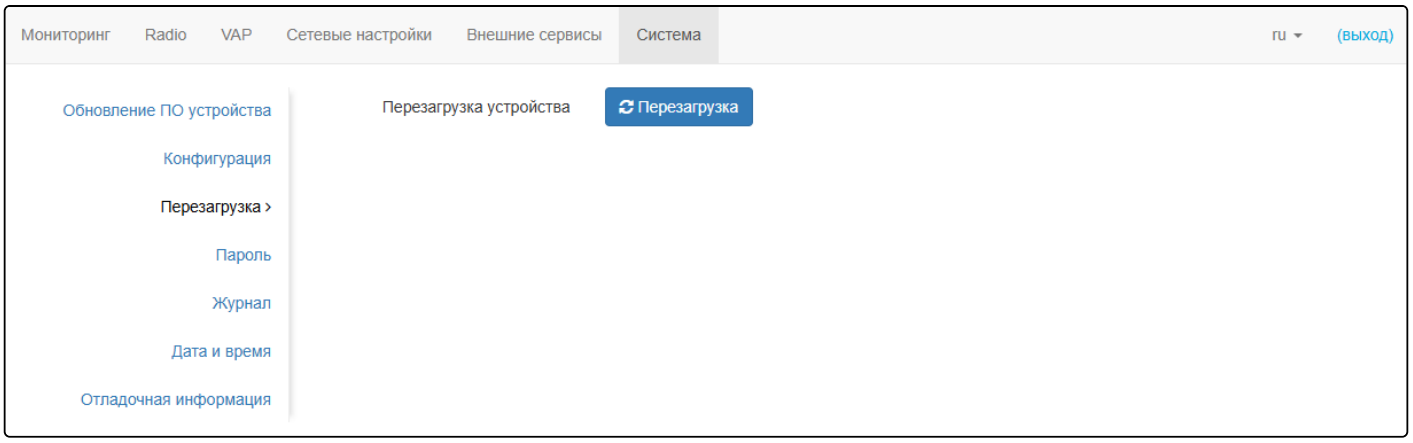
Для загрузки сохраненного на локальном компьютере файла конфигурации используется пункт «*Загрузить архив конфигурации на устройство*». Для обновления конфигурации устройства нажмите кнопку «Выберите файл», укажите файл (в формате .tar.gz) и нажмите кнопку «Загрузить файл». Загруженная конфигурация применяется автоматически без перезагрузки устройства.

Сброс устройства на заводские настройки

Чтобы сделать сброс всех настроек устройства на стандартные заводские установки, нажмите кнопку «Сброс». Если активирован флаг «Сохранить параметры доступа», то будут сохранены те параметры конфигурации, которые отвечают за доступ к устройству (настройка IP-адреса, настройки доступа по Telnet/SSH/NETCONF/Web).

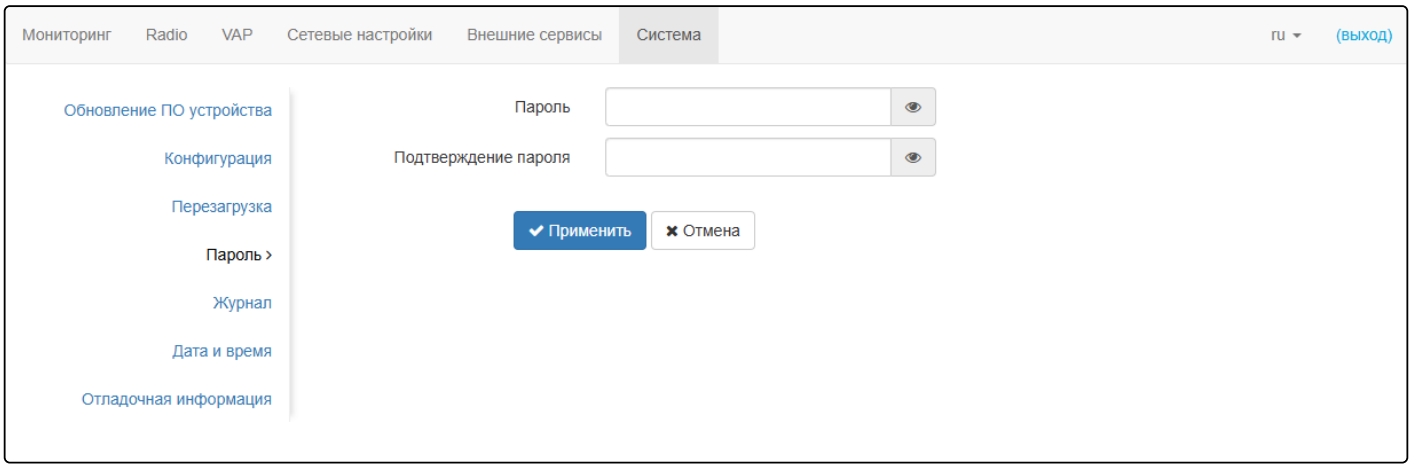
5.9.3 Подменю «Перезагрузка»

Для перезагрузки устройства нажмите на кнопку «Перезагрузка». Процесс перезапуска устройства занимает примерно 1,5 минуты.



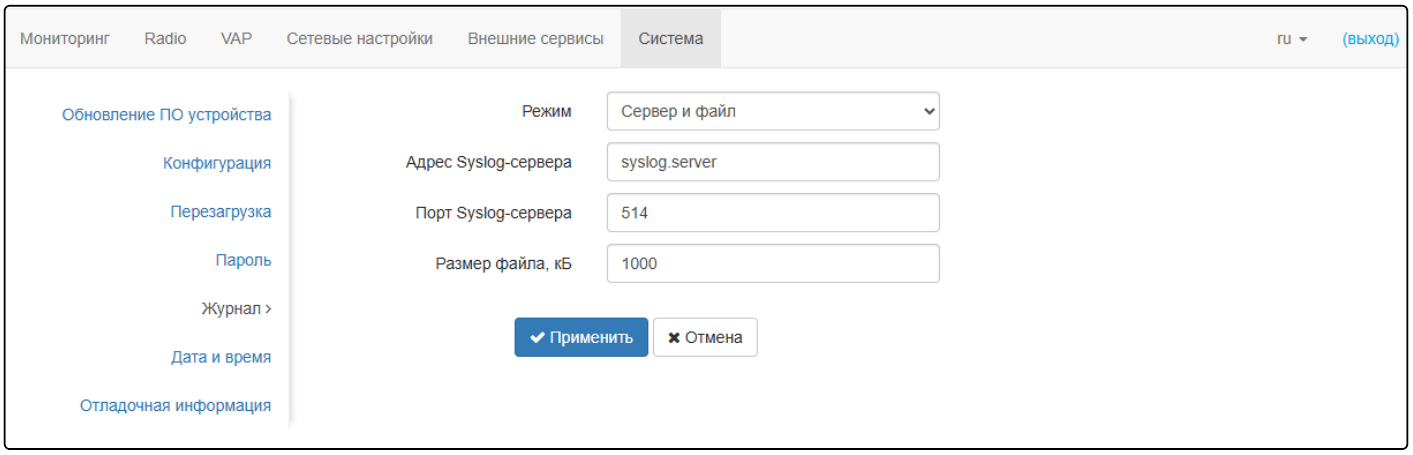
5.9.4 Подменю «Пароль»

При входе через web-интерфейс администратор (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства.
Для смены пароля введите новый пароль сначала в поле «Пароль», затем в поле «Подтверждение пароля» и нажмите кнопку «Применить» для сохранения нового пароля.



5.9.5 Подменю «Журнал»

Подменю «**Журнал**» предназначено для настройки вывода разного рода отладочных сообщений системы в целях обнаружения причин проблем в работе устройства.



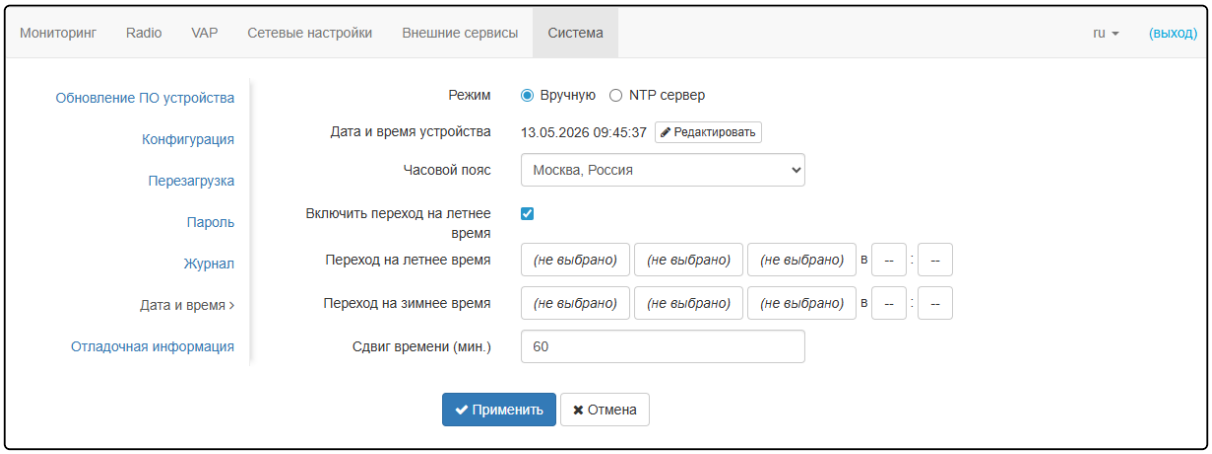
- *Режим* — режим работы Syslog-агента:
  - *Локальный файл* — информация журнала сохраняется в локальном файле и доступна в web-интерфейсе устройства на вкладке «Мониторинг/Журнал событий»;
  - *Сервер и файл* — информация журнала отправляется на удаленный Syslog-сервер и сохраняется в локальном файле.
- *Адрес Syslog-сервера* — IP-адрес или доменное имя Syslog-сервера;
- *Порт Syslog-сервера* — порт для входящих сообщений Syslog-сервера (по умолчанию — 514, допустимые значения 1–65535);
- *Размер файла, кБ* — максимальный размер файла журнала (допустимые значения 1–1000 кБ).

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.9.6 Подменю «Дата и время»

В подменю «**Дата и время**» можно настроить время вручную или с помощью протокола синхронизации времени (NTP).

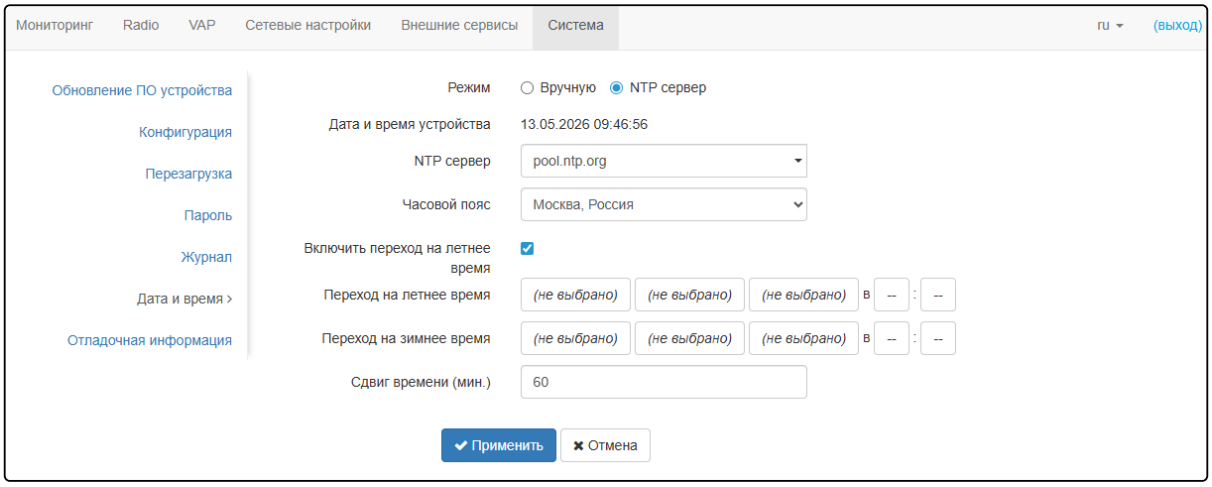
5.9.6.1 Вручную



- *Дата и время устройства* — дата и время на устройстве в данный момент. Если требуется коррекция, нажмите кнопку «Редактировать».
  - *Дата, время* — задайте текущую дату и время или нажмите кнопку «Текущая дата и время» для установки времени ПК на устройство.
- *Часовой пояс* — позволяет установить часовой пояс в соответствии с ближайшим городом в вашем регионе из заданного списка;
- *Включить переход на летнее время* — при установленном флаге переход на летнее/зимнее время будет выполняться автоматически в заданный период времени:
  - *Переход на летнее время* — день и время, когда будет выполняться переход на летнее время;
  - *Переход на зимнее время* — день и время, когда будет выполняться переход на зимнее время;
  - *Сдвиг времени (мин.)* — период времени в минутах, на который выполняется сдвиг времени. Может принимать значение от 0 до 720 мин.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

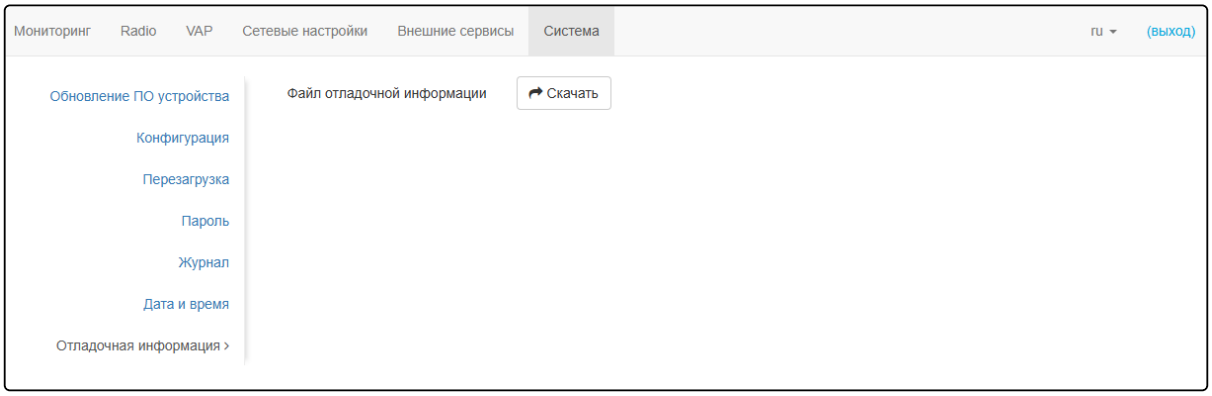
5.9.6.2 NTP-сервер



- *Дата и время устройства* – дата и время на устройстве в данный момент;
- *NTP сервер* – IP-адрес/доменное имя сервера синхронизации времени. Возможно задать адрес или выбрать из существующего списка;
- *Часовой пояс* – позволяет установить часовой пояс в соответствии с ближайшим городом в вашем регионе из заданного списка;
- *Включить переход на летнее время* – при установленном флаге переход на летнее/зимнее время будет выполняться автоматически в заданный период времени:
  - *Переход на летнее время* – день и время, когда будет выполняться переход на летнее время;
  - *Переход на зимнее время* – день и время, когда будет выполняться переход на зимнее время;
  - *Сдвиг времени (мин.)* – период времени в минутах, на который выполняется сдвиг времени. Может принимать значение от 0 до 720 мин.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.9.7 Подменю «Отладочная информация»



Файл отладочной информации

Чтобы получить архив *troubleshooting.tar.gz* с устройства на локальный компьютер, нажмите кнопку «Скачать».

6 Управление устройством с помощью командной строки

Для отображения имеющихся настроек определенного раздела конфигурации введите команду **show-config**.
Для получения подсказки о том, какое значение может принимать тот или иной параметр конфигурации устройства, нажмите сочетание клавиш (в английской раскладке) **[Shift + ?]**.
Для получения списка параметров, доступных для редактирования в данном разделе конфигурации, нажмите клавишу **Tab**.
Для сохранения настроек введите команду **save**.
Для перехода в предыдущий раздел конфигурации введите команду **exit**.
Для перехода в корневой раздел введите команду **end**.

6.1 Подключение к устройству

По умолчанию устройство WEP-500K настроено на получение адреса по DHCP. Если этого не произошло, подключиться к устройству можно по заводскому IP-адресу.

Заводской IP-адрес устройства WEP-500K: **192.168.1.10**, маска подсети: **255.255.255.0**.

Подключение к устройству осуществляется с помощью SSH/Telnet:

ssh admin@<IP-адрес устройства>, далее вводим пароль

telnet <IP-адрес устройства>, вводим логин и пароль

6.2 Настройка сетевых параметров

Настройка статических сетевых параметров точки доступа

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **br0**
WEP-500K(config):/interface/br0# **common**
WEP-500K(config):/interface/br0/common# **static-ip X.X.X.X** (где X.X.X.X — IP-адрес WEP-500K)
WEP-500K(config):/interface/br0/common# **netmask X.X.X.X** (где X.X.X.X — маска подсети)
WEP-500K(config):/interface/br0/common# **dns-server-1 X.X.X.X** (где X.X.X.X — IP-адрес dns-сервера №1)
WEP-500K(config):/interface/br0/common# **dns-server-2 X.X.X.X** (где X.X.X.X — IP-адрес dns-сервера №2)
WEP-500K(config):/interface/br0/common# **protocol static-ip** (изменение режима работы с DHCP на Static-IP)
WEP-500K(config):/interface/br0/common# **save** (сохранение настроек)

Добавление статического маршрута:

WEP-500K(config):/interface/br0/common# **exit**
WEP-500K(config):/interface/br0# **exit**
WEP-500K(config):/interface# **exit**
WEP-500K(config):/# **route**
WEP-500K(config):/route# **add default** (где default — название маршрута)
WEP-500K(config):/route# **default**
WEP-500K(config):/route/default# **destination X.X.X.X** (где X.X.X.X — IP-адрес сети или узла назначения, для дефолтного маршрута — 0.0.0.0)
WEP-500K(config):/route/default# **netmask X.X.X.X** (где X.X.X.X — маска сети назначения, для дефолтного маршрута — 0.0.0.0)
WEP-500K(config):/route/default# **gateway X.X.X.X** (где X.X.X.X — IP-адрес шлюза)
WEP-500K(config):/route/default# **save** (сохранение настроек)

Настройка получения сетевых параметров по DHCP

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **br0**
WEP-500K(config):/interface/br0# **common**
WEP-500K(config):/interface/br0/common# **protocol dhcp**
WEP-500K(config):/interface/br0/common# **save** (сохранение настроек)

6.2.1 Настройка удалённого управления

Настройка SSH

WEP-500K(root):/# **configure**
WEP-500K(config):/# **ssh**
WEP-500K(config):/ssh# **enable true** (управление удалённым доступом по SSH. Для отключения введите **false**. По умолчанию: true)
WEP-500K(config):/ssh# **port X** (где X — порт SSH-сервера. По умолчанию: 22)
WEP-500K(config):/ssh# **session-limit X** (где X — максимальное количество SSH-сессий. По умолчанию: 7)
WEP-500K(config):/ssh# **save** (сохранение настроек)

Настройка Telnet

WEP-500K(root):/# **configure**
WEP-500K(config):/# **telnet**
WEP-500K(config):/telnet# **enable true** (управление удалённым доступом по Telnet. Для отключения введите **false**. По умолчанию: false)
WEP-500K(config):/telnet# **port X** (где X — порт. По умолчанию: 23)
WEP-500K(config):/telnet# **session-limit X** (где X — максимальное количество Telnet-сессий. По умолчанию: 7)
WEP-500K(config):/telnet# **save** (сохранение настроек)

6.3 Настройка виртуальных точек доступа Wi-Fi (VAP)

При настройке VAP следует помнить, что название интерфейсов в диапазоне 2.4 ГГц начинается с wlan0, в диапазоне 5 ГГц — wlan1 и в диапазоне 6 ГГц — wlan2.

Для подключения устройств в стандарте IEEE 802.11be (Wi-Fi 7), рекомендуется настройка режима безопасности WPA2/WPA3, WPA3 или OWE.

Для 6 ГГц доступны режимы безопасности только OWE, WPA3, WPA3-Enterprise.

Таблица 9 — Команды для настройки режима безопасности на VAP

Режим безопасности	**Команда для настройки режима безопасности**
Без пароля	mode off
WPA	mode WPA
WPA2	mode WPA2
WPA/WPA2	mode WPA_WPA2
WPA3	mode WPA3
WPA2/WPA3	mode WPA2_WPA3
OWE	mode OWE
WPA-Enterprise	mode WPA_1X
WPA2-Enterprise	mode WPA2_1X
WPA/WPA2-Enterprise	mode WPA_WPA2_1X
WPA2/WPA3-Enterprise	mode WPA2_WPA3_1X
WPA3-Enterprise	mode WPA3_1X

Ниже представлены примеры настройки VAP с различными режимами безопасности для Radio 5 ГГц (wlan1).

6.3.1 Настройка VAP без шифрования

Создание VAP без шифрования с периодической отправкой аккаунтинга на RADIUS-сервер

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **ssid 'SSID_WEP-500K_open'** (изменение имени SSID)
WEP-500K(config):/interface/wlan1-vap0/vap# **ap-security**
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mode off** (режим шифрования off — без пароля)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-enable true** (включение отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-periodic true** (включение периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-interval 600** (интервал отправки сообщений «Accounting» на RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **exit**
WEP-500K(config):/interface/wlan1-vap0# **common**
WEP-500K(config):/interface/wlan1-vap0/common# **enabled true** (включение виртуальной точки доступа)
WEP-500K(config):/interface/wlan1-vap0/common# **save** (сохранение настроек)

6.3.2 Настройка VAP с шифрованием OWE

К VAP с режимом безопасности OWE смогут подключиться клиенты Wi-Fi 6 и выше.

Создание VAP с шифрованием OWE

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **ssid 'SSID_WEP-500K_owe'** (изменение имени SSID)
WEP-500K(config):/interface/wlan1-vap0/vap# **ap-security**
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mode OWE** (режим шифрования OWE — шифрованное соединение без ввода пароля. В таком режиме смогут подключиться клиенты Wi-Fi 6 и выше)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-enable true** (включение отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-periodic true** (включение периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-interval 600** (интервал отправки сообщений «Accounting» на RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **exit**
WEP-500K(config):/interface/wlan1-vap0# **common**
WEP-500K(config):/interface/wlan1-vap0/common# **enabled true** (включение виртуальной точки доступа)
WEP-500K(config):/interface/wlan1-vap0/common# **save** (сохранение настроек)

6.3.3 Настройка VAP с режимом безопасности WPA-Personal

Создание VAP с режимом безопасности WPA-Personal с периодической отправкой аккаунтинга на Radius-сервер

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **ssid 'SSID_WEP-500K_Wpa2'** (изменение имени SSID)
WEP-500K(config):/interface/wlan1-vap0/vap# **ap-security**
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mode WPA_WPA2** (режим шифрования — WPA/WPA2)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **key-wpa password123** (ключ/пароль, необходимый для подключения к виртуальной точке доступа. Длина ключа должна составлять от 8 до 63 символов)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-enable true** (включение отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-periodic true** (включение периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-interval 600** (интервал отправки сообщений «Accounting» на RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **exit**
WEP-500K(config):/interface/wlan1-vap0# **common**
WEP-500K(config):/interface/wlan1-vap0/common# **enabled true** (включение виртуальной точки доступа)
WEP-500K(config):/interface/wlan1-vap0/common# **save** (сохранение настроек)

6.3.4 Настройка VAP с Enterprise-авторизацией

Создание VAP с режимом безопасности WPA2-Enterprise с периодической отправкой аккаунтинга на Radius-сервер

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **ssid 'SSID_WEP-500K_enterprise'** (изменение имени SSID)
WEP-500K(config):/interface/wlan1-vap0/vap# **ap-security**
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mode WPA_WPA2_1X** (режим шифрования — WPA/WPA2-Enterprise)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **domain root** (где root — домен пользователя)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-port X** (где X — порт RADIUS-сервера, который используется для аутентификации и авторизации. По умолчанию: 1812)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-password secret** (где secret — пароль для RADIUS-сервера, используемого для аутентификации и авторизации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-enable true** (включение отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-periodic true** (включение периодической отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-interval 600** (интервал отправки сообщений «Accounting» на RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **exit**
WEP-500K(config):/interface/wlan1-vap0# **common**
WEP-500K(config):/interface/wlan1-vap0/common# **enabled true** (включение виртуальной точки доступа)
WEP-500K(config):/interface/wlan1-vap0/common# **save** (сохранение настроек)

6.3.5 Настройка VAP с внешней портальной авторизацией

Команды для настройки внешней портальной авторизации

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **vlan-id X** (где X — VLAN-ID на VAP)
WEP-500K(config):/interface/wlan1-vap0/vap# **ap-security**
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mode off** (режим шифрования off — без пароля)
WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **ssid 'Portal_WEP-500K'** (изменение имени SSID)
WEP-500K(config):/interface/wlan1-vap0/vap# **captive-portal**
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **verification-mode external-portal** (включение поддержки внешней портальной авторизации. По умолчанию: portal)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **scenarios**
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# **scenario-redirect**
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# **redirect-url "https://X.X.X.X/<NAS_ID>/?switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID>&original-url=<ORIGINAL_URL>&nas-ip=<NAS_IP>&ap_location=<AP_LOCATION>&nas_id=<NAS_ID>"** (указать URL внешнего виртуального портала в соответствии с таблицей 10)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios/scenario-redirect# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal/scenarios# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **enabled true** (включение функционала captive-portal)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для авторизации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-password secret** (где secret — пароль для RADIUS-сервера, используемого для авторизации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **save** (сохранение настроек)

Дополнительные команды для настройки внешней портальной авторизации

WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **preauth-filter-mode acl** (параметр, определяющий на основании чего будет фильтроваться трафик неавторизованных клиентов. Возможные значения: **acl**, **white-list**. По умолчанию: white-list)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **http-auth false** (отключение авторизации по http. По умолчанию: true)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **ipv4-acl ipv4_list** (где ipv4_list — имя списка правил ipv4-acl)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **url-acl url_list** (где url_list — имя списка правил url-acl)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **filter-dns-by-acl true** (включение фильтрации DNS-запросов по правилам preauth-acl. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **client-mac-format XX-XX-XX-XX-XX-XX** (где XX-XX-XX-XX-XX-XX — формат MAC-адреса клиента, который будет подставляться вместо **<AP_MAC>** в запросах на внешний портал. Возможные значения: **XX-XX-XX-XX-XX-XX**, **XX:XX:XX:XX:XX:XX**, **XXXXXXXXXXXX**, **xx-xx-xx-xx-xx-xx**, **xx:xx:xx:xx:xx:xx**, **xxxxxxxxxxxx**. По умолчанию: xxxxxxxxxxxx)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **nas-id-format XX-XX-XX-XX-XX-XX** (где XX-XX-XX-XX-XX-XX — формат MAC-адреса точки доступа, который будет подставляться вместо **<NAS_ID>** в запросах на внешний портал. Возможные значения: **XX-XX-XX-XX-XX-XX**, **XX:XX:XX:XX:XX:XX**, **XXXXXXXXXXXX**, **xx-xx-xx-xx-xx-xx**, **xx:xx:xx:xx:xx:xx**, **xxxxxxxxxxxx**. По умолчанию: xxxxxxxxxxxx)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **disconnect-on-reject true** (параметр, отвечающий за отключение клиента после получения Access-Reject. Для отключения введите **false**)
WEP-500K(config):/interface/wlan1-vap0/vap/captive-portal# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **use-macaddr-as-password true** (передавать MAC-адрес клиента в качестве пароля в RADIUS запросах. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **macaddr-format XX-XX-XX-XX-XX-XX** (где XX-XX-XX-XX-XX-XX — формат MAC-адреса клиента, который будет фигурировать в RADIUS-запросах. Функционал работает только при условии use-macaddr-as-password = true. Возможные значения: **XX-XX-XX-XX-XX-XX**, **XX:XX:XX:XX:XX:XX**, **XXXXXXXXXXXX**, **xx-xx-xx-xx-xx-xx**, **xx:xx:xx:xx:xx:xx**, **xxxxxxxxxxxx**. По умолчанию: xxxxxxxxxxxx)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **save** (сохранение настроек)

Для получения информации об алгоритме взаимодействия с внешним порталом см. схему.

Таблица 10 — Настройка URL шаблона для внешней портальной авторизации

Параметр	Описание
<NAS_ID>	NAS ID, заданный на VAP или в system. Если не задан ни один из этих параметров, то в качестве NAS ID в RADIUS- и HTTP(S)-пакетах будет использоваться MAC-адрес ТД в формате "nas-id-format"
<NAS_IP>	IP-адрес ТД
<SWITCH_URL>	Доменное имя, которое показывается клиенту при перенаправлении
<AP_MAC>	MAC-адрес точки доступа
<CLIENT_MAC>	MAC-адрес клиента
<SSID>	SSID
<ORIGINAL_URL>	URL, который изначально запрашивал клиент
<AP_LOCATION>	AP-location ТД

6.3.6 Настройка дополнительного RADIUS-сервера на VAP

Данный функционал доступен только для режимов портальной и Enterprise-авторизации.

Команды для настройки дополнительного RADIUS-сервера на VAP

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan1-vap0**
WEP-500K(config):/interface/wlan1-vap0# **vap**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius** (настройка основного RADIUS-сервера)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **backup** (настройка дополнительного RADIUS-сервера)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup# **add <IP-адрес дополнительного RADIUS-сервера в конфигурации>** (создание раздела конфигурации дополнительного RADIUS-сервера. Максимальное количество: 4)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup# **X.X.X.X** (где X.X.X.X — IP-адрес дополнительного RADIUS-сервера в конфигурации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **auth-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **auth-port X** (где X — порт RADIUS-сервера, который используется для аутентификации и авторизации. По умолчанию: 1812)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **auth-password secret** (где secret — пароль для RADIUS-сервера, используемого для аутентификации и авторизации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **acct-port X** (где X — порт RADIUS-сервера, который используется для аккаунтинга. По умолчанию: 1813)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **order 1** (где order — приоритет RADIUS-сервера. Если приоритет не был указан явно, то считается, что он равен 0. В этом случае очередность выбора сервера будет соответствовать порядку добавления RADIUS-сервера в конфигурацию)
WEP-500K(config):/interface/wlan1-vap0/vap/radius/backup/X.X.X.X# **save** (сохранение настроек)

6.3.7 Дополнительные настройки VAP

Назначение VLAN-ID на VAP

WEP-500K(config):/interface/wlan1-vap0/vap# **vlan-id X** (где X — номер VLAN-ID на VAP)

Включение режима Band Steer

WEP-500K(config):/interface/wlan1-vap0/vap# **band-steer-mode true** (включение режима Band Steer. Для отключения введите **false**)

Включение режима MFP (802.11W)

WEP-500K(config):/interface/wlan1-vap0/vap/ap-security# **mfp required** (включить защиту management-кадров (фреймов). **required** — требуется поддержка MFP от клиента, клиенты без MFP не смогут подключиться. **capable** — совместимо с MFP, клиенты без поддержки MFP могут подключиться. Для отключения введите **off**)

Включение использования TLS при авторизации

WEP-500K(config):/interface/wlan1-vap0/vap/radius# **tls-enable true** (использовать TLS при авторизации. Для отключения введите **false**)

Включение скрытого SSID

WEP-500K(config):/interface/wlan1-vap0/vap# **hidden true** (включение скрытого SSID. Для отключения введите **false**)

Включение изоляции клиентов на VAP

WEP-500K(config):/interface/wlan1-vap0/vap# **station-isolation true** (включение изоляции трафика между клиентами в пределах одной VAP. Для отключения введите **false**)

Ограничение количества клиентов на VAP

WEP-500K(config):/interface/wlan1-vap0/vap# **sta-limit X** (где X — максимально допустимое число подключаемых к виртуальной сети клиентов)

Включение Minimal Signal

WEP-500K(config):/interface/wlan1-vap0/vap# **check-signal-enable true** (включение использования функционала Minimal Signal. Для отключения введите **false**)
WEP-500K(config):/interface/wlan1-vap0/vap# **min-signal X** (где X — пороговое значение RSSI, при достижении которого точка будет отключать клиента от VAP. Параметр может принимать значения от -100 до -1)
WEP-500K(config):/interface/wlan1-vap0/vap# **check-signal-timeout X** (где X — период времени в секундах, по истечении которого принимается решение об отключении клиентского оборудования от виртуальной сети)
WEP-500K(config):/interface/wlan1-vap0/vap# **save** (сохранение настроек)

Включение передачи абоненского трафика вне GRE-туннеля

WEP-500K(config):/interface/wlan1-vap0/vap# **local-switching true** (включение передачи абонентского трафика вне GRE-туннеля. Для отключения введите **false**. По умолчанию выключено)

Настройка контроля доступа по MAC через RADIUS-сервер

WEP-500K(config):/interface/wlan1-vap0/vap# **acl**
WEP-500K(config):/interface/wlan1-vap0/vap/acl# **mode radius** (выбор режима radius — проверка MAC-адресов через RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/acl# **policy allow** (выбор политики. Возможные значения: **allow** — разрешать подключение только тем клиентам, которых одобрил RADIUS-сервер; **deny** — запрещать подключение клиентам, которых одобрил RADIUS-сервер. Значение по умолчанию: deny)
WEP-500K(config):/interface/wlan1-vap0/vap/acl# **enable true** (включение контроля доступа по MAC через RADIUS-сервер. Для отключения введите **false**)
WEP-500K(config):/interface/wlan1-vap0/vap/acl# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **radius**
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **domain root** (где root — домен пользователя)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-port X** (где X — порт RADIUS-сервера, который используется для аутентификации и авторизации. По умолчанию: 1812)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **auth-password secret** (где secret — пароль для RADIUS-сервера, используемого для аутентификации и авторизации)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-enable true** (включение отправки сообщений «Accounting» на RADIUS-сервер. По умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-address X.X.X.X** (где X.X.X.X — IP-адрес RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-password secret** (где secret — пароль для RADIUS-сервера, используемого для аккаунтинга)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-periodic true** (включение периодической отправки сообщений «Accounting» на RADIUS-сервер. по умолчанию: false)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **acct-interval 600** (интервал отправки сообщений «Accounting» на RADIUS-сервер)
WEP-500K(config):/interface/wlan1-vap0/vap/radius# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap# **save** (сохранение настроек)

Настройка 802.11r

Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11r.

Роуминг 802.11r возможен только между VAP с режимом безопасности WPA2/WPA3-Personal и WPA2/WPA3-Enterprise.
С инструкцией по настройке VAP с режимом безопасности WPA2-Personal и другими можно ознакомиться в разделе Настройка VAP с режимом безопасности WPA-Personal.

Каждую VAP на точках доступа нужно настраивать индивидуально, например, ТД1(wlan1)↔ТД2(wlan1), ТД1(wlan0)↔ТД2(wlan0), ТД1(wlan1)↔ТД3(wlan1) и т. д.

Ниже представлен пример настройки 802.11r на двух точках доступа: ТД1 и ТД2.

Настройка 802.11r на ТД1

WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **enabled false**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **r1-key-holder-id E8:28:C1:FC:D6:80** (MAC-адрес VAP. Можно посмотреть в выводе команды **ifconfig**)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **r0-key-holder-id 12345** (уникальный ключ для данной VAP)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **mobility-domain 100** (домен должен совпадать на встречных VAP)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **mac**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **add E4:5A:D4:E2:C4:B0** (MAC-адрес VAP интерфейса встречной точки доступа — ТД2)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **E4:5A:D4:E2:C4:B0**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-id 23456** (уникальный ключ встречной VAP точки доступа ТД2 — r0-key-holder-id)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-id E4:5A:D4:E2:C4:B0** (MAC-адрес встречной VAP на ТД2)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r0-kh-key 0102030405060708** (случайный ключ. Не должен совпадать с r1-kh-key ТД1, но обязательно должен совпадать с r1-kh-key встречной ТД2)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **r1-kh-key 0001020304050607** (случайный ключ. Не должен совпадать с r0-kh-key ТД1, но обязательно должен совпадать с r0-kh-key встречной ТД2)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E4:5A:D4:E2:C4:B0# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **enabled true** (включение работы точки доступа по протоколу 802.11r)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **save** (сохранение настроек)

Настройка 802.11r на ТД2

WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **enabled false**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **r1-key-holder-id E4:5A:D4:E2:C4:B0** (MAC-адрес VAP. Можно посмотреть в выводе команды **ifconfig**)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **r0-key-holder-id 23456** (уникальный ключ для данного VAP)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **mobility-domain 100** (домен должен совпадать на встречных VAP)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **mac**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **add E8:28:C1:FC:D6:80** (MAC-адрес VAP-интерфейса встречной точки доступа — ТД1)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **E8:28:C1:FC:D6:80**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-id 12345** (уникальный ключ встречной VAP точки доступа ТД1 — r0-key-holder-id)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-id E8:28:C1:FC:D6:80** (MAC-адрес встречного VAP на ТД1)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r0-kh-key 0001020304050607** (случайный ключ. Не должен совпадать с r1-kh-key ТД2, но обязательно должен совпадать с r1-kh-key встречной ТД1)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **r1-kh-key 0102030405060708** (случайный ключ. Не должен совпадать с r0-kh-key ТД2, но обязательно должен совпадать с r0-kh-key встречной ТД1)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac/E8:28:C1:FC:D6:80# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config/mac# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **enabled true** (включение работы точки доступа по протоколу 802.11r)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **save** (сохранение настроек)

Настройка 802.11k

Роуминг по протоколу 802.11k может быть организован между любыми сетями (открытые/шифрованные). Если на точке доступа настроена работа по протоколу 802.11k, то при подключении клиента точка доступа передает ему список «дружественных» точек доступа, на которые клиент может переключиться в процессе роуминга. Список содержит информацию о MAC-адресах точек доступа и каналах, на которых они работают.

Использование 802.11k позволяет сократить время на поиск другой сети при роуминге, так как клиенту не нужно производить сканирование каналов, на которых нет доступных для переключения целевых точек доступа.

Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11k.

Ниже представлен пример настройки 802.11k на точке доступа — составление списка «дружественных» точек доступа.

Настройка 802.11k

WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **enabled false**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **mac**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:90** (где E8:28:C1:FC:D6:90 — MAC-адрес «дружественной» точки доступа)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:90**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **channel 132** (где 132 — канал, на котором работает точка доступа с MAC-адресом E8:28:C1:FC:D6:90)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:90# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# **add E8:28:C1:FC:D6:70** (где E8:28:C1:FC:D6:70 — MAC-адрес «дружественной» точки доступа)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# **E8:28:C1:FC:D6:70**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **channel 36** (где 36 — канал, на котором работает точка доступа с MAC-адресом E8:28:C1:FC:D6:70)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac/E8:28:C1:FC:D6:70# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config/mac# **exit**
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **enabled true** (включение работы точки доступа по протоколу 802.11k)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **save** (сохранение настроек)

Настройка 802.11v

Роуминг по протоколу 802.11v может быть организован между любыми сетями (открытые/шифрованные). Если на точке доступа настроена работа по протоколу 802.11v, то в процессе своей работы устройство отправляет специальный пакет (BSS Transition) по команде администратора/контроллера (AirTune) в сторону клиента с рекомендацией об осуществлении клиентом роуминга. Последует ли клиентское устройство совету точки доступа или нет, гарантировать невозможно, так как в конечном счете решение о переключении на другую точку доступа принимает клиентская сторона. В совокупности со стандартом 802.11k, в сообщении с рекомендацией о переключении клиенту также передается список рекомендуемых для роуминга точек доступа с указанием, на каком канале работает каждая точка и по какому стандарту (IEEE 802.11n/ac/ax). После чего клиент анализирует эфир и принимает решение в зависимости от уровня сигнала, загруженности канала, конфигурации встречной точки доступа.

Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11v.

Настройка 802.11v

WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **enabled true** (включение работы точки доступа по протоколу 802.11k/v)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **save** (сохранение настроек)

6.4 Настройка MLO

MLO-группа задействует VAP по одному из каждого диапазона (2.4, 5 и 6 ГГц), при этом номер задействованного VAP равен N-1, где N — номер группы. Например MLO-группа 4 использует следующие VAP: wlan0-vap3, wlan1-vap3 и wlan2-vap3.
При включении MLO-группы настройки соответствующих VAP будут игнорироваться.

6.4.1 Настройка MLO-группы с режимом шифрования OWE

Создание MLO-группы с режимом шифрования OWE

WEP-500K(root):/# **configure**
WEP-500K(config):/# **mlo**
WEP-500K(config):/mlo# **mlo-group**
WEP-500K(config):/mlo/mlo-group# **1**
WEP-500K(config):/mlo/mlo-group/1# **ssid SSID_WEP-500K_MLO_owe** (изменение имени SSID)
WEP-500K(config):/mlo/mlo-group/1# **ap-security**
WEP-500K(config):/mlo/mlo-group/1/ap-security# **mode OWE** (режим шифрования — OWE)
WEP-500K(config):/mlo/mlo-group/1/ap-security# **exit**
WEP-500K(config):/mlo/mlo-group/1# **enabled true** (включение MLO-группы)
WEP-500K(config):/mlo/mlo-group/1# **save** (сохранение настроек)

6.4.2 Настройка MLO-группы с режимом безопасности WPA-Personal

Создание MLO-группы с режимом безопасности WPA3-Personal

```
WEP-500K(root):/# configure
WEP-500K(config):/# mlo
WEP-500K(config):/mlo# mlo-group
WEP-500K(config):/mlo/mlo-group# 1
WEP-500K(config):/mlo/mlo-group/1# ssid SSID_WEP-500K_MLO_Wpa3 (изменение имени SSID)
WEP-500K(config):/mlo/mlo-group/1# ap-security
WEP-500K(config):/mlo/mlo-group/1/ap-security# mode WPA3 (режим шифрования — WPA3)
WEP-500K(config):/mlo/mlo-group/1/ap-security# key-wpa password123 (ключ/пароль, необходимый для подключения к виртуальной точке доступа. Длина ключа должна составлять от 8 до 63 символов)
WEP-500K(config):/mlo/mlo-group/1/ap-security# exit
WEP-500K(config):/mlo/mlo-group/1# enabled true (включение MLO-группы)
WEP-500K(config):/mlo/mlo-group/1# save (сохранение настроек)
```

6.4.3 Настройка MLO-группы с Enterprise-авторизацией

Создание MLO-группы с режимом безопасности WPA3-Enterprise

```
WEP-500K(root):/# configure
WEP-500K(config):/# mlo
WEP-500K(config):/mlo# mlo-group
WEP-500K(config):/mlo/mlo-group# 1
WEP-500K(config):/mlo/mlo-group/1# ssid SSID_WEP-500K_MLO_Wpa3E (изменение имени SSID)
WEP-500K(config):/mlo/mlo-group/1# ap-security
WEP-500K(config):/mlo/mlo-group/1/ap-security# mode WPA3_1X (режим шифрования — WPA3-Enterprise)
WEP-500K(config):/mlo/mlo-group/1/ap-security# exit
WEP-500K(config):/mlo/mlo-group/1# radius
WEP-500K(config):/mlo/mlo-group/1/radius# auth-address X.X.X.X (где X.X.X.X — IP-адрес RADIUS-сервера)
WEP-500K(config):/mlo/mlo-group/1/radius# auth-port X (где X — порт RADIUS-сервера, который используется для аутентификации и авторизации. По умолчанию: 1812)
WEP-500K(config):/mlo/mlo-group/1/radius# auth-password secret (где secret — пароль для RADIUS-сервера, используемого для аутентификации и авторизации)
WEP-500K(config):/mlo/mlo-group/1/radius# exit
WEP-500K(config):/mlo/mlo-group/1# enabled true (включение MLO-группы)
WEP-500K(config):/mlo/mlo-group/1# save
```

6.5 Настройка AirTune

Настройка AirTune

WEP-500K(config):/# **airtune**
WEP-500K(config):/airtune# **airtune_service_url ws://192.168.1.20:8099/apb/rrm** (где 192.168.1.20 — IP-адрес сервера, на котором установлен сервис AirTune)
WEP-500K(config):/airtune# **enabled true** (включение взаимодействия с сервисом AirTune. Для отключения введите **false**)
WEP-500K(config):/airtune# **save** (сохранение настроек)

Для автоматической настройки 802.11r через сервис AirTune на точке доступа необходимо включить функционал 802.11r, для этого выполните следующие настройки:

Настройка 802.11r через AirTune

WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **enabled true** (включение работы точки доступа по протоколу 802.11r)
WEP-500K(config):/interface/wlan1-vap0/vap/ft-config# **save** (сохранение настроек)

Для автоматической настройки 802.11k/v через сервис AirTune на точке доступа необходимо включить функционал 802.11k/v на SSID, для этого выполните следующие настройки:

Настройка 802.11k/v через AirTune

WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **enabled true** (включение поддержки протокола 802.11k/v на виртуальной точке доступа)
WEP-500K(config):/interface/wlan1-vap0/vap/w80211kv-config# **save** (сохранение настроек)

Настройка сервиса AirTune описана в документации контроллера SoftWLC.

6.6 Настройки Radio

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

Смена рабочего канала и мощности радиоинтерфейса

WEP-500K(root):/# **configure**
WEP-500K(config):/# **interface**
WEP-500K(config):/interface# **wlan0**
WEP-500K(config):/interface/wlan0# **wlan**
WEP-500K(config):/interface/wlan0/wlan# **radio**
WEP-500K(config):/interface/wlan0/wlan/radio# **channel X** (где X — номер статического канала, на котором будет работать точка)
WEP-500K(config):/interface/wlan0/wlan/radio# **auto-channel false** (отключение автовыбора канала. Для включения введите **true**)
WEP-500K(config):/interface/wlan0/wlan/radio# **use-limit-channels false** (отключение использования ограниченного списка каналов. Для включения введите **true**)
WEP-500K(config):/interface/wlan0/wlan/radio# **bandwidth X** (где X — ширина канала. Параметр может принимать значение: для Radio 1: 20, 40; Radio 2: 20, 40, 80)
WEP-500K(config):/interface/wlan0/wlan/radio# **tx-power X** (где X — уровень мощности в дБм. Параметр может принимать значение: для Radio 1: 0–16 дБм; для Radio 2: 0–19 дБм)
WEP-500K(config):/interface/wlan0/wlan/radio# **save** (сохранение настроек)

Списки доступных каналов

Для Radio 2.4 ГГц 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 «control-sideband» = lower: 1, 2, 3, 4, 5, 6, 7, 8, 9.
  - если «control-sideband» = upper: 5, 6, 7, 8, 9, 10, 11, 12, 13.

Для Radio 5 ГГц 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 «control-sideband» = lower: 36, 44, 52, 60, 132, 140, 149, 157.
  - если «control-sideband» = 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.
- при ширине канала 160 МГц: 36, 40, 44, 48, 52, 56, 60, 64.

Для Radio 6 ГГц для выбора доступны следующие каналы:

- при ширине канала 20 МГц: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.
- при ширине канала 40 МГц:
  - если «control-sideband» = lower: 1, 9, 17, 25, 33, 41, 49, 57, 65, 73, 81, 89.
  - если «control-sideband» = upper: 5, 13, 21, 29, 37, 45, 53, 61, 69, 77, 85, 93.
- при ширине канала 80/160 МГц: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.
- при ширине канала 320 МГц:
  - если «control-sideband» = lower: 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61.
  - если «control-sideband» = upper: 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93.

6.6.1 Дополнительные настройки Radio

Настройка ограниченного списка каналов

WEP-500K(config):/interface/wlan0/wlan/radio# **use-limit-channels true** (включение использования ограниченного списка каналов в работе автовыбора каналов. Для отключения введите **false**. По умолчанию: true)
WEP-500K(config):/interface/wlan0/wlan/radio# **limit-channels '1 6 11'** (где 1, 6, 11 — каналы диапазона, в котором может работать настраиваемый радиоинтерфейс)

Изменение основного канала

WEP-500K(config):/interface/wlan0/wlan/radio# **control-sideband lower** (параметр может принимать значение: **lower**, **upper**. По умолчанию: для Radio 1: lower; для Radio 2: upper)

Включение использования короткого защитного интервала

WEP-500K(config):/interface/wlan0/wlan/radio# **sgi true** (включение использования укороченного защитного интервала для передачи данных — 400 нс, вместо 800 нс. Для отключения введите **false**)

Включение STBC

WEP-500K(config):/interface/wlan0/wlan/radio# **stbc true** (включение метода пространственно-временного блочного кодирования (STBC), направленного на повышение надежности передачи данных. Для отключения введите **false**)

Включение использования короткой преамбулы

WEP-500K(config):/interface/wlan0/wlan/radio# **short-preamble true** (включение использования короткой преамбулы пакета. Для отключения введите **false**)

Включение Wi-Fi Multimedia (WMM)

WEP-500K(config):/interface/wlan0/wlan/radio# **wmm true** (включение поддержки WMM (Wi-Fi Multimedia) Для отключения введите **false**)

Настройка механизма DFS

Настройка производится только на Radio 5 ГГц (wlan1)

WEP-500K(config):/interface/wlan1/wlan/radio# **dfs X** (где X — режим работы механизма DFS. Может принимать значения: **forced** — механизм выключен, DFS-каналы доступны для выбора; **auto** — механизм включен; **disabled** — механизм выключен, DFS-каналы недоступны для выбора)

Включение режима автоматической смены ширины канала

WEP-500K(config):/interface/wlan0/wlan/radio# **obss-coex true** (включение режима автоматической смены ширины канала с 40 МГц на 20 МГц при загруженном радиоэфире. Для отключения введите **false**)

6.7 Системные настройки

6.7.1 Обновление ПО устройства

Обновление ПО точки доступа по tftp

WEP-500K(root):/# **firmware upload tftp <IP-адрес TFTP-сервера> <Название файла ПО>** (пример: firmware upload tftp 192.168.1.15 WEP-500K-1.3.1_build_X.tar.gz)
WEP-500K(root):/# **firmware upgrade**

Обновление ПО точки доступа по http

WEP-500K(root):/# **firmware upload http <URL для скачивания файла ПО>** (пример: firmware upload http http://192.168.1.100:8080/files/WEP-500K-1.3.1_build_X.tar.gz)
WEP-500K(root):/# **firmware upgrade**

Переключение на резервную версию ПО точки доступа

WEP-500K(root):/# **firmware switch**

6.7.2 Управление конфигурацией устройства

Сброс конфигурации устройства в дефолтное состояние без сохранения параметров доступа

WEP-500K(root):/# **manage-config reset-to-default**

Сброс конфигурации устройства в дефолтное состояние с сохранением параметров доступа

WEP-500K(root):/# **manage-config reset-to-default-without-management**

Скачать конфигурационный файл устройства на TFTP-сервер

WEP-500K(root):/# **manage-config download tftp <IP-адрес TFTP-сервера>** (пример: manage-config download tftp 192.168.1.15)

Скачать конфигурационный файл устройства на сервер/ПК через SCP

scp <Пользователь>@<IP-адрес устройства>:/etc/config/config.json config.json (пример: scp admin@192.168.1.15:/etc/config/config.json config.json. Данная команда выполняется на сервере/ПК)

Загрузить конфигурационный файл на устройство с TFTP-сервера

WEP-500K(root):/# **manage-config upload tftp <IP-адрес TFTP-сервера> <Название файла конфигурации>** (пример: manage-config upload tftp 192.168.1.15 config.json)
WEP-500K(root):/# **manage-config apply** (применение конфигурации на точку доступа)

6.7.3 Перезагрузка устройства

Команда для перезагрузки устройства

WEP-500K(root):/# **reboot**

6.7.4 Настройка режима аутентификации

Устройство имеет заводскую учетную запись *admin* с паролем *password*. Удалить данную учетную запись нельзя. Изменить пароль можно с помощью указанных ниже команд.

Изменение пароля для учетной записи admin

WEP-500K(root):/# **configure**
WEP-500K(config):/# **authentication**
WEP-500K(config):/authentication# **admin-password <Новый пароль для учетной записи admin>** (от 1 до 64 символов, включая латинские буквы и цифры)
WEP-500K(config):/authentication# **save**

6.7.5 Настройка даты и времени

Команды для настройки синхронизации времени с сервером NTP

WEP-500K(root):/# **configure**
WEP-500K(config):/# **date-time**
WEP-500K(config):/date-time# **mode ntp** (включение режима работы с NTP)
WEP-500K(config):/date-time# **ntp**
WEP-500K(config):/date-time/ntp# **server <IP-адрес NTP-сервера>** (установка NTP-сервера)
WEP-500K(config):/date-time/ntp# **alt-servers** (установка дополнительных NTP-серверов)
WEP-500K(config):/date-time/ntp/alt-servers# **add <Доменное имя/IP-адрес NTP-сервера в конфигурации>** (создание раздела конфигурации дополнительного NTP-сервера. Максимальное количество: 8. Для удаления используйте команду **del**)
WEP-500K(config):/date-time/ntp/alt-servers# **exit**
WEP-500K(config):/date-time/ntp# **exit**
WEP-500K(config):/date-time# **common**
WEP-500K(config):/date-time/common# **timezone 'Asia/Novosibirsk (Novosibirsk)'** (установка временной зоны)
WEP-500K(config):/date-time/common# **save** (сохранение настроек)

6.7.6 Дополнительные настройки системы

Изменение имени устройства

WEP-500K(root):/# **configure**
WEP-500K(config):/# **system**
WEP-500K(config):/system# **hostname WEP-500K_room2** (где WEP-500K_room2 — новое имя устройства. Параметр может содержать от 1 до 63 символов: латинские заглавные и строчные буквы, цифры, знак дефис «-» (дефис не может быть последним символом в имени). По умолчанию: WEP-500K)
WEP-500K(config):/system# **save** (сохранение настроек)

Изменение географического домена

WEP-500K(root):/# **configure**
WEP-500K(config):/# **system**
WEP-500K(config):/system# **ap-location ap.test.root** (где ap.test.root — домен узла дерева устройств системы управления EMS, в котором располагается точка доступа. По умолчанию: root)
WEP-500K(config):/system# **save** (сохранение настроек)

Изменение Radius NAS-ID

WEP-500K(root):/# **configure**
WEP-500K(config):/# **system**
WEP-500K(config):/system# **nas-id Lenina_1.Novovsibirsk.root** (где Lenina_1.Novovsibirsk.root — идентификатор данной ТД. Параметр предназначен для идентификации устройства на RADIUS-сервере, в случае если RADIUS ожидает значение, отличное от MAC-адреса. По умолчанию: MAC-адрес ТД)
WEP-500K(config):/system# **save** (сохранение настроек)

Настройка LLDP

WEP-500K(root):/# **configure**
WEP-500K(config):/# **lldp**
WEP-500K(config):/lldp# **enabled true** (включение функционала LLDP. Для отключения введите **false**. По умолчанию: true)
WEP-500K(config):/lldp# **tx-interval 60** (изменение периода отправки LLDP-сообщений. По умолчанию: 30)
WEP-500K(config):/lldp# **system-name WEP-500K_reserv** (где WEP-500K_reserv — новое имя устройства. По умолчанию: WEP-500K)
WEP-500K(config):/lldp# **save** (сохранение настроек)

6.8 Настройка параметров портальной авторизации

Настройка имен параметров, передаваемых веб-сервером авторизации

WEP-500K(root):/# **configure**
WEP-500K(config):/# **captive-portal**
WEP-500K(config):/captive-portal# **web-redirector**
WEP-500K(config):/captive-portal/web-redirector# **param-names**
WEP-500K(config):/captive-portal/web-redirector/param-names# **redirect_url original_url** (настройка имени параметра, содержащего исходный URL, запрошенный клиентом. Клиент будет переадресован на данный URL в случае успешной авторизации)
WEP-500K(config):/captive-portal/web-redirector/param-names# **error_url err_url** (настройка имени параметра, содержащего URL, куда будет переадресован клиент в случае ошибки авторизации)
WEP-500K(config):/captive-portal/web-redirector/param-names# **username login** (настройка имени параметра, содержащего логин для клиента)
WEP-500K(config):/captive-portal/web-redirector/param-names# **password pass** (настройка имени параметра, содержащего пароль для клиента)
WEP-500K(config):/captive-portal/web-redirector/param-names# **save** (сохранение настроек)

Настройка нужна, если имена параметров в ответе http с кодом 302 отличаются от дефолтных имен, принимающихся точкой доступа.

В значениях параметров **redirect_url**, **error_url**, **username**, **password** можно использовать только следующие символы [a-zA-Z0-9$\-_.!*'(),]{0,255}

Настройка адаптивного режима работы портальной авторизации

WEP-500K(root):/# **configure**
WEP-500K(config):/# **captive-portal**
WEP-500K(config):/captive-portal# **web-redirector**
WEP-500K(config):/captive-portal/web-redirector# **captive-adaptive true** (включение адаптивного режима работы портальной авторизации для устройств iOS. Для отключения введите **false**. По умолчанию: false)
WEP-500K(config):/captive-portal/web-redirector# **save** (сохранение настроек)

При включенном адаптивном режиме работы при сворачивании окна авторизации на устройствах iOS разрыва соединения происходить не будет.

Настройка правил ipv4-acl

WEP-500K(root):/# **configure**
WEP-500K(config):/# **acl**
WEP-500K(config):/acl# **ipv4**
WEP-500K(config):/acl/ipv4# **add ipv4_list** (создание списка ACL-правил)
WEP-500K(config):/acl/ipv4# **ipv4_list**
WEP-500K(config):/acl/ipv4/ipv4_list# **entry**
WEP-500K(config):/acl/ipv4/ipv4_list/entry# **add 0** (создание ACL-правила)
WEP-500K(config):/acl/ipv4/ipv4_list/entry# **0**
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **action permit** (указание действия для правила. Возможные варианты: **permit** — разрешить, **deny** — запретить)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **protocol-mode any** (настройка режима работы протокола, по которому будет отрабатывать правило. Возможные значения: **any** — любой протокол, **value** — конкретный протокол)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **protocol gre** (выбор протокола. Возможные значения: **gre**, **icmp**, **igmp**, **tcp**, **udp**)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-port-start X** (где X — начальный порт источника)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-port-end X** (где X — конечный порт источника. Используется только для src-port-mode range)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-mode host** (настройка режима фильтрации источника. Возможные варианты: **any** — любой источник, **host** — фильтрация по адресу хоста, **network** — фильтрация по адресу сети)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-ip X.X.X.X** (где X.X.X.X — IP-адрес хоста источника)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-mask X.X.X.X** (где X.X.X.X — маска подсети хоста источника)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **src-port-mode any** (настройка режима работы порта источника. Возможные значения: **any** — любой режим, **eq** — равно, **gt** — больше, **lt** — меньше, **neq** — не равно, **range** — диапазон портов)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **dst-mode host** (настройка режима фильтрации назначения. Возможные варианты: **any** — любой источник, **host** — фильтрация по адресу хоста, **network** — фильтрация по адресу сети)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **dst-ip X.X.X.X** (где X.X.X.X — IP-адрес хоста назначения)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **dst-mask X.X.X.X** (где X.X.X.X — маска подсети хоста назначения)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **dst-port-mode any** (настройка режима работы порта назначения. Возможные значения: **any** —любой режим, **eq** — равно, **gt** — больше, **lt** — меньше, **neq** — не равно, **range** — диапазон портов)
WEP-500K(config):/acl/ipv4/ipv4_list/entry/0# **dst-port-start X** (где X — начальный порт назначения)
WEP-500K(config):/acl/ipv4/ipv4-acl/ipv4_list/entry/0# **dst-port-end X** (где X — конечный порт назначения. Используется только для dst-port-mode range)
WEP-500K(config):/acl/ipv4/ipv4-acl/ipv4_list/entry/0# **save** (сохранение настроек)

Настройка правил url-acl

WEP-500K(root):/# **configure**
WEP-500K(config):/# **acl**
WEP-500K(config):/acl# **url**
WEP-500K(config):/acl/url# **add url_list** (создание списка ACL-правил)
WEP-500K(config):/acl/url# **url_list**
WEP-500K(config):/acl/url/url_list# **action permit** (указание действия для списка. Возможные варианты: **permit** — разрешить, **deny** — запретить)
WEP-500K(config):/acl/url/url_list# **entry**
WEP-500K(config):/acl/url/url_list/entry# **add 0** (создание ACL-правила)
WEP-500K(config):/acl/url/url_list/entry# **0**
WEP-500K(config):/acl/url/url_list/entry/0# **domain <Доменное имя>** (указание домена или регулярного выражения)
WEP-500K(config):/acl/url/url_list/entry/0# **save** (сохранение настроек)

6.9 Настройка DAS-сервера

Функционал DAS-сервера обеспечивает обработку запросов динамической авторизации RADIUS точками доступа.

Команды для настройки DAS-сервера

WEP-500K(root):/# **configure**
WEP-500K(config):/# **das-server**
WEP-500K(config):/das-server# **enabled true** (включение DAS-сервера. Для отключения введите **false**)
WEP-500K(config):/das-server# **auth-password secret** (где secret — пароль для DAS-сервера, используется при шифровании RADIUS-запросов)
WEP-500K(config):/das-server# **save** (сохранение настроек)

6.10 Мониторинг

6.10.1 Wi-Fi клиенты

WEP-500K(root):/# **monitoring associated-clients**

```
index                          | 0
ssid                           | Virtual Access Point 0 (6GHz)
hw-addr                        | 0a:a5:08:xx:xx:xx
ip-addr                        | 192.168.1.15
hostname                       | client
domain                         | root
authenticated                  | yes
associated                     | yes
authorized                     | yes
captive-portal-vap             | no
enterprise-vap                 | no
band                           | 6
tx-fails                       | 14
link-capacity                  | 100%
link-quality                   | 100%
uptime                         | 00:12:05
interface                      | wlan2-vap0
rfid                           | 2
wid                            | 0
tx-bw                          | 320M
rx-bw                          | 320M
rx-bw-all                      | 320M
rssi-1                         | -30
rssi-2                         | -32
rssi                           | -32
snr-1                          | 55
snr-2                          | 54
snr                            | 54
mfp                            | yes
tx-rate                        | EHT NSS2-MCS10 ?xLTF GI 0.8us 4322
rx-rate                        | EHT NSS2-MCS12 ?xLTF GI 0.8us 5188
tx-retry-count                 | 14
rx-retry-count                 | 1156
tx-period-retry                | 0
using-802.11r                  | no
using-802.11k                  | no
using-802.11v                  | no
wireless-mode                  | be
mlo-enabled                    | yes
mld-mac                        | 0a:a5:08:15:aa:dc
mlo-link-1-band                | 6
mlo-link-1-mac                 | 0a:a5:08:15:aa:61
name                           | wlan2-vap0:sta-0
```

```
Counter                 Transmitted             Received
---------------------   ---------------------   -------------------------
Total Packets:          7110                    9168
TX success:             100
Total Bytes:            5454016                 1939584
Data Packets:           0                       4263
Data Bytes:             0                       1169546
Mgmt Packets:           7                       32
Mgmt Bytes:             0                       0
Dropped Packets:        0                       0
Dropped Bytes:          0                       0
Lost Packets:           0

Multicast groups: none
```

6.10.2 Информация об устройстве

WEP-500K(root):/# **monitoring information**

```
system-time                  | 07:54:17 13.05.2026
uptime                       | 00:01:42
hostname                     | WEP-500K
software-version             | 1.3.1 build X
secondary-software-version   | 1.3.1 build X
boot-version                 | 1.3.1 build X
uboot-version                | 1.3.1 build X
memory-usage                 | 52%
memory-free                  | 466M
memory-used                  | 515M
memory-total                 | 981M
cpu-load                     | 2.9%
cpu-average                  | 2.30%
is-default-config            | true
vendor                       | Eltex
device-type                  | Access Point
board-type                   | WEP-500K
hw-platform                  | WEP-500K
factory-wan-mac              | 0C:EE:20:xx:xx:xx
factory-lan-mac              | 0C:EE:20:xx:xx:xx
factory-serial-number        | WPxxxxxxxx
hw-revision                  | 1v2
session-password-initialized | false
ott-mode                     | false
last-reboot-reason           | reboot by user
test-changes-mode            | false
```

6.10.3 Сетевая информация

WEP-500K(root):/# **monitoring wan-status**

```
Common information:

 interface                | br0
 mac                      | 0c:ee:20:xx:xx:xx
 rx-bytes                 | 456875
 rx-packets               | 5835
 tx-bytes                 | 24328
 tx-packets               | 241

IPv4 information:

 protocol                 | dhcp
 ip-address               | 192.168.1.15
 netmask                  | 255.255.255.0
 gateway                  | 192.168.1.1
 DNS-1                    | 192.168.1.100
 DNS-2                    | 8.8.8.8
```

WEP-500K(root):/# **monitoring ethernet-ports**

```
   ETH0:
      name: ETH0
      link: up
      speed: 1000
      duplex: enabled
      media-type: copper
      rx-bytes: 69952
      rx-packets: 662
      tx-bytes: 22397
      tx-packets: 143
   ETH1:
      name: ETH1
      link: down
      speed: 10
      duplex: disabled
      media-type: copper
      rx-bytes: 0
      rx-packets: 0
      tx-bytes: 0
      tx-packets: 0
```

WEP-500K(root):/# **monitoring arp**

```
#        ip               mac
-------------------------------------------
0        192.168.1.1      02:00:48:xx:xx:xx
1        192.168.1.151    2c:fd:a1:xx:xx:xx
```

WEP-500K(root):/# **monitoring route**

```
Destination       Gateway           Mask              Flags      Interface
-------------------------------------------------------------------------
0.0.0.0           192.168.1.1       0.0.0.0           UG         br0
192.168.1.0       0.0.0.0           255.255.255.0     U          br0
```

WEP-500K(root):/# **monitoring lldp**

```
System capability legend:
        B - Bridge; R - Router; W - Wlan Access Point; T - Telephone;
        D - DOCSIS Cable Device; H - Host; r - Repeater; O - Other;

Port        Device ID           Port ID       System Name     Capabilities   TTL
---------   -----------------   -----------   -------------   ------------   ---
eth0        e0:d9:e3:xx:xx:xx   gi 0/16       MES             B,R            120
```

6.10.4 Беспроводные интерфейсы

WEP-500K(root):/# **monitoring radio-interface**

```
name                    | wlan0
rfid                    | 0
status                  | on
band                    | 2.4 GHz
hwaddr                  | 0C:EE:20:xx:xx:xx
tx-power                | 15 dBm
connection status       | AP mode
operation mode          | vap
mode                    | b/g/n/ax/be
noise-1                 | -92 dBm
noise-2                 | -92 dBm
channel                 | 6
frequency               | 2437 MHz
bandwidth               | 20 MHz
utilization             | 5%
thermal                 | 41

name                    | wlan1
rfid                    | 1
status                  | on
band                    | 5 GHz
hwaddr                  | 0C:EE:20:xx:xx:xx
tx-power                | 19 dBm
connection status       | AP mode
operation mode          | vap
mode                    | a/n/ac/ax/be
noise-1                 | -92 dBm
noise-2                 | -92 dBm
channel                 | 36
frequency               | 5180 MHz
bandwidth               | 20 MHz
utilization             | 1%
thermal                 | 40

name                    | wlan2
rfid                    | 2
status                  | on
band                    | 6 GHz
hwaddr                  | 0C:EE:20:xx:xx:xx
tx-power                | 19 dBm
connection status       | AP mode
operation mode          | vap
mode                    | ax/be
noise-1                 | -92 dBm
noise-2                 | -92 dBm
channel                 | 1
frequency               | 5955 MHz
bandwidth               | 20 MHz
utilization             | 0%
thermal                 | 45
```

6.10.5 Журнал событий

WEP-500K(root):/# **monitoring events**

```
Jan  1 00:00:36 WEP-500K user.notice root: The AP startup configuration was updated
successfully by root
Jan  1 00:00:36 WEP-500K daemon.info networkd[4442]: DHCP-client: Interface br0 obtained
lease on 192.168.1.15.
Oct 1 06:03:13 WEP-500K daemon.info configd[4390]: The AP running configuration was updated
successfully by admin
Oct 1 06:08:42 WEP-500K auth.info login[24431]: root login on 'pts/0'
Oct 1 06:16:41 WEP-500K daemon.info hostapd: wlan0-vap2: STA 16:40:ee:xx:xx:xx IEEE 802.11:
associated
Oct 1 06:16:41 WEP-500K daemon.info hostapd: Client '16:40:ee:xx:xx:xx' successfull
authorized with 'wlan0-vap2', SSID 'eltex', Domain '', RSSI '-34'
```

6.10.6 Сканирование эфира

Во время осуществления сканирования эфира радиоинтерфейс устройства будет отключен, что приведет к невозможности передачи данных до Wi-Fi клиентов во время сканирования.

WEP-500K(root):/#**monitoring scan-wifi**

SSID	Mode	Security	BSSID	Channel	RSSI, dBm	Bandwidth, MHz
[redacted]	AP	off	[redacted]	6	-37	20
[redacted]	AP	wpa2	[redacted]	9	-51	40L
[redacted]	AP	wpa2	[redacted]	1	-54	20
[redacted]	AP	wpa2	[redacted]	11	-61	20
[redacted]	AP	off	[redacted]	6	-62	40L
[redacted]	AP	off	[redacted]	6	-62	40L
[redacted]	AP	wpa/wpa2	[redacted]	2	-79	40L
[redacted]	AP	off	[redacted]	149	-79	80
[redacted]	AP	off	[redacted]	48	-79	20
[redacted]	AP	off	[redacted]	52	-79	20
[redacted]	AP	wpa2	[redacted]	40	-79	20
[redacted]	AP	wpa/wpa2	[redacted]	11	-79	20
[redacted]	AP	off	[redacted]	11	-80	20
[redacted]	AP	wpa2-1x	[redacted]	11	-80	20
[redacted]	AP	off	[redacted]	1	-81	20
[redacted]	AP	wpa3-1x	[redacted]	77	-81	20
[redacted]	AP	wpa2-1x	[redacted]	1	-82	20
[redacted]	AP	off	[redacted]	64	-82	160
[redacted]	AP	wpa2	[redacted]	11	-82	20
[redacted]	AP	wpa2	[redacted]	11	-82	20
[redacted]	AP	owe	[redacted]	64	-83	160
[redacted]	AP	wpa2-1x	[redacted]	64	-83	80
[redacted]	AP	wpa3	[redacted]	53	-83	320L

6.11 Получение отладочной информации

Команда для сбора отладочной информации

WEP-500K(root):/# **get-troubleshooting-file**

После выполнения команды будет создан архив *troubleshooting.tar.gz*, содержащий отладочные данные и сведения о состоянии устройства.

Получить архив *troubleshooting.tar.gz* с устройства можно по протоколу TFTP на сервер.

Команда для получения отладочной информации

WEP-500K(root):/# **tftp -pl troubleshooting.tar.gz <IP-адрес TFTP-сервера>**

```
troubleshooting.tar. 100% |*******************************| 62755 0:00:00 ETA
```

Получить архив *troubleshooting.tar.gz* с устройства на сервер/ПК можно по протоколу SCP:

scp <Пользователь>@<IP-адрес точки доступа>:troubleshooting.tar.gz troubleshooting.tar.gz (пример: scp admin@192.168.1.15:troubleshooting.tar.gz troubleshooting.tar.gz. Данная команда выполняется на сервере/ПК)

7 Вспомогательные утилиты

7.1 Утилита traceroute

Утилита показывает, через какие узлы (маршрутизаторы) проходит пакет, сколько времени занимает обработка пакета на каждом узле.

Команда запуска трассировки

WEP-500K(root):/# **traceroute <тестируемый хост>**

7.2 Утилита tcpdump

Утилита tcpdump позволяет захватывать пакеты на указанном интерфейсе.

Получить подсказку по работе с утилитой можно командой:

WEP-500K(config):/# **tcpdump --help**

7.2.1 Захват трафика с любого активного интерфейса

Например, можем включить захват пакетов Ethernet-интерфейса.

Пример команды

WEP-500K(root):/# **tcpdump -i eth0**

7.3 Утилита iperf

Данная утилита используется для запуска потока трафика с одного устройства на другое. Отправляющая сторона называется клиентом, принимающая — сервером.

Получить подсказку по работе с утилитой можно командой:

WEP-500K(root):/# **iperf --help**

Пример запуска потока трафика с ТД на сервер:

Настройка сервера на приём трафика

root@server:/# **iperf -s**

Запуск трафика с ТД-client в сторону сервера

WEP-500K(root):/# **iperf -c X.X.X.X** (где X.X.X.X — IP-адрес сервера)

8 Список изменений

Версия документа	Дата выпуска	Содержание изменений
Версия 1.0	06.2026	Первая публикация
Версия программного обеспечения 1.3.1		

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.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.ru/

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

Центр загрузок: https://eltex.ru/download