Сервисные маршрутизаторы серии ESR
ESR-15, ESR-15R, ESR-30, ESR-3200
Контроллеры беспроводного доступа
WLC-15, WLC-30, WLC-3200

Руководство по эксплуатации
Версия ПО 1.26

Содержание

1 Введение

⚠ Функционал WLC можно активировать на сервисных маршрутизаторах ESR-15, ESR-15R, ESR-30 и ESR-3200 по инструкции.

1.1 Аннотация

WLC — это программно-аппаратный комплекс для самостоятельного управления беспроводными сетями корпоративного уровня для малого и среднего бизнеса. Устройство позволяет оперативно конфигурировать сеть Wi-Fi и добавлять в нее точки доступа ЭЛТЕКС разной производительности и назначения. В данном руководстве по эксплуатации изложены назначение, технические характеристики, порядок установки, рекомендации по начальной настройке и обновлению программного обеспечения контроллера беспроводного доступа WLC (далее "контроллер" или "устройство").

1.2 Использование контроллера

Изначально заводская конфигурация контроллера WLC не совсем пустая. Она содержит базовый набор параметров, который позволяет быстро подключить к контроллеру точку доступа и запустить на ней Wi-Fi. При подключении к контроллеру с заводской конфигурацией необходимо использовать первый порт для линка с Интернетом, а второй для точки доступа Eltex (ТД). При таком подключении ТД получит от контроллера IP-адрес, автоматически зарегистрируется на нем и получит профили конфигурации, которые содержат SSID (отобразится на вашем смартфоне в разделе Wi-Fi сетей). Для того чтобы авторизоваться на данном SSID заведите учетную запись пользователя Wi-Fi после подключения к контроллеру. Более подробную информацию по алгоритму авторизации см. в разделе Quickstart. Для управления контроллером см. раздел Настройка WLC, в котором подробно описан пример конфигурирования сети Wi-Fi с GRE-тунеллированием абонентского трафика между точкой доступа и контроллером, а также приведены все команды, которые необходимы для реалиизации такой схемы. Конфигурирование настроек Wi-Fi возможно через CLI и WEB-интерфейс.

⚠ Конфигурирование таких настроек как Bridges, VLANs, Object-groups и т.д. в части сервисного маршрутизатора ESR не поддержаны в WEB-интерфейсе данной версии.

1.3 Целевая аудитория

Данное руководство пользователя предназначено для технического персонала, выполняющего установку, настройку и мониторинг устройства посредством интерфейса командной строки (CLI), а также процедуры по обслуживанию системы и обновлению ПО. Квалификация технического персонала предполагает знание основ работы стеков протоколов TCP/IP, принципов построения Ethernet-сетей.

1.4 Условные обозначения

Обозначение	Описание
[ ]	В квадратных скобках в командной строке указываются необязательные параметры, но их ввод предоставляет определенные дополнительные опции.
{ }	В фигурных скобках в командной строке указываются возможные обязательные параметры. Необходимо выбрать один из параметров.
«,» **«-»**	Данные знаки в описании команды используются для указания диапазонов.
«|»	Данный знак в описании команды обозначает «или».
Полужирный шрифт	Полужирным шрифтом выделены примечания, предупреждения или информация.
<Полужирный курсив>	Полужирным курсивом в угловых скобках указываются названия клавиш на клавиатуре.
`Текст в рамке`	В рамках с текстом указаны примеры и результаты выполнения команд.

1.5 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.

Информация содержит справочные данные об использовании устройства.

2 Quickstart

Заводская конфигурация WLC преднастроена таким образом, чтобы от пользователя потребовалось минимум настроек для получения первой работоспособной Wi-Fi сети. Для быстрого подключения WLC к рабочему стенду необходимо выполнить следующие шаги:

1. Убедиться, что WLC и подключаемая к нему точка доступа сброшены до заводских настроек. Если есть сомнения в том, что конфигурация устройств заводская, нужно сбросить их в дефолт путем зажатия кнопки "F", расположенной на передней или задней панели, на 20 секунд. После этого произойдет перезагрузка устройства и оно загрузится с заводской конфигурацией.
2. Подключить точку доступа напрямую в порт gi1/0/2. Если для питания точки доступа используется PoE-инжектор, то подключить точку в порт gi1/0/2 нужно через PoE-инжектор. Если для питания точки доступа используется PoE-коммутатор, то точка включается в access-порт коммутатора, а коммутатор включается в порт gi1/0/2 WLC другим access-портом.
3. Порт gi1/0/1 WLC нужно включить в любой access-порт вышестоящей сети, где имеется доступ в интернет и выдается IP-адрес с DHCP-сервера. Интерфейс gi1/0/1 является аплинком в заводской конфигурации и получает адрес по DHCP. Интерфейс, получивший адрес по DHCP, используется в WLC для NAT. После подключения к WLC аплинка и точки доступа точка доступа автоматически получит с WLC адрес по DHCP из сети 192.168.0.1/24, зарегистрируется на встроенном Wi-Fi контроллере, получит конфигурацию, включая SSID, построит GRE-туннель до WLC для передачи абонентского трафика и будет готова для подключения enterprise-клиентов.
4. Для успешной авторизации клиента необходимо создать для него учетную запись в БД локального RADIUS-сервера, встроенного в WLC. Создать ее можно следующими командами:

```
Логин для авторизации в WLC: "admin", пароль: "password".
После авторизации необходимо поменять пароль:
wlc(change-expired-password)# password newpassword
wlc(change-expired-password)# commit
wlc(change-expired-password)# confirm
wlc# configure
wlc(config)# radius-server local
wlc(config-radius)# domain default

#Создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:
wlc(config-radius-domain)# user name1
wlc(config-radius-user)# password ascii-text password1
wlc(config-radius-user)# end
wlc# commit
wlc# confirm
```

   После этого можно подключиться к SSID "default-ssid" с логином "name1" и паролем "password1" и получить услугу Интернет.
   Посмотреть статус точки доступа на контроллере можно командой:

```
wlc# show wlc ap
```

Полная конфигурация WLC описана в разделе Настройка WLC. Вся приведенная в разделе Настройка WLC конфигурация уже содержится в заводской конфигурации WLC, кроме настроек учетной записи пользователя Wi-Fi, которые были приведены выше. Изучение полной конфигурации WLC дает понимание, за что отвечают различные объекты в этой конфигурации и каким образом они между собой связаны.

3 Описание изделий

3.1 Назначение

Контроллер беспроводного доступа WLC предназначен для управления беспроводными сетями. Устройство позволяет самостоятельно конфигурировать сеть Wi-Fi и добавлять в нее точки доступа ЭЛТЕКС разной производительности и назначения.

Enterprise-авторизация (WPA/WPA2/WPA3 Enterprise, WPA/WPA2/WPA3 Personal) пользователей с шифрованием трафика происходит по логину/паролю. В зависимости от задач и схемы сети данные решения позволяет подключать до 50 точек доступа для WLC-15, 150 точек доступа для WLC-30 и 1000 точек доступа для WLC-3200.

Устройство обеспечивает мониторинг всех точек доступа, анализирует статистику трафика и время сессий, выполняет индивидуальные настройки Wi-Fi.

Устройства серии WLC являются высокопроизводительными многоцелевыми сетевыми контроллерами и маршрутизаторами. Устройство объединяет в себе традиционные сетевые функции и комплексный многоуровневый подход к безопасности маршрутизации, что позволяет обеспечить надежную защиту для корпоративной среды.

Устройство поддерживает функции межсетевого экрана для защиты сети организации и своей сетевой инфраструктуры, а также сочетает в себе новейшие средства обеспечения безопасности данных, шифрования, аутентификации и защиты от вторжений.

Устройство содержит в себе средства для программной и аппаратной обработки данных. Максимальная производительность достигается за счет оптимального распределения функций обработки данных между частями.

3.2 Функции

3.2.1 Функции интерфейсов

В таблице 1 приведен список функций интерфейсов устройства.

Таблица 1 – Функции интерфейсов устройства

Определение полярности подключения кабеля (Auto MDI/MDIX)	Автоматическое определение типа кабеля – перекрестный кабель или кабель прямого подключения. • **MDI** (Medium Dependent Interface – прямой) – стандарт кабелей для подключения оконечных устройств; • **MDIX** (Medium Dependent Interface with Crossover – перекрестный) – стандарт кабелей для подключения концентраторов и коммутаторов.
Поддержка обратного давления (Back pressure)	Метод обратного давления используется на полудуплексных соединениях для регулирования потока данных от встречного устройства путем создания коллизий. Метод позволяет избежать переполнения буферной памяти устройства и потери данных.
Управление потоком (IEEE 802.3X)	Управление потоком позволяет соединять низкоскоростное устройство с высокоскоростным. Для предотвращения переполнения буфера низкоскоростное устройство имеет возможность отправлять пакет PAUSE, тем самым информируя высокоскоростное устройство о необходимости сделать паузу при передаче пакетов.
Агрегирование каналов (LAG, Link aggregation)	Агрегирование (объединение) каналов позволяет увеличить пропускную способность канала связи и повысить его надежность. Контроллер поддерживает статическое и динамическое агрегирование каналов. При динамическом агрегировании используется протокол LACP для управления группой каналов.

3.2.2 Функции при работе с MAC-адресами

В таблице 2 приведены функции устройства при работе с MAC-адресами.

Таблица 2 – Функции работы с MAC-адресами

Таблица MAC-адресов	Таблица MAC-адресов устанавливает соответствие между MAC-адресами и интерфейсами устройства и используется для маршрутизации пакетов данных. Контроллеры имеют таблицу емкостью до 128k MAC-адресов и резервируют определенные MAC-адреса для использования системой.

Режим обучения	MAC-таблица может содержать либо статические адреса, либо адреса, изученные при прохождении пакетов данных через устройство. Изучение происходит за счет регистрации MAC-адресов отправителей пакетов с привязкой их к портам и VLAN. Впоследствии эти данные используются для маршрутизации встречных пакетов. Время хранения зарегистрированных MAC-адресов ограничено, его продолжительность может настраиваться администратором. Если MAC-адрес получателя, указанный в принятом устройством пакете, отсутствует в таблице, то такой пакет отправляется далее как широковещательный в пределах L2-сегмента сети.

3.2.3 Функции второго уровня сетевой модели OSI

В таблице 3 приведены функции и особенности второго уровня (уровень 2 OSI).

Таблица 3 – Описание функций второго уровня (уровень 2 OSI)

Поддержка VLAN	VLAN (Virtual Local Area Network) – это средство разделения сети на изолированные сегменты на уровне L2. Использование VLAN позволяет повысить устойчивость работы крупных сетей за счет деления их на более мелкие сети, изолировать разнородный трафик данных между собой и решить многие другие задачи. Маршрутизаторы поддерживают различные способы организации VLAN: • VLAN на базе меток пакетов данных, в соответствии с IEEE 802.1Q; • VLAN на базе портов устройства (port-based); • VLAN на базе использования правил классификации данных (policy-based).
Протокол связующего дерева (Spanning Tree Protocol)	Задачей протокола Spanning Tree является исключение избыточных сетевых соединений и приведение топологии сети к древовидной. Основные применения протокола связаны с предотвращением зацикливания сетевого трафика и с организацией резервных каналов связи.

3.2.4 Функции третьего уровня сетевой модели OSI

В таблице 4 приведены функции третьего уровня (уровень 3 OSI).

Таблица 4 – Описание функций третьего уровня (Layer 3)

Статические IP-маршруты	Администратор маршрутизатора имеет возможность добавлять и удалять статические записи в таблицу маршрутизации.
Динамическая маршрутизация	Протоколы динамической маршрутизации позволяют устройству обмениваться маршрутной информацией с соседними маршрутизаторами и автоматически составлять таблицу маршрутов. Маршрутизатор поддерживает следующие протоколы: RIPv2, RIPng, OSPFv2, OSPFv3, IS-IS, BGP.

Таблица ARP	ARP (Address Resolution Protocol) – протокол для выяснения соответствия адресов сетевого и канального уровней. Таблица ARP содержит информацию об изученном соответствии. Соответствие устанавливается на основе анализа ответов от сетевых устройств, адреса устройств запрашиваются с помощью широковещательных пакетов.
Клиент DHCP	Протокол DHCP (Dynamic Host Configuration Protocol) даёт возможность автоматизировать управление сетевыми устройствами. Клиент DHCP позволяет маршрутизатору получать сетевой адрес и дополнительные параметры от внешнего DHCP-сервера. Как правило, этот способ используется для получения сетевых настроек оператора публичной сети (WAN).
Сервер DHCP	Сервер DHCP предназначен для автоматизации и централизации конфигурирования сетевых устройств. Размещение DHCP-сервера на контроллере позволяет получить законченное решение для поддержки локальной сети. DHCP-сервер, входящий в состав контроллера, позволяет назначать IP-адреса сетевым устройствам и передавать дополнительные сетевые параметры – адреса серверов, адреса шлюзов сети и другие необходимые параметры.
DHCP Relay	Функционал DHCP Relay предназначен для перенаправления широковещательных DHCP Discover-пакетов из одного широковещательного домена в одноадресные (unicast) DHCP Discover-пакеты в другом широковещательном домене.
Трансляция сетевых адресов (NAT, Network Address Translation)	Трансляция сетевых адресов – это механизм, который позволяет преобразовывать IP-адреса и номера портов транзитных пакетов. Функция NAT позволяет использовать меньшее количество IP-адресов, транслируя несколько IP-адресов внутренней сети в один внешний публичный IP-адрес. Использование NAT позволяет увеличить защищённость локальной сети за счёт скрытия её внутренней структуры. Контроллеры поддерживают следующие варианты NAT: • **Source NAT** (SNAT) – выполняется замена адреса, а также номера порта источника при прохождении пакета в одну сторону и обратной замене адреса назначения в ответном пакете; • **Destination NAT** (DNAT) – когда обращения извне транслируются контроллером на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

3.2.5 Функции туннелирования трафика

Таблица 5 – Функции туннелирования трафика

Протоколы туннелирования	Туннелирование – это способ преобразования пакетов данных при передаче их по сети, при котором происходит замена, модификация или добавление нового сетевого заголовка пакета. Такой способ может быть использован для согласования транспортных протоколов при прохождении данных через транзитную сеть, для создания защищенных соединений, при которых туннелированные данные подвергаются шифрованию. Контроллеры поддерживают следующие виды туннелей: • **GRE** – инкапсуляция IP-пакета/Ethernet-кадра в другой IP-пакет с добавлением GRE (General Routing Encapsulation)-заголовка; • **IPv4-IPv4** – туннель, использующий инкапсуляцию исходных IP-пакетов в IP-пакеты с другими сетевыми параметрами; • **L2TPv3** – туннель для передачи L2-трафика с помощью IP-пакетов; • **IPsec** – туннель с шифрованием передаваемых данных; • **L2TP, PPTP, PPPoE, OpenVPN** – туннели, использующиеся для организации удаленного доступа клиент-сервер.

3.2.6 Функции управления и конфигурирования

Таблица 6 – Основные функции управления и конфигурирования

Загрузка и выгрузка файла настройки	Параметры устройства сохраняются в файле настройки, который содержит данные конфигурации как всей системы в целом, так и определенного порта устройства. Для передачи файлов могут использоваться протоколы TFTP, FTP, SCP.
Интерфейс командной строки (CLI)	Управление посредством CLI осуществляется локально через последовательный порт RS-232 либо удаленно через Telnet, SSH. Интерфейс командной строки консоли (CLI) является промышленным стандартом. Интерпретатор CLI предоставляет список команд и ключевых слов для помощи пользователю и сокращению объема вводимых данных.
Syslog	Протокол Syslog обеспечивает передачу информационных сообщений о происходящих в системе событиях и ведение журнала событий.
Сетевые утилиты ping, traceroute	Утилиты ping и traceroute предназначены для проверки доступности сетевых устройств и для определения маршрутов передачи данных в IP-сетях.
Управление контролируемым доступом – уровни привилегий	Контроллеры поддерживают управление уровнем доступа пользователей к системе. Уровни доступа позволяют управлять зонами ответственности администраторов устройств. Уровни доступа нумеруются от 1 до 15, уровень 15 соответствует полному доступу к управлению устройством.
Аутентификация	Аутентификация – это процедура проверки подлинности пользователя. Контроллеры поддерживают следующие методы аутентификации: • **локальная** – для аутентификации используется локальная база данных пользователей, хранящаяся на самом устройстве; • **групповая** – база данных пользователей хранится на сервере аутентификации. Для взаимодействия с сервером используются протоколы RADIUS и TACACS.

Сервер SSH/ сервер Telnet	Функции сервера SSH и Telnet позволяют установить соединение с устройством для управления им.
Автоматическое восстановление конфигурации	Устройство поддерживает автоматическую систему восстановления конфигурации, которая предотвращает ситуации потери удаленного доступа к устройству после смены конфигурации. Если в течение заданного времени после изменения конфигурации не было введено подтверждение − произойдет автоматический откат конфигурации до предыдущего использовавшегося состояния.

3.2.7 Функции сетевой защиты

В таблице 7 приведены функции сетевой защиты, выполняемые устройством.

Таблица 7 − Функции сетевой защиты

Зоны безопасности	Все интерфейсы контроллера распределяются по зонам безопасности. Для каждой пары зон настраиваются правила, определяющие возможность или невозможность прохождения данных между зонами, правила фильтрации трафика данных.
Фильтрация данных	Для каждой пары зон безопасности составляется набор правил, которые позволяют управлять фильтрацией данных, проходящих через контроллер. Командный интерфейс устройства предоставляет средства для детальной настройки правил классификации трафика и для назначения результирующего решения о пропуске трафика.

3.3 Основные технические характеристики

Основные технические параметры контроллера приведены в таблице 8.

Таблица 8 – Основные технические характеристики

Общие параметры		
Интерфейсы	WLC-15	4 × Ethernet 10/100/1000BASE-T 2 × 1000BASE-X (SFP) 1 × Консольный порт RJ-45 1 × USB 2.0 1 × Разъем для установки жесткого диска
	WLC-30	4 × Ethernet 10/100/1000BASE-T 2 × 10GBASE-R (SFP+)/1000BASE-X 1 × Консольный порт RJ-45 1 × USB 3.0 1 × USB 2.0 1 × Разъем для установки жесткого диска 1 × Слот для microSD-карты
	WLC-3200	12 × 1000BASE-X/10GBASE-R/25GBASE-R 1 × Консольный порт RJ-45 1 × Порт OOB 1 × USB 2.0 1 × Разъем для установки жесткого диска 1 × Слот для microSD-карты
Типы оптических трансиверов	WLC-15	1000BASE-X SFP
	WLC-30	1000BASE-X SFP 10GBASE-R SFP+

	WLC-3200	1000BASE-X SFP 10GBASE-R SFP+ 25GBASE-R SFP28
Дуплексный и полудуплексный режимы интерфейсов		• дуплексный и полудуплексный режим для электрических портов • дуплексный режим для оптических портов
Скорость передачи данных	WLC-15	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1 Гбит/с
	WLC-30	• электрические интерфейсы 10/100/1000 Мбит/с • оптические интерфейсы 1/10 Гбит/с
	WLC-3200	• оптические интерфейсы 1/10/25 Гбит/с
Количество поддерживаемых точек доступа	WLC-15	50, доступно расширение по лицензии до 100
	WLC-30	150, доступно расширение по лицензии до 500
	WLC-3200	1000, доступно расширение по лицензии до 1200
Количество SoftGRE-туннелей	WLC-15	100
	WLC-30	600
	WLC-3200	4000
Количество VPN-туннелей	WLC-15	10
	WLC-30	250
	WLC-3200	500
Количество статических маршрутов	WLC-15	1k
	WLC-30 WLC-3200	11k
Количество конкурентных сессий	WLC-15	4k
	WLC-30	256k
	WLC-3200	512k

Поддержка VLAN		до 4k активных VLAN в соответствии с 802.1Q
Количество маршрутов BGPv4/BGPv6	WLC-15	1M
	WLC-30	2,5M
	WLC-3200	5M
Количество маршрутов OSPFv2/OSPFv3/IS-IS	WLC-15	30k
	WLC-30	300k
	WLC-3200	500k
Количество маршрутов RIP/RIPng	WLC-15	1k
	WLC-30 WLC-3200	10k
Таблица MAC-адресов	WLC-15	2k записей на бридж
	WLC-30 WLC-3200	16k записей
Размер базы FIB	WLC-15	1M
	WLC-30	1,4M
	WLC-3200	1,7M
VRF		32
Количество L3-интерфейсов	WLC-15	200
	WLC-30 WLC-3200	4000

Соответствие стандартам		IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-T Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE 802.3z Fiber Gigabit Ethernet IEEE 802.3cc 25GBASE-LR Ethernet IEEE 802.3by 25GBASE-SR Ethernet ANSI/IEEE 802.3 автоопределение скорости IEEE 802.3x контроль потоков данных IEEE 802.3ad объединение каналов LACP IEEE 802.1Q виртуальные локальные сети VLAN IEEE 802.1v IEEE 802.3ac IEEE 802.3ae IEEE 802.1D IEEE 802.1w IEEE 802.1s
Управление		
Локальное управление		CLI
Удаленное управление		TELNET, SSH, WEB
Физические характеристики и условия окружающей среды		
Источники питания	WLC-15 WLC-30	Сеть переменного тока: 100–264 В, 50–60 Гц
	WLC-3200	Сеть переменного тока: 100–240 В, 50–60 Гц Сеть постоянного тока: 36–72 В Варианты питания: • один источник питания постоянного или переменного тока; • два источника питания постоянного или переменного тока, с возможностью горячей замены.

Максимальная потребляемая мощность	WLC-15	18 Вт
	WLC-30	26 Вт
	WLC-3200	118 Вт
Масса	WLC-15	2,7 кг
	WLC-30	2,934 кг
	WLC-3200	6,08 кг
Габаритные размеры (Ш × В × Г)	WLC-15	430 × 44 × 226 мм
	WLC-30	430 × 40 × 225 мм
	WLC-3200	430 × 44 × 330 мм
Интервал рабочих температур	WLC-15	от 0 до +40 °C
	WLC-30 WLC-3200	от -10 до +45 °C
Интервал температуры хранения		от -40 до +70 °C
Относительная влажность при эксплуатации (без образования конденсата)		не более 80 %
Относительная влажность при хранении (без образования конденсата)		от 10 до 95 %
Срок службы		не менее 15 лет

3.4 Конструктивное исполнение

В данном разделе описано конструктивное исполнение устройства. Представлены изображения передней, задней и боковых панелей устройства. Описаны разъемы, светодиодные индикаторы и органы управления.

Устройство выполнено в металлическом корпусе с возможностью установки в 19” конструктив, высота корпуса 1U.

3.4.1 Конструктивное исполнение WLC-15

Передняя панель устройства WLC-15

Внешний вид передней панели показан на рисунке 1.

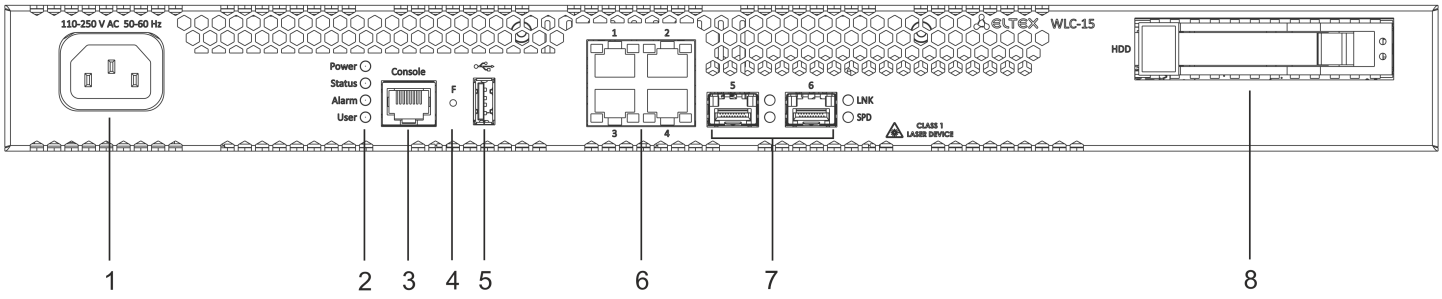


Рисунок 1 – Передняя панель WLC-15

Таблица 9 – Описание разъемов, индикаторов и органов управления передней панели WLC-15

№	Элемент передней панели	Описание
1	110-250 V AC 50–60 Hz	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использущийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
5	USB	Разъем USB 2.0 для подключения внешних USB-устройств.
6	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T.
7	[5-6]	2 порта 1000BASE-X SFP.
8	HDD	Разъем для установки жесткого диска памяти.

Задняя панель устройства WLC-15

Внешний вид задней панели устройства WLC-15 приведен на рисунке ниже.

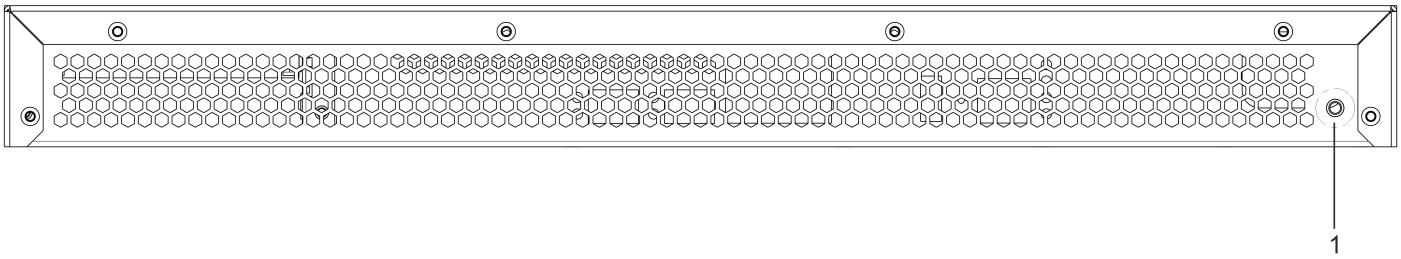


Рисунок 2 – Задняя панель WLC-15

Таблица 10 – Описание разъемов задней панели контроллера WLC-15

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства WLC-15

Внешний вид боковых панелей устройства WLC-15 приведен на рисунках ниже.

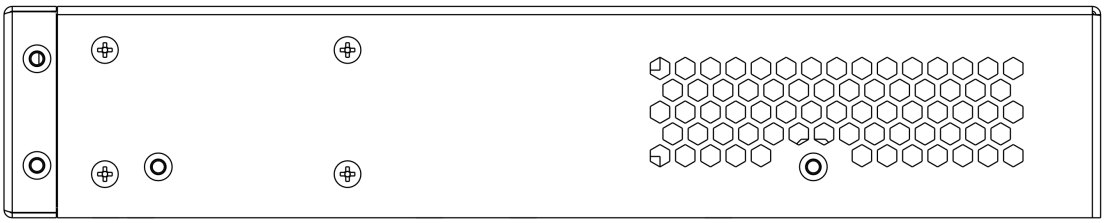


Рисунок 3 – Правая боковая панель WLC-15

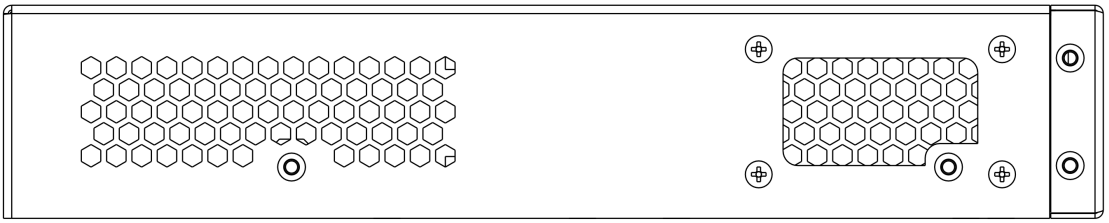


Рисунок 4 – Левая боковая панель WLC-15

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. С рекомендациями по установке устройства можно ознакомиться в разделе Установка и подключение.

3.4.2 Конструктивное исполнение WLC-30

Передняя панель устройства WLC-30

Внешний вид передней панели показан на рисунке 5.

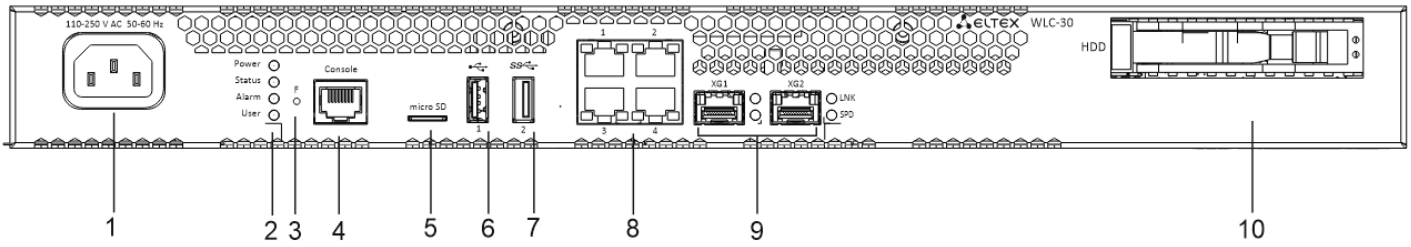


Рисунок 5 – Передняя панель WLC-30

Таблица 11 – Описание разъемов, индикаторов и органов управления передней панели WLC-30

№	Элемент передней панели	Описание
1	110-250 V AC 50–60 Hz	Источник питания.
2	Power	Индикатор питания устройства.
	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использущийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
3	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.
4	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
5	microSD	Разъем для установки microSD-карт памяти.
6	USB1	Разъем USB 2.0 для подключения внешних USB-устройств.
7	USB2	Разъем USB 3.0 для подключения внешних USB-устройств.
8	[1 .. 4]	4 порта Ethernet 10/100/1000BASE-T.

№	Элемент передней панели	Описание
9	XG1, XG2	2 порта 10GBASE-R (SFP+)1000BASE-X.
10	HDD	Разъем для установки жесткого диска памяти.

Задняя панель устройства WLC-30

Внешний вид задней панели устройства WLC-30 приведен на рисунке ниже.

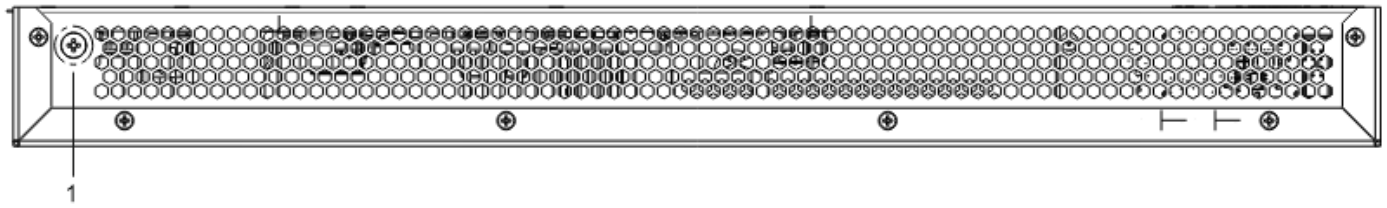


Рисунок 6 – Задняя панель WLC-30

Таблица 12 – Описание разъемов задней панели контроллера WLC-30

№	Описание
1	Клемма для заземления устройства.

Боковые панели устройства WLC-30

Внешний вид боковых панелей устройства WLC-30 приведен на рисунках ниже.

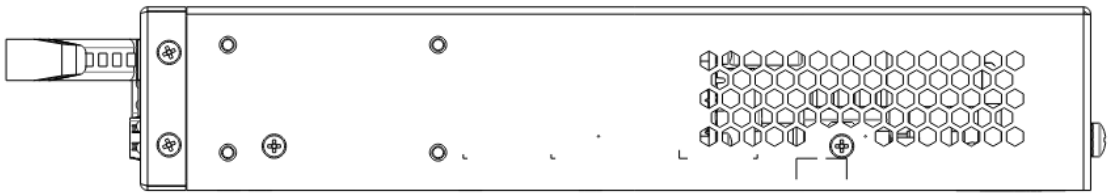


Рисунок 7 – Правая боковая панель WLC-30

Рисунок 8 – Левая боковая панель WLC-30

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к

перегреву компонентов устройства и вызвать нарушения в его работе. С рекомендациями по установке устройства можно ознакомиться в разделе Установка и подключение.

3.4.3 Конструктивное исполнение WLC-3200

Передняя панель устройства WLC-3200

Внешний вид передней панели показан на рисунке 9.

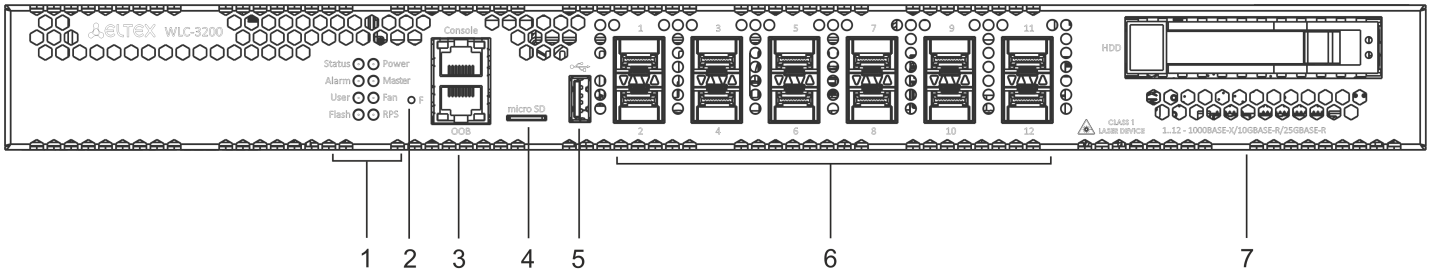


Рисунок 9 – Передняя панель WLC-3200

Таблица 13 – Описание разъемов, индикаторов и органов управления передней панели WLC-3200

№	Элемент передней панели	Описание
1	Status	Индикатор текущего состояния устройства.
	Alarm	Индикатор наличия и уровня аварии устройства.
	User	Индикатор, использущийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.
	Flash	Индикатор активности обмена с накопителем данных – microSD-картой или USB Flash.
	Power	Индикатор питания устройства.
	Master	Индикатор работы устройства в failover-режимах (не используется в текущей версии).
	Fan	Индикатор аварии вентиляторов.
	RPS	Индикатор резервного источника электропитания.
2	F	Функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам: • при удержании кнопки менее 10 секунд происходит перезагрузка устройства; • при удержании кнопки более 10 секунд происходит перезагрузка устройства и сброс к заводским настройкам.

№	Элемент передней панели	Описание
3	OOB	Ethernet-порт используется только для обновления программного обеспечения через загрузчик U-Boot. Данный порт не используется для удаленного доступа и управления.
	Console	Консольный порт RS-232 (RJ-45) для локального управления устройством.
4	microSD	Разъем для установки microSD-карт памяти.
5	USB	Порт USB 2.0 для подключения USB-устройств.
6	[1 .. 12]	Слоты для установки трансиверов 25G SFP28/10G SFP+/1G SFP.
7	HDD	Разъем для установки жесткого диска памяти.

Задняя панель устройства WLC-3200

Внешний вид задней панели устройства WLC-3200 приведен на рисунке ниже.

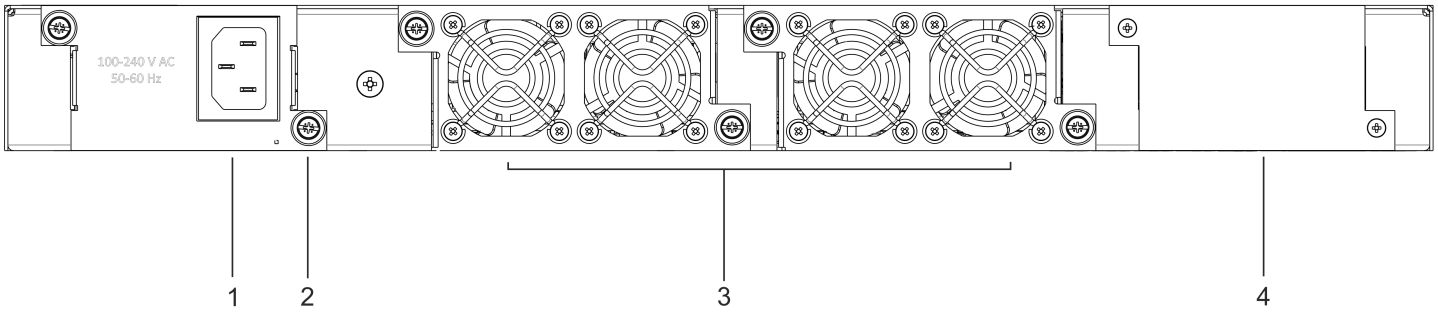


Рисунок 10 – Задняя панель WLC-3200

Таблица 14 – Описание разъемов задней панели контроллера WLC-3200

№	Описание
1	Основной источник питания.
2	Клемма для заземления устройства.
3	Съемные вентиляционные модули с возможностью горячей замены.
4	Место для установки резервного источника питания.

Боковые панели устройства WLC-3200

Внешний вид боковых панелей устройства WLC-3200 приведен на рисунках ниже.

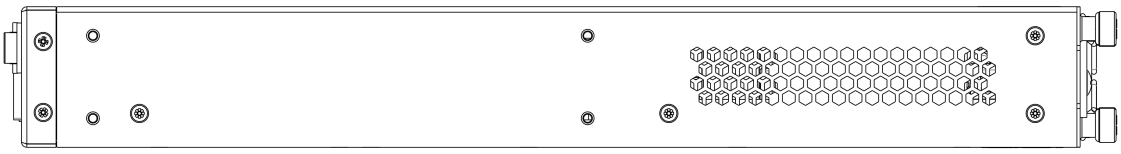


Рисунок 11 – Правая боковая панель WLC-3200

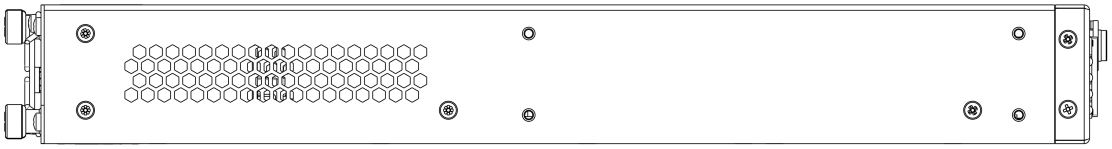


Рисунок 12 – Левая боковая панель WLC-3200

На боковых панелях устройства расположены вентиляционные решетки, которые служат для отвода тепла. Не закрывайте вентиляционные отверстия посторонними предметами. Это может привести к перегреву компонентов устройства и вызвать нарушения в его работе. Рекомендации по установке устройства расположены в разделе Установка и подключение.

Световая индикация WLC-3200

Состояние медных интерфейсов Gigabit Ethernet отображается двумя светодиодными индикаторами – *LINK/ACT* зеленого цвета и *SPEED* янтарного цвета. Расположение индикаторов медных интерфейсов показано на рисунке 13. Состояние SFP-интерфейсов отображается двумя индикаторами RX/ACT и TX/ACT и указано на рисунке 14. Значения световой индикации описаны в таблицах 15 и 16 соответственно.

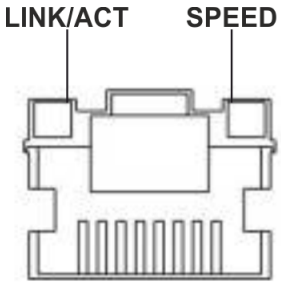


Рисунок 13 – Расположение индикаторов разъема RJ-45

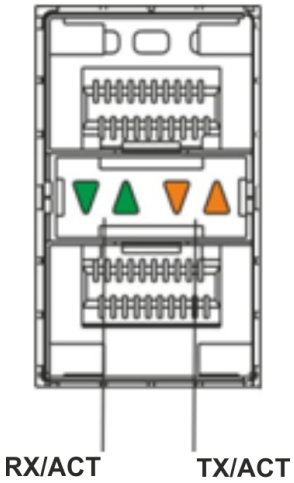


Рисунок 14 – Расположение индикаторов оптических интерфейсов

Таблица 15 – Световая индикация состояния медных интерфейсов

Свечение индикатора SPEED	Свечение индикатора LINK/ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно	Установлено соединение на скорости 10 или 100 Мбит/с.
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000 Мбит/с.
X	Мигание	Идет передача данных.

Таблица 16 – Световая индикация состояния SFP/SFP+/QSFP+-интерфейсов

Свечение индикатора RX/ACT	Свечение индикатора TX/ ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Горит постоянно	Горит постоянно	Соединение установлено.
Мигание	X	Идет прием данных.
X	Мигание	Идет передача данных.

В следующей таблице приведено описание состояний системных индикаторов устройства и их значений.

Таблица 17 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Мигает зеленым	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
VPN	Индикатор наличия активных VPN-сессий.	-	-

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Flash	Индикатор активности обмена с накопителем данных: SD-картой или USB Flash.	Зеленый	Выполнение операций чтения/записи по команде «copy».
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Основной источник питания, если он установлен, работает нормально.
		Красный	Неработоспособность основного источника питания, авария или отсутствие первичной сети.
		Выключен	Отказ внутренних источников питания устройства.
Master	Индикатор работы устройства в failover-режимах.	-	-
Fan	Состояние вентилятора охлаждения.	Выключен	Все вентиляторы исправны.
		Красный	Отказ одного или более вентиляторов. Причиной возникновения аварии может быть неработоспособность хотя бы одного из вентиляторов – остановка или пониженная частота оборотов.
RPS	Режим работы резервного источника питания.	Зеленый	Резервный источник установлен и исправен.
		Выключен	Резервный источник не установлен.
		Красный	Отсутствие первичного питания резервного источника или его неисправность.

Световая индикация WLC-30

Состояние медных интерфейсов Gigabit Ethernet отображается двумя светодиодными индикаторами – LINK/ACT зеленого цвета и SPEED янтарного цвета.

Таблица 18 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

Свечение индикатора SPEED	Свечение индикатора LINK/ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно	Установлено соединение на скорости 10 или 100 Мбит/с.
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000 Мбит/с.
X	Мигание	Идет передача данных.

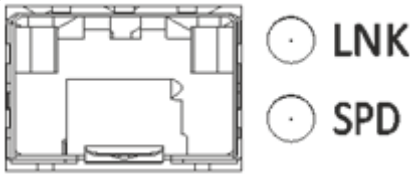


Рисунок 15 – Расположение индикаторов разъема SFP

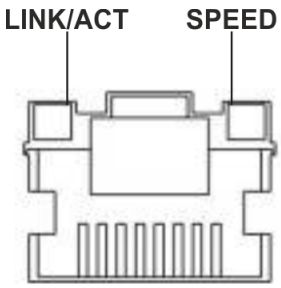


Рисунок 16 – Расположение индикаторов разъема RJ-45

В следующей таблице приведено описание состояний системных индикаторов устройства и их значений.

Таблица 19 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Мигает зеленым	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-

Световая индикация WLC-15

Состояние медных интерфейсов Gigabit Ethernet отображается двумя светодиодными индикаторами – LINK/ACT зеленого цвета и SPEED янтарного цвета.

Таблица 20 – Световая индикация состояния медных интерфейсов и SFP-интерфейсов

Свечение индикатора SPEED	Свечение индикатора LINK/ ACT	Состояние интерфейса Ethernet
Выключен	Выключен	Порт выключен или соединение не установлено.
Выключен	Горит постоянно	Установлено соединение на скорости 10 или 100 Мбит/с.
Горит постоянно	Горит постоянно	Установлено соединение на скорости 1000 Мбит/с.
X	Мигает	Идет передача данных.

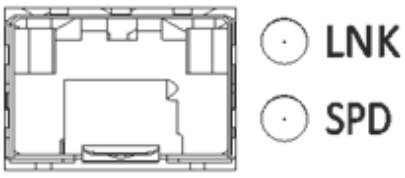


Рисунок 17 – Расположение индикаторов разъема SFP

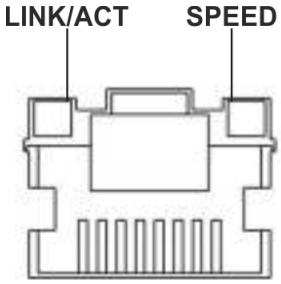


Рисунок 18 – Расположение индикаторов разъема RJ-45

В следующей таблице приведено описание состояний системных индикаторов устройства и их значений.

Таблица 21 – Состояния системных индикаторов

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Power	Индикатор питания устройства.	Зеленый	Питание устройства в норме. Источник питания работает нормально, основное ПО прогружено.
		Красный	Не прогружено основное ПО.
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.
		Красный	Устройство находится в состоянии загрузки ПО.
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
User	Индикатор, использующийся для пользовательских сценариев, которые можно назначить в режиме конфигурирования устройства.	-	-

3.5 Комплект поставки

В базовый комплект поставки WLC-15 входят:

- контроллер WLC-15;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19";
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки WLC-30 входят:

- контроллер WLC-30;
- кабель питания;
- консольный кабель;
- комплект для крепления устройства в стойку 19";
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

В базовый комплект поставки WLC-3200 входят:

- контроллер WLC-3200;
- консольный кабель;
- комплект для крепления устройства в стойку 19”;
- сертификат соответствия;
- паспорт;
- документация (опционально);
- памятка о документации.

По заказу покупателя для WLC-3200 в комплект поставки может быть включен модуль питания (PM160-220/12).

По заказу покупателя в комплект поставки могут быть включены SFP/SFP+-трансиверы.

4 Установка и подключение

В данном разделе описаны процедуры установки устройства в стойку и подключения к питающей сети.

4.1 Крепление кронштейнов

В комплект поставки устройства входят кронштейны для установки в стойку и винты для крепления кронштейнов к корпусу устройства. Для установки кронштейнов:

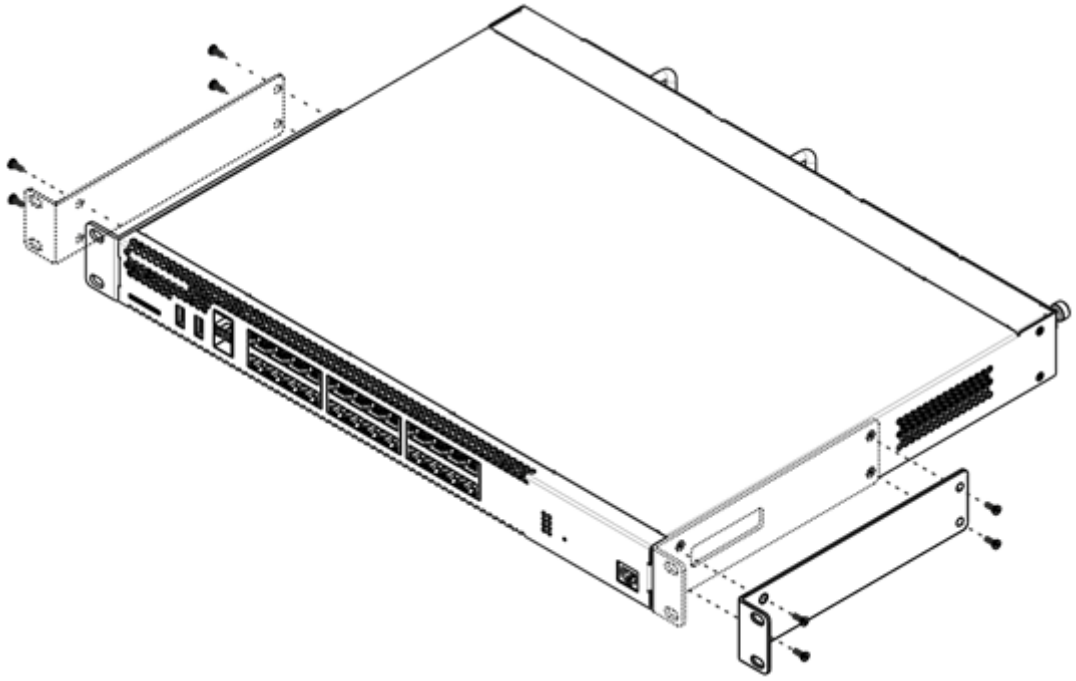


Рисунок 19 – Крепление кронштейнов

1. Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на боковой панели устройства.
2. С помощью отвертки прикрепите кронштейн винтами к корпусу.
3. Повторите действия 1, 2 для второго кронштейна.

4.2 Установка устройства в стойку

Для установки устройства в стойку:

1. Приложите устройство к вертикальным направляющим стойки.
2. Совместите отверстия кронштейнов с отверстиями на направляющих стойки. Используйте отверстия в направляющих на одном уровне с обеих сторон стойки для того, чтобы устройство располагалось горизонтально.
3. С помощью отвертки прикрепите контроллера к стойке винтами.

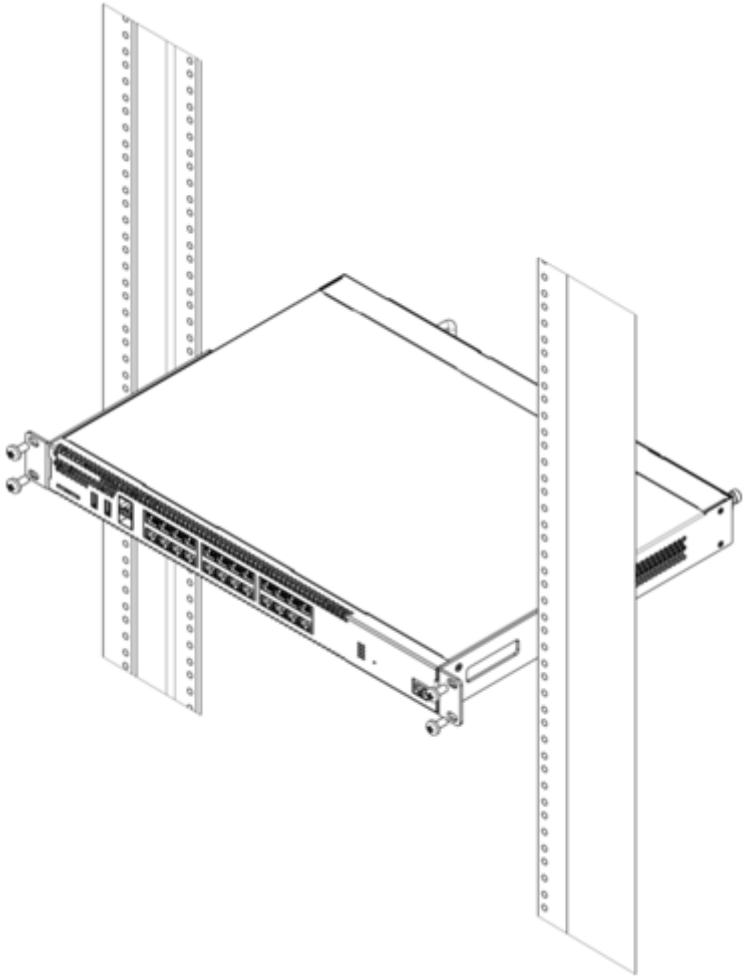


Рисунок 20 – Установка устройства в стойку

Вентиляция устройства организована по схеме фронт-тыл. На передней и боковых панелях устройства расположены вентиляционные отверстия, с задней стороны устройства расположены вентиляционные модули. Не закрывайте входные и выходные вентиляционные отверстия посторонними предметами во избежание перегрева компонентов устройства и нарушения его работы.

4.3 Установка модулей питания WLC-3200

Контроллер WLC-3200 могут работать с одним или двумя модулями питания. Установка второго модуля питания необходима в случае использования устройства в условиях, требующих повышенной надежности.

Места для установки модулей питания с электрической точки зрения равноценны. С точки зрения использования устройства, модуль питания может находиться в основном и резервном разъеме, информация о приоритетности находится в таблице "Описание разъемов задней панели контроллера". Модули питания могут устанавливаться и извлекаться без выключения устройства. При установке или извлечении дополнительного модуля питания контроллера продолжает работу без перезапуска.

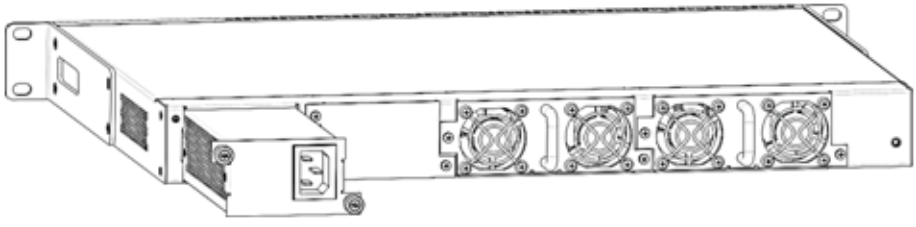


Рисунок 21 – Установка модулей питания

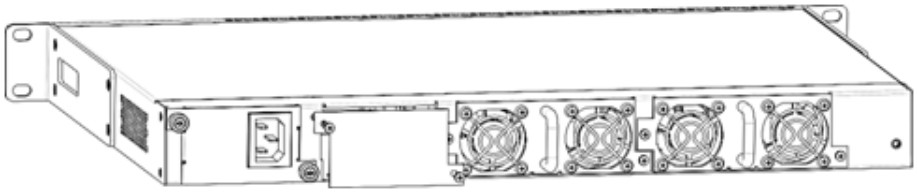


Рисунок 22 – Установка заглушки

Индикация аварии модуля питания может быть вызвана не только отказом модуля, но и отсутствием первичного питания.

Состояние модулей питания может быть проверено по индикации на передней панели контроллера (см. раздел Световая индикация) или по диагностике, доступной через интерфейсы управления контроллера.

4.4 Подключение питающей сети

1. Прежде чем к устройству будет подключена питающая сеть, необходимо заземлить корпус устройства через заземляющий винт М4. Заземление необходимо выполнять изолированным многожильным проводом. Устройство заземления и сечение заземляющего провода должны соответствовать требованиями Правил устройства электроустановок (ПУЭ).
2. Если предполагается подключение компьютера или иного оборудования к консольному порту контроллера, это оборудование также должно быть надежно заземлено.
3. Подключите к устройству кабель питания. В зависимости от комплектации устройства, питание может осуществляться от сети переменного тока либо от сети постоянного тока. При подключении сети переменного тока следует использовать кабель, входящий в комплект устройства. Для подключения к сети постоянного тока используйте провод сечением не менее 1 мм^2.
4. Включите питание устройства и убедитесь в отсутствии аварий по состоянию индикаторов на передней панели.

4.5 Установка и удаление SFP-трансиверов

Установка оптических модулей может производиться как при выключенном, так и при включенном устройстве.

4.5.1 Установка трансивера

1. Вставьте верхний SFP-модуль в слот открытой частью разъема вниз, а нижний SFP-модуль – открытой частью разъема вверх.

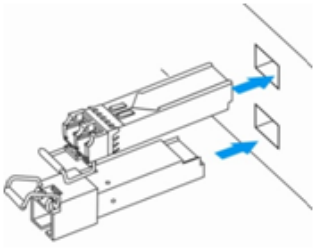


Рисунок 23– Установка SFP-трансиверов

2. Надавите на модуль по направлению внутрь корпуса устройства до появления характерного щелчка фиксации модуля.

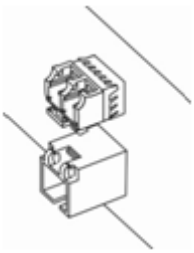


Рисунок 24 – Установленные SFP-трансиверы

4.5.2 Удаление трансивера

1. Откиньте рукоятку модуля, это приведет к разблокированию удерживающей защелки.

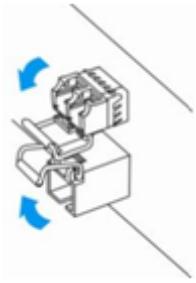


Рисунок 25 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

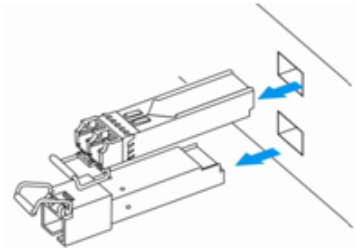


Рисунок 26 – Извлечение SFP-трансиверов

5 Интерфейсы управления

Настройка и мониторинг устройства могут осуществляться через различные интерфейсы управления.

Для доступа к устройству может использоваться сетевое подключение по протоколам Telnet и SSH или прямое подключение через консольный порт, соответствующий спецификации RS-232. При доступе по протоколам Telnet, SSH и при подключении через консольный порт для управления устройством используется интерфейс командной строки.

Заводская конфигурация содержит описание доверенной зоны trusted и IP-адрес для доступа к управлению устройством – 192.168.1.1/24.
В доверенную зону входят интерфейсы:
- **для WLC-15: GigabitEthernet 1/0/2-5;**
- **для WLC-30: GigabitEthernet 1/0/2-4, TengigabitEthernet 1/0/1-2;**
- **для WLC-3200: Twentyfivegigabitethernet 1/0/3-12;**

В заводской конфигурации по умолчанию создан пользователь «admin» с паролем «password».

При использовании любого из перечисленных интерфейсов управления действуют единые принципы работы с конфигурацией. Должна соблюдаться определенная, описанная здесь, последовательность изменения и применения конфигурации, позволяющая защитить устройство от некорректного конфигурирования.

5.1 Интерфейс командной строки (CLI)

Интерфейс командной строки (Command Line Interface, CLI) – интерфейс, предназначенный для управления, просмотра состояния и мониторинга устройства. Для работы потребуется любая установленная на ПК программа, поддерживающая работу по протоколам Telnet, SSH или прямое подключение через консольный порт (например, HyperTerminal).

Интерфейс командной строки обеспечивает авторизацию пользователей и ограничивает их доступ к командам на основании уровня доступа, заданного администратором.

В системе может быть создано необходимое количество пользователей, права доступа задаются индивидуально для каждого из них.

Для обеспечения безопасности командного интерфейса, все команды разделены на две категории – привилегированные и непривилегированные. К привилегированным в основном относятся команды конфигурирования. К непривилегированным – команды мониторинга.

Система позволяет нескольким пользователям одновременно подключаться к устройству.

5.2 Типы и порядок именования интерфейсов контроллера

При работе контроллера используются сетевые интерфейсы различного типа и назначения. Система именования позволяет однозначно адресовать интерфейсы по их функциональному назначению и местоположению в системе. Далее в таблице приведен перечень типов интерфейсов.

Таблица 22 – Типы и порядок именования интерфейсов контроллера

Тип интерфейса	Обозначение
Физические интерфейсы	Обозначение физического интерфейса включает в себя его тип и идентификатор. Идентификатор физических интерфейсов имеет вид **<UNIT>/<SLOT>/<PORT>**, где: • **<UNIT>** – номер устройства в группе устройств, • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта.
Порты 1 Гбит/с	**gigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **gigabitethernet 1/0/12** ⚠ **Допускается использовать сокращенное наименование, например gi1/0/12.**
Порты 10 Гбит/с	**tengigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **tengigabitethernet 1/0/2** ⚠ **Допускается использовать сокращенное наименование, например te1/0/2.**
Порты 25 Гбит/с	**twentyfivegigabitethernet <UNIT>/<SLOT>/<PORT>** Пример обозначения: **twentyfivegigabitethernet 1/0/2** ⚠ **Допускается использовать сокращенное наименование, например twe1/0/2.**

Тип интерфейса	Обозначение
Группы агрегации каналов	Обозначение группы агрегации каналов включает в себя его тип и порядковый номер интерфейса: **port-channel <CHANNEL_ID>** Пример обозначения: **port-channel 6** ⚠ **Допускается использовать сокращенное наименование, например, po1.**
Саб-интерфейсы	Обозначение саб-интерфейса образуется из обозначения базового интерфейса и идентификатора (VLAN) саб-интерфейса, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/12.100** • **tengigabitethernet 1/0/2.123** • **twentyfivegigabitethernet 1/0/2.200** • **port-channel 1.6** ⚠ **Идентификатор саб-интерфейса может принимать значения [1..4094].**
Q-in-Q интерфейсы	Обозначение Q-in-Q интерфейса образуется из обозначения базового интерфейса, идентификатора сервисного VLAN и идентификатора пользовательского VLAN, разделенных точкой. Примеры обозначений: • **gigabitethernet 1/0/12.100.10** • **tengigabitethernet 1/0/2.45.12** • **twentyfivegigabitethernet 1/0/2.100.200** • **port-channel 1.6.34** ⚠ **Идентификатор сервисного и пользовательского VLAN может принимать значения [1..4094].**
E1-интерфейсы	Обозначение E1-интерфейса включает в себя его тип и идентификатор. Идентификатор E1-интерфейсов имеет вид **<UNIT>/<SLOT>/<STREAM>**, где: • **<UNIT>** – номер устройства в группе устройств, • **<SLOT>** – номер E1-модуля в составе устройства, • **<STREAM>** – порядковый номер E1-потока. Пример обозначения: **e1 1/0/1**

Тип интерфейса	Обозначение
Группы агрегации E1-каналов	Обозначение группы агрегации E1-каналов включает в себя его тип и порядковый номер интерфейса: **multilink <CHANNEL_ID>** Пример обозначения: **multilink <CHANNEL_ID>**
Логические интерфейсы	Обозначение логического интерфейса является порядковым номером интерфейса: Примеры обозначений: • **loopback 4** • **bridge 60** • **service-port 1**
Последовательные интерфейсы	Обозначение последовательного интерфейса включает в себя его тип и идентификатор. Идентификатор последовательного интерфейса имеет вид **<UNIT>/<SLOT>/<STREAM>**, где: • **<UNIT>** – номер устройства в группе устройств [1..1], • **<SLOT>** – номер модуля в составе устройства или 0 при отсутствии деления устройства на модули, • **<PORT>** – порядковый номер порта. Пример обозначения: **serial 1/0/1**
USB-модемы	Обозначение USB-модема включает в себя его тип и порядковый номер: **cellular modem <MODEM-NUM>** Пример обозначения: **modem 1**

1. Количество интерфейсов каждого типа зависит от модели контроллера.
2. Текущая версия ПО не поддерживает стекирование устройств. Номер устройства в группе устройств unit может принимать только значение 1.
3. Некоторые команды поддерживают одновременную работу с группой интерфейсов. Для указания группы интерфейсов может быть использовано перечисление через запятую или указание диапазона идентификаторов через дефис «-».
Примеры указания групп интерфейсов:

```
interface gigabitethernet 1/0/1, gigabitethernet 1/0/5
interface tengigabitethernet 1/0/1-2
interface twentyfivegigabitethernet 1/0/3-4
interface gi1/0/1-3,gi1/0/7,te1/0/1,fo1/0/1
```

5.3 Типы и порядок именования туннелей контроллера

При работе контроллера используются сетевые туннели различного типа и назначения. Система именования позволяет однозначно адресовать туннели по их функциональному назначению. Далее в таблице приведен перечень типов туннелей.

Таблица 23 – Типы и порядок именования туннелей контроллера

Тип туннеля	Обозначение
L2TP-туннель	Обозначение L2TP-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tp <L2TP_ID>** Пример обозначения: **l2tp 1**
L2TPv3-туннель	Обозначение L2TPv3-туннеля состоит из обозначения типа и порядкового номера туннеля: **l2tpv3 <L2TPV3_ID>** Пример обозначения: **l2tpv3 1**
GRE-туннель	Обозначение GRE-туннеля состоит из обозначения типа и порядкового номера туннеля: **gre <GRE_ID>** Пример обозначения: **gre 1**
SoftGRE-туннель	Обозначение SoftGRE-туннеля состоит из обозначения типа, порядкового номера туннеля и, опционально, VLAN ID виртуального интерфейса: **softgre <GRE_ID>[.<VLAN>]** Примеры обозначения: **softgre 1, softgre 1.10**
IPv4-over-IPv4-туннель	Обозначение IPv4-over-IPv4-туннеля состоит из обозначения типа и порядкового номера туннеля: **ip4ip4 <IPIP_ID>** Пример обозначения: **ip4ip4 1**
IPsec-туннель	Обозначение виртуального IPsec-туннеля состоит из обозначения типа и порядкового номера туннеля: **vti <VTI_ID>** Пример обозначения: **vti 1**

Тип туннеля	Обозначение
Логический туннель (туннель между VRF)	Обозначение логического туннеля состоит из обозначения типа и порядкового номера туннеля: **lt <LT_ID>** Пример обозначения: **lt 1**
PPPoE-туннель	Обозначение PPPoE-туннеля состоит из обозначения типа и порядкового номера туннеля: **pppoe <PPPOE_ID>** Пример обозначения: **pppoe 1**
OpenVPN-туннель	Обозначение OpenVPN-туннеля состоит из обозначения типа и порядкового номера туннеля: **openvpn <OPENVPN_ID>** Пример обозначения: **openvpn 1**
PPTP-туннель	Обозначение PPTP-туннеля состоит из обозначения типа и порядкового номера туннеля: **pptp <PPTP_ID>** Пример обозначения: **pptp 1**

Количество туннелей каждого типа зависит от модели и ПО контроллера.

6 Начальная настройка устройств

6.1 Заводская конфигурация устройств

При отгрузке устройства клиенту на устройство будет загружена заводская конфигурация, которая включает минимально необходимые базовые настройки. Заводская конфигурация позволяет использовать контроллер в качестве шлюза с функцией SNAT без необходимости применять дополнительные настройки. Кроме того, заводская конфигурация содержит настройки, позволяющие получить сетевой доступ к устройству для выполнения расширенного конфигурирования.

6.1.1 Описание заводской конфигурации

Для подключения к сетям в конфигурации описаны 2 зоны безопасности с наименованиями «Trusted» для локальной сети и «Untrusted» для публичной сети. Все интерфейсы разделены между двух зон безопасности:

1. **Зона «Untrusted»** предназначена для подключения к публичной сети (WAN). В этой зоне открыты порты DHCP-протокола для получения динамического IP-адреса от провайдера. Все входящие соединения из данной зоны на контроллер запрещены.
   В данную зону безопасности входят интерфейсы:
   - для WLC-15: GigabitEthernet1/0/1; GigabitEthernet1/0/6;
   - для WLC-30: GigabitEthernet 1/0/1, TengigabitEthernet 1/0/1-2;
   - для WLC-3200: Twentyfivegigabitethernet 1/0/1-2;

   Интерфейсы зоны объединены в один L2-сегмент через сетевой мост *Bridge 2*.
2. **Зона «Trusted»** предназначена для подключения к локальной сети (LAN). В этой зоне открыты порты протоколов Telnet и SSH для удаленного доступа, ICMP-протокола для проверки доступности контроллера, DHCP-протокола для получения клиентами IP-адресов от контроллера. Исходящие соединения из данной зоны в зону «Untrusted» разрешены.
   В данную зону безопасности входят интерфейсы:
   - для WLC-15: GigabitEthernet 1/0/2-5;
   - для WLC-30: GigabitEthernet 1/0/2-4;
   - для WLC-3200: Twentyfivegigabitethernet 1/0/3-12;

   Интерфейсы зоны объединены в один L2-сегмент через сетевой мост *Bridge 1*.

На интерфейсе *Bridge 2* включен DHCP-клиент для получения динамического IP-адреса от провайдера. На интерфейсе *Bridge 1* сконфигурирован статический IP-адрес 192.168.1.1/24. Созданный IP-интерфейс выступает в качестве шлюза для клиентов локальной сети. Для клиентов локальной сети настроен DHCP-пул адресов 192.168.1.2-192.168.1.254 с маской 255.255.255.0. Для получения клиентами локальной сети доступа к Internet на контроллере включен сервис Source NAT.

Политики зон безопасности настроены следующим образом:

Таблица 24 – Описание политик зон безопасности

Зона, из которой идет трафик	Зона, в которую идет трафик	Тип трафика	Действие
Trusted	Untrusted	TCP, UDP, ICMP	разрешен
Trusted	Trusted	TCP, UDP, ICMP	разрешен
Trusted	self	TCP/22 (SSH), ICMP, UDP/67 (DHCP Server), UDP/123 (NTP)	разрешен
Untrusted	self	UDP/68 (DHCP Client)	разрешен

Для обеспечения возможности конфигурирования устройства при первом включении в конфигурации контроллера создана учётная запись администратора "admin" с паролем "password".
Пользователю будет предложено изменить пароль администратора при начальном конфигурирование контроллера.

Для сетевого доступа к управлению контроллером при первом включении в конфигурации задан статический IP-адрес на интерфейсе Bridge 1 – 192.168.1.1/24.

6.2 Подключение и конфигурирование устройства

Контроллеры беспроводного доступа WLC предназначены для выполнения функций пограничного шлюза и обеспечения безопасности сети пользователя при подключении его к публичным сетям передачи данных.

Базовая настройка данных устройств должна включать:

- назначение IP-адресов (статических или динамических) интерфейсам, участвующим в маршрутизации данных;
- создание зон безопасности и распределение интерфейсов по зонам;
- создание политик, регулирующих прохождение данных между зонами;
- настройка сервисов, сопутствующих маршрутизации данных (NAT, Firewall и прочие).

Расширенные настройки зависят от требований конкретной схемы применения устройства и легко могут быть добавлены или изменены с помощью имеющихся интерфейсов управления.

6.2.1 Подключение к устройству

Предусмотрены следующие способы подключения к устройству:

Подключение по локальной сети Ethernet

При первоначальном старте устройство загружается с заводской конфигурацией.
Описание заводской конфигурации приведено в разделе Заводская конфигурация устройств **данного руководства.**

Подключите сетевой кабель передачи данных (патч-корд) к любому порту, входящему в зону «***Trusted***», и к компьютеру, предназначенному для управления.

В заводской конфигурации контроллера активирован DHCP-сервер с пулом IP-адресов в подсети **192.168.1.0/24**.

При подключении сетевого интерфейса управляющего компьютера он должен получить сетевой адрес от сервера.

Если IP-адрес не получен по какой-либо причине, то следует назначить адрес интерфейса вручную, используя любой адрес, кроме 192.168.1.1, в подсети 192.168.1.0/24.

Подключение через консольный порт RS-232

При помощи кабеля RJ-45/DBF9, который входит в комплект поставки устройства, соедините порт **«Console»** контроллера с портом RS-232 компьютера.

Запустите терминальную программу (например, HyperTerminal или Minicom) и создайте новое подключение. Должен быть использован режим эмуляции терминала VT100.

Выполните следующие настройки интерфейса RS-232:

```
Скорость: 115200 бит/с
Биты данных: 8 бит
Четность: нет
Стоповые биты: 1
Управление потоком: нет
```

6.2.2 Применение изменения конфигурации

Любые изменения, внесенные в конфигурацию, вступят в действие только после применения команды:

```
wlc# commit
Configuration has been successfully committed
```

После применения данной команды запускается таймер "отката" конфигурации. Для остановки таймера и механизма "отката" используется команда:

```
wlc# confirm
Configuration has been successfully confirmed
```

Значение таймера "отката" по умолчанию – 600 секунд. Для изменения данного таймера используется команда:

```
wlc(config)# system config-confirm timeout <TIME>
```

- <TIME> – интервал времени ожидания подтверждения конфигурации, принимает значение в секундах [120..86400].

6.2.3 Базовая настройка устройств

Процедура настройки устройств при первом включении состоит из следующих этапов:

- Изменение пароля пользователя «admin».
- Создание новых пользователей.
- Назначение имени устройства (Hostname).
- Установка параметров подключения к публичной сети в соответствии с требованиями провайдера.
- Настройка удаленного доступа к контроллеру.
- Применение базовых настроек.

Изменение пароля пользователя «admin»

Для защищенного входа в систему необходимо сменить пароль привилегированного пользователя «admin».

Учетная запись techsupport необходима для удаленного обслуживания сервисным центром;
Учетная запись remote – аутентификация RADIUS, TACACS+, LDAP;
Удалить пользователей admin, techsupport, remote нельзя. Можно только сменить пароль и уровень привилегий.

Если информация о пользователе "admin" не отображается в конфигурации, значит параметры данного пользователя настроены по умолчанию (пароль "password", уровень привилегий 15).

Имя пользователя и пароль вводятся при входе в систему во время сеансов администрирования устройства.

Для изменения пароля пользователя «admin» используются следующие команды:

```
wlc# configure
wlc(config)# username admin
wlc(config-user)# password <new-password>
wlc(config-user)# exit
```

Создание новых пользователей

Для создания нового пользователя системы или настройки любого из параметров: имени пользователя, пароля, уровня привилегий – используются команды:

```
wlc(config)# username <name>
wlc(config-user)# password <password>
wlc(config-user)# privilege <privilege>
wlc(config-user)# exit
```

Уровни привилегий 1-9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10-14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

Пример команд для создания пользователя **«fedor»** с паролем **«12345678»** и уровнем привилегий **15** и создания пользователя **«ivan»** с паролем **«password»** и уровнем привилегий **1**:

```
wlc# configure
wlc(config)# username fedor
wlc(config-user)# password 12345678
wlc(config-user)# privilege 15
wlc(config-user)# exit
wlc(config)# username ivan
wlc(config-user)# password password
wlc(config-user)# privilege 1
wlc(config-user)# exit
```

Уровни привилегий 1-9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10-14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

Пример команд для создания пользователя **«fedor»** с паролем **«12345678»** и уровнем привилегий **15** и создания пользователя **«ivan»** с паролем «**password**» и уровнем привилегий **1**:

```
wlc# configure
wlc(config)# username fedor
wlc(config-user)# password 12345678
wlc(config-user)# privilege 15
wlc(config-user)# exit
wlc(config)# username ivan
wlc(config-user)# password password
wlc(config-user)# privilege 1
wlc(config-user)# exit
```

Назначение имени устройства

Для назначения имени устройства используются следующие команды:

```
wlc# configure
wlc(config)# hostname <new-name>
```

После применения конфигурации приглашение командной строки изменится на значение, заданное параметром **<new-name>**.

Настройка параметров публичной сети

Для настройки сетевого интерфейса контроллера в публичной сети необходимо назначить устройству параметры, определённые провайдером сети – IP-адрес, маска подсети и адрес шлюза по умолчанию.

Пример команд настройки статического IP-адреса для саб-интерфейса **Gigabit Ethernet 1/0/2.150** для доступа к контроллеру через **VLAN 150**.

Параметры интерфейса:

- IP-адрес – 192.168.16.144;
- Маска подсети – 255.255.255.0;
- IP-адрес шлюза по умолчанию – 192.168.16.1.

```
wlc# configure
wlc(config)# interface gigabitethernet 1/0/2.150
wlc(config-subif)# ip address 192.168.16.144/24
wlc(config-subif)# exit
wlc(config)# ip route 0.0.0.0/0 192.168.16.1
```

Для того чтобы убедиться, что адрес был назначен интерфейсу, после применения конфигурации введите следующую команду:

```
wlc# show ip interfaces
IP address           Interface                          Type
-------------------  ---------------------------------  -------
192.168.16.144/24    gigabitethernet 1/0/2.150          static
```

Провайдер может использовать динамически назначаемые адреса в своей сети. Для получения IP-адреса может использоваться протокол DHCP, если в сети присутствует сервер DHCP.

Пример настройки, предназначенной для получения динамического IP-адреса от DHCP-сервера на интерфейсе **Gigabit Ethernet 1/0/10**:

```
wlc# configure
wlc(config)# interface gigabitethernet 1/0/10
wlc(config-if)# ip address dhcp
wlc(config-if)# exit
```

Для того чтобы убедиться, что адрес был назначен интерфейсу, введите следующую команду после применения конфигурации:

```
wlc# show ip interfaces
IP address            Interface                          Type
-------------------   --------------------------------   -------
192.168.11.5/25       gigabitethernet 1/0/10             DHCP
```

Настройка удаленного доступа к устройству

В заводской конфигурации разрешен удаленный доступ к контроллеру по протоколам Telnet или SSH из зоны «**trusted**». Для того чтобы разрешить удаленный доступ к контроллеру из других зон, например, из публичной сети, необходимо создать соответствующие правила в firewall.

При конфигурировании доступа к контроллеру правила создаются для пары зон:

- **source-zone** – зона, из которой будет осуществляться удаленный доступ;
- **self** – зона, в которой находится интерфейс управления устройством.

Для создания разрешающего правила используются следующие команды:

```
wlc# configure
wlc(config)# security zone-pair <source-zone> self
wlc(config-zone-pair)# rule <number>
wlc(config-zone-rule)# action permit
wlc(config-zone-rule)# match protocol tcp
wlc(config-zone-rule)# match source-address <network object-group>
wlc(config-zone-rule)# match destination-address <network object-group>
wlc(config-zone-rule)# match destination-port <service object-group>
wlc(config-zone-rule)# enable
wlc(config-zone-rule)# exit
wlc(config-zone-pair)# exit
```

Пример команд для разрешения пользователям из зоны **«untrusted»** с IP-адресами **132.16.0.5-132.16.0.10** подключаться к утизатору или контроллеру с IP-адресом **40.13.1.22** по протоколу SSH:

```
wlc# configure
wlc(config)# object-group network clients
wlc(config-addr-set)# ip address-range 132.16.0.5-132.16.0.10
wlc(config-addr-set)# exit
wlc(config)# object-group network gateway
wlc(config-addr-set)# ip address-range 40.13.1.22
wlc(config-addr-set)# exit
wlc(config)# object-group service ssh
wlc(config-port-set)# port-range 22
wlc(config-port-set)# exit
wlc(config)# security zone-pair untrusted self
wlc(config-zone-pair)# rule 10
wlc(config-zone-rule)# action permit
wlc(config-zone-rule)# match protocol tcp
wlc(config-zone-rule)# match source-address clients
wlc(config-zone-rule)# match destination-address gateway
wlc(config-zone-rule)# match destination-port ssh
wlc(config-zone-rule)# enable
wlc(config-zone-rule)# exit
wlc(config-zone-pair)# exit
```

7 Обновление программного обеспечения

7.1 Обновление программного обеспечения средствами системы

Для обновления программного обеспечения понадобится один из следующих серверов: TFTP, FTP, SCP. На сервер должны быть помещены файлы программного обеспечения устройства, полученные от производителя.
На устройстве хранится две копии программного обеспечения. Для обеспечения надежности процедуры обновления программного обеспечения доступна для обновления только копия, которая не была использована для последнего старта устройства.

При обновлении программного обеспечения конфигурация контроллера конвертируется в соответствии с новой версией.
При загрузке контроллера с более старой версией программного обеспечения, чем загруженная ранее, конфигурация не конвертируется и впоследствии удаляется.

Обновление ПО с более ранних версий можно произвести, воспользовавшись инструкцией, приведенной в разделе Обновление программного обеспечения из начального загрузчика**.**

Обновление программного обеспечения на устройстве, работающем под управлением операционной системы, выполняется в следующем порядке.

1. Подготовьте для работы выбранный сервер. Должен быть известен адрес сервера, на сервере должен быть размещен дистрибутивный файл программного обеспечения.
2. Контроллер должен быть подготовлен к работе в соответствии с требованиями документации. Конфигурация контроллера должна позволять обмениваться данными по протоколам TFTP/FTP/SCP и ICMP с сервером. При этом должна быть учтена принадлежность сервера к зонам безопасности контроллера.
3. Подключитесь к контроллеру локально через консольный порт Console или удаленно, используя проколы Telnet или SSH.
   Проверьте доступность сервера для контроллера, используя команду *ping*. Если сервер не доступен, проверьте правильность настроек контроллера и состояние сетевых интерфейсов сервера.
4. Для обновления программного обеспечения устройства введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя файла программного обеспечения, помещенного на сервер (при использовании SCP нужно указать полный путь − параметр *<folder>*). После ввода команды устройство скопирует файл во внутреннюю память, проверит целостность данных и сохранит его в энергонезависимую память устройства.
   TFTP:

   ```
   esr# copy tftp://<server>:/<file_name> system:firmware
   ```

   FTP:

   ```
   esr# copy ftp://[<user>[:<password>]@]<server>:/<file_name> system:firmware
   ```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>system:firmware
```

SFTP:

```
esr# copy sftp://[<user>[:<password>]@]<server>:/<file_name> system:firmware
```

Для примера обновите основное ПО через SCP:

```
esr# copy scp://adm:password123@192.168.16.168://home/tftp/firmware system:firmware
```

5. Для того чтобы устройство работало под управлением новой версии программного обеспечения, необходимо произвести переключение активного образа. С помощью команды *show bootvar* следует выяснить номер образа, содержащего обновленное ПО.

```
esr# show bootvar
Image   Version                      Date                  Status         After reboot
-----  --------------               --------------------   ------------   ------------
1       1.0.7 build 141[f812808]     date 18/02/2015 time    Active         *
                                     16:12:54

2       1.0.7 build 141[f812808]     date 18/02/2015 time   Not Active
                                     16:12:54
```

Для выбора образа используйте команду:

```
esr# boot system image-[1|2]
```

6. Для обновления вторичного загрузчика (U-Boot) введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя файла вторичного загрузчика, помещенного на сервер (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды контроллер скопирует файл во внутреннюю память, проверит целостность данных и сохранит его в энергонезависимую память устройства.
TFTP:

```
esr# copy tftp://<server>:/<file_name> system:boot-2
```

FTP:

```
esr# copy ftp://<server>:/<file_name> system:boot-2
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name>system:boot-2
```

SFTP:

```
esr# copy sftp://<server>:/<file_name> system:boot-2
```

7.2 Обновление программного обеспечения из начального загрузчика

Программное обеспечение контроллера можно обновить из начального загрузчика следующим образом:

1. Остановите загрузку устройства после окончания инициализации устройства загрузчиком U-Boot, нажав клавишу ***<Esc>***:

```
Configuring PoE...
distribution 1 dest_threshold 0xa drop_timer 0x0
Configuring POE in bypass mode
NAE configuration done!
initializing port 0, type 2.
initializing port 1, type 2.
SMC Endian Test:b81fb81f
nae-0, nae-1
  =======Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.
Hit any key to stop autoboot:  2
```

2. Укажите IP-адрес TFTP-сервера:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip 10.100.100.1
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip 10.100.100.1
```

3. Укажите IP-адрес контроллера:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

4. Укажите имя файла программного обеспечения на TFTP-сервере:

```
BRCM.XLP316Lite Rev B0.u-boot# firmware_file firmware
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# firmware_file firmware
```

5. Можно сохранить окружение командой «saveenv» для будущих обновлений.

6. Запустите процедуру обновления программного обеспечения:

```
BRCM.XLP316Lite Rev B0.u-boot# run tftp_update_image1
Using nae-0-3 device
TFTP from server 10.100.100.1; our IP address is 10.100.100.2
Filename 'esr1000/firmware'.
Load address: 0xa800000060000000
Loading: TftpStart:TftpTimeoutMsecs = 10000, TftpTimeoutCountMax = 6
#################################################################
#################################################################
#################################################################
########################
##################################
done
Bytes transferred = 64453909 (3d77d15 hex)
Device 0: MT29F8G08ABBCAH4 ... is now current device

NAND erase: device 0 offset 0x1440000, size 0x6400000
Bad block table found at page 262080, version 0x01
Bad block table found at page 262016, version 0x01
Erasing at 0x7800000 -- 1895825408% complete..
OK

NAND write: device 0 offset 0x1440000, size 0x6400000
104857600 bytes written: OK
```

7. Установите загруженное программное обеспечение в качестве образа для запуска системы и перезагрузите роутер:

```
BRCM.XLP316Lite Rev B0.u-boot# run set_bootpart_1
```

Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# boot_system image1
BRCM.XLP316Lite Rev B0.u-boot# reset
```

7.3 Обновление вторичного загрузчика (U-Boot)

Вторичный загрузчик занимается инициализацией NAND контроллера. При обновлении новый файл вторичного загрузчика сохраняется на flash на месте старого.

Для просмотра текущей версии загрузочного файла, работающего на устройстве, введите команду «version» в CLI U-Boot, также версия отображается в процессе загрузки устройства:

```
BRCM.XLP316Lite Rev B0.u-boot# version
BRCM.XLP.U-Boot:1.1.0.47 (29/11/2016 - 19:00:24)
```

Процедура обновления ПО:

1. Остановите загрузку устройства после окончания инициализации устройства загрузчиком U-Boot, нажав клавишу ***<Esc>***:

```
Configuring PoE...
distribution 1 dest_threshold 0xa drop_timer 0x0
Configuring POE in bypass mode
NAE configuration done!
initializing port 0, type 2.
initializing port 1, type 2.
SMC Endian Test:b81fb81f
nae-0, nae-1
  =======Skip: Load SYS UCORE for old 8xxB1/3xxB0 revision on default.
Hit any key to stop autoboot:  2
```

2. Укажите IP-адрес TFTP-сервера:

```
BRCM.XLP316Lite Rev B0.u-boot# setenv serverip 10.100.100.1
```

   Для версии 1.5 и выше:

```
BRCM.XLP316Lite Rev B0.u-boot# serverip10.100.100.2
```

3. Укажите IP-адрес контроллера:

```
BRCM.XLP316Lite Rev B0.u-boot# ipaddr 10.100.100.2
```

4. Укажите имя файла загрузчика на TFTP-сервере:

```
BRCM.XLP316Lite Rev B0.u-boot# uboot_file u-boot.bin
```

5. Можно сохранить окружение командой «saveenv» для будущих обновлений.
6. Запустите процедуру обновления программного обеспечения:

```
BRCM.XLP316LiteRevB0.u-boot# run tftp_update_uboot
Using nae-1 device
TFTP from server 10.100.100.1; our IP address is 10.100.100.2
Filename 'esr1000/u-boot.bin'.
Load address: 0xa800000078020000
Loading: ##################################################################
done
Bytes transferred = 852648 (d02a8 hex)
SF: Detected MX25L12805D with page size 256, total 16777216 bytes
16384 KiB MX25L12805D at 0:0 is now current device
```

7. Перезагрузите устройство:

```
BRCM.XLP316Lite Rev B0.u-boot# reset
```

8 Рекомендации по безопасной настройке

Рекомендации по безопасной настройке носят общий характер и подходят для большинства инсталляций. Настоящие рекомендации в значительной степени повышают безопасность эксплуатации устройства, но не являются исчерпывающими. В зависимости от схемы применения устройства необходимо настраивать и другие параметры безопасности. В некоторых специфических случаях выполнение данных рекомендаций может привести к неработоспособности сети. При настройке устройства стоит в первую очередь следовать техническим требованиям и регламентам сетей, в которых будет эксплуатироваться данное устройство.

8.1 Общие рекомендации

- Рекомендуется всегда отключать неиспользуемые физические интерфейсы с помощью команды **shutdown.** Команда подробно описана в разделе Конфигурирование и мониторинг интерфейсов справочника команд CLI.
- Рекомендуется всегда настраивать синхронизацию системных часов с доверенными источниками сетевого времени (NTP). Алгоритм настройки NTP приведён в разделе Настройка NTP настоящего руководства. Подробная информация о командах для настройки NTP приведена в разделе Управление системными часами справочника команд CLI.
- Рекомендуется отключать NTP broadcast client, включённый по умолчанию в заводской конфигурации.
- Не рекомендуется использовать команду **ip firewall disable,** отключающую межсетевое экранирование. Следует всегда назначать интерфейсам соответствующие зоны безопасности и настраивать корректные правила межсетевого экрана. Алгоритм настройки межсетевого экрана приведён в разделе Конфигурирование Firewall настоящего руководства. Подробная информация о командах для настройки межсетевого экрана приведена в разделе Управление Firewall справочника команд CLI.

8.2 Настройка системы логирования событий

Алгоритмы настройки системы логирования событий приведены в подразделе «Настройка Syslog» раздела Мониторинг настоящего руководства.

Подробная информация о командах для настройки системы логирования событий приведена в разделе Управление SYSLOG справочника команд CLI.

8.2.1 Рекомендации

- Рекомендуется настроить хранение сообщений о событиях в файл syslog на устройстве и передачу этих событий на внешний syslog-сервер.
- Рекомендуется ограничивать размер syslog-файла на устройстве.
- Рекомендуется настраивать ротацию syslog-файлов на устройстве.
- Рекомендуется включать нумерацию сообщений syslog.
- Рекомендуется включать добавление меток timestamp msec к syslog-сообщениям на устройствах ESR-1500 и ESR-1511.

8.2.2 Предупреждения

- Данные, хранящиеся в файловой системе **tmpsys:syslog,** не сохраняются при перезагрузке устройства. Этот тип файловой системы рекомендуется использовать для хранения оперативных логов.
- Не рекомендуется использовать файловую систему **flash:syslog** для хранения логов, так как это может привести к преждевременному выходу из строя устройства.

8.2.3 Пример настройки

Задача:

Настроить хранение сообщений о событиях уровня info и выше в файл syslog на устройстве и настроить передачу этих событий на внешний syslog-сервер. Ограничить файл размером 512 Кбайт. Включить ротацию 3 файлов. Включить нумерацию сообщений syslog.

Решение:

Настраиваем хранение syslog-сообщений в файле:

```
wlc(config)# syslog file tmpsys:syslog/default info
```

Настраиваем ограничение размера и ротацию файлов:

```
wlc(config)# syslog max-files 3
wlc(config)# syslog file-size 512
```

Настраиваем передачу сообщений на внешний сервер:

```
wlc(config)# syslog host mylog 192.168.1.2 info udp 514
```

Включаем нумерацию сообщений syslog:

```
wlc(config)# syslog sequence-numbers
```

8.3 Настройка политики использования паролей

Алгоритмы настройки политики использования паролей приведены в разделе Настройка AAA настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе Настройка AAA справочника команд CLI.

8.3.1 Рекомендации

- Рекомендуется всегда включать требования на смену пароля по умолчанию пользователя admin.
- Рекомендуется ограничивать время жизни паролей и запрещать повторно использовать, как минимум, предыдущий пароль.
- Рекомендуется выставлять требования минимальной длины пароля больше 8 символов.
- Рекомендуется выставлять требования на использование строчных и прописных букв, цифр и спецсимволов.

8.3.2 Пример настройки

Задача:

- Настроить парольную политику с обязательным требованием смены пароля по умолчанию, временем действия пароля 1 месяц и запретом на использование 12 последних паролей.
- Задать минимальную длину пароля 16 символов, максимальную — 64 символа.
- Пароль должен содержать не менее 3 прописных букв, не менее 5 строчных букв, не менее 4 цифр и не менее 2 спецсимволов. Пароль в обязательном порядке должен содержать все 4 типа символов.

Решение:

Включаем запрос на смену пароля по умолчанию для пользователя admin:

```
wlc(config)# security passwords default-expired
```

Устанавливаем время жизни пароля 30 дней и запрет на использование предыдущих 12 паролей:

```
wlc(config)# security passwords lifetime 30
wlc(config)# security passwords history 12
```

Устанавливаем ограничения на длину пароля:

```
wlc(config)# security passwords min-length 16
wlc(config)# security passwords max-length 24
```

Устанавливаем ограничения по минимальному количеству символов соответствующих типов:

```
wlc(config)# security passwords upper-case 3
wlc(config)# security passwords lower-case 5
wlc(config)# security passwords special-case 2
wlc(config)# security passwords numeric-count 4
wlc(config)# security passwords symbol-types 4
```

8.4 Настройка политики AAA

Алгоритмы настройки политики AAA приведены в разделе Настройка AAA настоящего руководства.

Подробная информация о командах для настройки политики AAA приведена в разделе Настройка AAA справочника команд CLI.

8.4.1 Рекомендации

- Рекомендуется использовать ролевую модель доступа на устройство.
- Рекомендуется использовать персональные учетные записи для аутентификации на устройстве.
- Рекомендуется включать логирование вводимых пользователем команд.
- Рекомендуется использовать несколько методов аутентификации для входа на устройства через консоль, удалённого входа на устройства и повышения привилегий. Оптимальной считается комбинация из аутентификации по одному из протоколов RADIUS/TACACS/LDAP и локальной аутентификации.
- Рекомендуется понизить уровень привилегий встроенной учётной записи **admin** до 1.
- Рекомендуется настроить логирование изменений локальных учётных записей.
- Рекомендуется настроить логирование изменений политики AAA.

8.4.2 Предупреждения

- Встроенную учётную запись admin удалить нельзя.
- Команда **no username admin** не удаляет пользователя **admin**, сбрасывает его конфигурацию в значения по умолчанию. После применения этой команды пользователь **admin** не будет отображаться в конфигурации.
- Команда **no password** для пользователя **admin** также не удаляет пароль пользователя **admin**, а сбрасывает его в значение по умолчанию. После применения этой команды пароль пользователя **admin** перестаёт отображаться в конфигурации и становится ‘password'.
- Перед установкой пользователю admin пониженных привилегий у вас должен быть настроен пользователь с уровнем привилегий 15 или задан ENABLE-пароль.

8.4.3 Пример настройки

Задача:

Настроить политику AAA:

- Для удалённого входа по протоколу SSH использовать аутентификации через RADIUS.
- Для входа через локальную консоль использовать аутентификации через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальную аутентификацию.
- Использовать ENABLE-пароль заданный через RADIUS, в случае отсутствия связи с RADIUS-серверами использовать локальный ENABLE-пароль.
- Установить пользователю admin пониженный уровень привилегий.
- Настроить логирование изменений локальных учётных записей.
- Настроить логирование изменений политик AAA.
- Настроить логирование вводимых команд.

Решение:

Создаем локального пользователя **local-operator** с уровнем привилегий 8:

```
wlc(config)# username local-operator
wlc(config-user)# password Pa$$w0rd1
wlc(config-user)# privilege 8
wlc(config-user)# exit
```

Задаём локальный ENABLE-пароль:

```
wlc(config)# enable password $6e5c4r3e2t!
```

Понижаем привилегии пользователя admin:

```
wlc(config)# username admin
wlc(config-user)# privilege 1
wlc(config-user)# exit
```

Настраиваем связь с двумя RADIUS-серверами, основным 192.168.1.11 и резервным 192.168.2.12:

```
wlc(config)# radius-server host 192.168.1.11
wlc(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
wlc(config-radius-server)# priority 100 wlc(config-radius-server)# exit
wlc(config)# radius-server host 192.168.2.12
wlc(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
wlc(config-radius-server)# priority 150
wlc(config-radius-server)# exit
```

Настраиваем политику AAA:

```
wlc(config)# aaa authentication login CONSOLE radius local
wlc(config)# aaa authentication login SSH radius
wlc(config)# aaa authentication enable default radius enable
wlc(config)# aaa authentication mode break
wlc(config)# line console
wlc(config-line-console)# login authentication CONSOLE
wlc(config-line-console)# exit wlc(config)# line ssh
wlc(config-line-ssh)# login authentication SSH
wlc(config-line-ssh)# exit
```

Настраиваем логирование:

```
wlc(config)# logging userinfo
wlc(config)# logging aaa
wlc(config)# syslog cli-commands
```

8.5 Настройка удалённого управления

Подробная информация о командах настройки удалённого доступа приведена в разделе Настройка доступа SSH, Telnet справочника команд CLI.

8.5.1 Рекомендации

- Рекомендуется отключить удалённое управление по протоколу telnet.
- Рекомендуется использовать криптостойкие алгоритмы аутентификации sha2-512 и отключить все остальные.
- Рекомендуется использовать криптостойкие алгоритмы шифрования aes256ctr и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм обмена ключами шифрования dh-group-exchange-sha256 и отключить все остальные.
- Рекомендуется использовать криптостойкий алгоритм верификации Host-Key для SSH rsa и отключить все остальные.
- Рекомендуется разрешить доступ к удалённому управлению устройством только с определённых IP-адресов.
- Перед началом эксплуатации рекомендуется перегенерировать ключи шифрования.

8.5.2 Пример настройки

Задача:

Отключить протокол telnet. Сгенерировать новые ключи шифрования. Использовать криптостойкие алгоритмы.

Решение:

Отключаем удаленное управление по протоколу telnet:

```
wlc(config)# no ip telnet server
```

Отключаем устаревшие и не криптостойкие алгоритмы:

```
wlc(config)# ip ssh server
wlc(config)# ip ssh authentication algorithm md5 disable
wlc(config)# ip ssh authentication algorithm md5-96 disable
wlc(config)# ip ssh authentication algorithm ripemd160 disable
wlc(config)# ip ssh authentication algorithm sha1 disable
wlc(config)# ip ssh authentication algorithm sha1-96 disable
wlc(config)# ip ssh authentication algorithm sha2-256 disable
wlc(config)# ip ssh encryption algorithm 3des disable
wlc(config)# ip ssh encryption algorithm aes128 disable
wlc(config)# ip ssh encryption algorithm aes128ctr disable
wlc(config)# ip ssh encryption algorithm aes192 disable
wlc(config)# ip ssh encryption algorithm aes192ctr disable
wlc(config)# ip ssh encryption algorithm aes256 disable
wlc(config)# ip ssh encryption algorithm arcfour disable
wlc(config)# ip ssh encryption algorithm arcfour128 disable
wlc(config)# ip ssh encryption algorithm arcfour256 disable
wlc(config)# ip ssh encryption algorithm blowfish disable
wlc(config)# ip ssh encryption algorithm cast128 disable
wlc(config)# ip ssh key-exchange algorithm dh-group-exchange-sha1 disable
wlc(config)# ip ssh key-exchange algorithm dh-group1-sha1 disable
wlc(config)# ip ssh key-exchange algorithm dh-group14-sha1 disable
wlc(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp256 disable
wlc(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp384 disable
wlc(config)# ip ssh key-exchange algorithm ecdh-sha2-nistp521 disable
wlc(config)# ip ssh host-key algorithm dsa disable
wlc(config)# ip ssh host-key algorithm ecdsa256 disable
wlc(config)# ip ssh host-key algorithm ecdsa384 disable
wlc(config)# ip ssh host-key algorithm ecdsa521 disable
wlc(config)# ip ssh host-key algorithm ed25519 disable
```

Генерируем новые ключи шифрования:

```
wlc# update ssh-host-key rsa
wlc# update ssh-host-key rsa 2048
```

8.6 Настройка механизмов защиты от сетевых атак

Алгоритмы настройки механизмов защиты от сетевых атак приведены в разделе Настройка логирования и защиты от сетевых атак настоящего руководства.

Подробная информация о командах для настройки политики использования паролей приведена в разделе Управление логированием и защитой от сетевых атак справочника команд CLI.

8.6.1 Рекомендации

- Рекомендуется всегда включать защиту от ip spoofing.
- Рекомендуется всегда включать защиту от TCP-пакетов с неправильно выставленными флагами.
- Рекомендуется всегда включать защиту от фрагментированных TCP-пакетов с выставленным флагом SYN.
- Рекомендуется всегда включать защиту от фрагментированных ICMP-пакетов.
- Рекомендуется всегда включать защиту ICMP-пакетов большого размера.
- Рекомендуется всегда включать защиту от незарегистрированных IP-протоколов.
- Рекомендуется включать логирование механизма защиты от сетевых атак.

8.6.2 Пример настройки

Задача:

Настроить механизм защиты от сетевых атак в соответствии с рекомендациями.

Решение:

Включаем защиту от ip spoofing и логирование механизма защиты:

```
wlc(config)# ip firewall screen spy-blocking spoofing
wlc(config)# logging firewall screen spy-blocking spoofing
```

Включаем защиту от TCP-пакетов с неправильно выставленными флагами и логирование механизма защиты:

```
wlc(config)# ip firewall screen spy-blocking syn-fin
wlc(config)# logging firewall screen spy-blocking syn-fin
wlc(config)# ip firewall screen spy-blocking fin-no-ack
wlc(config)# logging firewall screen spy-blocking fin-no-ack
wlc(config)# ip firewall screen spy-blocking tcp-no-flag
wlc(config)# logging firewall screen spy-blocking tcp-no-flag
wlc(config)# ip firewall screen spy-blocking tcp-all-flags
wlc(config)# logging firewall screen spy-blocking tcp-all-flags
```

Включаем защиту от фрагментированных ICMP-пакетов и логирование механизма защиты:

```
wlc(config)# ip firewall screen suspicious-packets icmp-fragment
wlc(config)# logging firewall screen suspicious-packets icmp-fragment
```

Включаем защиту от ICMP-пакетов большого размера и логирование механизма защиты:

```
wlc(config)# ip firewall screen suspicious-packets large-icmp
wlc(config)# logging firewall screen suspicious-packets large-icmp
```

Включаем защиту от незарегистрированных IP-протоколов и логирование механизма защиты:

```
wlc(config)# ip firewall screen suspicious-packets unknown-protocols
wlc(config)# logging firewall screen suspicious-packets unknown-protocols
```

9 Управление интерфейсами

Алгоритм и примеры настройки функций управления интерфейсами см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

10 Управление контроллером WLC

10.1 Настройка WLC

10.1.1 Настройка контроллера WLC

> ⚠ Функционал WLC можно активировать на сервисных маршрутизаторах ESR-15, ESR-15R, ESR-30 и ESR-3200 по инструкции.

Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Настроить локальный RADIUS-сервер и перейти в режим его конфигурирования.	**wlc(config)# radius-server local** **wlc(config-radius)#**	

Шаг	Описание	Команда	Ключи
2	Активировать работу локального RADIUS-сервера.	**wlc(config-radius)# enable**	
3	Добавить NAS и перейти в режим его конфигурирования.	**wlc(config-radius)# nas <NAME>** **wlc(config-radius-nas)#**	<NAME> – название NAS, задается строкой до 235 символов.
4	Задать ключ аутентификации.	**wlc(config-radius-nas)# key ascii-text { <KEY> | encrypted <ENCRYPTED-KEY> }**	<KEY> – строка из [4..64] ASCII-символов; <ENCRYPTED-KEY> – зашифрованный ключ, задаётся строкой [8..128] символов.
5	Указать сеть.	**wlc(config-radius-nas)# network <ADDR/LEN>**	<ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].
6	Создать домен.	**wlc(config-radius)# domain <NAME>**	<NAME> – идентификатор домена, задается строкой до 235 символов.
7	Добавить виртуальный RADIUS-сервер и перейти в режим его конфигурирования.	**wlc(config-radius)# virtual-server <NAME>** **wlc(config-radius-vserver)#**	<NAME> – название виртуального RADIUS-сервера, задается строкой до 235 символов.
8	Активировать работу виртуального RADIUS-сервера.	**wlc(config-radius-vserver)# enable**	
9	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**wlc(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }** **[vrf <VRF>]** **wlc(config-radius-server)#**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
10	Задать ключ аутентификации.	**wlc(config-radius-server)# key ascii-text { <KEY> | encrypted <ENCRYPTED-KEY> }**	<KEY> – строка из [4..64] ASCII-символов; <ENCRYPTED-KEY> – зашифрованный ключ, задаётся строкой [8..128] символов.

Шаг	Описание	Команда	Ключи
11	Создать профиль AAA и перейти в режим его конфигурирования.	**wlc(config)# aaa radius-profile <NAME>** **wlc(config-aaa-radius-profile)#**	<NAME> – имя профиля сервера, задается строкой до 31 символа.
12	В профиле AAA указать RADIUS-сервер.	**wlc(config-aaa-radius-profile)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
13	Перейти в настройки конфигурирования SoftGRE-контроллера.	**wlc(config)# softgre-controller** **wlc(config-softgre-controller)#**	
14	Определить IP-адрес маршрутизатора, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS-пакетах.	**wlc(config-softgre-controller)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
15	Установить режим конфигурации SoftGRE DATA туннелей.	**wlc(config-softgre-controller)# data-tunnel configuration { local | radius | wlc}**	local – режим конфигурации, при котором параметры SoftGRE DATA туннелей получаются из локальной конфигурации маршрутизатора; radius – режим, при котором параметры SoftGRE DATA туннелей запрашиваются у RADIUS-сервера; wlc – режим, при котором параметры SoftGRE DATA туннелей запрашиваются у WLC.
16	Указать профиль AAA.	**wlc(config-softgre-controller)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
17	Отключить обмен ICMP-сообщениями, которые используются для проверки доступности удаленного шлюза туннелей Wi-Fi контроллера.	**wlc(config-softgre-controller)# keepalive-disable**	
18	Разрешить трафик в пользовательском vlan.	**wlc(config-softgre-controller)# service-vlan add {<VLAN-ID> | <LIST_ID> | <RANGE_ID> }**	**<**VLAN-ID**>** – номер vlan, в котором проходит пользовательский трафик, принимает значения [2..4094]; **<**LIST_ID**>** – список vlan, указываемый через запятую (1,2,3), принимает значения [2..4094]; **<**RANGE_ID**>** – диапазон vlan, указывается через тире (1-3), принимает значения [2..4094].
19	Активировать работу контроллера Wi-Fi.	**wlc(config-softgre-controller)# enable**	
20	Перейти в настройки SoftGRE-туннеля.	**wlc(config)# tunnel softgre <TUN>**	<TUN> – имя туннеля устройства, задаётся в виде, описанном в разделе Типы и порядок именования туннелей маршрутизатора.
21	Задать режим работы SoftGRE-туннеля.	**wlc(config-softgre)# mode <MODE>**	<MODE> – режим работы туннеля, возможные значения: • data – режим данных; • management – режим управления.
22	Устанавить IP-адрес локального шлюза туннеля.	**wlc(config-softgre)# local address <ADDR>**	<ADDR> – IP-адрес локального шлюза, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
23	Активировать использование конфигурации данного SoftGRE-туннеля для автоматического создания туннелей с такими же mode и local address.	**wlc(config-softgre)# default-profile**	
24	Включить туннель.	**wlc(config-softgre)# enable**	
25	Перейти в раздел конфигурирования контроллера.	**wlc(config)# wlc**	

Шаг	Описание	Команда	Ключи
26	Создать профиль конфигурирования общих настроек точки доступа.	**wlc(config-wlc)# ap-profile <NAME>** **wlc(config-wlc-ap-profile)#**	<NAME> – название профиля, задается строкой до 235 символов.
27	Задать пароль для подключения к точкам доступа.	**wlc(config-wlc-ap-profile)# password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }** **wlc(config-wlc-ap-profile)# exit**	<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символов. <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.
28	Создать профиль конфигурирования радиоинтерфейса, работающего в частотном диапазоне 2,4 ГГц.	**wlc(config-wlc)# radio-2g-profile <NAME>**	<NAME> – название профиля, задается строкой до 235 символов.
29	Настроить работу режима автоматического уменьшения ширины канала при загруженном радиоэфире	**wlc(config-wlc-radio-2g-profile)# obss-coexistence {on | off}**	on – режим автоматического уменьшения ширины канала активирован; off – режим автоматического уменьшения ширины канала выключен.
30	Установить режим работы радиоинтерфейса.	**wlc(config-wlc-radio-2g-profile)# work-mode <WORK-MODE>**	<WORK-MODE> – режим работы, доступные значения: • bg, nax, bgnax – для частотного диапазона 2,4 ГГц.
31	Задать список каналов для динамического выбора канала.	**wlc(config-wlc-radio-2g-profile)# limit-channels <CHANNEL>[,<CHANNEL>]**	<CHANNEL> – номер используемого канала, доступные значения: Для 2g каналы из диапазона: [1.. 13].
32	Настроить ширину канала.	**wlc(config-wlc-radio-2g-profile)# bandwidth <BANDWIDTH>**	<BANDWIDTH> – ширина канала, доступные значения: • 20; • 40L; • 40U.

<table>
<tr><th>Шаг</th><th>Описание</th><th>Команда</th><th>Ключи</th></tr>
<tr><td>33</td><td>Настроить уровень мощности для радиоинтерфейса.</td><td>wlc(config-wlc-radio-2g-profile)# tx-power {minimal | low | middle | high | maximal}</td><td>Возможные значения параметра в зависимости от модели точки доступа устанавливают следующие значения мощности в дБм:
<table>
<tr><th rowspan="2">Модель</th><th colspan="5">2,4 ГГц</th></tr>
<tr><th>min</th><th>low</th><th>middle</th><th>high</th><th>max</th></tr>
<tr><td>WEP-1L</td><td>11</td><td>12</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td>WEP-2L</td><td>11</td><td>12</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td>WOP-2L</td><td>11</td><td>12</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td>WOP-20L</td><td>8</td><td>10</td><td>12</td><td>14</td><td>16</td></tr>
<tr><td>WEP-200L</td><td>4</td><td>7</td><td>10</td><td>13</td><td>16</td></tr>
<tr><td>WEP-30L</td><td>0</td><td>4</td><td>8</td><td>12</td><td>16</td></tr>
<tr><td>WOP-30L</td><td>0</td><td>4</td><td>8</td><td>12</td><td>16</td></tr>
<tr><td>WOP-30LS</td><td>0</td><td>3</td><td>6</td><td>9</td><td>11</td></tr>
<tr><td>WEP-3ax</td><td>6</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
</table></td></tr>
<tr><td>34</td><td>Создать профиль конфигурирования радиоинтерфейса, работающего в частотном диапазоне 5 ГГц.</td><td>wlc(config-wlc)# radio-5g-profile <NAME></td><td><NAME> – название профиля, задается строкой до 235 символов.</td></tr>
<tr><td>35</td><td>Настроить работу режима автоматического уменьшения ширины канала при загруженном радиоэфире</td><td>wlc(config-wlc-radio-5g-profile)# obss-coexistence {on | off}</td><td>on – режим автоматического уменьшения ширины канала активирован;

off – режим автоматического уменьшения ширины канала выключен.</td></tr>
<tr><td>36</td><td>Установить режим работы радиоинтерфейса.</td><td>wlc(config-wlc-radio-5g-profile)# work-mode <WORK-MODE></td><td><WORK-MODE> – режим работы, доступные значения:

• anacax – для частотного диапазона 5 ГГц.</td></tr>
<tr><td>37</td><td>Задать список каналов для динамического выбора канала.</td><td>wlc(config-wlc-radio-5g-profile)# limit-channels <CHANNEL>[,<CHANNEL>]</td><td><CHANNEL> – номер используемого канала, доступные значения:
Для 5g каждый 4 канал из диапазонов:
[36.. 64]
[100.. 144]
[149.. 165]</td></tr>
</table>

<table>
<tr><th>Шаг</th><th>Описание</th><th>Команда</th><th>Ключи</th></tr>
<tr><td>38</td><td>Настроить ширину канала.</td><td>wlc(config-wlc-radio-5g-profile)# bandwidth <BANDWIDTH></td><td><BANDWIDTH> – ширина канала, доступные значения:
20;
40L;
40U;
80.</td></tr>
<tr><td>39</td><td>Настроить уровень мощности для радиоинтерфейса.</td><td>wlc(config-wlc-radio-5g-profile)# tx-power {minimal | low | middle | high | maximal}</td><td>Возможные значения параметра в зависимости от модели точки доступа устанавливают следующие значения мощности в дБм:<table><tr><th rowspan="2">Модель</th><th colspan="5">5 ГГц</th></tr><tr><th>min</th><th>low</th><th>middle</th><th>high</th><th>max</th></tr><tr><td>WEP-1L</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td></tr><tr><td>WEP-2L</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td></tr><tr><td>WOP-2L</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td></tr><tr><td>WOP-20L</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td></tr><tr><td>WEP-200L</td><td>8</td><td>11</td><td>14</td><td>17</td><td>19</td></tr><tr><td>WEP-30L</td><td>0</td><td>5</td><td>10</td><td>15</td><td>19</td></tr><tr><td>WOP-30L</td><td>0</td><td>5</td><td>10</td><td>15</td><td>19</td></tr><tr><td>WOP-30LS</td><td>0</td><td>3</td><td>6</td><td>9</td><td>11</td></tr><tr><td>WEP-3ax</td><td>10</td><td>12</td><td>15</td><td>17</td><td>19</td></tr></table></td></tr>
<tr><td>40</td><td>Настроить режим динамического выбора частоты.</td><td>wlc(config-wlc-radio-5g-profile)# dfs {auto | disabled | forced}</td><td>auto — механизм включен;

disabled— механизм выключен. DFS-каналы не доступны для выбора;

forced — механизм выключен. DFS-каналы доступны для выбора;</td></tr>
<tr><td>41</td><td>Создать профиль конфигурирования RADIUS-сервера.</td><td>wlc(config-wlc)# radius-profile <RADIUS-ID>

wlc(config-wlc-radius-profile)#</td><td><RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов.</td></tr>
<tr><td>42</td><td>Указать IP-адрес RADIUS-сервера, который отвечает за аутентификацию.</td><td>wlc(config-wlc-radius-profile)# auth-address <ADDR></td><td><ADDR> – IP-адрес RADIUS-сервера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].</td></tr>
</table>

Шаг	Описание	Команда	Ключи
43	Указать пароль RADIUS-сервера, который отвечает за аутентификацию.	**wlc(config-wlc-radius-profile)# auth-password ascii-text { <CLEAR-TEXT> | encrypted <HASH_SHA512> }**	<CLEAR-TEXT> – пароль, задаётся строкой [8-64] символа. <HASH_SHA512> – хеш пароля по алгоритму sha512, задаётся строкой [16-128] символов.
44	Указать домен.	**wlc(config-wlc-radius-profile)# domain <NAME>**	<NAME> – идентификатор домена, задается строкой до 235 символов.
45	Создать профиль конфигурирования SSID.	**wlc(config-wlc)# ssid-profile <NAME>** **wlc(config-wlc-ssid-profile)#**	<NAME> – название профиля SSID, задается строкой до 235 символов.
46	Задать описание профиля.	**wlc(config-wlc-ssid-profile)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.
47	Настроить частотный диапазон, в котором будет происходить вещание SSID.	**wlc(config-wlc-ssid-profile)# band <BAND>**	<BAND> – диапазон частот, доступные значения: • 2g; • 5g.
48	Указать пользовательский vlan.	**wlc(config-wlc-ssid-profile)# vlan-id <ID>**	<ID> – идентификатор vlan, принимает значения в диапазоне [0-4094].
49	Установить режим безопасности подключения к SSID.	**wlc(config-wlc-ssid-profile)# security-mode <MODE>**	<MODE> – режим безопасности, доступные значения: • WPA; • WPA2; • WPA2_1X; • WPA2_WPA3; • WPA2_WPA3_1X; • WPA3; • WPA3_1X; • WPA_1X; • WPA_WPA2; • WPA_WPA2_1X; • off. Режим безопасности WPA3 поддерживается только на точках доступа моделей WEP-3ax, WEP-30L, WOP-30L, WOP-30LS. При выборе смешанного режима безопасности (например, WPA2_WPA3) WPA3 будет применен только для тех точек доступа, которые его поддерживают, для остальных будет применен второй режим (WPA2).

Шаг	Описание	Команда	Ключи
50	Указать профиль RADIUS-сервера.	**wlc(config-wlc-ssid-profile)# radius-profile <RADIUS-ID>**	<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов.
51	Задать название SSID, который будет вещаться пользователям.	**wlc(config-wlc-ssid-profile)# ssid <NAME>**	<NAME> – название SSID, задается строкой до 32 символов. Названия, содержащие пробел, необходимо заключать в кавычки.
52	Активировать работу SSID.	**wlc(config-wlc-ssid-profile)# enable**	
53	Создать профиль локации.	**wlc(config-wlc)# ap-location <NAME>** **wlc(config-wlc-ap-location)#**	<NAME> – название профиля локального конфигурирования, задается строкой до 235 символов.
54	Задать описание профиля.	**wlc(config-wlc-ap-location)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.
55	Указать для точек доступа существующие профили настроек радиоинтерфейсов.	**wlc(config-wlc-ap-location)# radio-5g-profile <NAME>** **wlc(config-wlc-ap-location)# radio-2g-profile <NAME>**	<NAME> – название профиля, задается строкой до 235 символов.
56	Указать для точек доступа существующий профиль общих настроек.	**wlc(config-wlc-ap-location)# ap-profile <PROFILE-ID>**	<PROFILE-ID> – идентификатор профиля, задается строкой до 235 символов и должен совпадать с названием описанного профиля из ap-profile.
57	Указать профиль SSID, который будет назначен точкам доступа.	**wlc(config-wlc-ap-location)# ssid-profile <NAME>**	<NAME> – название профиля SSID, задается строкой до 235 символов.
58	Создать адресное пространство для доступа к контроллеру.	**wlc(config-wlc)# ip-pool <NAME>** **wlc(config-wlc-ip-pool)#**	<NAME> – название адресного пространства, задается строкой до 235 символов.
59	Указать подсеть точек доступа.	**wlc(config-wlc-ip-pool)# network <ADDR/LEN>**	<ADDR/LEN> – IP-адрес и маска подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32].

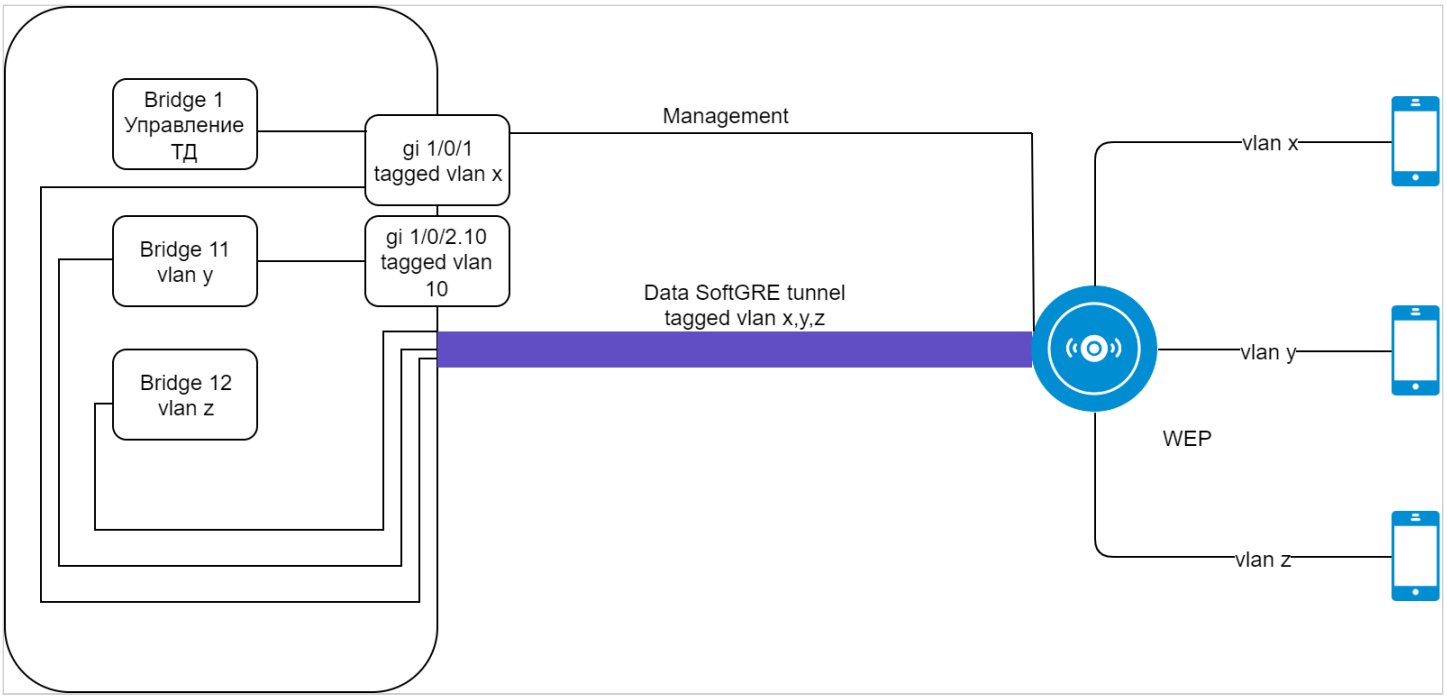
Шаг	Описание	Команда	Ключи
60	Указать название профиля локации, который применяется к заданному адресному пространству.	**wlc(config-wlc-ip-pool)# ap-location <NAME>**	<NAME> – название локации, задается строкой до 235 символов.
61	Перейти в настройки сервис-активатора.	**wlc(config-wlc)# service-activator** **wlc(config-wlc-service-activator)#**	
62	Настроить автоматическую регистрацию точек доступа на контроллере.	**wlc(config-wlc-service-activator)# aps join auto**	
63	Указать IP-адрес контроллера, который виден точкам доступа.	**wlc(config-wlc)# outside-address <ADDR>**	<ADDR> – IP-адрес контроллера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
64	Активировать работу контроллера.	**wlc(config-wlc)# enable**	

Пример настройки

Задача

Организовать управление беспроводными точками доступа с помощью контроллера WLC. В частности, необходимо настроить подключение точек доступа, обновить и сконфигурировать их для предоставления доступа до ресурсов Интернет авторизованным пользователям Wi-Fi.

Пример настройки приведен на основе заводской конфигурации для схемы с построением SoftGRE-туннелей.



Решение

Архитектура решения предполагает автоматическое подключение точек доступа к контроллеру WLC. При подключении к сети точка доступа запрашивает адрес по DHCP и вместе с ним должна получить URL сервиса инициализации точек доступа в 43 (vendor specific) опции DHCP.

Получив данную опцию, точка доступа приходит на контроллер и появляется в базе обслуживаемых точек доступа (команда для мониторинга списка: show wlc ap). Далее контроллер инициализирует ее в соответствии со своей конфигурацией:

1. Выполняет обновление, если версия ПО на точке доступа не соответствует версии, которая размещена на контроллере.
2. Устанавливает пароль доступа.
3. Выполняет конфигурирование в соответствии с настройками для данной локации (ap-location): выбранным профилем конфигурации для данного типа точек доступа и SSID.

Точки доступа могут быть подключены к контроллеру WLC через L2- или L3-сеть предприятия.

Выделение и настройка VLAN при подключении новых точек доступа может оказаться трудоемкой задачей, особенно если на сети предприятия между точками доступа и контроллером используется большое количество коммутаторов. Поэтому заводская конфигурация WLC предполагает построение SoftGRE DATA туннелей для передачи пользовательского трафика. Такое решение даже в L2-сети позволяет упростить подключение точек доступа, так как отсутствует необходимость прокидывать VLAN для каждого SSID через все коммутаторы.

При организации связи в L3-сети необходимо обеспечить настройку DHCP-relay на оборудовании сети предприятия для перенаправления DHCP-запросов точек доступа на WLC, где настроен пул IP-адресов для управления точками доступа, а также выдача 43 опции 15 подопции DHCP, содержащая URL контроллера.

Последовательность настройки контроллера беспроводных сетей WLC:

1. Настройка интерфейсов, сетевых параметров и firewall.
2. Настройка контроллера для организации SoftGRE DATA туннелей.
3. Настройка DHCP-сервера.
4. Настройка RADIUS-сервера.
5. Настройка модуля управления точками доступа WLC:
    - Настройка SSID.
    - Настройка профилей конфигурации для каждого типа точек доступа.

- Создание локации (ap-location) и определение правил конфигурирования точек доступа, входящих в данную локацию.
- Определение подсетей обслуживаемых точек доступа.

6. Настройка обновления точек доступа.

Настройка интерфейсов, сетевых параметров и firewall

Настройте профили TCP/UDP-портов для необходимых сервисов:

```
wlc# configure

wlc(config)# object-group service ssh
wlc(config-object-group-service)# port-range 22
wlc(config-object-group-service)# exit

wlc(config)# object-group service dns
wlc(config-object-group-service)# port-range 53
wlc(config-object-group-service)# exit

wlc(config)# object-group service dhcp_server
wlc(config-object-group-service)# port-range 67
wlc(config-object-group-service)# exit

wlc(config)# object-group service dhcp_client
wlc(config-object-group-service)# port-range 68
wlc(config-object-group-service)# exit

wlc(config)# object-group service ntp
wlc(config-object-group-service)# port-range 123
wlc(config-object-group-service)# exit

wlc(config)# object-group service netconf
wlc(config-object-group-service)# port-range 830
wlc(config-object-group-service)# exit

wlc(config)# object-group service radius_auth
wlc(config-object-group-service)# port-range 1812
wlc(config-object-group-service)# exit

wlc(config)# object-group service sa
wlc(config-object-group-service)# port-range 8043-8044
wlc(config-object-group-service)# exit

wlc0(config)# object-group service airtune
wlc(config-object-group-service)# port-range 8099
wlc(config-object-group-service)# exit
```

Создайте три зоны безопасности — зона пользователей (users), доверенная зона для точек доступа (trusted) и недоверенная зона для выхода в Интернет (untrusted):

```
wlc(config)# security zone users
wlc(config-zone)# exit

wlc(config)# security zone trusted
wlc(config-zone)# exit

wlc(config)# security zone untrusted
wlc(config-zone)# exit
```

Настройте правила firewall:

```
wlc(config)# security zone-pair trusted untrusted
wlc(config-zone-pair)# rule 1
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair trusted trusted
wlc(config-zone-pair)# rule 1
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair trusted self
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port ssh
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 20
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol icmp
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 30
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match source-port dhcp_client
wlc(config-zone-pair-rule)# match destination-port dhcp_server
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 40
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match destination-port ntp
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 50
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port dns
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 60
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match destination-port dns
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 70
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port netconf
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
```

```
wlc(config-zone-pair)# rule 80
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port sa
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 90
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match destination-port radius_auth
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 100
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol gre
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair users self
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol icmp
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 20
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match source-port dhcp_client
wlc(config-zone-pair-rule)# match destination-port dhcp_server
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 30
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port dns
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 40
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match destination-port dns
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair untrusted self
wlc(config-zone-pair)# rule 1
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match source-port dhcp_server
wlc(config-zone-pair-rule)# match destination-port dhcp_client
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair users untrusted
wlc(config-zone-pair)# rule 1
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
```

Настройте NAT:

```
wlc(config)# nat source
wlc(config-snat)# ruleset factory
wlc(config-snat-ruleset)# to zone untrusted
wlc(config-snat-ruleset)# rule 10
wlc(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
wlc(config-snat-rule)# action source-nat interface
wlc(config-snat-rule)# enable
wlc(config-snat-rule)# exit
wlc(config-snat-ruleset)# exit
wlc(config-snat)# exit
```

Создайте VLAN для uplink:

```
wlc(config)# vlan 2
wlc(config-vlan)# exit
```

Создайте пользовательский VLAN:

```
wlc(config)# vlan 3
wlc(config-vlan)# force-up
wlc(config-vlan)# exit
```

Создайте интерфейсы для взаимодействия с подсетями управления точками доступа, пользователей Wi-Fi и Интернет:

```
#Конфигурируем параметры интерфейса для точек доступа:
wlc(config)# bridge 1
wlc(config-bridge)# vlan 1
wlc(config-bridge)# security-zone trusted
wlc(config-bridge)# ip address 192.168.1.1/24
wlc(config-bridge)# enable
wlc(config-bridge)# exit

#Конфигурируем параметры публичного интерфейса:
wlc(config)# bridge 2
wlc(config-bridge)# vlan 2
wlc(config-bridge)# security-zone untrusted
wlc(config-bridge)# ip address dhcp
wlc(config-bridge)# enable
wlc(config-bridge)# exit

#Конфигурируем параметры интерфейса для пользователей Wi-Fi:
wlc(config)# bridge 3
wlc(config-bridge)# security-zone users
wlc(config-bridge)# ip address 192.168.2.1/24
wlc(config-bridge)# vlan 3
wlc(config-bridge)# enable
wlc(config-bridge)# exit
```

Настройте порты:

```
#Конфигурируем интерфейсы для uplink:
wlc(config)# interface gigabitethernet 1/0/1
wlc(config-if-gi)# mode switchport
wlc(config-if-gi)# switchport access vlan 2
wlc(config-if-gi)# exit
wlc(config)# interface tengigabitethernet 1/0/1
wlc(config-if-te)# mode switchport
wlc(config-if-te)# switchport access vlan 2
wlc(config-if-te)# exit


#Конфигурируем интерфейсы для подключения точек доступа:
wlc(config)# interface gigabitethernet 1/0/2
wlc(config-if-gi)# mode switchport
wlc(config-if-gi)# exit
wlc(config)# interface gigabitethernet 1/0/3
wlc(config-if-gi)# mode switchport
wlc(config-if-gi)# exit
wlc(config)# interface gigabitethernet 1/0/4
wlc(config-if-gi)# mode switchport
wlc(config-if-gi)# exit
wlc(config)# interface tengigabitethernet 1/0/2
wlc(config-if-te)#  mode switchport
wlc(config-if-te)# exit
```

Включите разрешение DNS-имен:

```
wlc(config)# domain lookup enable
```

Настройте профиль для поднятия туннелей:

```
wlc(config)# tunnel softgre 1
wlc(config-softgre)# mode data
wlc(config-softgre)# local address 192.168.1.1
wlc(config-softgre)# default-profile
wlc(config-softgre)# enable
wlc(config)# exit
```

Настройка DHCP-сервера

> ⚠ **Необходимо обязательно указывать NTP-сервер, т.к. корректное время позволяет пройти проверку валидности сертификатов.**

Настройте адресное пространство для устройств, которые будут подключены к контроллеру:

```
wlc(config)# ip dhcp-server pool ap-pool

#Определяем подсеть:
wlc(config-dhcp-server)# network 192.168.1.0/24

#Задаем диапазон выдаваемых IP-адресов:
wlc(config-dhcp-server)# address-range 192.168.1.2-192.168.1.254

#Шлюз по умолчанию. Им является адрес бриджа управления ТД:
wlc(config-dhcp-server)# default-router 192.168.1.1

#Выдаем адрес DNS-сервера:
wlc(config-dhcp-server)# dns-server 192.168.1.1

#Необходимо обязательно указывать NTP-сервер, т.к. корректное время позволяет пройти проверку
валидности сертификатов.

#Выдаем 42 опцию DHCP, содержащую адрес NTP-сервера, для синхронизации времени на точках
доступа:
wlc(config-dhcp-server)# option 42 ip-address 192.168.1.1

#Выдаем 43 vendor specific опцию DHCP, которая содержит:

- 12 подопцию, необходимую для построения SoftGRE data туннелей. Опция содержит IP-адрес
 softgre-интерфейса контроллера.
wlc(config-dhcp-server)# vendor-specific
wlc(config-dhcp-server-vendor-specific)# suboption 12 ascii-text "192.168.1.1"

- 15 подопцию, необходимую для того, чтобы точка доступа автоматически пришла на контроллер и
включилась в работу под его управлением. Опция содержит HTTPS URL контроллера.
wlc(config-dhcp-server-vendor-specific)# suboption 15 ascii-text "https://192.168.1.1:8043"
wlc(config-dhcp-server-vendor-specific)# exit
wlc(config-dhcp-server)# exit
```

Настройте адресное пространство для пользователей:

```
wlc(config)# ip dhcp-server pool users-pool

#Определяем подсеть:
wlc(config-dhcp-server)# network 192.168.2.0/24

#Задаем диапазон выдаваемых пользователям Wi-Fi IP-адресов:
wlc(config-dhcp-server)# address-range 192.168.2.2-192.168.2.254

#Шлюз по умолчанию:
wlc(config-dhcp-server)# default-router 192.168.2.1

#Выдаем адрес DNS-сервера:
wlc(config-dhcp-server)# dns-server 192.168.2.1
wlc(config-dhcp-server)# exit
```

Настройка RADIUS-сервера

Настройте локальный RADIUS-сервер.

```
wlc(config)# radius-server local

#Настраиваем NAS ap. Содержит подсети точек доступа, которые будут обслуживаться локальным
 RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:
wlc(config-radius)# nas ap
wlc(config-radius-nas)# key ascii-text password
wlc(config-radius-nas)# network 192.168.1.0/24
wlc(config-radius-nas)# exit

#Настраиваем NAS local. Используется при обращении WLC к локальному RADIUS-серверу при
построении SoftGRE-туннелей:
wlc(config-radius)# nas local
wlc(config-radius-nas)# key ascii-text password
wlc(config-radius-nas)# network 127.0.0.1/32
wlc(config-radius-nas)# exit

#Создаем домен для пользователей:
wlc(config-radius)# domain default

#Создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:
wlc(config-radius-domain)# user name1
wlc(config-radius-user)# password ascii-text password1
wlc(config-radius-user)# exit
wlc(config-radius-domain)# exit

#Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга,
настройки проксирования на внешний RADIUS server. Использование стандартных портов (1812 для
аутентификации и 1813 для аккаунтинга) не требует настройки. В таком случае достаточно просто
включения виртуального сервера (enable).
wlc(config-radius)# virtual-server default
wlc(config-radius-vserver)# enable
wlc(config-radius-vserver)# exit
wlc(config-radius)# enable
wlc(config)# exit
```

В заводской конфигурации учетная запись пользователя не настроена в целях безопасности, поэтому для подключения к Enterprise SSID в заводской конфигурации необходимо создать учетную запись.

Определите параметры для взаимодействия с RADIUS-сервером: IP-адрес и ключ. Так как RADIUS-сервер находится локально на контроллере, в качестве адреса хоста задайте 127.0.0.1. Ключ должен совпадать с ключом, указанным для nas local.

```
wlc(config)# radius-server host 127.0.0.1
wlc(config-radius-server)# key ascii-text password
wlc(config-radius-server)# exit
```

Добавьте профиль AAA, укажите адрес сервера, который будет использоваться:

```
wlc(config)# aaa radius-profile default_radius
wlc(config-aaa-radius-profile)# radius-server host 127.0.0.1
wlc(config-aaa-radius-profile)# exit
```

Настройте и включите функционал автоматического поднятия SoftGRE-туннелей:

```
wlc(config)# softgre-controller

#Так как RADIUS-сервер находится локально на контроллере,указываем nas-ip-address 127.0.0.1:
wlc(config-softgre-controller)# nas-ip-address 127.0.0.1

#Выбираем режим создания data SoftGRE туннелей – WLC:
wlc(config-softgre-controller)# data-tunnel configuration wlc

#Выбираем созданный ранее AAA-профиль:
wlc(config-softgre-controller)# aaa radius-profile default_radius
wlc(config-softgre-controller)# keepalive-disable

#Разрешаем трафик в пользовательском vlan:
wlc(config-softgre-controller)# service-vlan add 3
wlc(config-softgre-controller)# enable
wlc(config-softgre-controller)# exit
```

Настройка модуля управления точками доступа WLC

Перейдите к настройкам модуля управления конфигурацией точек доступа:

```
wlc(config)# wlc
wlc(config-wlc)#
```

Настройте профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi. Если предполагается аутентификация клиентов на внешнем RADIUS-сервере, то здесь указывается его адрес и ключ. При такой настройке точка доступа будет проводить аутентификацию клиентов без участия WLC.

```
wlc(config-wlc)# radius-profile default-radius

#Так как RADIUS-сервер находится локально на контроллере, указываем адрес контроллера в подсети
точек доступа:
wlc(config-wlc-radius-profile)# auth-address 192.168.1.1

#Ключ RADIUS-сервера должен совпадать с ключом, указанным для NAS ap:
wlc(config-wlc-radius-profile)# auth-password ascii-text password

#Указываем домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные
записи пользователей Enterprise.
wlc(config-wlc-radius-profile)# domain default
wlc(config-wlc-radius-profile)# exit
```

Настройка SSID
Профиль SSID содержит настройки SSID точки доступа. Для примера приведена настройка Enterprise SSID:

```
wlc(config-wlc)# ssid-profile default-ssid

#Description может содержать краткое описание профиля:
wlc(config-wlc-ssid-profile)# description default-ssid

#SSID – название беспроводной сети, которое будут видеть пользователи при сканировании эфира:
wlc(config-wlc-ssid-profile)# ssid default-ssid

#VLAN ID – номер VLAN для передачи пользовательского трафика. При передаче трафика Wi-Fi
клиентам метка будет сниматься точкой доступа. При прохождении трафика в обратную сторону на
нетегированный трафик от клиентов метка будет навешиваться:
wlc(config-wlc-ssid-profile)# vlan-id 3

#Security mode – режим безопасности доступа к беспроводной сети. Для Enterprise авторизации
выберите режим WPA2_1X:
wlc(config-wlc-ssid-profile)# security-mode WPA2_1X

#Указываем профиль настроек RADIUS-сервера, который будет использоваться для авторизации
пользователей Wi-Fi:
wlc(config-wlc-ssid-profile)# radius-profile default-radius

#Далее необходимо указать хотя бы один диапазон, в котором будет работать SSID: 2.4/5 ГГц:
wlc(config-wlc-ssid-profile)# band 2g
wlc(config-wlc-ssid-profile)# band 5g

#Активируем профиль SSID. В случае необходимости отключения SSID на всех локациях, SSID-профиль
можно выключить командой 'no enable':
wlc(config-wlc-ssid-profile)# enable
wlc(config-wlc-ssid-profile)# exit
```

Настройка профилей конфигурации
Создайте профиль общих настроек точек доступа:

```
wlc(config-wlc)# ap-profile default-ap

#Задаем пароль для подключения к точке доступа:
wlc(config-wlc-ap-profile)# password ascii-text password

#Если необходимо, можно активировать доступ к точкам доступа по ssh/telnet и web-интерфейс:
wlc(config-wlc-ap-profile)# services
wlc(config-wlc-ap-profile-services)# ip ssh server
wlc(config-wlc-ap-profile-services)# ip telnet server
wlc(config-wlc-ap-profile-services)# ip http server
wlc(config-wlc-ap-profile)# exit
```

Создайте профили конфигурации точек доступа:

Для каждой точки доступа можно переопределить параметры отдельно через индивидуальный профиль. Подробную информацию о точках доступа можно найти в официальной документации по ссылке.

Создайте профиль конфигурирования радиоинтерфейса, работающего в частотном диапазоне 2,4 ГГц:

```
wlc(config-wlc)# radio-2g-profile default_2g

#Задаем список каналов, из которых точка доступа будет автоматически выбирать наименее
загруженный радиоканал:
wlc(config-wlc-radio-2g-profile)# limit-channels 1,6,11

#Выбираем IEEE 802.11 режим работы радиоинтерфейса:
wlc(config-wlc-radio-2g-profile)# work-mode bgnax

#Задаем ширину радиоканала:
wlc(config-wlc-radio-2g-profile)# bandwidth 20

#Выставляем мощность сигнала передатчика в дБм:
wlc(config-wlc-radio-2g-profile)# tx-power maximal
wlc(config-wlc-radio-2g-profile)# exit
```

Создайте профиль конфигурирования радиоинтерфейса, работающего в частотном диапазоне 5 ГГц:

```
wlc(config-wlc)# radio-5g-profile default_5g

#Переводим режим динамического выбора частоты в принудительный режим:
wlc(config-wlc-radio-5g-profile)# dfs forced

#Задаем список каналов, из которых точка доступа будет автоматически выбирать наименее
загруженный радиоканал:
wlc(config-wlc-radio-5g-profile)# limit-channels 36,40,44,48,52,56,60,64

#Выбираем IEEE 802.11 режим работы радиоинтерфейса:
wlc(config-wlc-radio-5g-profile)# work-mode anacax

#Задаем ширину радиоканала:
wlc(config-wlc-radio-5g-profile)# bandwidth 20

#Выставляем мощность сигнала передатчика в дБм:
wlc(config-wlc-radio-5g-profile)# tx-power maximal
wlc(config-wlc-radio-5g-profile)# exit
```

Настройка локации

Под локацией понимается группа точек доступа, предназначенная для предоставления сервиса внутри топографического и/или логического сегмента сети, которые в общем случае будут конфигурироваться по одним и тем же правилам (профилям). Локация для точки (ap-location) определяется при подключении точки к контроллеру в зависимости от адресного пространства. Исключение составляет переопределение (override) радио-параметров и/или ap-location в индивидуально созданном шаблоне для точки доступа по ее MAC-адресу.

Создайте локацию и определите правила конфигурирования точек доступа, входящих в данную локацию:

```
wlc(config-wlc)# ap-location default-location

#Description может содержать краткое описание локации:
wlc(config-wlc-ap-location)# description default-location

#Указываем профили конфигурирования радиоинтерфейсов:
wlc(config-wlc-ap-location)# radio-2g-profile default_2g
wlc(config-wlc-ap-location)# radio-5g-profile default_5g

#Указываем профиль общих настроек точек доступа:
wlc(config-wlc-ap-location)# ap-profile default-ap

#Указываем профили беспроводных сетей, которые будут предоставлять услуги в данной локации:
wlc(config-wlc-ap-location)# ssid-profile default-ssid default

#Так как схема предполагает передачу пользовательского трафика через SoftGRE-туннели, то
необходимо указать, что локация работает в режиме туннелирования:
wlc(config-wlc-ap-location)# mode tunnel
wlc(config-wlc-ap-location)# exit
```

Определение подсетей обслуживаемых точек доступа
Определите адресное пространство подключаемых точек доступа:

```
wlc(config-wlc)# ip-pool default-ip-pool

#Description может содержать краткое описание пула адресов:
wlc(config-wlc-ip-pool)# description default-ip-pool

#Подсеть IP-адресов точек доступа указывается в параметре network. Если данный параметр не
определен, то все точки доступа будут попадать под данное правило.

#Указываем ap-location, которая будет присваиваться точкам доступа данного пула адресов:
wlc(config-wlc-ip-pool)# ap-location default-location
wlc(config-wlc-ip-pool)# exit
```

Точки доступа, подсети которых не определены в ip-pool, не будут обслуживаться контроллером.

Авторегистрация точек доступа
Активируйте авторегистрацию точек доступа на контроллере:

```
wlc(config-wlc)# service-activator
wlc(config-wlc-service-activator)# aps join auto
```

При подключении новых точек доступа не потребуется дополнительных действий, точки доступа будут зарегистроированы в автоматическом режиме.

Включение функционала WLC
Активируйте работу WLC, укажите IP-адрес контроллера для точек доступа и сохраните настройки:

```
wlc(config-wlc)# enable
wlc(config-wlc)# outside-address 192.168.1.1
wlc(config-wlc)# end
wlc# commit
wlc# confirm
```

Web-интерфейс для мониторинга

Для мониторинга точек доступа доступен web-интерфейс, который можно включить командой:

```
wlc(config)# ip http server
wlc(config)# end
wlc# commit
wlc# confirm
```

Web-интерфейс будет доступен по URL: http://<IP-address_wlc>, в конфигурации по умолчанию логин/пароль: admin/password.

Обновление точек доступа

В конфигурации по умолчанию при подключении точка доступа сразу автоматически обновится на прошивку, которая загружена на WLC. Если точка доступа уже находится под управлением WLC, то обновление произойдет при работе менеджера обновления ПО или при переподключение ТД к WLC. Переподключение можно выполнить через команду *clear wlc ap <mac>*.

Для загрузки прошивки используйте команду:

```
#IP-адрес TFTP-сервера – 192.168.1.2, WEP-1L-1.2.5_build_16.tar.gz – название файла ПО.
wlc# copy tftp://192.168.1.2:/WEP-1L-1.2.5_build_16.tar.gz system:access-points-firmwares
```

Если на WLC загружено несколько файлов ПО, то точка доступа будет обновляться на самую последнюю версию.

10.1.2 Настройка AirTune

Одним из приоритетных направлений по развитию точек доступа в области Enterprise&High-Density Wi-Fi является реализация сервиса AirTune, основной функцией которого является Radio Resource Management (RRM).

Radio Resource Management позволяет автоматически оптимизировать характеристики точек доступа в зависимости от текущих условий. **Сервис AirTune не заменяет собой процедуры радиопланирования**, но позволяет провести финальный этап оптимизации сети, а также вести постоянный контроль.

Используемые технологии и алгоритмы:

- Dynamic Channel Assignment (DCA) – алгоритм автоматического распределения частотных каналов каждой точки доступа в сети для избежания интерференции между ними;
- Transmit Power Control (TPC) – алгоритм управления мощностью передатчиков с целью обеспечения оптимальной зоны покрытия сети и минимизации «конфликтных» областей, где клиент находится в зоне уверенного приема нескольких соседних точек доступа;
- Load Balancing – алгоритм автоматического распределения клиентских устройств между точками. В случае перегрузки сервис определит более оптимальную ТД для подключения клиента и выдаст

рекомендации на точки доступа, клиент будет видеть в эфире только 1 ТД, рекомендованную для авторизации;
- Roaming – поддержка стандартов бесшовного роуминга 802.11 k/r.

Основными задачами функционала являются:

- Автоматическая настройка рабочих каналов между точками доступа;
- Автоматическая подстройка излучаемой мощности для стабильности зоны покрытия («соты»);
- Оптимизация пропускной способности беспроводной сети;
- Минимизация «конфликтных» областей между точками доступа;
- Равномерное распределение нагрузки между точками доступа;
- Поиск оптимальной точки доступа для клиента находящегося в «неуверенной» зоне приема;
- Минимизация «случайных» переподключений клиентов на границах «сот»;
- Поддержка бесшовного роуминга клиентов между точками доступа.

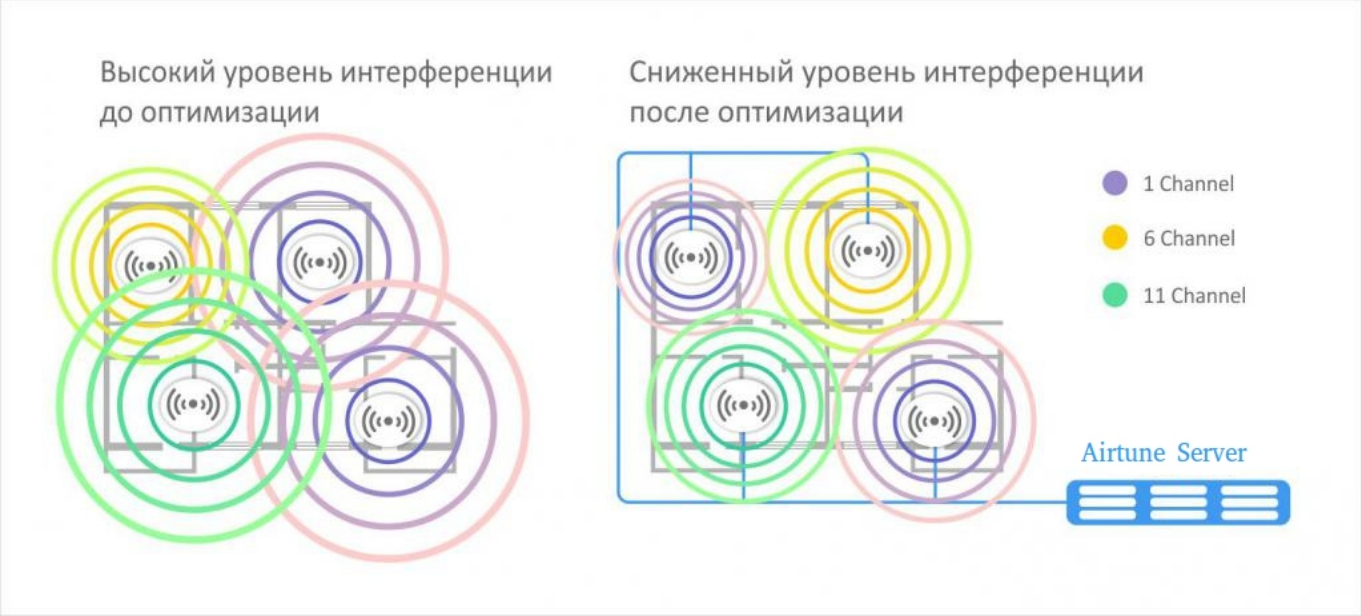
При работе функционала TPC/DCA точки доступа по команде от сервиса с помощью специальных пакетов (Action Frame) собирают информацию о радиосреде в текущий момент времени. Затем передают информацию на сервис, который выполняет анализ «качества радиоэфира» и проводит оптимизацию параметров для каждой точки доступа, что обеспечивает равномерность зоны покрытия и минимизацию интерференции.

Также сервис включает в себя функционал роуминга:

- Синхронизация списков соседних точек доступа стандарта 802.11k, который позволяет клиенту при ослабевании сигнала с текущей точки доступа искать более подходящую точку доступа из рекомендуемого списка, а не анализируя весь эфир.
- Согласование ключей между точками доступа для роуминга стандарта 802.11r, который позволяет значительно ускорять процесс переключения клиента между точками доступа, т.к. клиенту не нужно будет проходить повторную полную авторизацию на встречной точке доступа, только ускоренную.

ⓘ **Для работы роуминга стандартов 802.11k/r необходима поддержка стандарта со стороны клиентов.**

Простой пример работы оптимизации сети с помощью сервиса представлен на картинке (функционал DCA+TPC):



Алгоритм работы

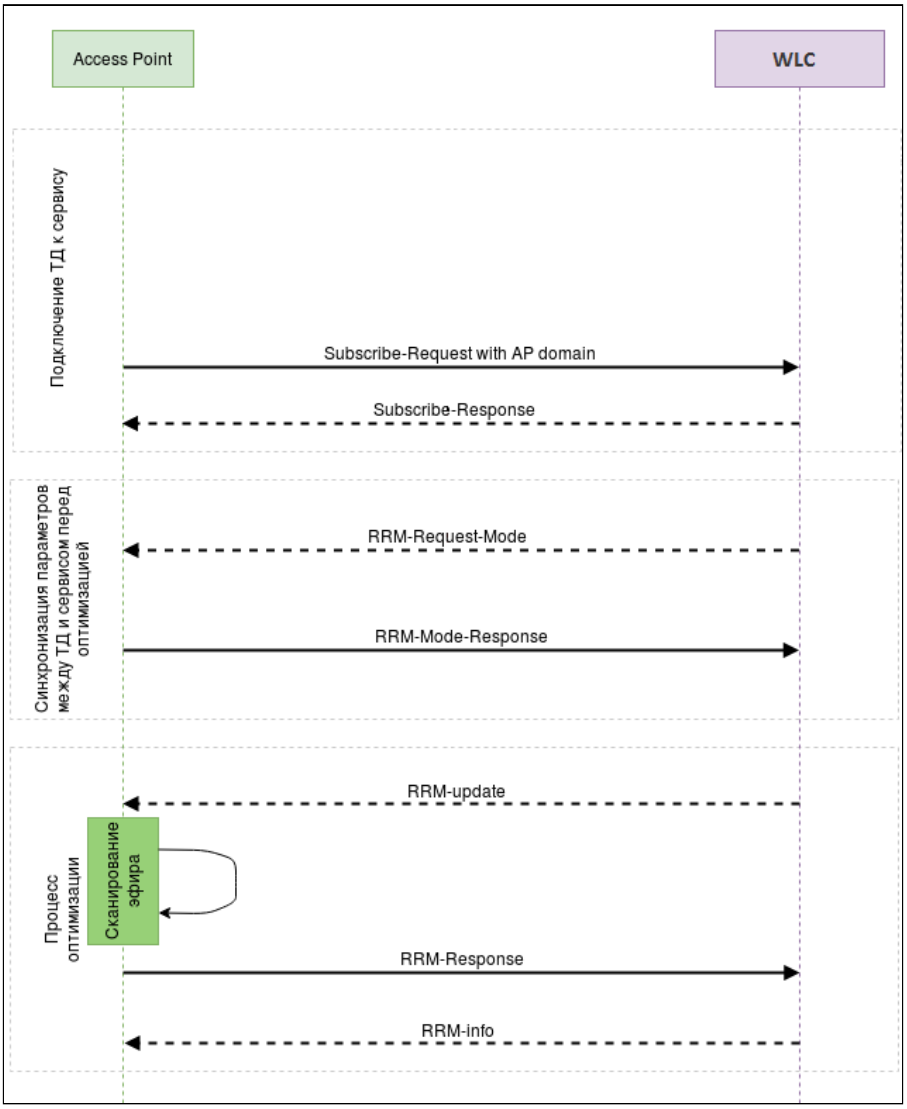
ТД при подключении к серверу (соединение между ТД и сервером осуществляется по протоколу WebSocket) отправляет сообщение "subscribe-request", где передает свои параметры, такие как:

- заводские установочные параметры (серийный номер, тип устройство, MAC-адрес);
- имя локации (географический домен);
- радио настройки (канал, мощность);
- список SSID;
- список подключенных клиентов.

После того как ТД построила сессию с сервисом, на AirTune точки группируются по доменам. Если на сервисе нет домена, которому принадлежит точка, AirTune отправляет отказ в обслуживании.

Если на AirTune домен настроен, то сервер отправляет "subscribe-response" с указанием какие функции (DCA, TPC, Load Balance) настроены для этого домена.

Оптимизация (DCA, TPC) проходит внутри домена по следующему сценарию:



1) На первом этапе происходит авторизация ТД на сервисе AirTune, для этого система управления посредством SNMP-set запроса конфигурирует на точках доступа URL сервиса AirTune;

2) ТД поднимают сессию с сервисом, обменявшись пакетами Subscribe-Request/Subscribe-Response, в которых ТД информирует сервис о текущей конфигурации. В случае если на сервисе не существует географический домен, переданный в сообщении от точки, сервис будет игнорировать запросы. Если домен найден, подключение происходит успешно;

3) Далее сервер отправляет на точки запрос "rrm-request-mode", чтобы актуализировать текущую информацию о них, т.к. оптимизация может начаться не только после подключения точки, а планово либо по команде администратора спустя долгое время после первичного подключения;

4) Точки доступа отвечают "rrm-response-mode", в котором передают свои текущие радио параметры;

5) Сервер отправляет запрос на сканирование окружения "rrm-update". В зависимости от опции eltex-rrm-scan сканирование может быть "обычным" (точка перебирает доступные каналы и детектирует все видимые точки) либо специальным, когда только точки из домена передают специальные action-пакеты в один, заранее определенный, момент времени;

6) Точки отправляют результат сканирования на сервер сообщением "rrm-response";

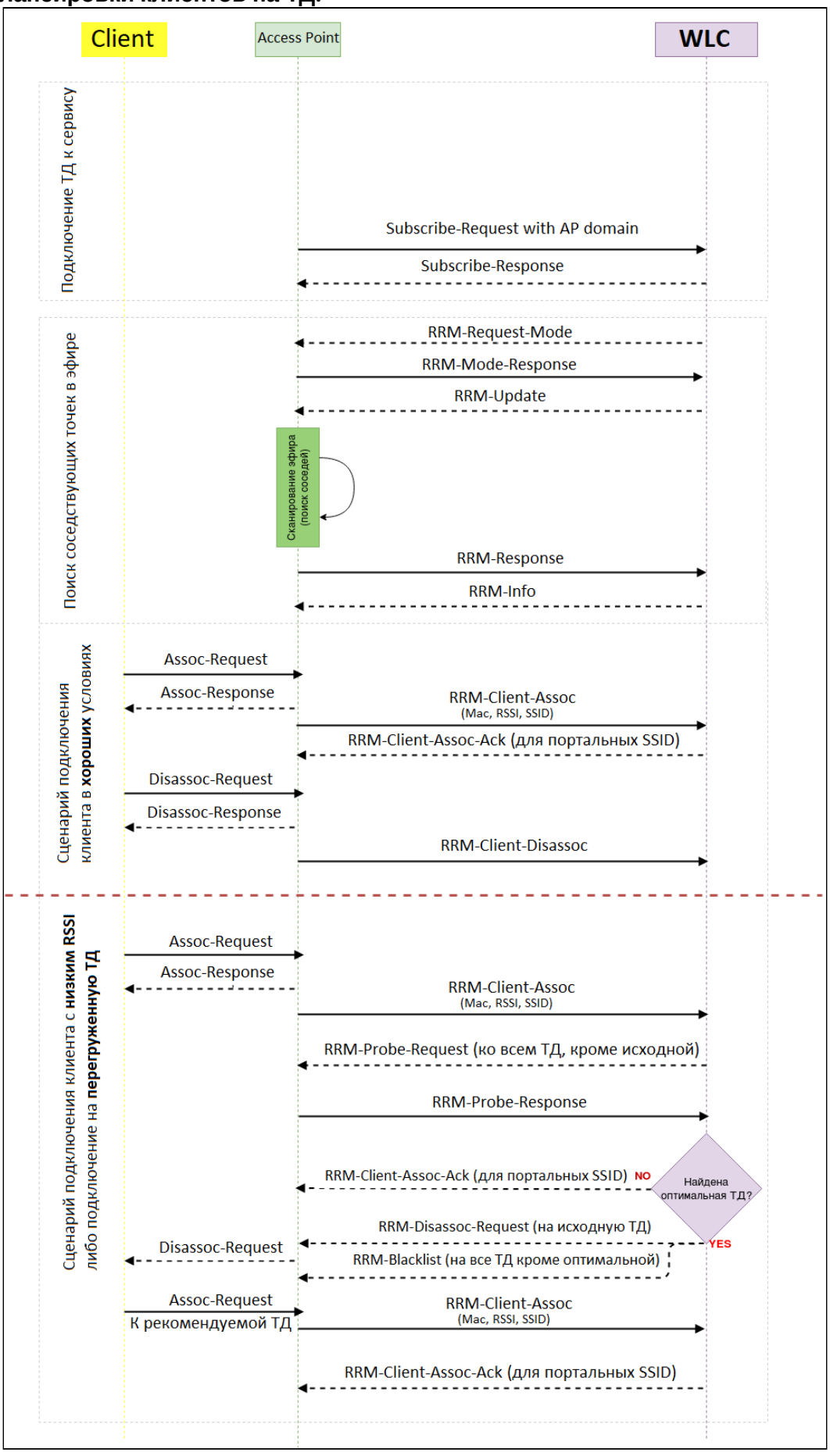
7) Получив результаты от всех ТД в домене, сервер в зависимости от настроек определяет для каждой точки оптимальную мощность, оптимальный канал, список соседей и отправляет сообщение "rrm-info";

8) После этого ТД применяют рекомендованные настройки, и оптимизация считается завершенной.

Оптимизация происходит в следующих случаях:
- новая точка добавилась в домен;
- одна из ТД была отключена;
- на одной из точек были изменены радио параметры;
- по таймеру (Optimization interval);
- по нажатию администратором соответствующей кнопки.

Оптимизация не происходит в случае:
- перезапуска ТД;
- короткого пропадания связи между ТД и сервисом;
- обновления ТД.

Сценарий балансировки клиентов на ТД:



1) В случае если алгоритмы TPC/DCA включены вместе с балансировщиком либо отключена опция "Use all AP for Balance", то первым этапом происходит поиск соседствующих точек в эфире;

> В случае если стоит флаг "Use all AP for Balance" в конфигурации AirTune, то пункт "Поиск соседствующих точек в эфире" будет пропущен, рассылка будет осуществляться всем ТД, находящимся в одном домене.

2) Далее начинаются сценарии работы балансировщика. При подключении нового клиента с ТД на сервер отправляется сообщение "rrm-client-assoc", в котором содержится MAC-адрес клиента SSID, к которому клиент подключился. В случае если подключенный клиент находится в зоне уверенного приема и ТД не является загруженной, сервисом никаких действий не предпринимается, отправляется только сообщение "RRM-Client-Assoc-Ack" для портальных клиентов, после него ТД разблокирует клиентов для доступа в интернет (если пользователь уже авторизовался на портале);

3) Если при подключении клиента данная точка является загруженной (превышен лимит клиентов) или клиент имеет сигнал ниже установленного уровня, сервер инициирует процесс балансировки этого клиента;

4) Сервис отправляет "соседним" ТД, на которых настроен такой же SSID, сообщение "rrm-probe-request", чтобы определить с каким уровнем сигнала ТД "видят" данного клиента;

5) ТД отвечают сообщением "rrm-probe-response", в котором указывают уровень сигнала RSSI;

6) Если сервер не нашел подходящей точки для клиента, он оставляет его на текущей. Если оптимальная точка найдена, отключаем клиента от текущей ТД командой "rrm-disassoc-request", на всех остальных, кроме оптимальной, блокируем клиента командой "rrm-blacklist", таким образом клиент видит в эфире только 1 целевую ТД и произойдет переключение клиента (роуминг).

> Балансировка клиентов между точками доступа происходит в рамках одного интерфейса (2.4 ГГц или 5 ГГц).
> Если клиент подключился в 2.4 ГГц к загруженной ТД, то его балансировка на свободный интерфейс 5 ГГц второй точки доступа происходить не будет, только на аналогичный интерфейс (2.4 ГГц).

> Если клиентское устройство поддерживает функционал рандомизации MAC-адреса в Probe Request, то для таких клиентов функционал работать не будет, т.к. анализ уровня сигнала от клиента на соседних точках доступа основывается на менеджмент-пакетах от клиента (Probe request).

Алгоритм настройки

По умолчанию все необходимые настройки для работы сервиса настроены, нужно только указать IP-адрес контроллера, который виден точкам доступа, включить сервис, создать профиль и привязать его к локации.

Настройки производятся в режиме конфигурирования (config) раздела настройки контроллера WLC (config-wlc).

Шаг	Описание	Команда	Ключи
1	Перейти в раздел конфигурирования WLC.	**wlc# configure** **wlc(config)# wlc** **wlc(config-wlc)#**	
2	Создать профиль AirTune.	**wlc(config-wlc)# airtune-profile <NAME>** **wlc(config-airtune-profile)#exit** **wlc(config-wlc)#**	<NAME> – название профиля, задается строкой до 235 символов.
3	Перейти в локацию, для которой требуется автоматическая оптимизация настроек точек доступа.	**wlc(config-wlc)# ap-location <NAME>** **wlc(config-wlc-ap-location)#**	<NAME> – название профиля локации, задается строкой до 235 символов.
4	Привязать созданный профиль к локации.	**wlc(config-wlc-ap-location)# airtune-profile <NAME>** **wlc(config-wlc-ap-location)#exit** **wlc(config-wlc)#**	<NAME> – название профиля локации, задается строкой до 235 символов.
5	Перейти в раздел общих настроек сервиса.	**wlc(config-wlc)# airtune** **wlc(config-airtune)#**	
6	Активировать работу сервиса.	**wlc(config-airtune)# enable** **wlc(config-airtune)#end**	

Пример настройки

```
#Создаем профиль airtune, по умолчанию в нем уже указаны оптимальные настройки сервиса, поэтому достаточно просто создать сам профиль:
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# airtune-profile default_airtune
wlc(config-airtune-profile)#exit

#Добавляем профиль в локацию, чтобы разрешить оптимизацию в выбранной локации:
wlc(config-wlc)#
wlc(config-wlc)# ap-location default-location
wlc(config-wlc-ap-location)# airtune-profile default_airtune
wlc(config-wlc-ap-location)#exit

#Глобально активируем функционал airtune в контроллере (оптимизация будет проходить только в локациях с профилем airtune):
wlc(config-wlc)# airtune
wlc(config-airtune)# enable
wlc(config-wlc)# end

wlc# commit
wlc# confirm
```

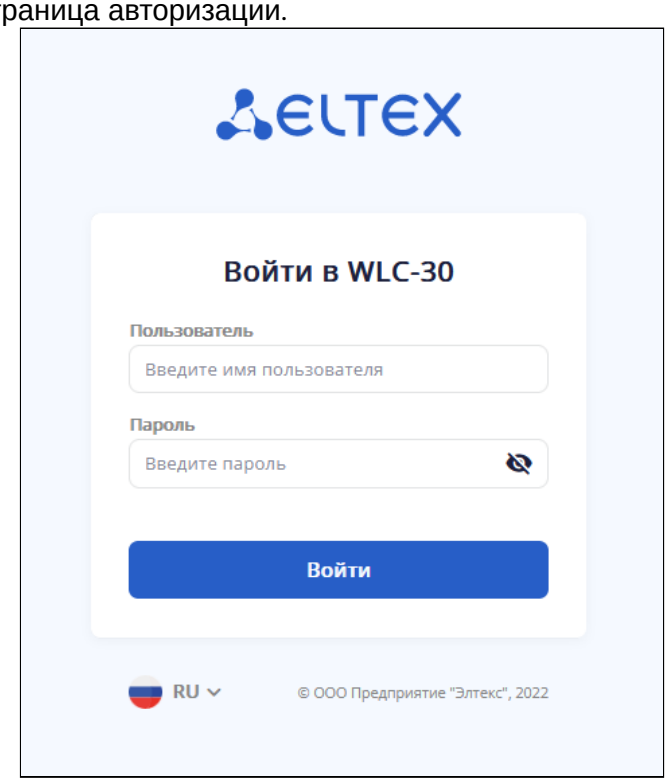
10.2 Управление через WEB-интерфейс

10.2.1 Начало работы

Начало работы на устройствах WLC

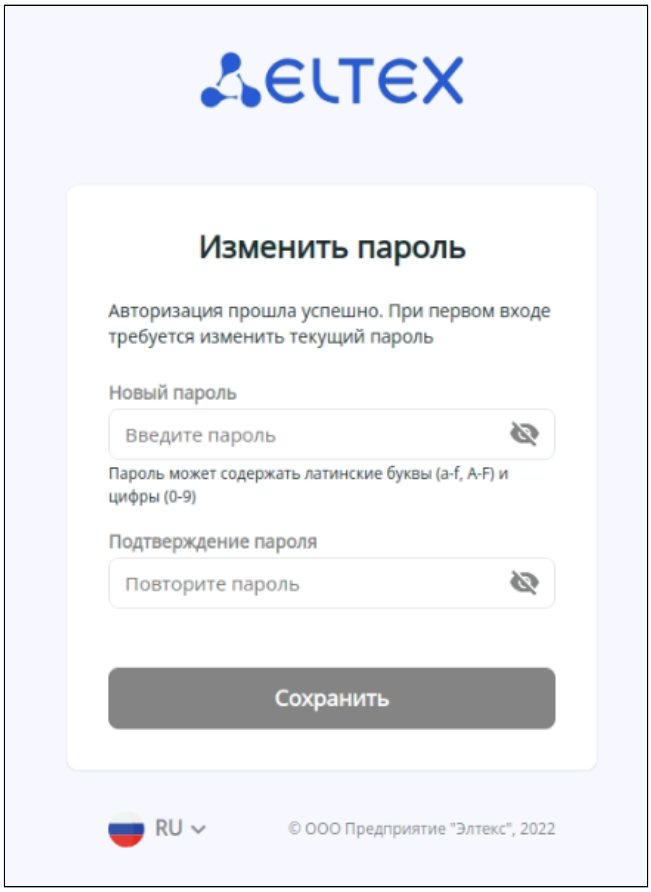
Web-интерфейс включен в заводской конфигурации на устройствах WLC и доступен по проколу HTTPS.

1. Откройте web-браузер, например Firefox, Opera, Chrome.
2. Введите в адресной строке браузера IP-адрес устройства. Для перехода в web-интерфейс можно использовать URL https://<ip-address_wlc>. При успешном обнаружении контроллера в окне браузера отобразится страница авторизации.

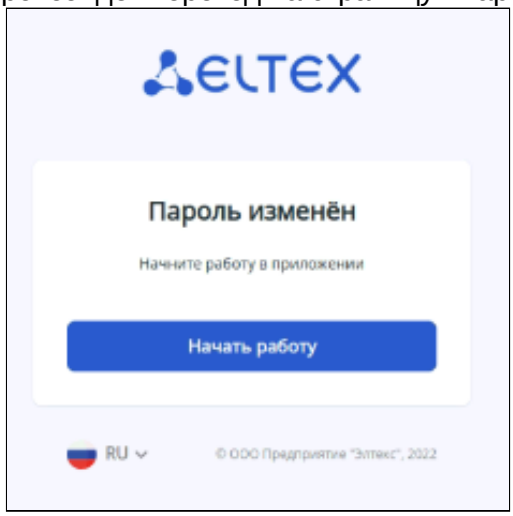


3. Введите имя пользователя и пароль в соответствующие поля.

> Заводские установки: пользователь — *admin*, пароль — *password*
> При первом входе требуется сменить пароль. Новый пароль должен отличаться от заводского.



4. При успешной смене пароля, произойдет переход на страницу «Пароль изменён».



5. Нажмите кнопку «Начать работу» для перехода в web-интерфейс устройства.

Начало работы на устройствах ESR с лицензией WLC

На устройствах ESR web-интерфейс по умолчанию отключен. Для активации выполните действия, описанные ниже.

1. Активируйте web-интерфейс по протоколу HTTP или HTTPS.

```
wlc# config
wlc(config)# ip http server
wlc(config)# ip https server
wlc(config)# end
wlc# commit
wlc# confirm
```

2. Откройте TCP-порт 80 для HTTP-сервера или 443 для HTTPS в Firewall. Пример ниже представлен для открытия 443 порта.
   Создайте группы web с портом 443.

```
object-group service web
  port-range 443
exit
```

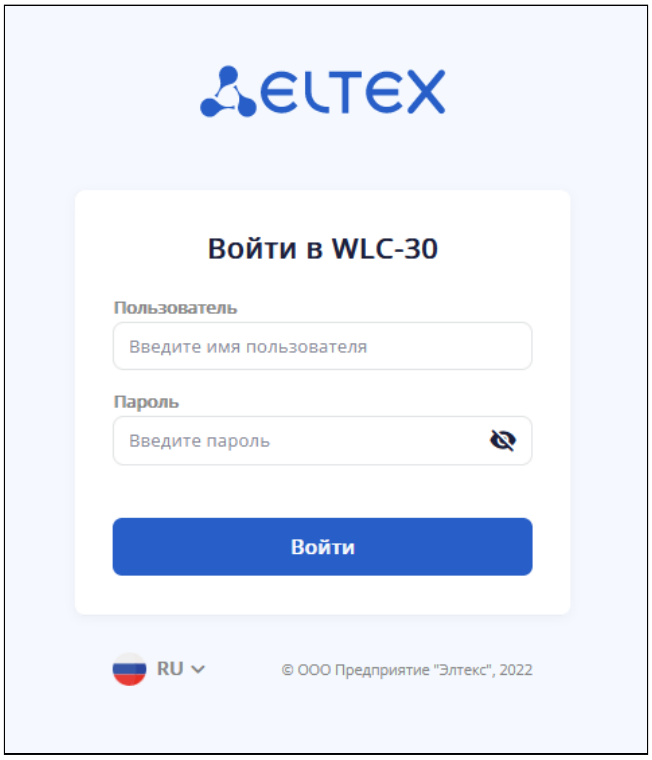
   Добавьте правило в зону trusted self.

```
security zone-pair trusted self
  rule 120
    action permit
    match protocol tcp
    match destination-port object-group web
    enable
  exit
exit
```

   Примените и подтвердите конфигурацию.

```
commit
confirm
```

3. Откройте web-браузер, например Firefox, Opera, Chrome.
4. Введите в адресной строке браузера IP-адрес устройства. Для перехода в web-интерфейс можно использовать URL: http://<ip-address_wlc> или https://<ip-address_wlc>. При успешном обнаружении контроллера в окне браузера отобразится страница авторизации.



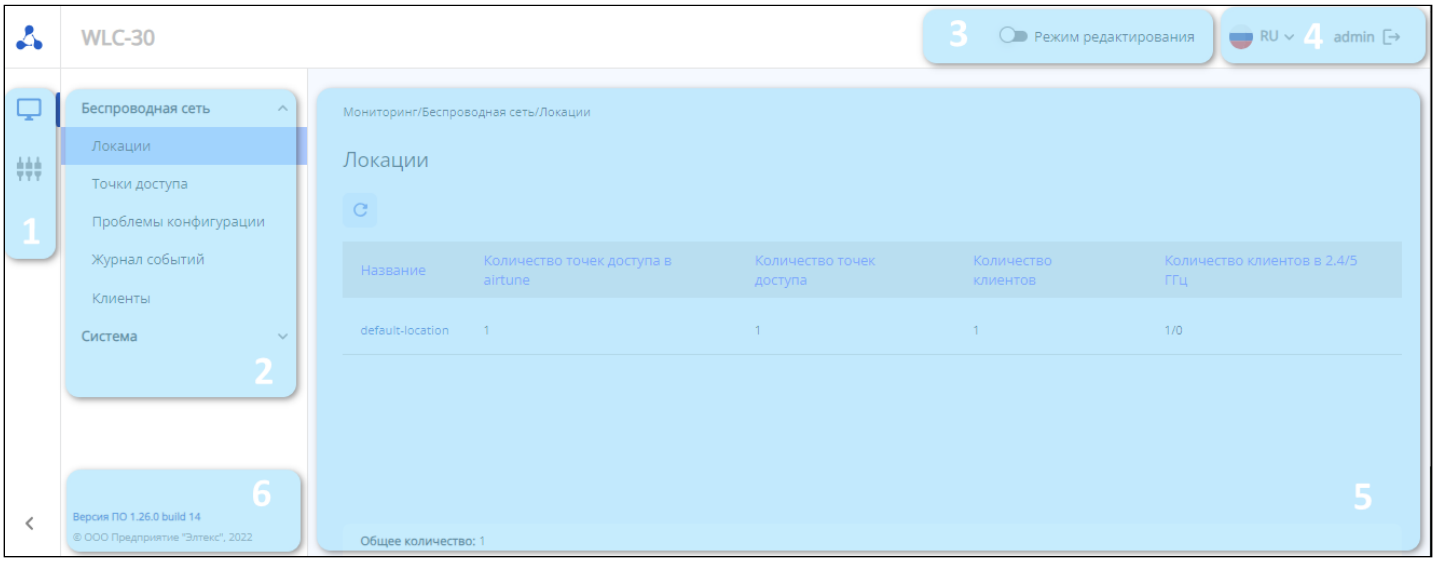
4. Введите имя пользователя и пароль в соответствующие поля.

Заводские установки: пользователь — *admin*, пароль — *password*

5. Нажмите кнопку «Войти». В окне браузера откроется меню «Беспроводная сеть».

10.2.2 Основные элементы web-интерфейса

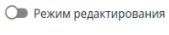
На рисунке ниже представлены элементы навигации web-интерфейса.



Окно пользовательского интерфейса разделено на шесть областей:

1. Кнопки главного меню — для группировки меню по категориям.
2. Вкладки меню и подменю — для управления полем основной информации.
3. Включение режима редактирования.
4. Кнопка выбора языка интерфейса (доступна русская и английская версии web-интерфейса) и кнопка выхода — для завершения сеанса работы в web-интерфейсе под данным пользователем.
5. Поле основной информации — для просмотра данных подменю.
6. Информационное поле — для отображения версии ПО, установленной на контроллере.

Основные элементы интерфейса:

Элемент	Действие
	Добавить новый объект
	Удалить один или несколько объектов
	Выбрать один или несколько объектов
	Контекстное меню для работы с выбранным объектом
	Обновить данные на странице
	Разрегистрировать точки доступа
	Зарегистрировать все точки доступа
	Разорвать сессии Airtune
	Включить режим редактирования конфигурации

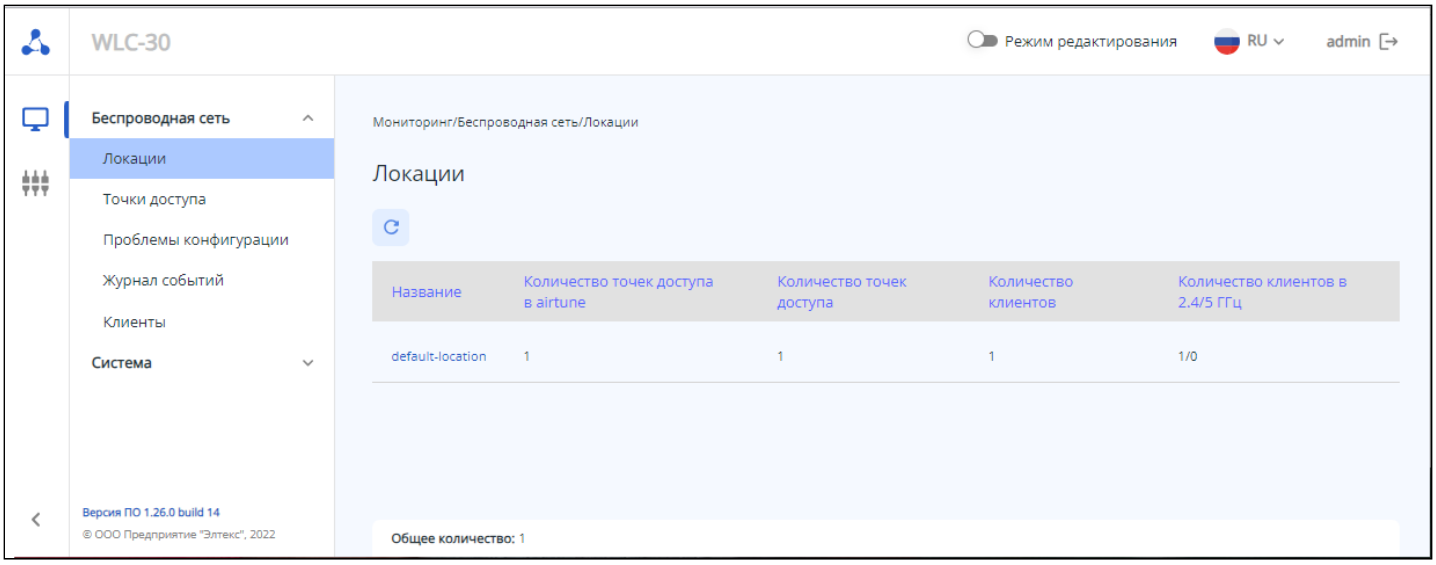
10.2.3 Мониторинг

Меню «Беспроводная сеть»

Подменю «Локации»

В подменю «Локации» отображается список локаций, распределение точек доступа по ним и количество точек доступа, которые управляются сервисом Airtune.

Также в данном подменю отображается информация по клиентам, их количество в каждой локации и распределение по диапазонам.



При переходе в локацию будет доступна таблица клиентов, отчеты оптимизации, сессии точек доступа, которые управляются сервисом Airtune, результат оптимизации и статистика роуминга.

Точки доступа

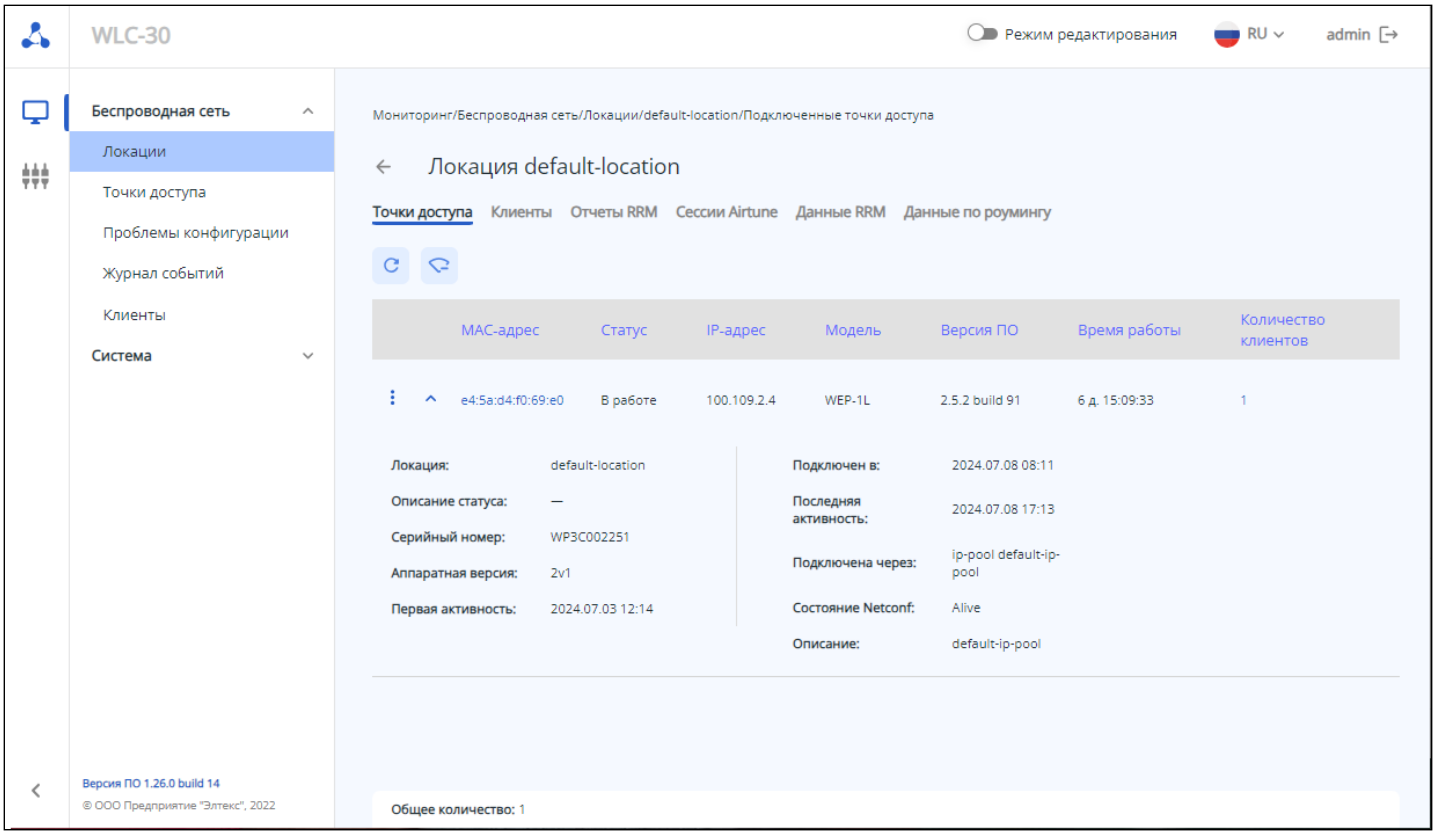
На странице отображены точки доступа, которые зарегистрированы и находятся в выбранной локации.

Параметр «Общее количество» показывает число зарегистрированных точек доступа, находящихся в выбранной локации.

С помощью кнопки «Разрегистрировать все» можно вывести из обслуживания точки доступа выбранной локации. После этого они перейдут в раздел «Точки доступа» → «Новые точки доступа», если авторегистрация выключена. В случае, если авторегистрация включена, то точки доступа в течение 5 минут снова появятся в локации.

Таблица содержит данные:

- *MAC-адрес* − MAC-адрес зарегистрированной точки доступа, при нажатии осуществляется переход на страницу «Точка доступа»;
- *Разрегистрировать* − кнопка расположена в контекстом меню, позволяет вывести из обслуживания выбранную точку доступа и перенести ее в список новых точек доступа;
- *Статус* − состояние работы точки доступа;
- *IP-адрес* − IP-адрес зарегистрированной точки доступа;
- *Модель* − модель зарегистрированной точки доступа;
- *Версия ПО* − версия программного обеспечения зарегистрированной точки доступа;
- *Время работы* − время работы с момента последнего включения или перезагрузки устройства;
- *Количество клиентов* − число клиентов, подключенных к зарегистрированной точке доступа, при нажатии осуществляется переход на страницу «Точка доступа» → «Клиенты».



При нажатии на кнопку будет раскрыта дополнительная информация:

- *Локация* − имя локации, к которой относится точка доступа;
- *Описание статуса* − дополнительная информация по статусу, в случае если на точке доступа обнаружены проблемы;
- *Серийный номер* − серийный номер устройства, установленный заводом-изготовителем;
- *HW-версия* − версия аппаратного обеспечения устройства;
- *Первая активность* − время первой регистрации точки доступа на контроллере;
- *Подключен в* − время последнего подключения точки доступа к контроллеру;
- *Последняя активность* − время, в которое контроллер последний раз настраивал точку доступа;
- *Подключена через* − профиль, с помощью которого точка доступа была настроена;
- *Состояние Netconf* − статус соединения точки доступа и контроллера по протоколу Netconf;
- *Описание* − текстовое описание точки доступа, которое ей было назначено при формировании профиля.

Клиенты

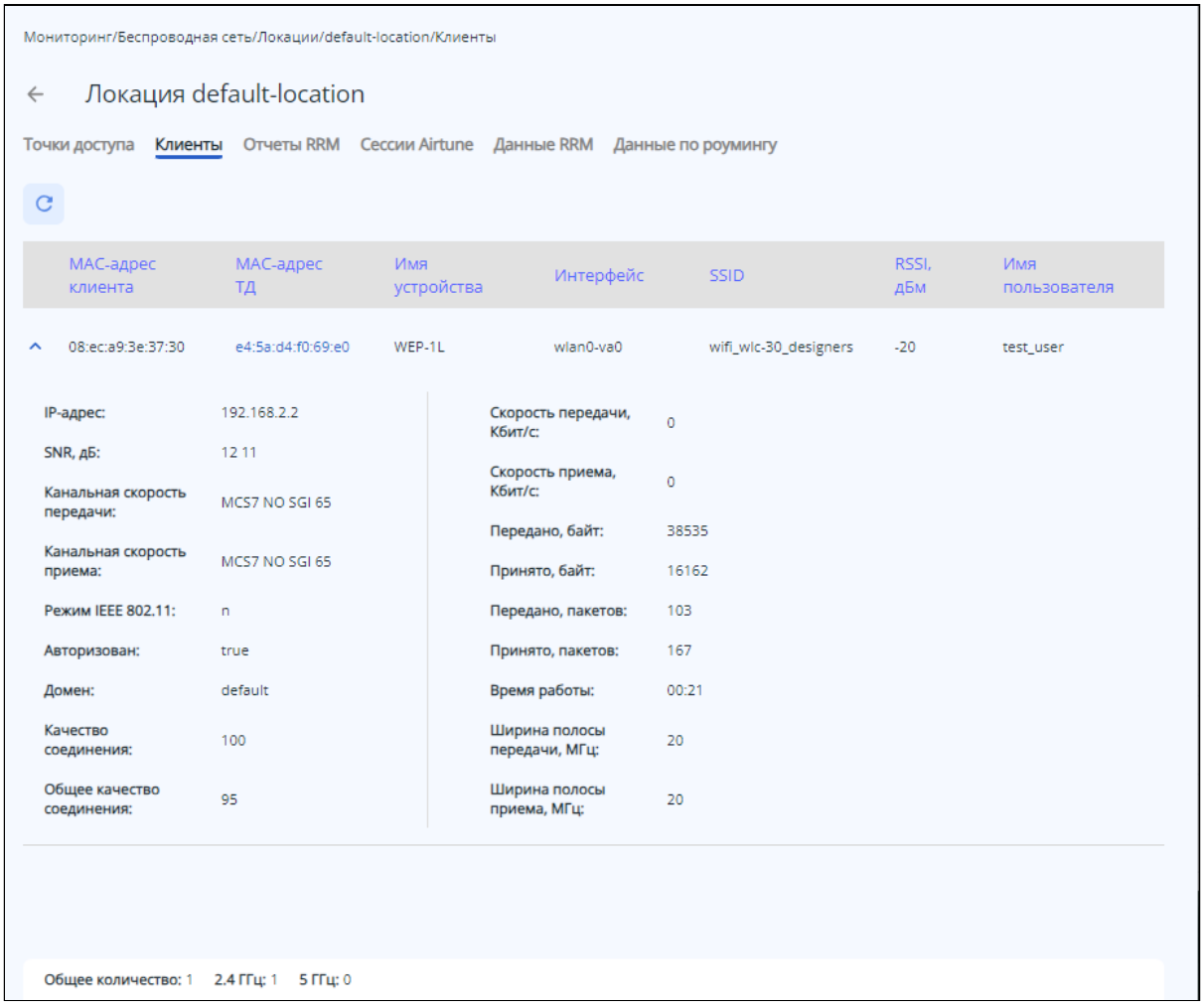
Страница содержит информацию об общем количестве клиентов, а также об их количественном распределении по частотным диапазонам.

Для того чтобы обновить информацию на странице, необходимо нажать на кнопку «Обновить».

Основная информация включает в себя следующие параметры:

- *MAC-адрес клиента* − MAC-адрес подключенного устройства;
- *MAC-адрес ТД* − MAC-адрес точки доступа, к которой подключено устройство;
- *Имя устройства* − имя устройства, по умолчанию задана модель точки доступа. Задать имя можно через конфигурацию;
- *Интерфейс* − интерфейс взаимодействия точки доступа с подключенным устройством;
- *RSSI, дБм* − уровень принимаемого сигнала;
- *SSID* − имя сети, к которой подключено устройство;
- *Имя пользователя* − имя пользователя, указанное при авторизации в сети. В случае personal-авторизации или при подключении к открытой сети, имя пользователя останется пустым.

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



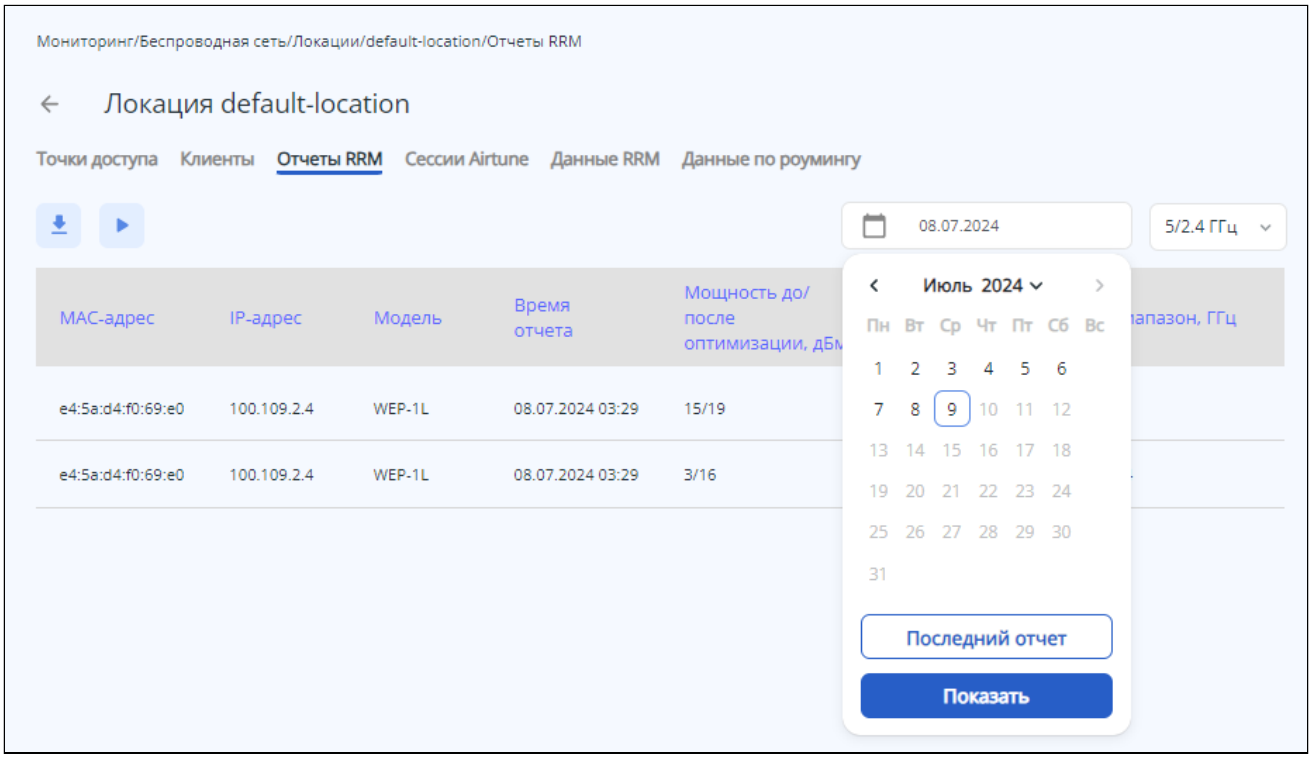
Подробная информация включает в себя следующие параметры:

- *IP-адрес* – IP-адрес подключенного устройства;
- *Имя хоста* – сетевое имя подключенного устройства;
- *SNR, дБ* – отношение сигнал/шум;
- *Канальная скорость передачи* – модуляция и канальная скорость при передаче;
- *Канальная скорость приема* – модуляция и канальная скорость при приеме;
- *Режим IEEE 802.11* – стандарт беспроводной сети;
- *Авторизован* – статус авторизации клиента;
- *Домен* – домен, к которому принадлежит пользователь;
- *Качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи пакетов, отправленных клиенту. Максимальное значение — 100 % (все переданные пакеты отправились с первой попытки), минимальное значение — 0 % (ни один пакет не был успешно отправлен до клиента). Значение параметра рассчитывается за последние 10 секунд;
- *Общее качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи пакетов, отправленных клиенту. Максимальное значение — 100 % (все переданные пакеты отправились с первой попытки), минимальное значение — 0 % (ни один пакет не был успешно отправлен до клиента). Значение параметра рассчитывается за все время подключения клиента;
- *Скорость передачи, Кбит/с* – актуальная скорость передачи трафика в настоящий момент времени;
- *Скорость приема, Кбит/с* – актуальная скорость приема трафика в настоящий момент времени;
- *Передано, байт* – количество байт, переданных на подключенное устройство;
- *Принято, байт* – количество байт, принятых от подключенного устройства;

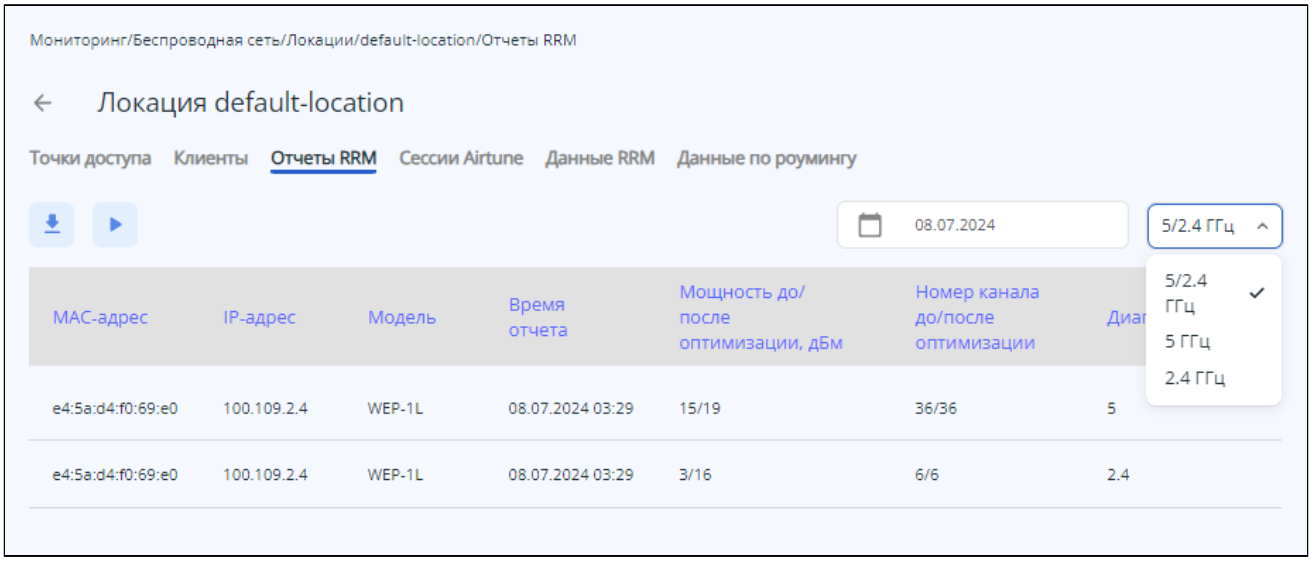
- *Передано, пакетов* − количество пакетов, переданных на подключенное устройство;
- *Принято, пакетов* − количество пакетов, принятых от подключенного устройства;
- *Время работы* − время соединения с Wi-Fi клиентом;
- *Ширина полосы передачи, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс при передаче;
- *Ширина полосы приема, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс при приеме.

Отчёты RRM

На странице отображаются отчеты оптимизации. По умолчанию выводится последний отчет. Необходимую дату отчета можно выбрать с помощью календаря.



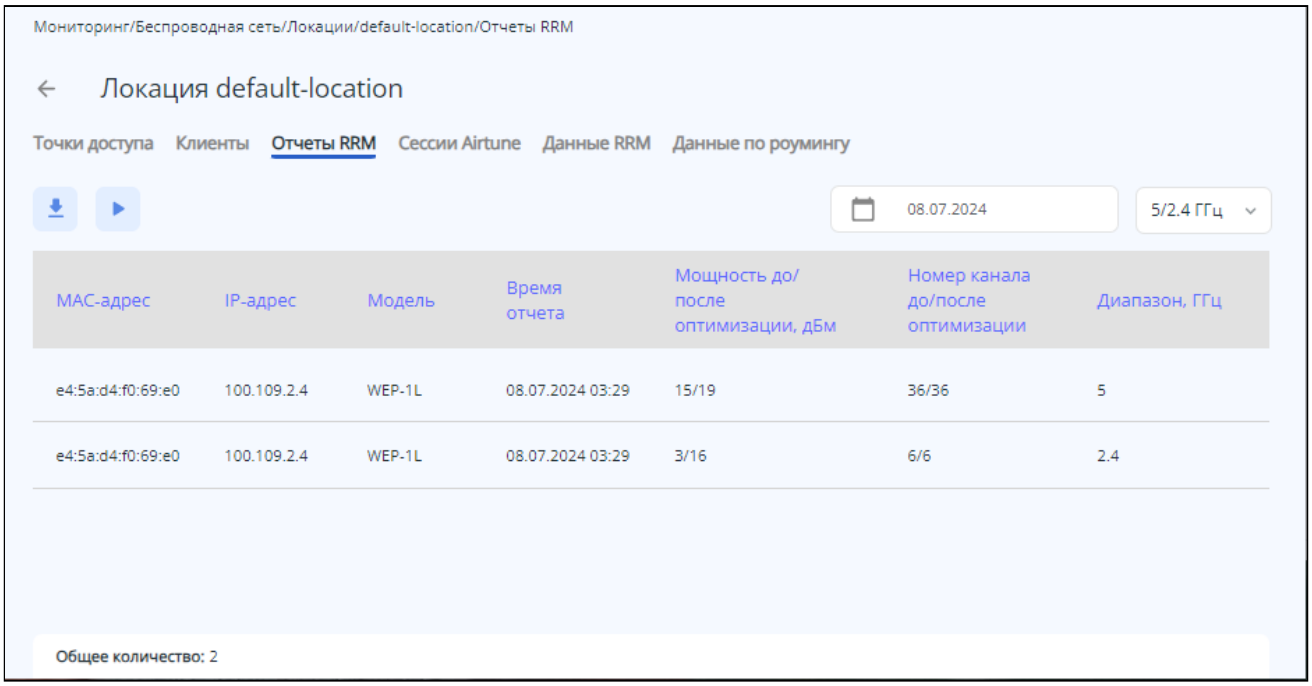
Отчеты RRM можно отфильтровать по частотному диапазону.



На странице можно запустить оптимизацию, нажав на кнопку «Запустить оптимизацию»  . Данный процесс займет несколько минут.

Также есть возможность выгрузить отчеты, нажав на кнопку «Скачать отчеты»  .

В параметре «Общее количество» отображается количество радиоинтерфейсов, для которых была произведена оптимизация.



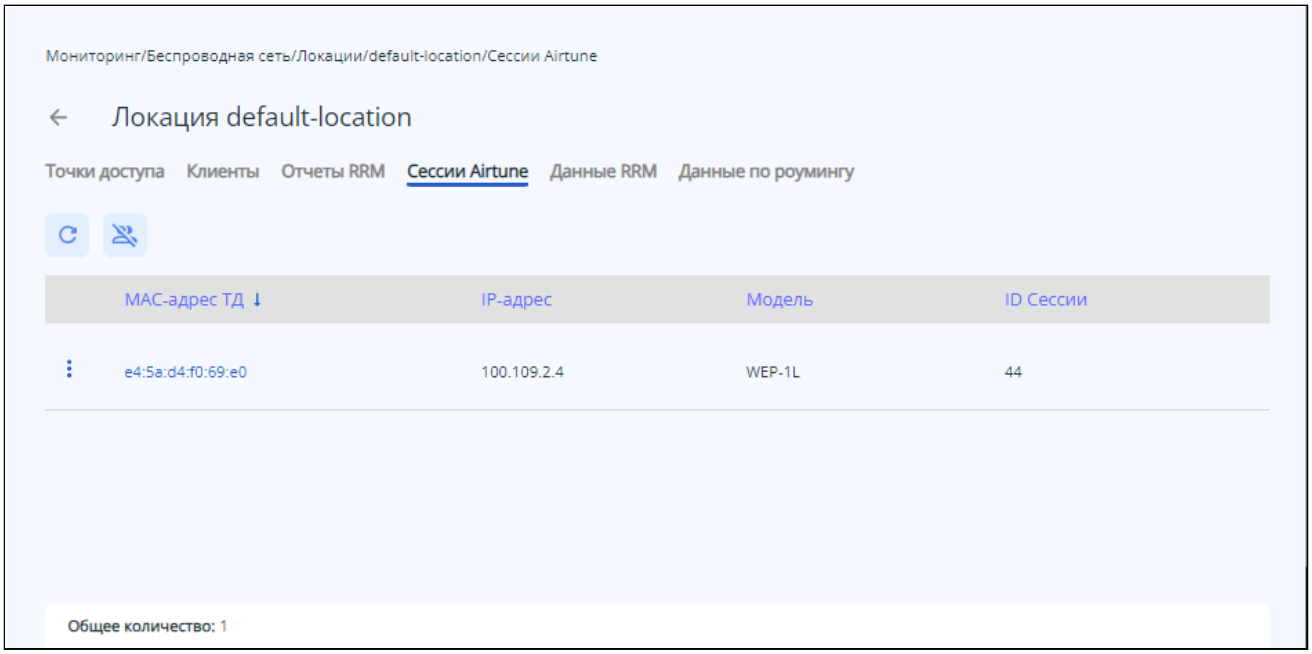
- *MAC-адрес* − MAC-адрес точки доступа, которая управляется Airtune;
- *IP-адрес* − IP-адрес точки доступа, которая управляется Airtune;
- *Модель* − тип точки доступа, которая управляется Airtune;
- *Время отчета* − время, в которое был сформирован отчет оптимизации;
- *Мощность до/после оптимизации, дБм* − мощность точки доступа, первое число показывает значение, которое было перед оптимизацией, второе значение − мощность после оптимизации;
- *Номер канала до/после оптимизации* − канал радиоинтерфейса точки доступа, первое число показывает значение, которое было перед оптимизацией, второе значение − канал радиоинтерфейса после оптимизации;
- *Диапазон, ГГц* − частотный диапазон радиоинтерфейса.

Сессии Airtune

На странице представлены данные о точках доступа, которые на данный момент находятся под управлением сервиса Airtune.

При нажатии на кнопку «Разорвать сессии Airtune» от сервиса будут отключены все точки доступа, но будут сразу переподключены, если для них не будет отключена работа сервиса в конфигурации.

В параметре «Общее количество» отображается число точек доступа, которые в данный момент управляются сервисом Airtune.



В таблице представлены данные:

- *MAC-адрес ТД* − MAC-адрес точки доступа, которая на данный момент находится под управлением сервиса Airtune, при нажатии будет осуществлен переход на страницу расширенной информации по сессии;
- *Разорвать сессию* − кнопка для разрыва сессии между выбранной точкой доступа и сервисом Airtune. Точка доступа будет сразу переподключена, если для нее не будет отключена работа сервиса в конфигурации;
- *IP-адрес* − IP-адрес точки доступа, которая на данный момент находится под управлением сервиса Airtune;
- *Модель* − модель точки доступа, которая на данный момент находится под управлением сервиса Airtune;
- *ID Сессии* − идентификационный номер сессии точки доступа, которая на данный момент находится под управлением сервиса Airtune.

Airtune-сессия

На странице представлены параметры радиоинтерфейсов и список SSID на них. Для того чтобы обновить информацию на странице, необходимо нажать на кнопку «Обновить» .

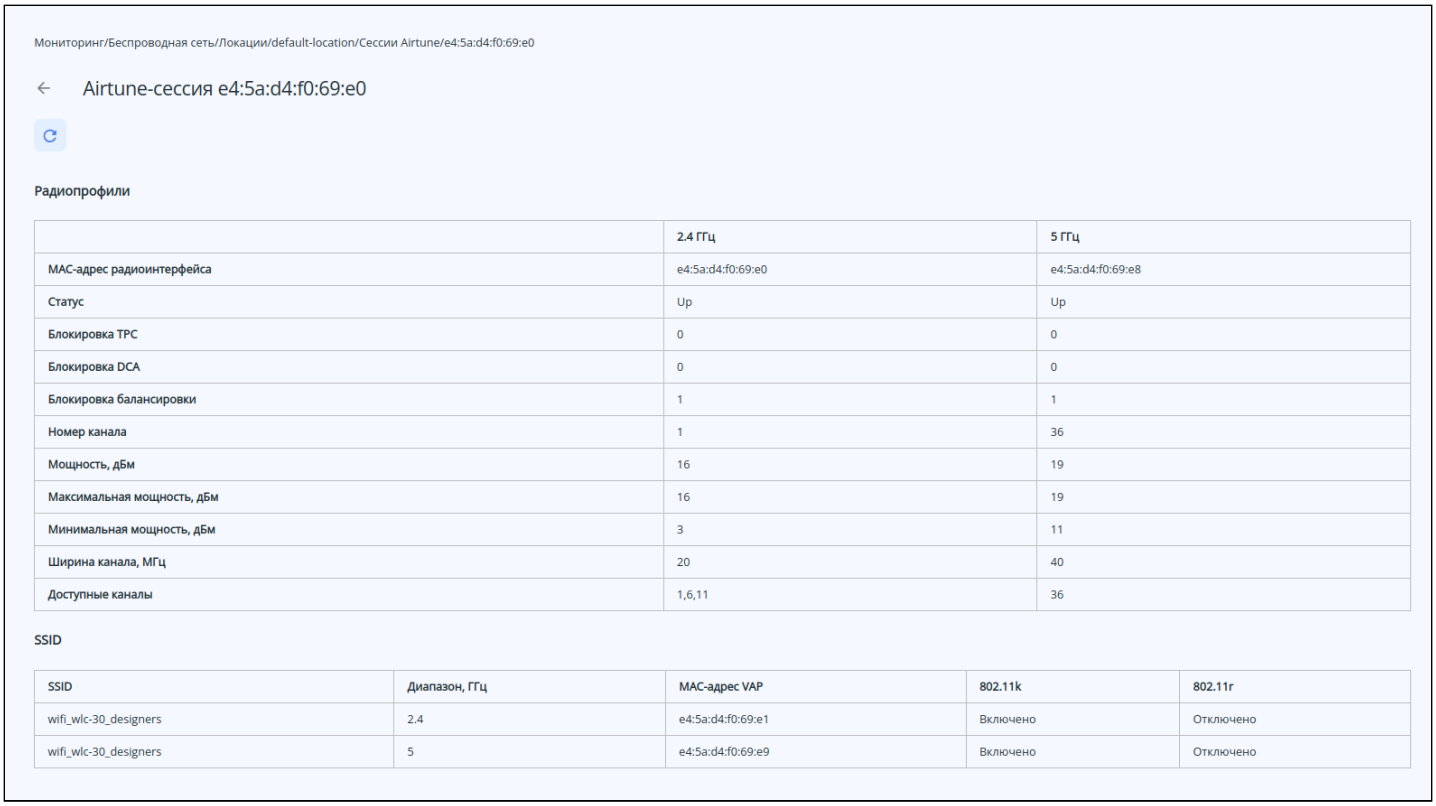


Таблица «Радиопрофили» разделена по частотным диапазонам и содержит параметры:

- *MAC-адрес радиоинтерфейса* – MAC-адрес радиоинтерфейса точки доступа, которая управляется Airtune;
- *Статус* – состояние радиоинтерфейса: *Up* – радиоинтерфейс работает, *Down* – радиоинтерфейс отключен;
- *Блокировка TPC* – статус блокировки автоматического управления мощностью: *0* – блокировка отключена, *1* – блокировка активирована;
- *Блокировка DCA* – статус блокировки динамического распределения каналов: *0* – блокировка отключена, *1* – блокировка активирована;
- *Номер канала* – номер беспроводного канала, на котором работает радиоинтерфейс;
- *Мощность, дБм* – мощность сигнала радиоинтерфейса;
- *Ширина канала, МГц* – ширина полосы частот канала, на которой работает радиоинтерфейс;
- *Максимальная мощность, дБм* – максимальная мощность сигнала, которая доступна для радиоинтерфейса;
- *Минимальная мощность, дБм* – минимальная мощность сигнала, которая доступна для радиоинтерфейса;
- *Доступные каналы* – список каналов, из которых выбирается один, который после оптимизации назначается на радиоинтерфейс.

Таблица «SSID» содержит:

- *SSID* – имя сети, которое вещается пользователям;
- *Диапазон, ГГц* – частотный диапазон радиоинтерфейса;
- *MAC-адрес VAP* – MAC-адрес виртуальной точки доступа;
- *802.11k* – статус активности синхронизации списков соседних точек доступа стандарта 802.11k, который позволяет клиенту, при ослабевании сигнала с текущей точки доступа, искать более подходящую точку доступа из рекомендуемого списка, не анализируя весь эфир;
- *802.11r* – статус активности согласования ключей между точками доступа для роуминга стандарта 802.11r, который позволяет значительно ускорять процесс переключения клиента между точками доступа, т.к. клиенту не нужно будет проходить повторную полную авторизацию на встречной точке доступа, только ускоренную.

Данные RRM

На странице представлены данные по радиоинтерфейсам точек доступа после последней оптимизации.

В параметре «Общее количество» отображается число радиоинтерфейсов. Данный список можно отсортировать по частотному диапазону.

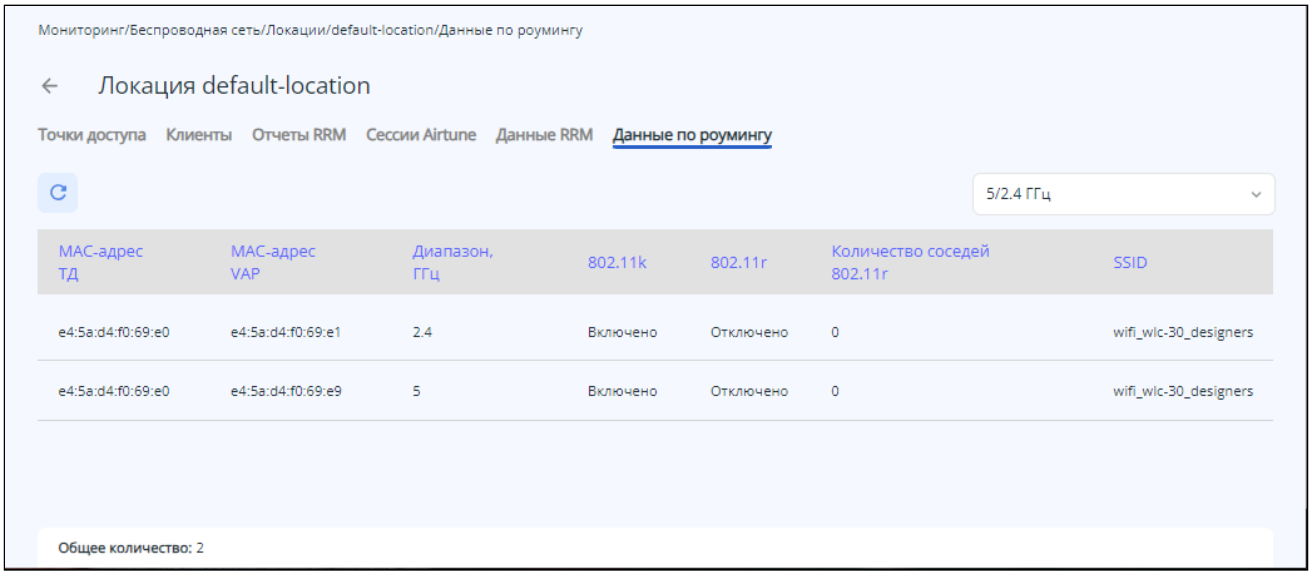
В таблице отображены:

- *MAC-адрес* − MAC-адрес точки доступа, которая управляется Airtune;
- *Диапазон, ГГц* − частотный диапазон радиоинтерфейса;
- *Статус* − состояние радиоинтерфейса: *Up* − радиоинтерфейс работает, *Down* − радиоинтерфейс отключен;
- *Блокировка DCA* − статус блокировки динамического распределения каналов: *0* − блокировка отключена, *1* − блокировка активирована;
- *Блокировка TPC* − статус блокировки автоматического управления мощностью: *0* − блокировка отключена, *1* − блокировка активирована;
- *Номер канала* − номер беспроводного канала, на котором работает радиоинтерфейс;
- *Ширина канала, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс;
- *Мощность, дБм* − мощность сигнала радиоинтерфейса;
- *Доступные каналы* − список каналов, из которых выбирается канал, который после оптимизации назначается на радиоинтерфейс;
- *Количество клиентов* − число клиентов, подключенных к радиоинтерфейсу.

Данные по роумингу

На странице отображен весь список виртуальных интерфейсов (SSID), которые обрабатываются сервисом Airtune. Страница предназначена для отображения текущего состояния конфигурации роуминга 802.11 k/r на всех точках доступа локации, а также списка всех соседей, между которыми сервис настроил роуминг.

В параметре «Общее количество» отображается число SSID, настроенных на всех точках доступа. Данный список можно отсортировать по частотному диапазону.

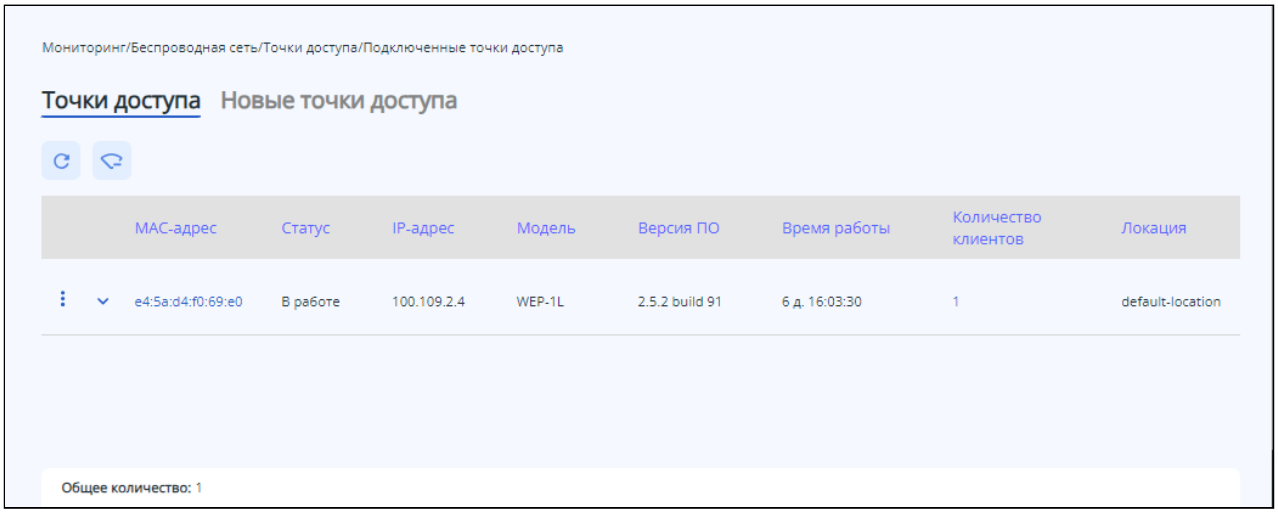


В таблице отображены следующие параметры:

- *MAC-адрес ТД* – MAC-адрес точки доступа;
- *MAC-адрес VAP* – MAC-адрес виртуальной точки доступа;
- *Диапазон, ГГц* – частотный диапазон радиоинтерфейса;
- *802.11k* – статус активности синхронизации списков соседних точек доступа стандарта 802.11k, который позволяет клиенту, при ослабевании сигнала с текущей точки доступа, искать более подходящую точку доступа из рекомендуемого списка, не анализируя весь эфир;
- *802.11r* – статус активности согласования ключей между точками доступа для роуминга стандарта 802.11r, который позволяет значительно ускорять процесс переключения клиента между точками доступа, т.к. клиенту не нужно будет проходить повторную полную авторизацию на встречной точке доступа, только ускоренную;
- *Количество соседей 802.11r* – количество точек доступа, с которыми был настроен бесшовный роуминг 802.11r, соседи по роумингу определяются по полному совпадению параметров SSID, таких как статус 802.11r, имя сети, диапазон;
- *SSID* – имя сети, которое вещается пользователям.

Подменю «Точки доступа»

Данная страница содержит списки точек доступа, которые можно зарегистрировать, и точки доступа, которые уже прошли авторизацию на контроллере.



Точки доступа

На странице отображены точки доступа, которые зарегистрированы и находятся под управлением контроллера. Параметр «Общее количество» показывает число зарегистрированных точек доступа.

С помощью кнопки «Разрегистрировать» можно вывести точки доступа из обслуживания. После этого они будут отображаться в разделе «Новые точки доступа».

Таблица содержит данные:

- *MAC-адрес* − MAC-адрес зарегистрированной точки доступа, при нажатии осуществляется переход на страницу «Точка доступа»;
- *Разрегистрировать* − кнопка позволяет вывести из обслуживания выбранную точку доступа и перенести ее в список новых точек доступа;
- *Статус* − состояние работы точки доступа;
- *IP-адрес* − IP-адрес зарегистрированной точки доступа;
- *Модель* − модель зарегистрированной точки доступа;
- *Версия ПО* − версия программного обеспечения зарегистрированной точки доступа;
- *Время работы* − время работы с момента последнего включения или перезагрузки устройства;
- *Количество клиентов* − число клиентов, подключенных к зарегистрированной точке доступа, при нажатии осуществляется переход на страницу «Точка доступа» → «Клиенты»;
- *Локация* − имя локации, к которой относится точка доступа.

При нажатии на кнопку будет раскрыта дополнительная информация:

- *Описание статуса* − дополнительная информация по статусу, в случае если для точки доступа обнаружены проблемы;
- *Серийный номер* − серийный номер устройства, установленный заводом-изготовителем;
- *HW-версия* − версия аппаратного обеспечения устройства;
- *Первая активность* − время первой регистрации точки доступа на контроллере;
- *Подключен в* − время последнего подключения точки доступа к контроллеру;
- *Последняя активность* − время, в которое контроллер последний раз настраивал точку доступа;
- *Подключена через* − профиль, с помощью которого точка доступа была настроена;
- *Состояние Netconf* − статус соединения точки доступа и контроллера по протоколу Netconf;
- *Описание* − текстовое описание точки доступа, которое ей было назначено при формировании профиля.

Точка доступа

При нажатии на MAC-адрес зарегистрированной точки доступа осуществляется переход на страницу точки доступа, где представлены данные по клиентам, радиоинтерфейсам и интерфейсам.

Клиенты

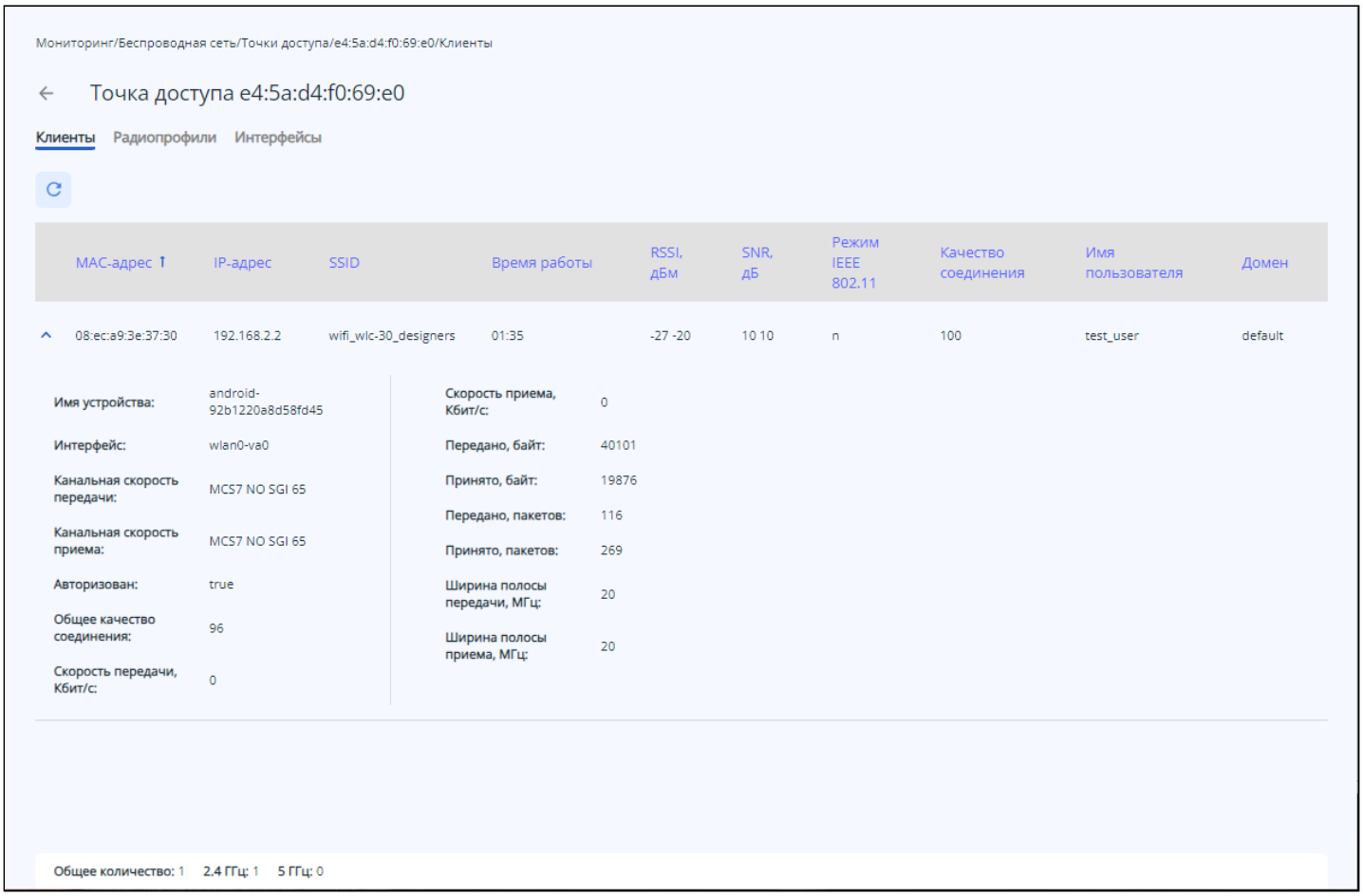
Страница содержит в себе таблицу клиентов, которые в данный момент подключены к точке доступа. В параметре «Общее количество» отображается количество клиентов со всех частотных диапазонов. «2.4», «5» − показывают количество клиентов в каждом диапазоне соответственно.

В таблице представлены данные:

- *MAC-адрес* − MAC-адрес клиентского устройства;
- *IP-адрес* − IP-адрес, который получило клиентское устройство;

- *SSID* – имя сети, к которой подключено устройство;
- *Время работы* – время работы с момента подключения клиентского устройства к SSID;
- *RSSI, дБм* – уровень принимаемого сигнала;
- *SNR, дБ* – отношение сигнал/шум;
- *Режим IEEE 802.11* – стандарт беспроводной сети;
- *Качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи 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);
- *Имя пользователя* – имя пользователя, указанное при авторизации в сети. В случае personal-авторизации или при подключении к открытой сети, имя пользователя останется пустым;
- *Домен* – домен, к которому принадлежит пользователь.

Чтобы просмотреть подробную информацию по клиенту, необходимо нажать на .

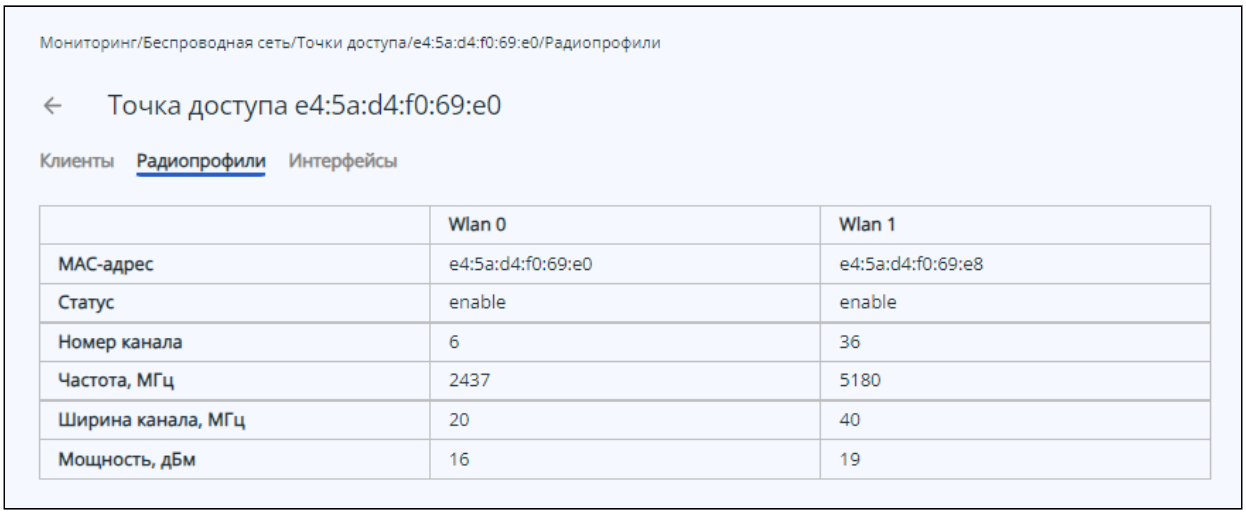


Подробная информация по клиенту содержит:

- *Имя хоста* – сетевое имя подключенного устройства;
- *Интерфейс* – интерфейс взаимодействия точки доступа с подключенным устройством;
- *Канальная скорость передачи* – модуляция и канальная скорость при передаче;
- *Канальная скорость приема* – модуляция и канальная скорость при приеме;
- *Авторизован* – статус авторизации клиента;
- *Общее качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи 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 все время подключения клиента;
- *Скорость передачи, Кбит/с* – актуальная скорость передачи трафика в настоящий момент времени;
- *Скорость приема, Кбит/с* – актуальная скорость приема трафика в настоящий момент времени;
- *Передано, байт* – количество байт, переданных на подключенное устройство;

- *Принято, байт* − количество байт, принятых от подключенного устройства;
- *Передано, пакетов* − количество пакетов, переданных на подключенное устройство;
- *Принято, пакетов* − количество пакетов, принятых от подключенного устройства;
- *Ширина полосы передачи, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс при передаче;
- *Ширина полосы приема, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс при приеме.

Радиопрофили



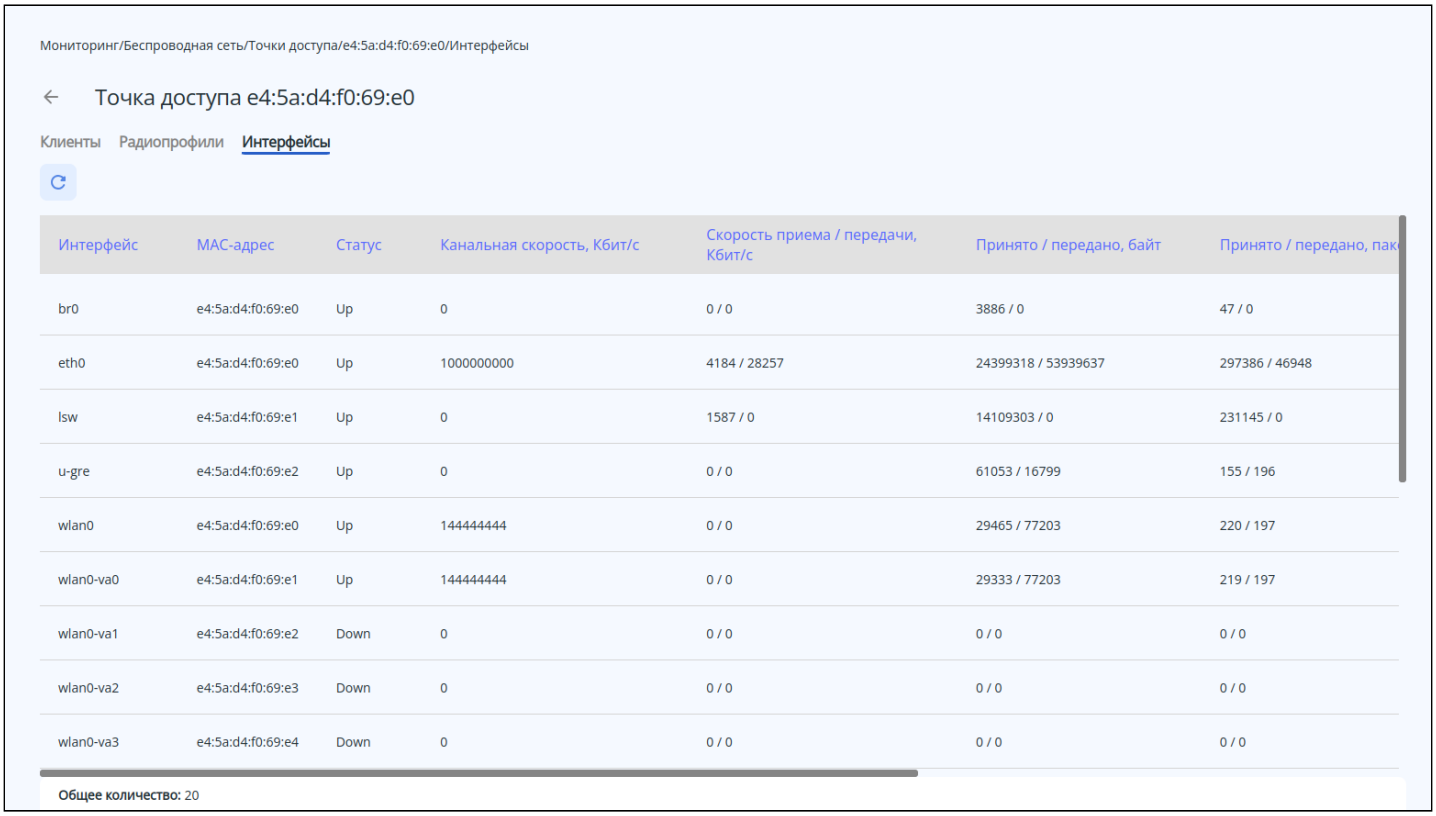
	Wlan 0	Wlan 1
MAC-адрес	e4:5a:d4:f0:69:e0	e4:5a:d4:f0:69:e8
Статус	enable	enable
Номер канала	6	36
Частота, МГц	2437	5180
Ширина канала, МГц	20	40
Мощность, дБм	16	19

На странице представлена таблица с основными параметрами радиоинтерфейсов точки доступа:

- *MAC-адрес* − MAC-адрес радиоинтерфейса;
- *Статус* − статус активности радиоинтерфейса;
- *Номер канала* − номер беспроводного канала, на котором работает радиоинтерфейс;
- *Частота, МГц* − частота, на которой работает радиоинтерфейс;
- *Ширина канала, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс;
- *Мощность, дБм* − мощность сигнала радиоинтерфейса.

Интерфейсы

На странице представлена информация по всем интерфейсам точки доступа. В параметре «Общее количество» отображается число интерфейсов на точке доступа.

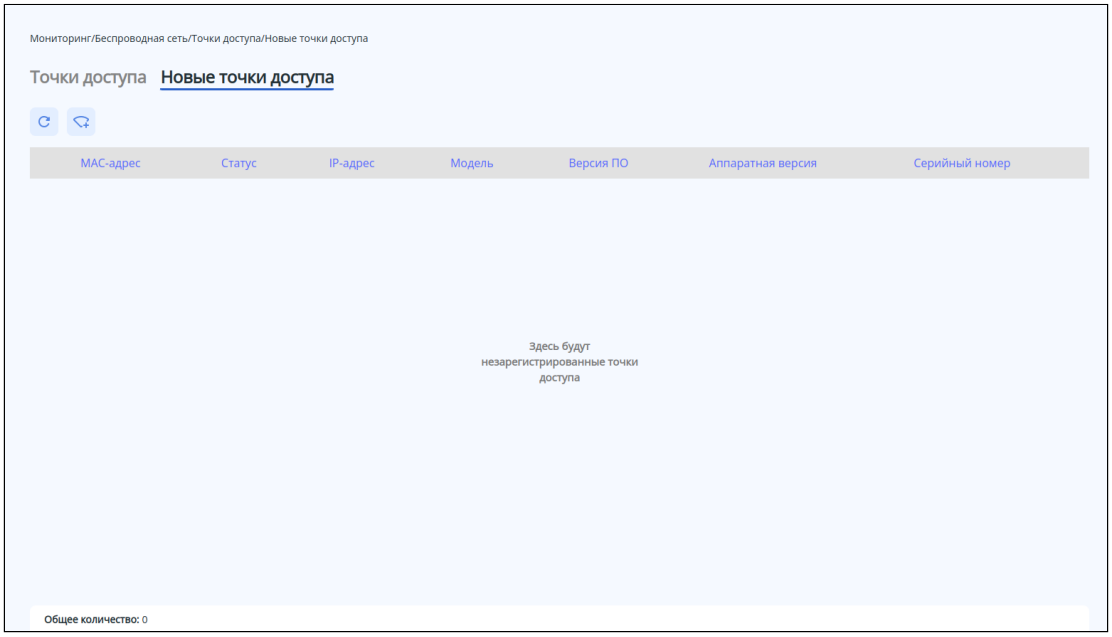


- *Интерфейс* − название интерфейса;
- *MAC-адрес* − MAC-адрес интерфейса;
- *Статус* − статус активности интерфейса;
- *Канальная скорость, Кбит/с* − скорость подключения на физическом уровне, которая используется в настоящий момент времени;
- *Скорость передачи/приема, Кбит/с* − актуальная скорость передачи трафика в настоящий момент времени;
- *Принято/передано, байт* − количество байт, принятых/переданных на подключенное устройство;
- *Принято/передано, пакетов* − количество пакетов, принятых/переданных на подключенное устройство;
- *Отброшено при приеме/передаче, пакетов* − количество пакетов, отброшенных при приеме/передачи;
- *Принято/передано, ошибок* − количество пакетов, принятых/переданных с ошибками на подключенное устройство;
- *Дуплексный режим* − режим работы дуплекса на интерфейсе.

Новые точки доступа

На странице отображены точки доступа, которые пришли на контроллер и ожидают регистрации или находятся в процессе регистрации. Параметр «Общее количество» показывает число незарегистрированных точек доступа.

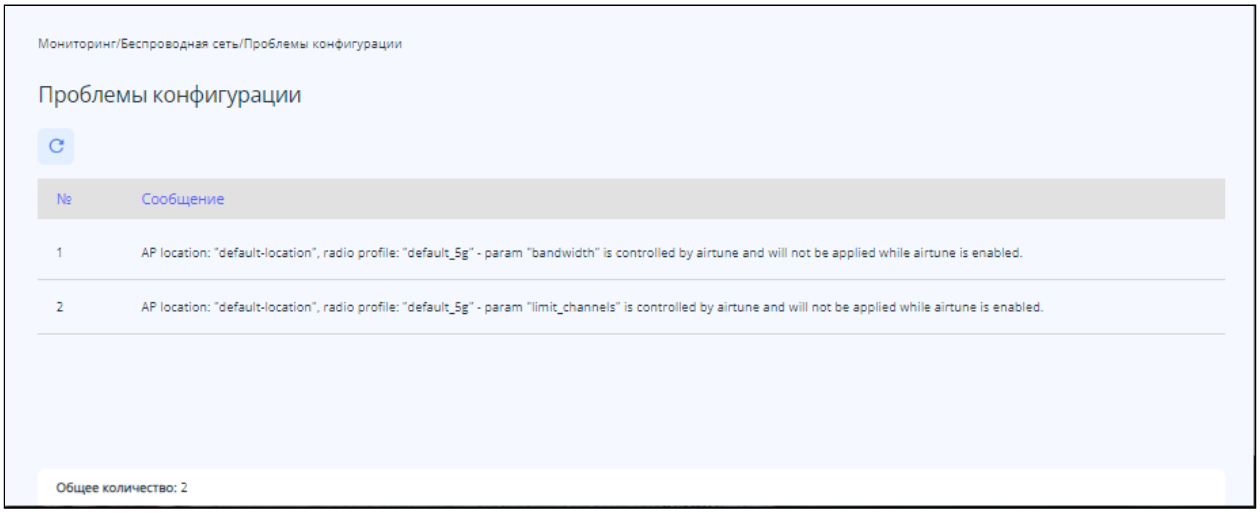
Точки доступа можно зарегистрировать кнопкой «Зарегистрировать все». После этого они перейдут в раздел «Точки доступа».



- *MAC-адрес* − MAC-адрес незарегистрированной точки доступа;
- *Статус* − состояние работы точки доступа;
- *IP-адрес* − IP-адрес незарегистрированной точки доступа;
- *Модель* − модель незарегистрированной точки доступа;
- *Версия ПО* − версия программного обеспечения незарегистрированной точки доступа;
- *HW-версия* − версия аппаратного обеспечения устройства;
- *Серийный номер* − серийный номер устройства, установленный заводом-изготовителем.

Подменю «Проблемы конфигурации»

На странице представлена таблица, содержащая ошибки, возникшие при настройке контроллера, или предупреждения о том, что параметры не будут применены по какой-либо причине. В параметре «Общее количество» отображается число предупреждений/ошибок конфигурирования.



Подменю «Журнал событий»

В подменю «Журнал событий» отображаются события и действия с точками доступа и клиентами.

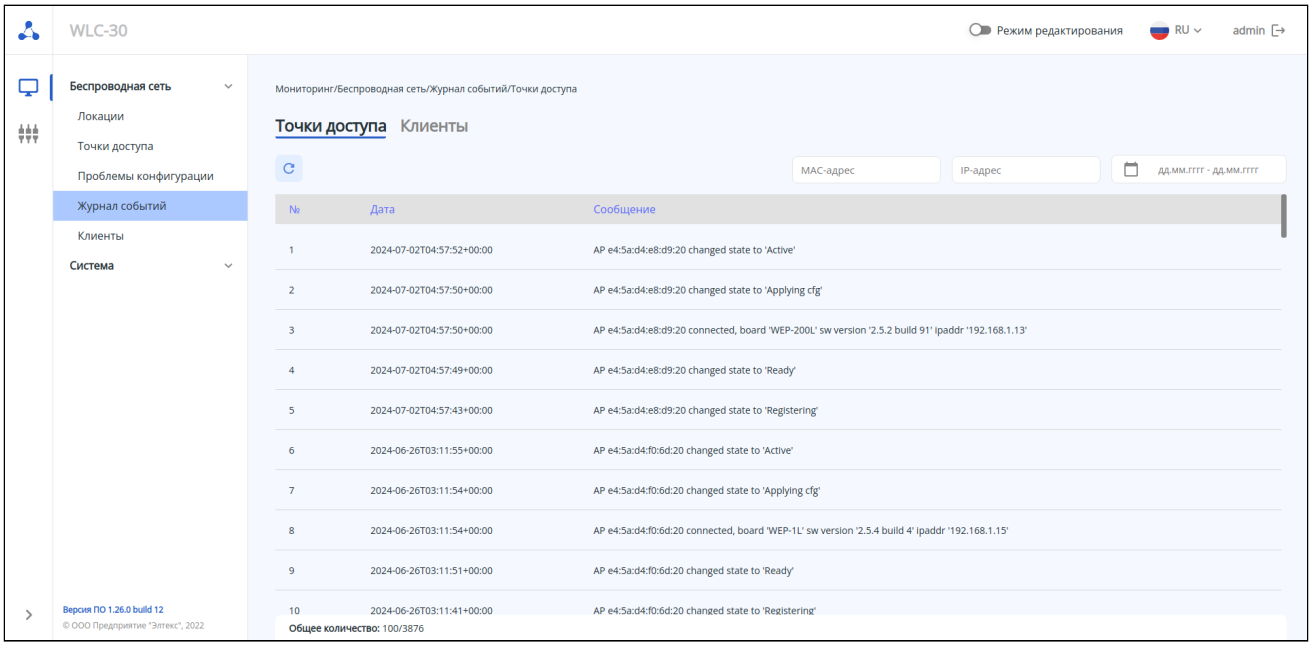
Точки доступа

На странице представлен журнал событий с точками доступа с временными метками. В параметре «Общее количество» отображается количество записей в журнале на странице и общее количество записей в журнале. Данные подгружаются автоматически по 100 записей при прокрутке.

Для удобства использования журнала предусмотрены фильтры по следующим ключевым параметрам:

- *MAC-адрес* – MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов.
- *IP-адрес* – IP-адрес точки доступа. Для поиска необходимо ввести IP-адрес полностью.
- *Дата* – дата фиксации события в журнале. Допускается ввод даты вручную или с помощью календаря. В фильтре доступен выбор диапазона дат от 1 до 7 дней.

При использовании фильтров, параметр «Общее количество» отображает количество отфильтрованных записей, показанных на странице. Данные подгружаются автоматически по 100 записей при прокрутке. Обновление журнала происходит при нажатии на кнопку «Обновить».



Клиенты

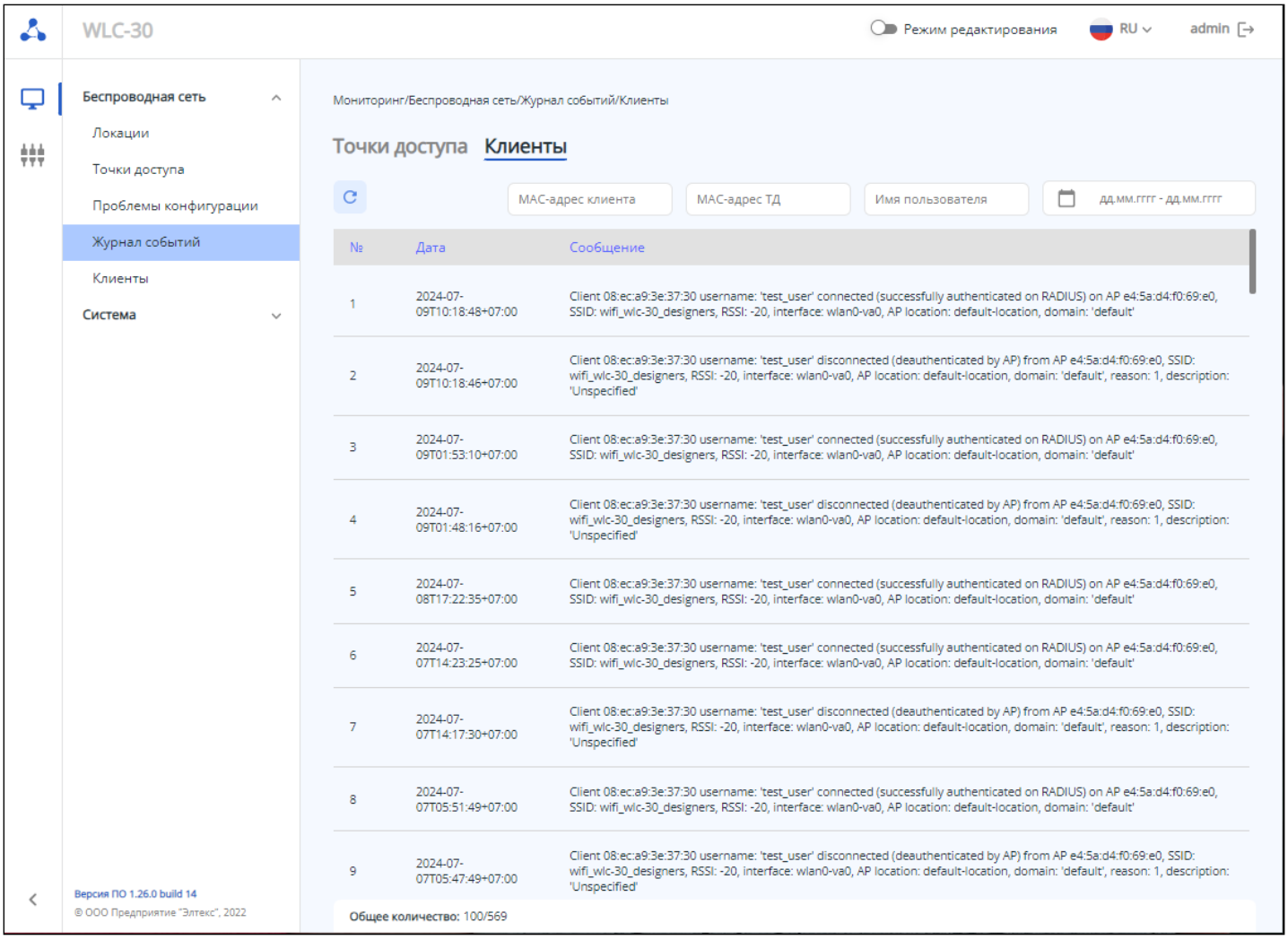
На странице представлен журнал событий для клиентов Wi-Fi с временными метками. Журнал содержит события, информирующие о подключении/отключении клиентов, ошибках регистрации, роуминге. В параметре «Общее количество» отображается количество записей в журнале на странице и общее количество записей в журнале. Данные подгружаются автоматически по 100 записей при прокрутке.

Для удобства использования журнала предусмотрены фильтры по следующим ключевым параметрам:

- *MAC-адрес клиента* – MAC-адрес беспроводного клиента. Для поиска достаточно ввести один или несколько целых октетов.
- *MAC-адрес ТД* – MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов.
- *Имя пользователя* – имя пользователя, указанное при регистрации в сети Wi-Fi. Поиск работает по частичному совпадению.
- *Дата* – дата фиксации события в журнале. Допускается ввод даты вручную или с помощью календаря. В фильтре доступен выбор диапазона дат от 1 до 7 дней.

При использовании фильтров параметр «Общее количество» отображает количество отфильтрованных записей, показанных на странице. Данные подгружаются автоматически по 100 записей при прокрутке.

Обновление журнала происходит при нажатии на кнопку «Обновить».



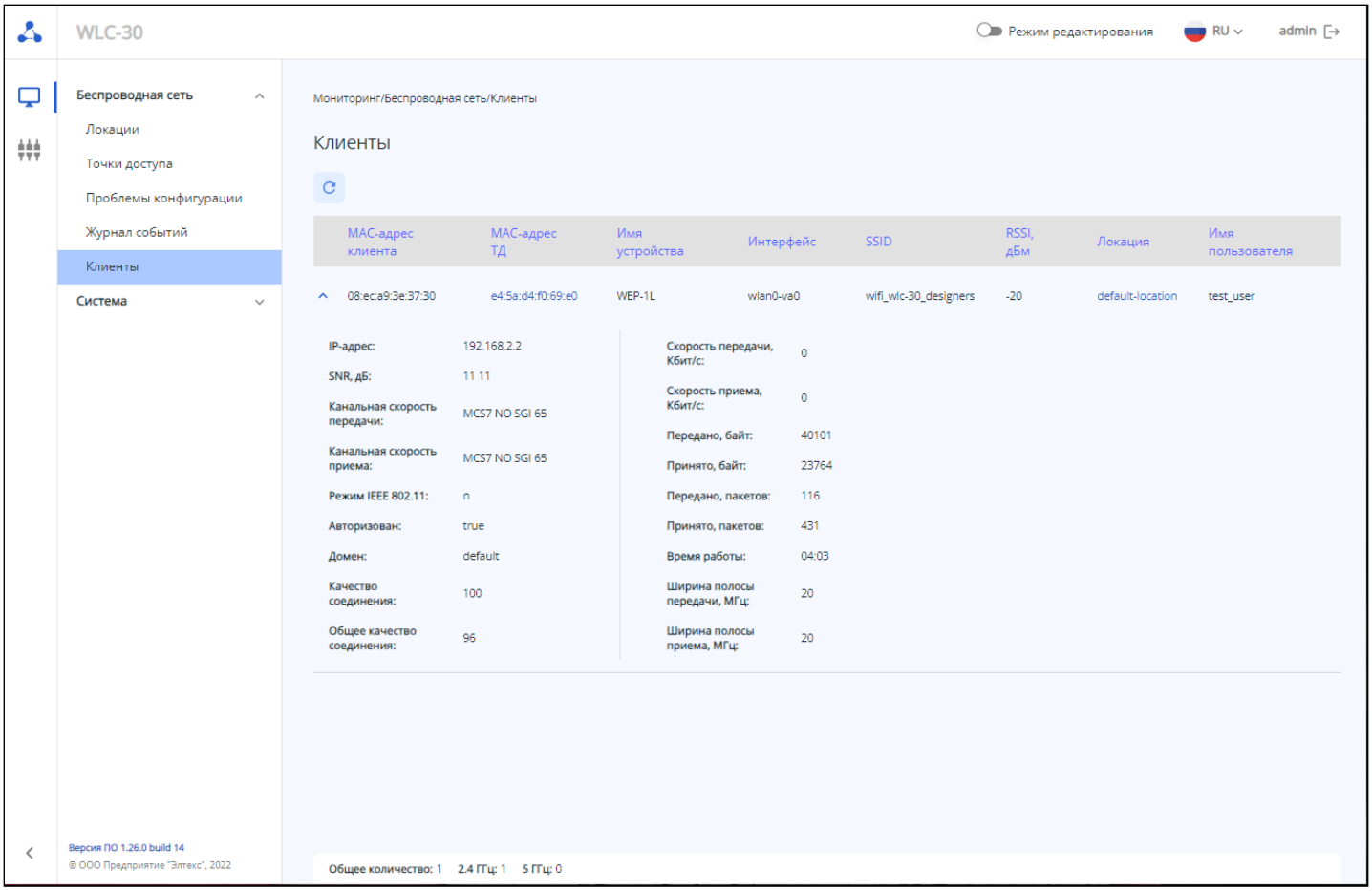
Подменю «Клиенты»

На странице отображено общее количество клиентов, а также их количественное распределение по частотным диапазонам. Для того чтобы обновить информацию на странице, необходимо нажать на кнопку «Обновить».

В таблице представлена основная информация по клиенту:

- *MAC-адрес клиента* − MAC-адрес подключенного устройства;
- *Имя устройства* − имя устройства, по умолчанию используется модель точки доступа. Задать имя можно через конфигурацию;
- *MAC-адрес ТД* − MAC-адрес точки доступа, к которой подключено устройство;
- *Интерфейс* − интерфейс взаимодействия точки доступа с подключенным устройством;
- *SSID* − имя сети, к которой подключено устройство;
- *RSSI, дБм* − уровень принимаемого сигнала;
- *Локация* − локация, в которой находится точка доступа, к которой подключилось клиентское устройство;
- *Имя пользователя* − имя пользователя, указанное при авторизации в сети. В случае personal-авторизации или при подключении к открытой сети, имя пользователя останется пустым.

Для просмотра подробной информации по клиенту необходимо нажать на .



Подробное описание включает в себя следующие параметры:

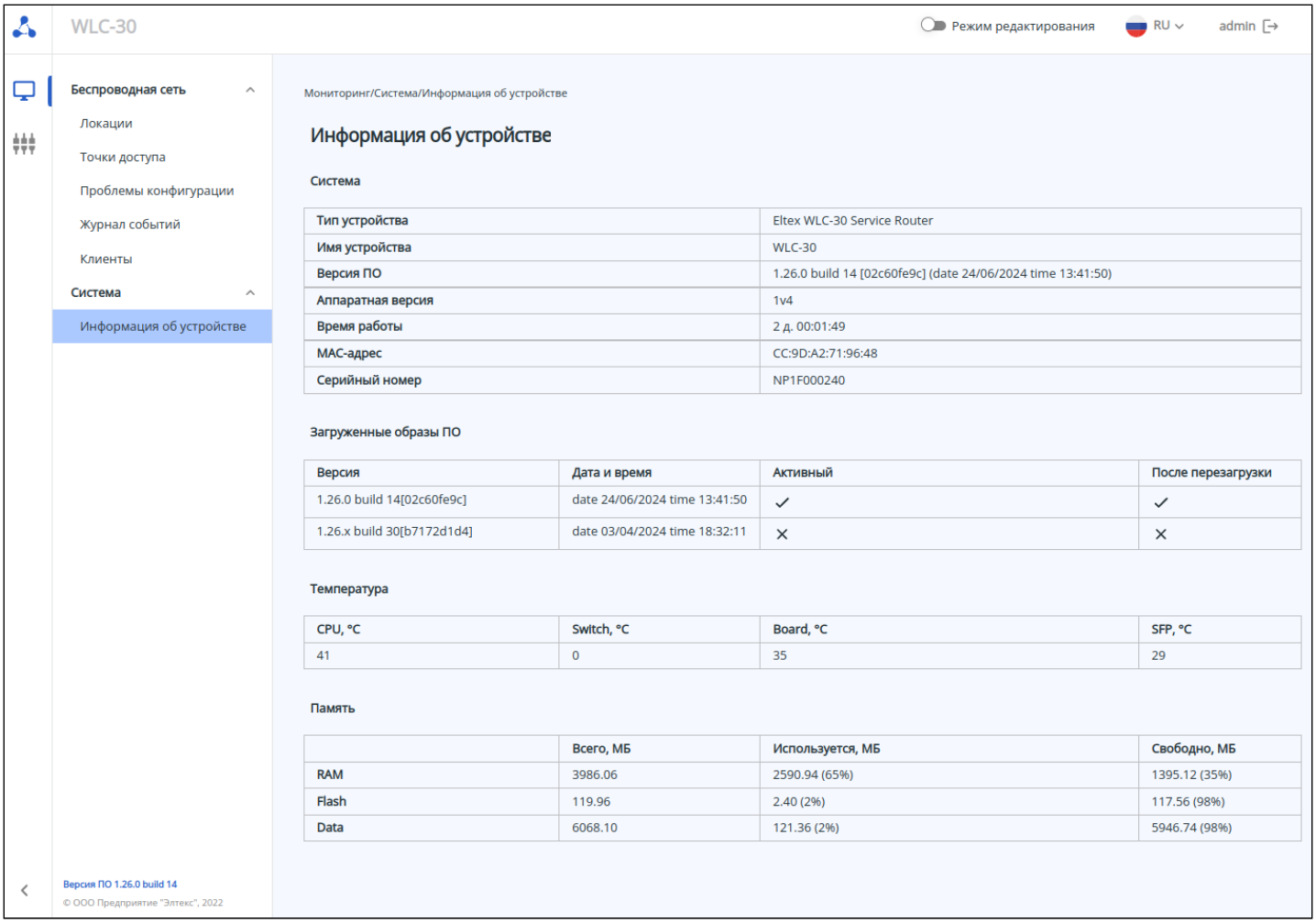
- *IP-адрес* – IP-адрес подключенного устройства;
- *Имя хоста* – сетевое имя подключенного устройства;
- *SNR, дБ* – отношение сигнал/шум;
- *Канальная скорость передачи* – модуляция и канальная скорость при передаче;
- *Канальная скорость приема* – модуляция и канальная скорость при приеме;
- *Режим IEEE 802.11* – стандарт беспроводной сети;
- *Авторизован* – статус авторизации клиента;
- *Домен* – домен, к которому принадлежит пользователь;
- *Качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи 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 секунд;
- *Общее качество соединения* – параметр, который отображает состояние линка до клиента, рассчитанный на основании количества повторной передачи 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 все время подключения клиента;
- *Скорость передачи, Кбит/с* – актуальная скорость передачи трафика в настоящий момент времени;
- *Скорость приема, Кбит/с* – актуальная скорость приема трафика в настоящий момент времени;
- *Передано, байт* – количество байт, переданных на подключенное устройство;
- *Принято, байт* – количество байт, принятых от подключенного устройства;
- *Передано, пакетов* – количество пакетов, переданных на подключенное устройство;
- *Принято, пакетов* – количество пакетов, принятых от подключенного устройства;
- *Время работы* – время соединения с Wi-Fi клиентом;
- *Ширина полосы передачи, МГц* – ширина полосы частот канала, на которой работает радиоинтерфейс при передаче;

- *Ширина полосы приема, МГц* − ширина полосы частот канала, на которой работает радиоинтерфейс при приеме.

Меню «Система»

Подменю «Информация об устройстве»

В подменю «Информация об устройстве» содержатся основные данные о системе контроллера, загруженных образах, температуре и памяти.



Система

Тип устройства	Eltex WLC-30 Service Router
Имя устройства	WLC-30
Версия ПО	1.26.0 build 14 [02c60fe9c] (date 24/06/2024 time 13:41:50)
Аппаратная версия	1v4
Время работы	2 д. 00:01:49
MAC-адрес	CC:9D:A2:71:96:48
Серийный номер	NP1F000240

Загруженные образы ПО

Версия	Дата и время	Активный	После перезагрузки
1.26.0 build 14[02c60fe9c]	date 24/06/2024 time 13:41:50	✓	✓
1.26.x build 30[b7172d1d4]	date 03/04/2024 time 18:32:11	×	×

Температура

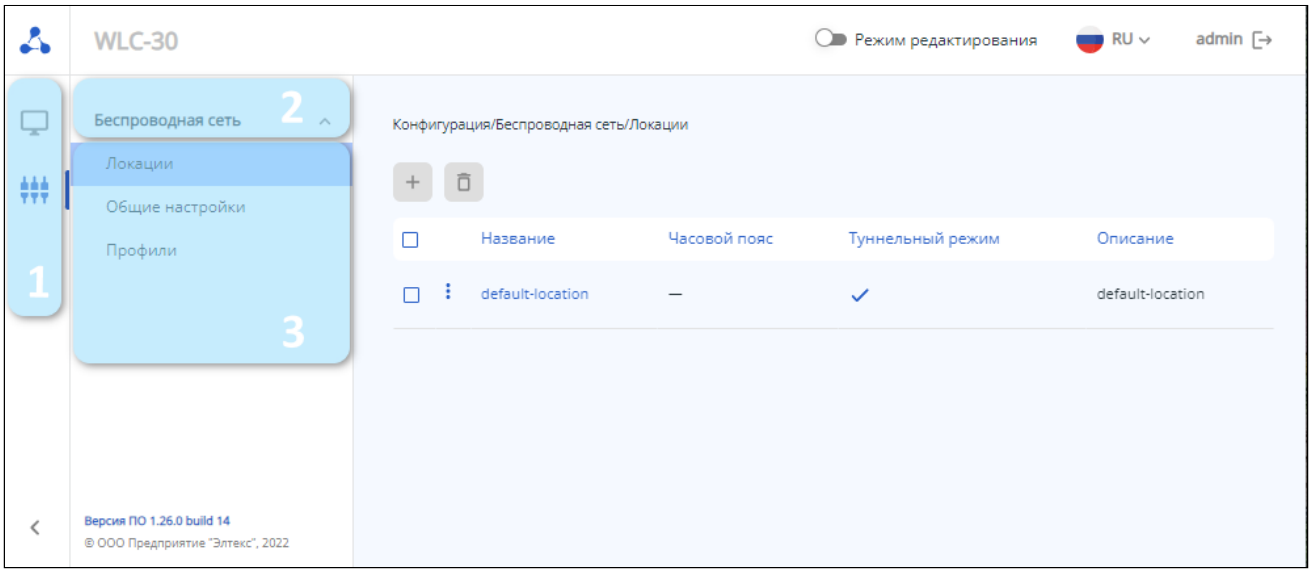
CPU, °C	Switch, °C	Board, °C	SFP, °C
41	0	35	29

Память

	Всего, МБ	Используется, МБ	Свободно, МБ
RAM	3986.06	2590.94 (65%)	1395.12 (35%)
Flash	119.96	2.40 (2%)	117.56 (98%)
Data	6068.10	121.36 (2%)	5946.74 (98%)

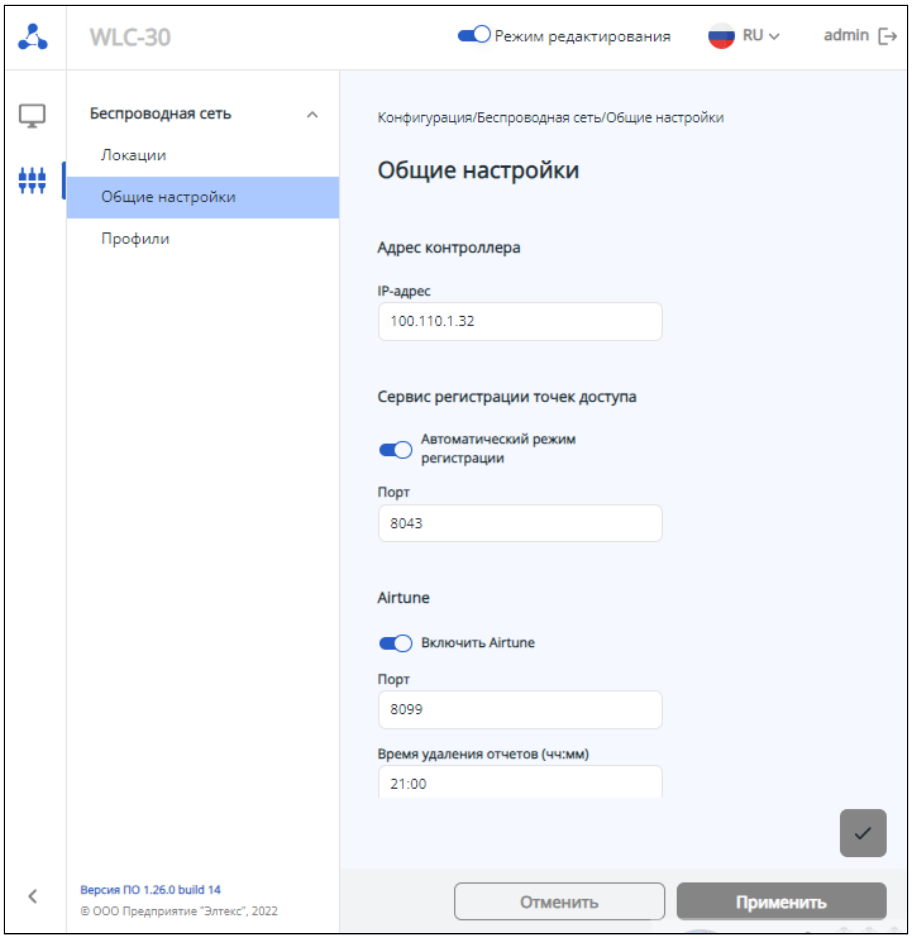
10.2.4 Конфигурирование

Для перехода к конфигурированию необходимо в главном меню выбрать элемент «Конфигурация» (1), развернуть меню «Беспроводная сеть» (2), выбрать нужный пункт подменю (3).



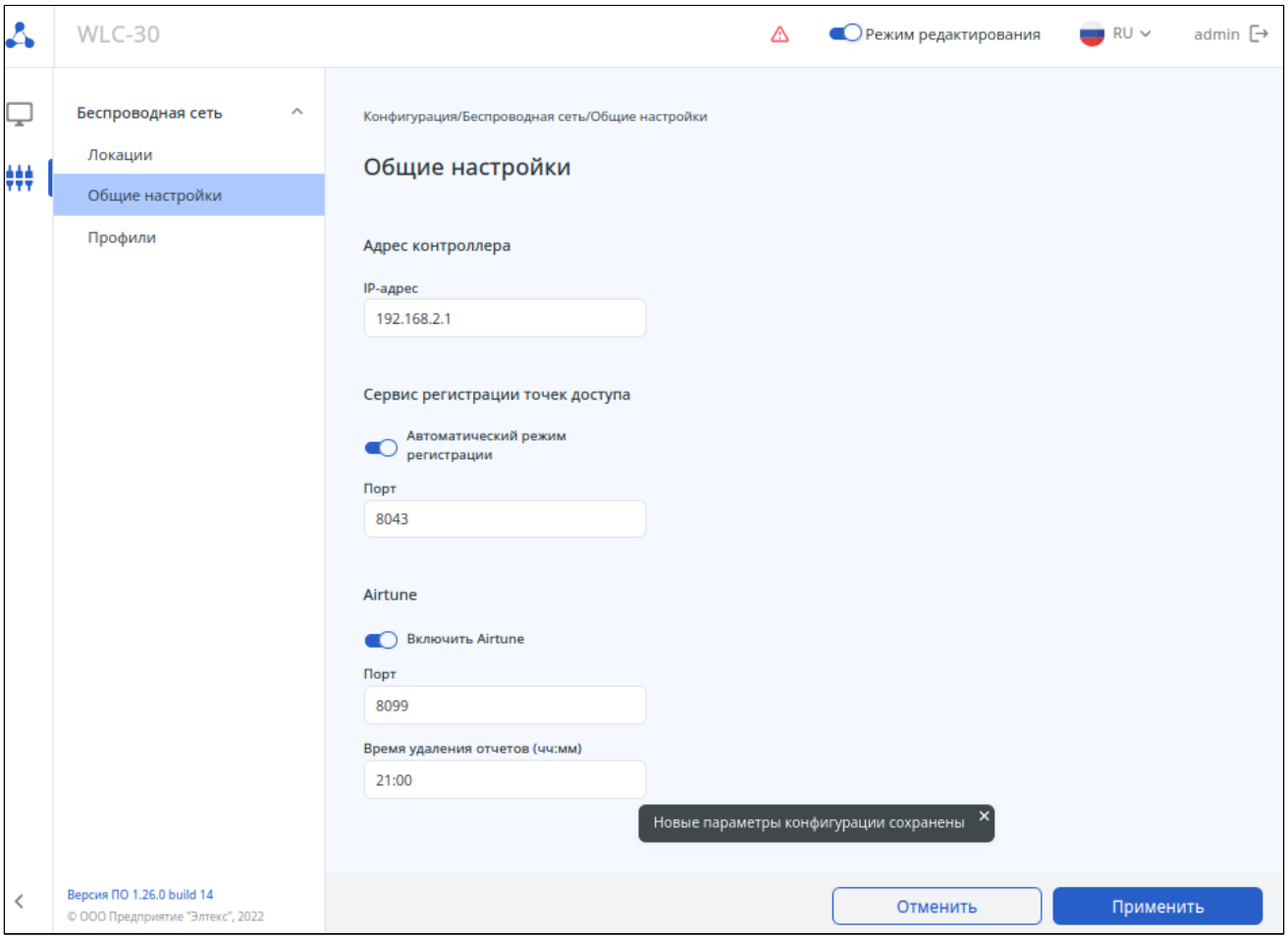
Режим редактирования

Для внесения изменений в конфигурацию необходимо включить режим редактирования переключателем на верхней панели страницы, по умолчанию данный режим отключен. После включения режима редактирования станет доступно изменение параметров.



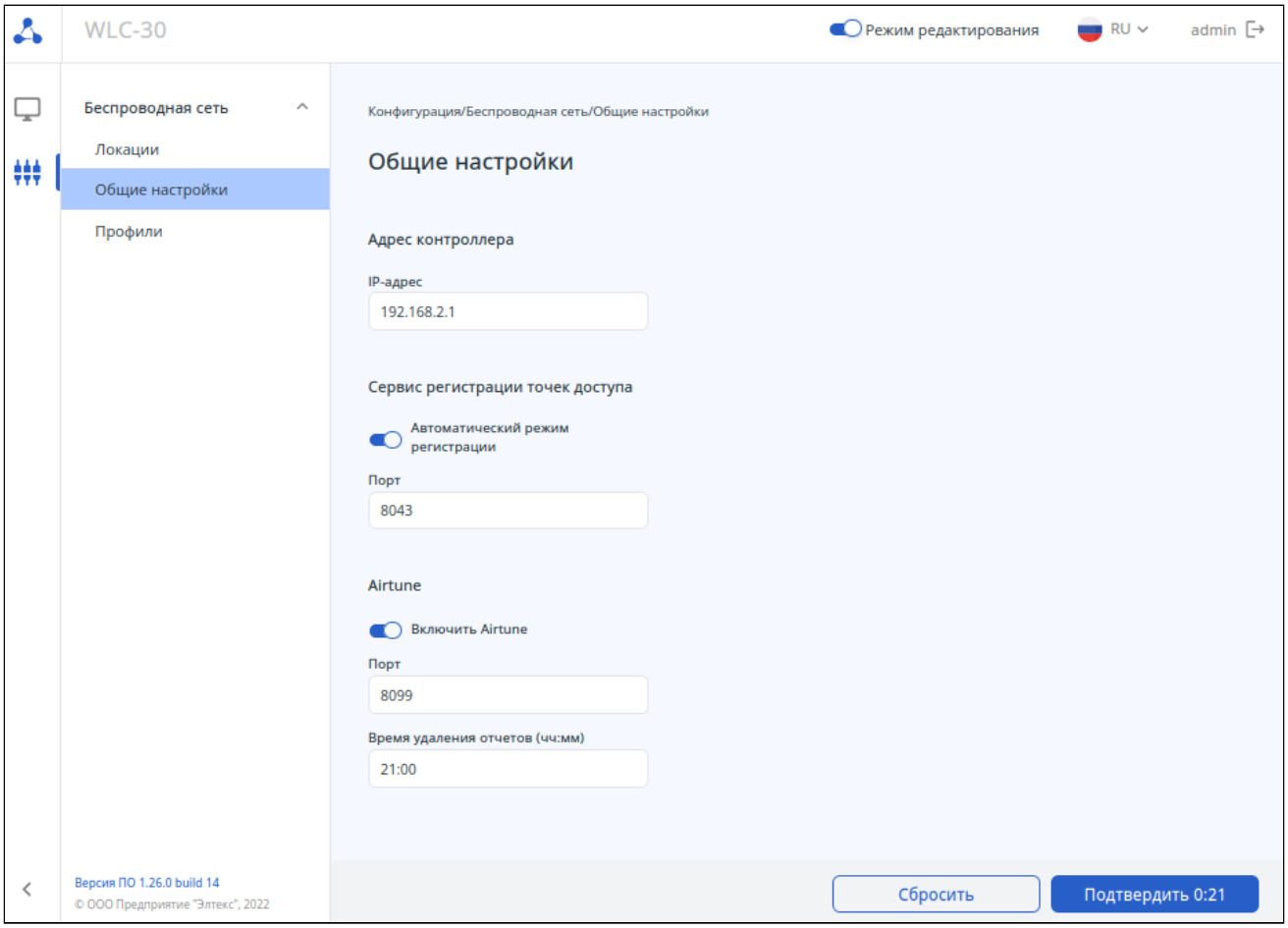
Сохранение изменений

После внесения изменений в правом нижнем углу страницы появится всплывающая кнопка «Сохранить», при нажатии на которую все изменения записываются в CANDIDATE конфигурацию.



Наличие любых изменений в текущей конфигурации отражается на верхней панели страницы с помощью иконки  .

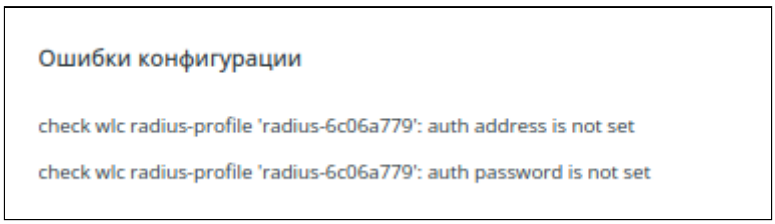
После сохранения настроек необходимо применить конфигурацию с помощью кнопки «Применить». Кнопка «Отменить» позволяет удалить все внесённые изменения.



После нажатия кнопки «Применить» запускается таймер, в течение которого действуют внесенные изменения. Чтобы полностью сохранить изменения необходимо нажать кнопку «Подтвердить».

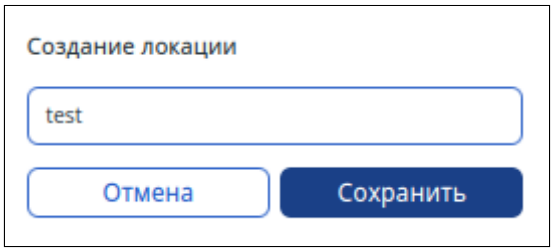
Кнопка «Сбросить» используется для отмены действия внесенных изменений. После окончания таймера внесённые изменения также будут отменены автоматически. Следует учитывать, что изменения при этом остаются в CANDIDATE конфигурации и могут быть снова применены с помощью кнопки «Применить» или могут быть удалены с помощью кнопки «Отменить».

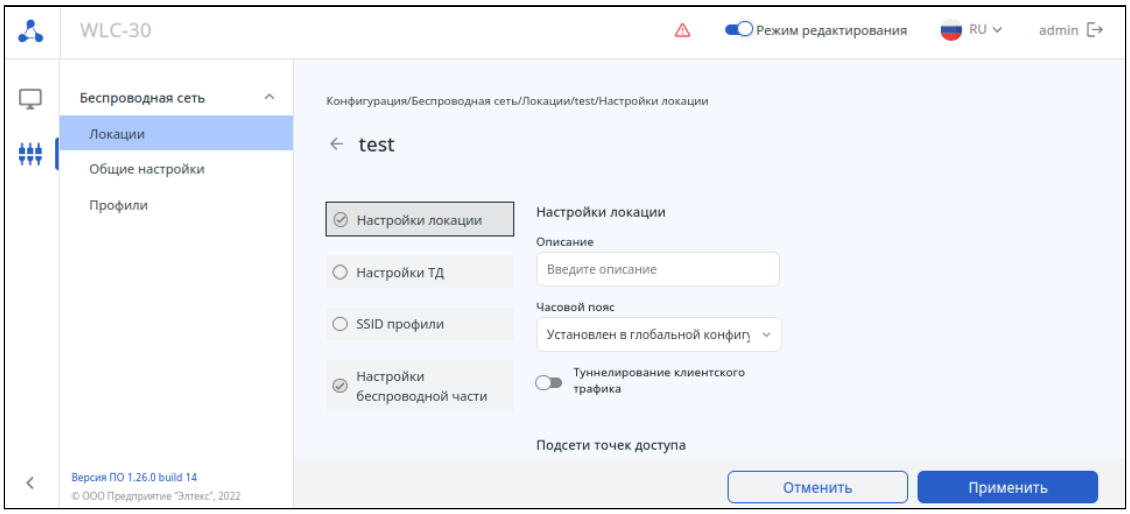
Если конфигурация не может быть применена по каким-то причинам, например, заданы некорректные параметры или не заданы обязательные параметры, появится всплывающее окно со списком обнаруженных проблем, которые необходимо исправить для успешного применения конфигурации. Пример всплывающего окна представлен на рисунке ниже.



Общие принципы создания объектов

Для создания новых объектов конфигурации (локации, профили и т. д.) используется кнопка «Создать». Пример представлен на рисунке ниже:



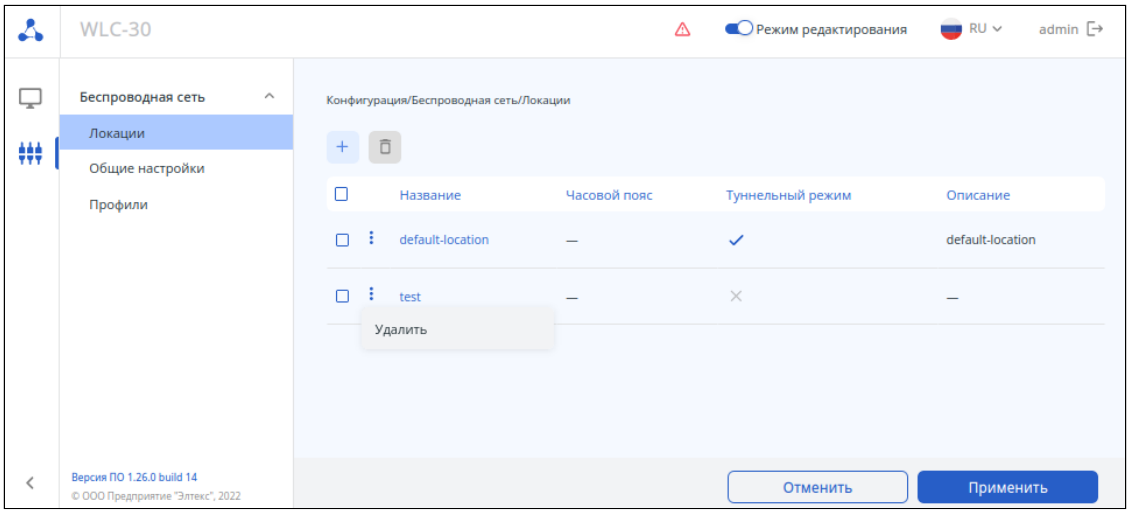


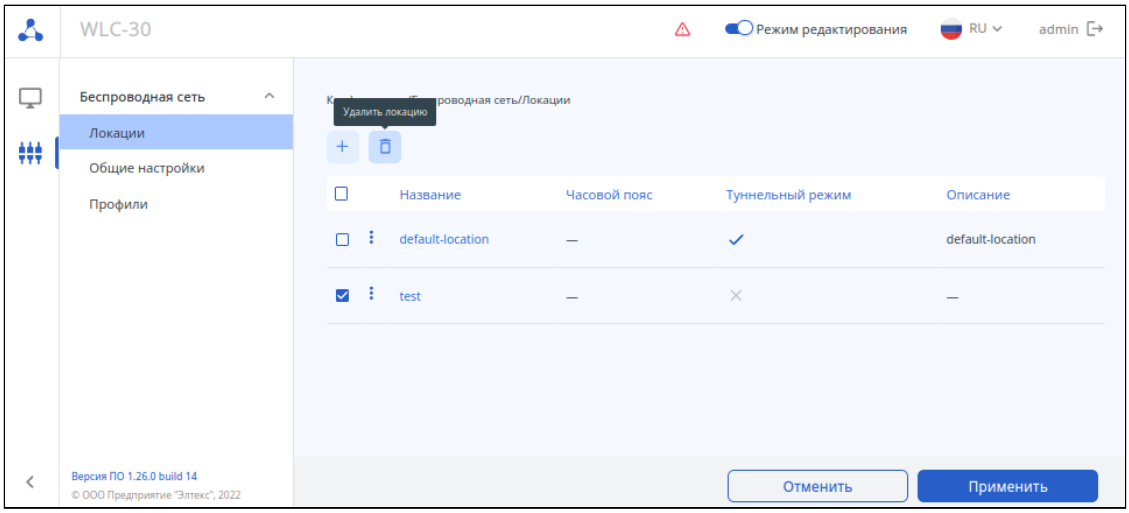
После создания объекта автоматически осуществляется переход на страницу его настройки.

Для удаления объекта конфигурации используются следующие варианты:

- Контекстное меню, кнопка вызова которого располагается слева от названия объекта. В открывшемся списке действий необходимо выбрать пункт «Удалить»;
- Кнопка «Удалить локацию»/«Удалить профиль». С помощью чекбоксов можно выбрать один, несколько или все объекты на странице, чтобы удалить их одновременно.

Примеры представлены на рисунках ниже:





Меню «Беспроводная сеть»

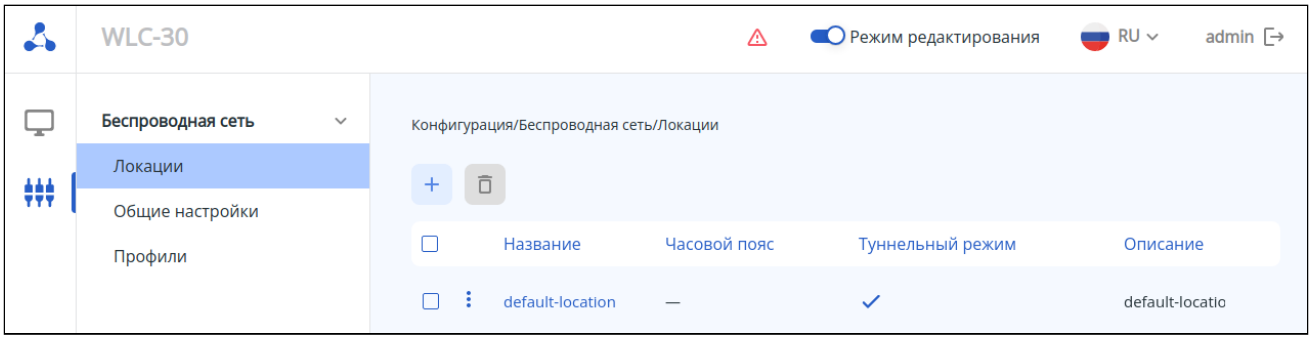
Подменю «Локации»

На странице «Локации» представлены локации, имеющиеся в конфигурации. В таблице содержатся основные настройки для каждой локации.

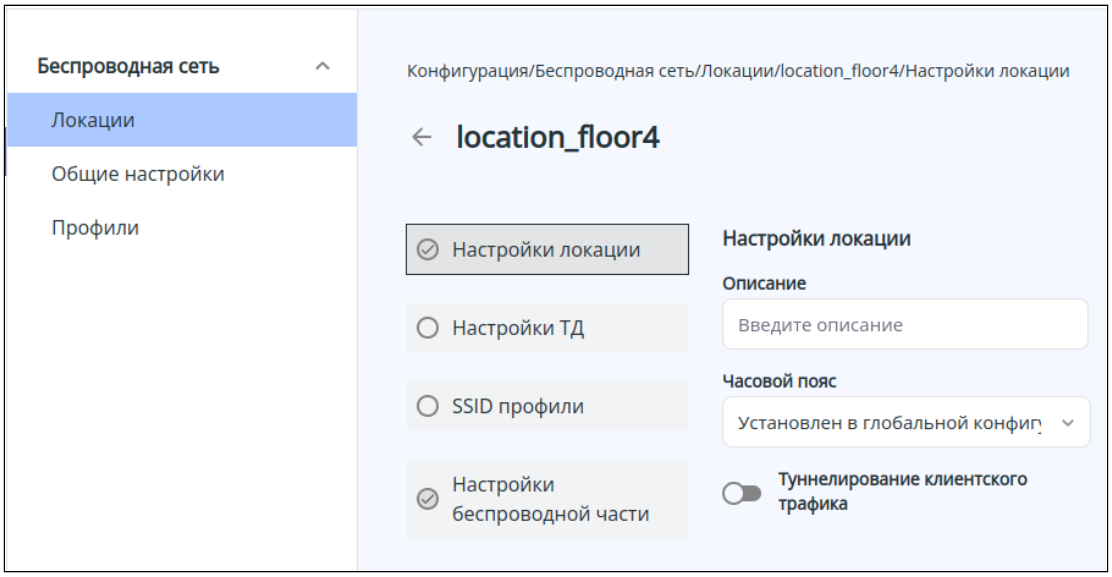
> Для создания, удаления и редактирования локации должен быть включен режим редактирования.

В таблице содержатся основные параметры для каждой локации, такие как:

- Название локации
- Часовой пояс
- Статус работы туннельного режима
- Описание локации



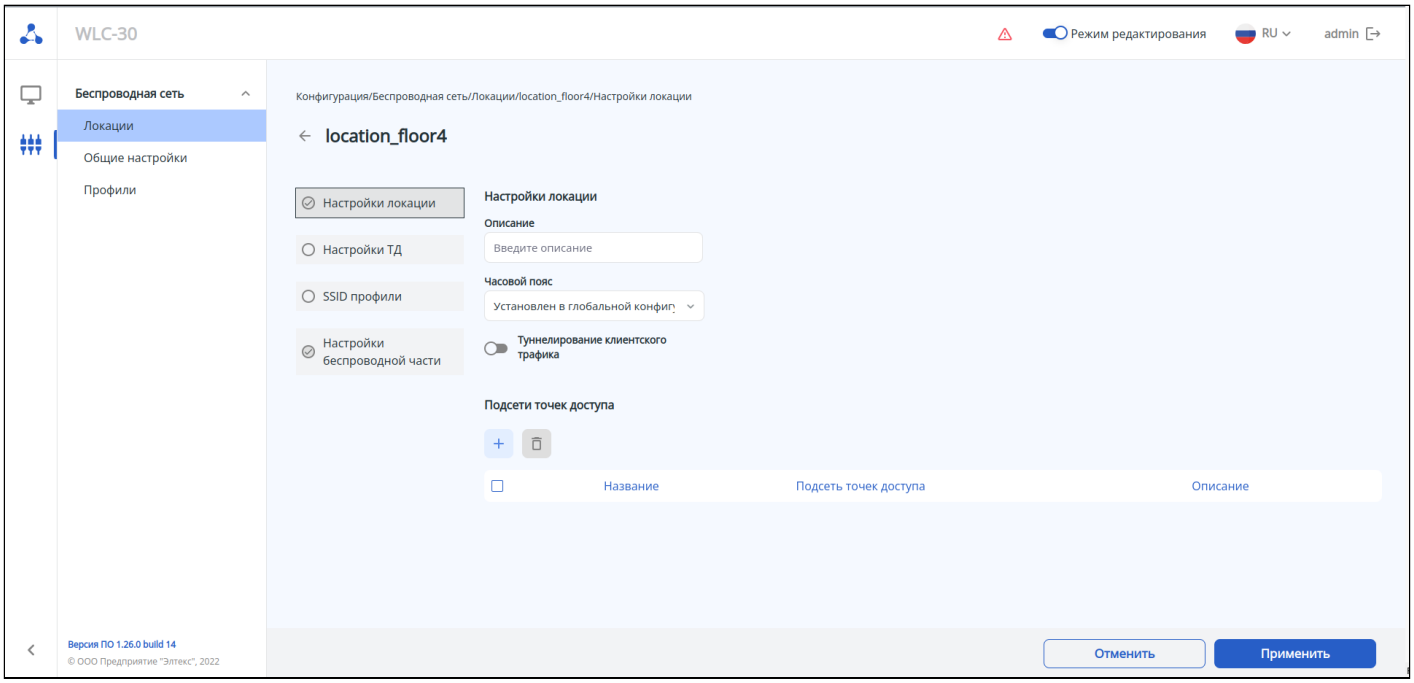
Для редактирования существующей локации нажмите на ее название в списке. Настройка локации разделена на несколько шагов, выполнять шаги можно в произвольном порядке.



В заводской конфигурации создана локация с названием «default-location» со следующими настройками:

- Описание: default-location
- Туннелирование клиентского трафика: включено
- Настройки ТД: выбран профиль default-ap
- SSID профили: выбран профиль default-ssid с Enterprise авторизацией на локальном сервере RADIUS
- Радиопрофили: выбраны профили default_2g и default_5g
- Профиль Airtune: выбран профиль default_airtune
- Подсети точек доступа: ТД любой подсети будут конфигурироваться по настройкам этой локации.

Настройки локации



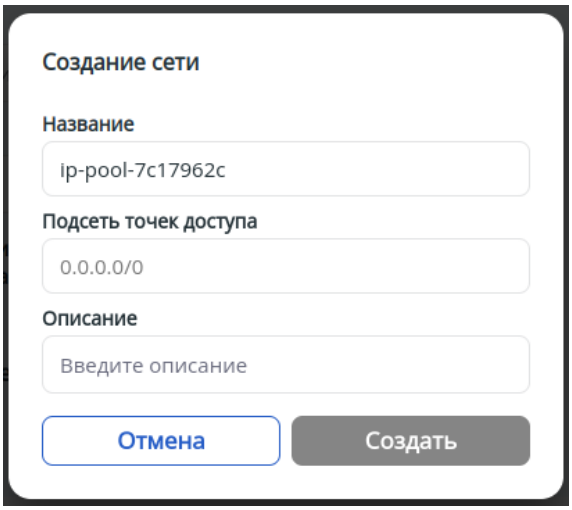
Данный шаг содержит общие настройки для локации:

- *Описание* – описание для локации. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Часовой пояс* – часовой пояс для выбранной локации. Оптимизация Airtune и обновление по расписанию ТД будут запускаться с учетом часового пояса. Возможные значения: от -12 до +12. Значение по умолчанию: часовой пояс установлен из конфигурации устройства.

- *Туннелирование клиентского трафика* − данный параметр позволяет включить режим работы с использованием туннелей SoftGRE Data для ТД находящихся в этой локации. Возможные значения: включено/отключено. Значение по умолчанию: отключено.

Подсети точек доступа

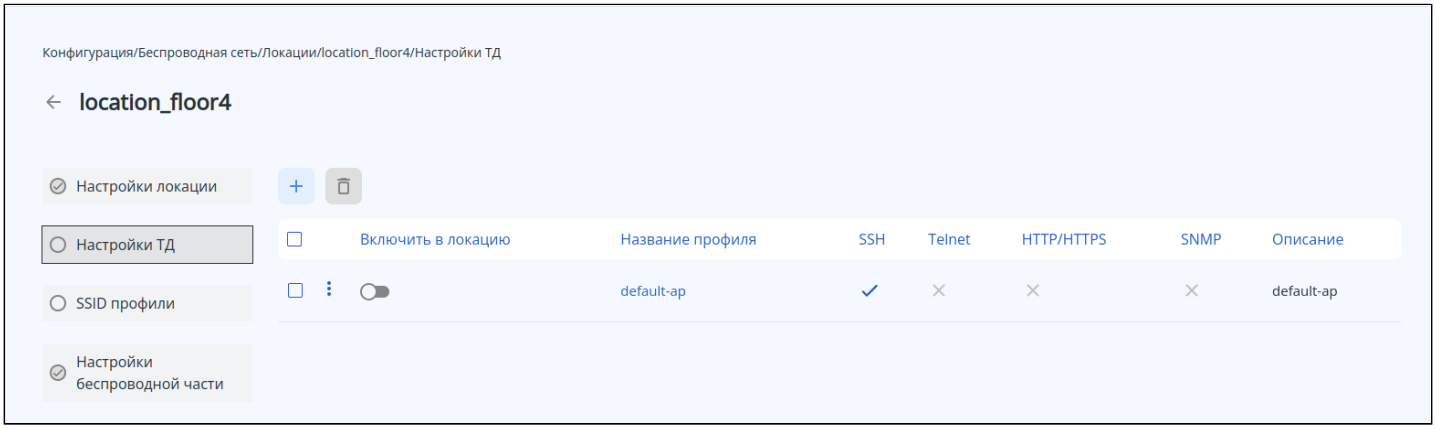
Данный раздел позволяет определить подсети ТД, которые будут конфигурироваться по правилам данной локации. Для создания новой подсети используйте кнопку «Создать подсеть ТД».



В открывшемся окне доступны следующие параметры:

- *Название* − название подсети. По умолчанию название генерируется автоматически, при необходимости его можно изменить;
  Подсеть точек доступа − подсеть ТД, параметр является обязательным. Если адрес точки доступа принадлежит указанной подсети, то точка доступа при регистрации попадет в данную локацию и будет сконфигурирована согласно набору включенных в локацию профилей конфигурации. Одна и та же подсеть не может быть настроена для разных локаций. Использование подсети 0.0.0.0/0 позволяет добавить в данную локацию точки доступа из любой
- подсети;
- *Описание* − описание для подсети.

Настройки ТД



На данном шаге в локацию добавляется профиль с настройками ТД. Наличие данного профиля в локации является обязательным.

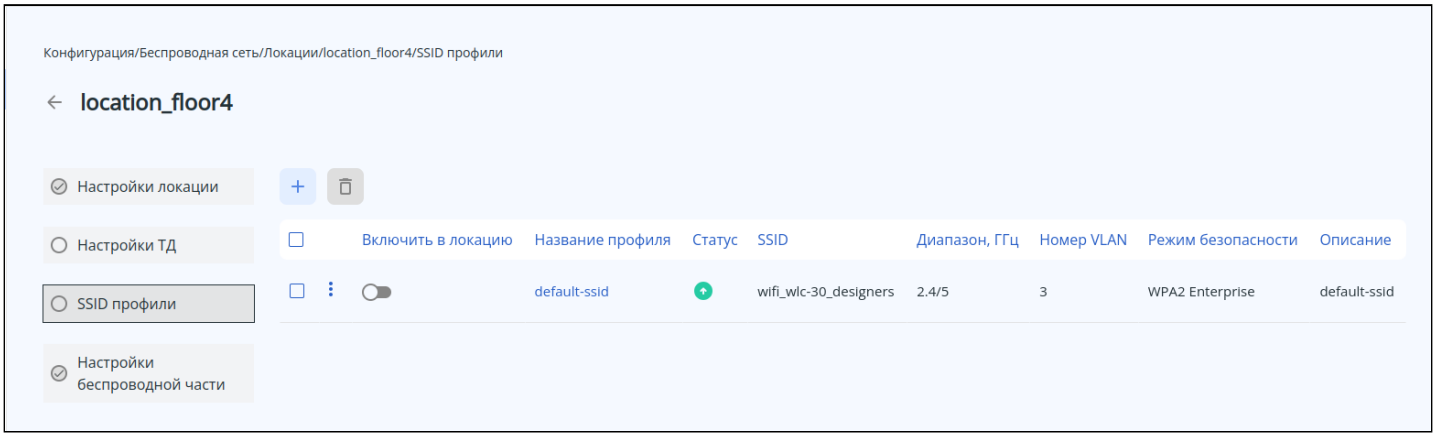
Для добавления существующего профиля в локацию используется переключатель «Включить в локацию».

На странице в таблице представлены основные настройки каждого профиля. Полные настройки профиля содержат:

- Пароль для доступа к ТД
- Настройки сервисов доступа ТД (HTTP/HTTPS/SSH/Telnet/SNMP)
- Настройки логирования различных сервисов ТД
- Настройки выгрузки логов с ТД на TFTP-сервер

При необходимости можно отредактировать существующий профиль, нажав на его название, или создать новый.
Процедура создания и описание параметров доступны в меню «Профили/Настройки ТД».

SSID профили



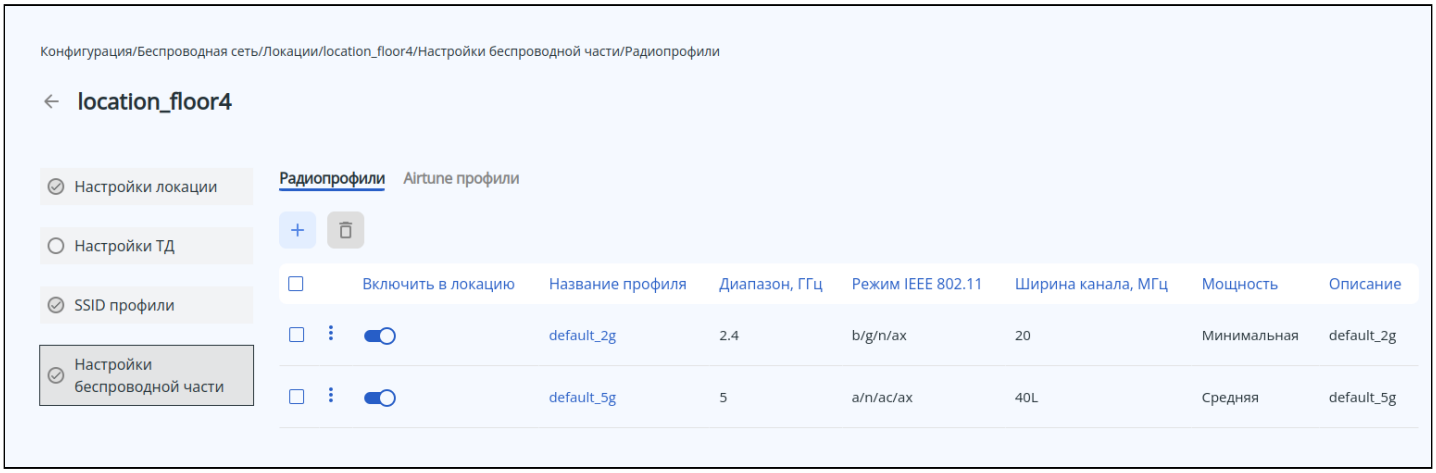
SSID-профиль может быть добавлен в локацию. Для этого используется переключатель «Включить в локацию».

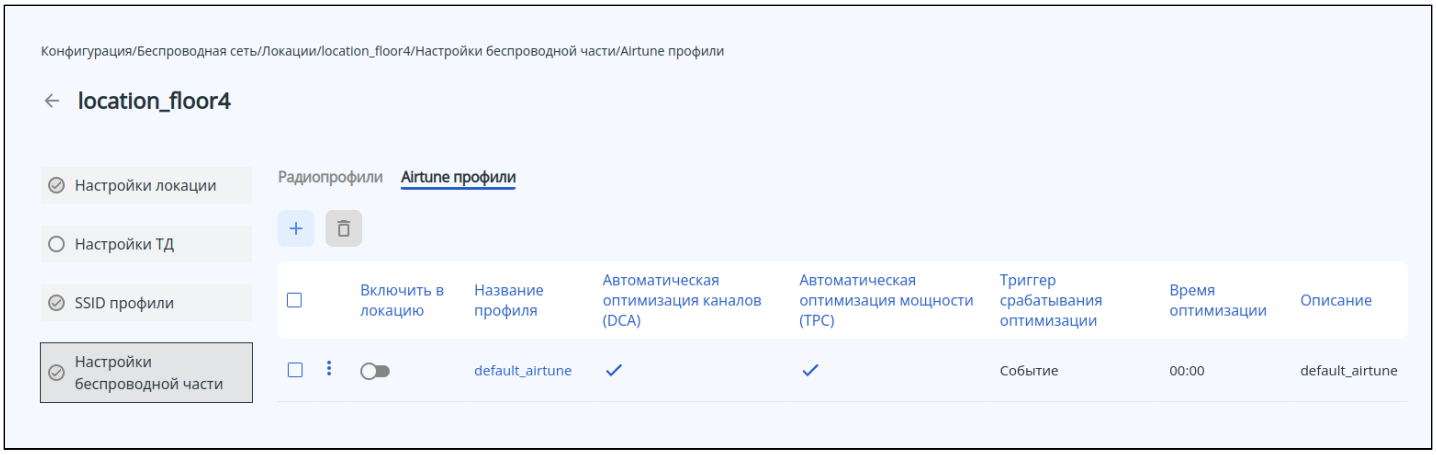
Основные настройки профиля SSID представленные в таблице:

- Название сети (SSID)
- Статус работы SSID
- Режим безопасности
- Диапазон вещания
- Номер VLAN

При необходимости можно отредактировать существующий профиль, нажав на его название, или создать новый.
Процедура создания и описание параметров доступны в меню «Профили/SSID профили».

Настройки беспроводной части





Для добавления в локацию радиопрофилей и airtune-профилей используются переключатели «Включить в локацию».

Наличие в локации радиопрофилей для каждого диапазона является обязательным. Наличие airtune-профиля указывает на то, что некоторые параметры радиоинтерфейсов точек доступа в данной локации будут находиться под управлением airtune (если airtune также включен глобально на странице «Общие настройки»). Соответственно, когда airtune включен в локации, менять параметры, связанные с мощностью и радиоканалами в радиопрофилях этой локации нецелесообразно, т.к. они не будут применены на точки доступа потому, что эти параметры автоматически настраиваются через airtune. При необходимости изменить ширину канала или список каналов для автовыбора на точках доступа, необходимо сначала отключить airtune, применить изменения, а затем снова включить airtune для автоматического управления каналами в соответствии с новыми настройками.

При необходимости можно отредактировать любой существующий профиль, нажав на его название, или создать новый.
Процедура создания радиопрофилей и описание параметров доступно в меню «Профили/Радиопрофили». Процедура создания aitune профилей и описание параметров доступны в меню «Профили/Airtune профили».

Подменю «Профили»

SSID

На данной странице в виде таблицы представлены SSID-профили, имеющиеся в конфигурации. Профили SSID предназначены для создания беспроводных сетей с различными типами авторизации для пользователей.

> ⓘ Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

В таблице содержатся основные настройки для каждого SSID-профиля, такие как:

- Название профиля
- Статус
- SSID
- Диапазон, ГГц
- Номер VLAN
- Режим безопасности
- Описание

В заводской конфигурации устройства уже создан SSID-профиль со следующими параметрами:

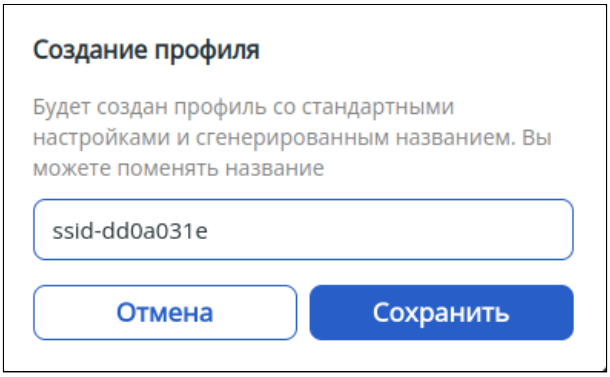
Общие настройки:

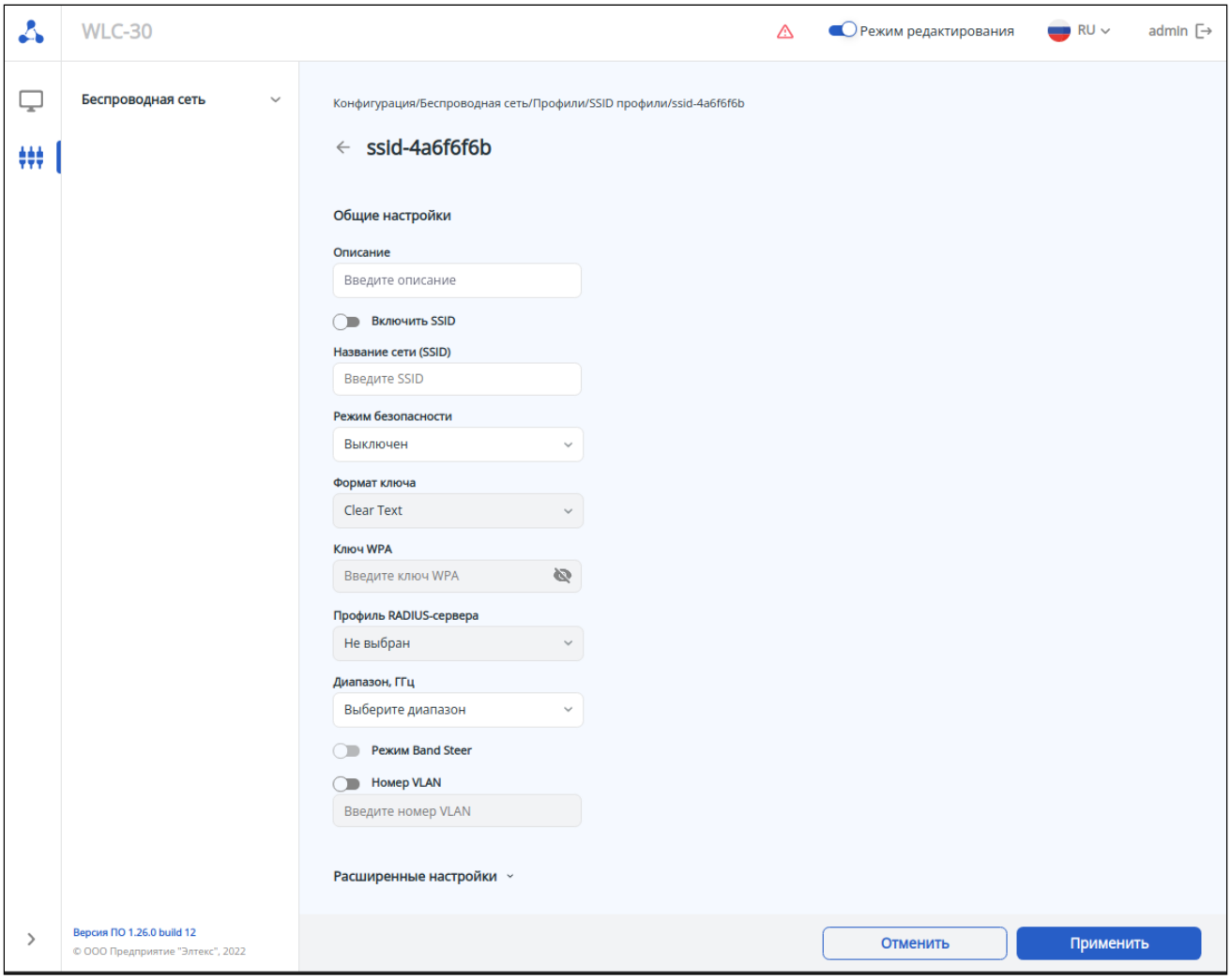
- Описание: default-ssid
- Статус: включен
- Название сети (SSID): default-ssid
- Режим безопасности: WPA2 Enterprise
- Профиль RADIUS-сервера: default-radius
- Диапазон, ГГц: 2.4/5
- Режим Band Steer: отключено
- Номер VLAN: 3

Расширенные настройки:

- Транслировать SSID: включено
- Максимальное количество клиентов: отключено
- Изоляция клиентских станций: отключено
- Поддержка 802.11kv: включено
- Поддержка 802.11r: отключено
- Кэширование PMKSA: отключено
- Проверка уровня сигнала: отключено
- Интервал проверки сигнала, с: 10 сек
- Минимальный уровень сигнала, дБм: -100
- Порог уровня сигнала при роуминге, дБм: -100
- Режим транковой передачи VLAN: отключено
- Передача нетегированного трафика: отключено
- General VLAN ID: отключено
- Тип приоритета: 802.1p
- Приоритет 802.1p при передаче в Ethernet: auto
- Local Switching: отключено

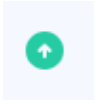
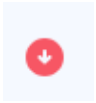
Для создания нового SSID-профиля используйте кнопку «Создать профиль». Откроется окно с предложением создать профиль со стандартными настройками и сгенерированным названием, которое можно изменить самостоятельно. После нажатия кнопки «Сохранить» откроется страница профиля для настройки параметров. При необходимости отмены создания нового профиля, используйте кнопку «Отмена».





Общие настройки

Раздел содержит следующие параметры:

- *Описание* − описание для SSID-профиля. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Включить SSID* − переключатель, который позволяет включить и выключить SSID-профиль. Возможные значения: включено/отключено. Значение по умолчанию: отключено.
  Если профиль включен, то в таблице профилей в столбце «Статус» отображается его наглядное цветовое обозначение:
  -  − SSID профиль включен
  -  − SSID профиль выключен
- *Название сети (SSID)* − название беспроводной сети, которая будет вещаться пользователям. Названия, содержащие пробел, необходимо заключать в кавычки. Возможные значения: строка до 32 символов. Значение по умолчанию: отсутствует.

  ⚠ Данный параметр является обязательным при создании SSID-профиля.
- *Режим безопасности* − определяет тип шифрования данных, используемый на виртуальной точке доступа. Значение по умолчанию: выключен.
  Возможные значения:
  - OWE
  - WPA PSK

- WPA2 PSK
- WPA3 PSK
- WPA/WPA2 PSK
- WPA2/WPA3 PSK
- WPA Enterprise
- WPA2 Enterprise
- WPA3 Enterprise
- WPA/WPA2 Enterprise
- WPA2/WPA3 Enterprise
- Выключен

> ⚠ Режимы безопасности WPA3 и WPA3 Enterprise поддерживается только на точках доступа моделей WEP-3ax, WEP-30L, WOP-30L, WOP-30LS.
> При выборе смешанного режима безопасности, содержащего WPA3 (например, WPA2/WPA3), он будет применен только на те точки доступа, которые поддерживают WPA3, для остальных будет применен максимально поддерживаемый режим, в данном случае WPA2.
> При выборе режима безопасности только с WPA3 – SSID будет применен только на те точки доступа, которые его поддерживают. На остальные точки доступа SSID не будет применен.

- *Формат ключа* – параметр, определяющий в каком формате далее будет задан ключ WPA. Значение по умолчанию: Clear-Text
  Возможные значения:
  - Clear-Text
  - Encrypted
- *Ключ WPA* – ключ для подключения к SSID, используется при выборе режима безопасности PSK. Ключ может быть задан как в открытом виде, так и в виде хеш sha512. Значение по умолчанию: отсутствует.
  Возможные значения:
  - если выбран формат ключа Clear-Text – ключ задаётся строкой от 8 до 63 символов
  - если выбран формат ключа Encrypted – задается хеш ключа по алгоритму sha512 строкой от 16 до 126 символов

  Иконка  используется, чтобы скрыть символы ключа при вводе, независимо от его формата.
- *Профиль RADIUS-сервера* – параметр позволяет выбрать созданный ранее профиль RADIUS-сервера, если используется режим безопасности Enterprise, а также позволяет создать и настроить новый профиль.
  Возможные значения для названия профиля: строка до 235 символов. Значение по умолчанию: отсутствует.

> ⓘ Для того чтобы создать и настроить новый профиль RADIUS, необходимо в раскрывающемся списке выбрать пункт «Создать новый RADIUS профиль».

> ⚠ Профиль RADIUS-сервера возможно задать только если выбран один из режимов безопасности:
> - WPA Enterprise
> - WPA2 Enterprise
> - WPA3 Enterprise
> - WPA/WPA2 Enterprise
> - WPA2/WPA3 Enterprise

- *Диапазон, ГГц* – выбор диапазона частот, в котором будет вещать SSID на беспроводной точке доступа. Возможные значения: 2.4 ГГц, 5 ГГц, 2.4 ГГц и 5 ГГц одновременно. Значение по умолчанию: отсутствует.

> ⚠ Профиль RADIUS-сервера возможно задать только если выбран один из режимов безопасности: является обязательным параметром при создании SSID-профиля.

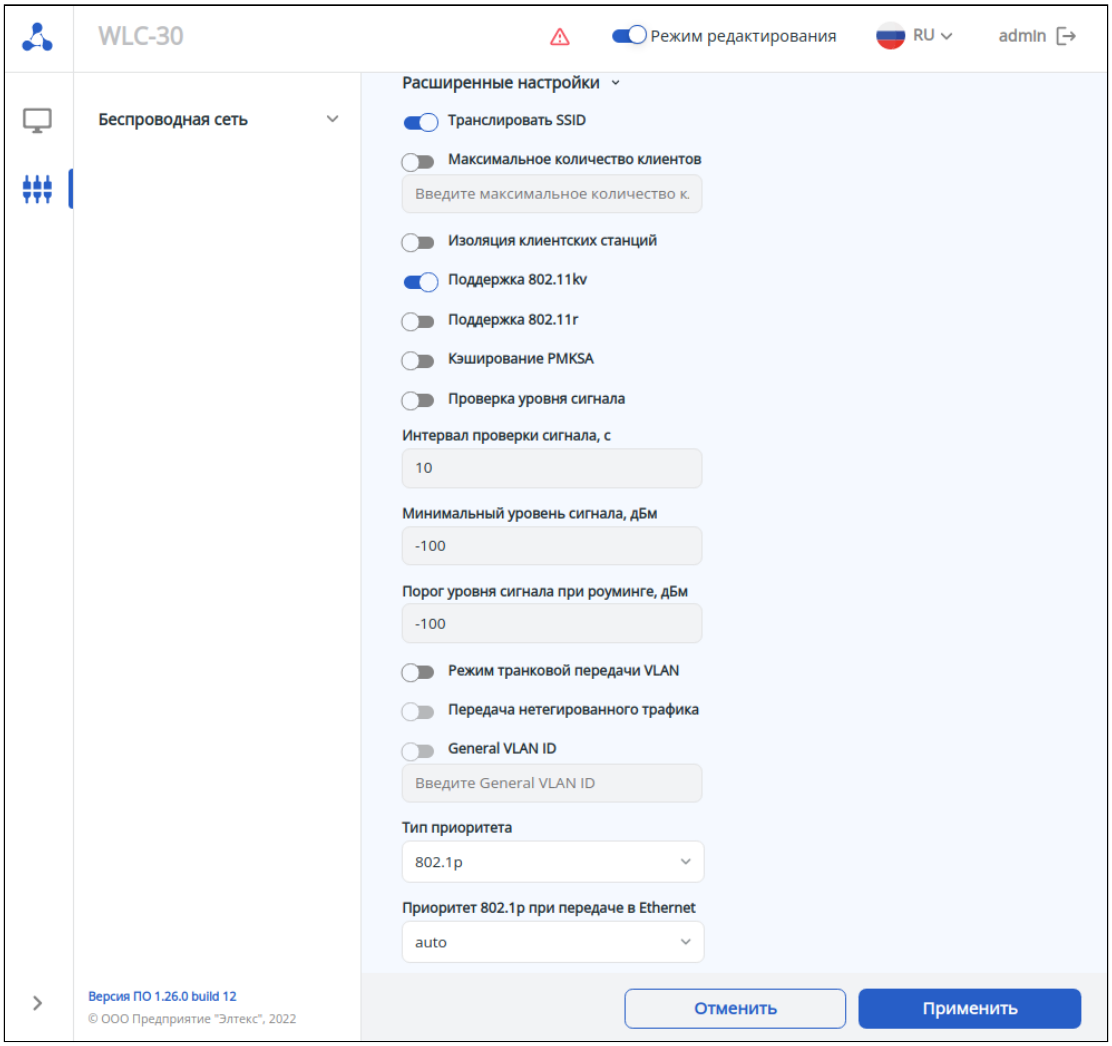
- *Режим Band Steer* – переключатель активирует на точках доступа функцию приоритетного подключения двухдиапазонных беспроводных клиентов к сети в 5 ГГц. Возможные значения: включено/отключено. Значение по умолчанию: отключено.

> ⚠ Для работы функции необходимо, чтобы в профиле SSID были включены оба диапазона: 2.4 ГГц и 5 ГГц.

- *Номер VLAN* – идентификатор VLAN, с которого будет сниматься метка при передаче трафика Wi-Fi клиентам, подключенным к данному SSID. При прохождении трафика в обратную сторону на нетегированный трафик от клиентов будет навешиваться метка VLAN ID (при отключенном режиме VLAN Trunk). Возможные значения: от 1 до 4094. Значение по умолчанию: отключено.

Расширенные настройки

Раздел с расширенными настройками находится внизу страницы и его параметры по умолчанию скрыты. Для доступа к расширенным настройкам используйте кнопку .



Раздел содержит следующие параметры:

- *Транслировать SSID* – переключатель позволяет включить или выключить вещание в эфир SSID. Возможные значения: включено/отключено. Значение по умолчанию: включено;

- *Максимальное количество клиентов* – с помощью параметра включается и задается ограничение максимального количества клиентских устройств, которые могут подключиться к виртуальной точке доступа. Возможные значения: от 1 до 64. Значение по умолчанию: ограничение отключено;
- *Изоляция клиентских станций* – переключатель активирует изоляцию трафика между клиентами в пределах одной виртуальной точки доступа. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Поддержка 802.11kv* – переключатель управляет поддержкой стандартов 802.11k/v на виртуальной точке доступа. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Поддержка 802.11r* – переключатель управляет поддержкой стандарта 802.11r на виртуальной точке доступа. Настройка доступна только при режимах безопасности: WPA2, WPA3, WPA2/WPA3, WPA2-Enterprise, WPA3-Enterprise, WPA2/WPA3-Enterprise. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Кэширование PMKSA* – переключатель 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. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Проверка уровня сигнала* – переключатель позволяет включить или выключить периодическую проверку сигнала. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Интервал проверки сигнала, с* – параметр определяет время, через которое будет производиться периодическая проверка сигнала. Возможные значения: 1-300 секунд. Значение по умолчанию: 10 секунд. Настройка доступна при включенной проверке уровня сигнала;
- *Минимальный уровень сигнала, дБм* – пороговое значение RSSI, при достижении которого точка доступа будет отключать клиента от виртуальной точки доступа. Возможные значения: от -100 до -1 дБм. Значение по умолчанию: -100 дБм. Настройка доступна при включенной проверке уровня сигнала;
- *Порог уровня сигнала при роуминге, дБм* – уровень RSSI, при достижении которого будет срабатывать роуминг. Параметр должен быть выше, чем «*Минимальный уровень сигнала*». Возможные значения: от -100 до -1 дБм. Значение по умолчанию: -100 дБм. Настройка доступна при включенной проверке уровня сигнала;
- *Режим транковой передачи VLAN* – переключатель позволяет включить передачу тегированного трафика клиенту. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Передача нетегированного трафика* – переключатель управляет возможностью передачи нетегированного трафика клиенту совместно с тегированным. Настройка доступна только при включенном режиме транковой передачи VLAN. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *General VLAN ID* – переключатель активирует использование General VLAN ID. Настройка доступна только при включенном режиме транковой передачи VLAN и передаче нетегированного трафика. В режиме транковой передачи с одного указанного VLAN ID будет сниматься метка и трафик этого VLAN пройдет на клиента без тега. При прохождении трафика в обратную сторону на нетегированный трафик будет навешиваться метка General VLAN ID. Возможные значения: от 0 до 4094. Значение по умолчанию: отключено;
- *Тип приоритета* – выбор способа приоритизации. Определяет поля из заголовков пакетов, на основании которого трафик, передающий в радиоинтерфейс, будет распределяться по очередям WMM. Значение по умолчанию: 802.1p. Возможные значения:
    - 802.1p – будет анализироваться приоритет из поля CoS (Class of Service) тегированных пакетов;
    - DSCP – будет анализироваться приоритет из поля DSCP заголовка IP-пакета. При этом если значение DSCP в тегированных кадрах равно 0, то анализироваться будет приоритет из поля CoS (Class of Service).

- *Приоритет 802.1p при передаче в Ethernet* – приоритет второго уровня, который будет назначаться на пакеты, приходящие от клиента, подключенного к данному SSID, и передаваться далее в проводную сеть. Возможные значения:
  - auto – приоритет, указанный в заголовке пакета не будет изменен;
  - значения от 0 до 7, которые будут установлены, независимо от приоритета в поступившем пакете.
- *Local Switching* – активирует функцию local-switching, клиентский трафик не будет туннелироваться для данного SSID, если используется схема с туннелированием. Возможные значения: включено/отключено. Значение по умолчанию: отключено.

После настройки параметров сохраните, а затем примените и подтвердите изменения конфигурации с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

Настройки ТД

На данной странице представлены в виде таблицы профили настроек точек доступа, имеющиеся в конфигурации. Данные профили позволяют управлять доступом к ТД, настраивать пароль и управлять сервисами SSH, Telnet, HTTP/HTTPS, SNMP, а также включать и настраивать логирование внутренних сервисов ТД и выгрузку логов с ТД на TFTP-сервер.

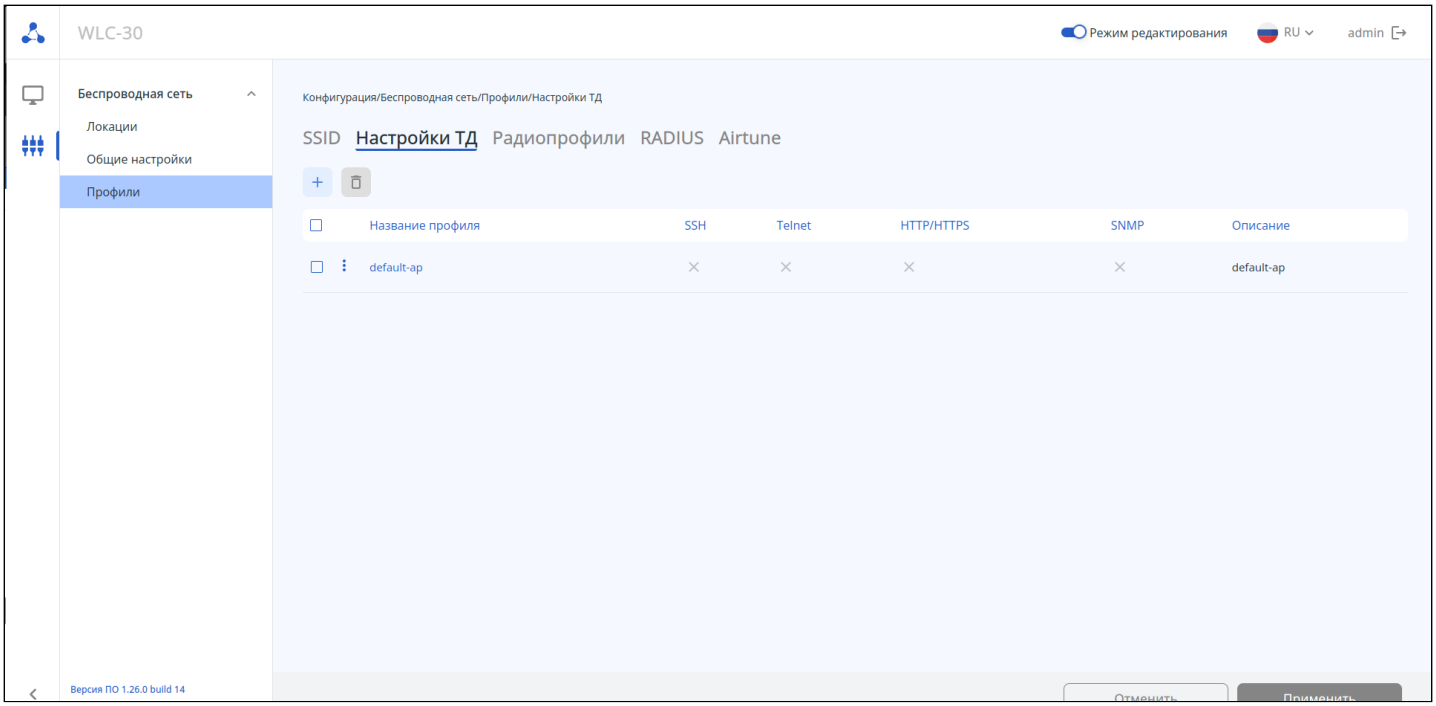
> ⓘ Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

В таблице содержатся основные параметры для каждого профиля, такие как:

- Название профиля
- Статус работы сервиса SSH на ТД
- Статус работы сервиса Telnet на ТД
- Статус работы сервисов HTTP/HTTPS на ТД
- Статус работы сервиса SNMP на ТД
- Описание профиля

Статусы сервисов **SSH/Telnet/HTTP/HTTPS/SNMP** отображаются иконками:

-  – сервис включен
-  – сервис выключен



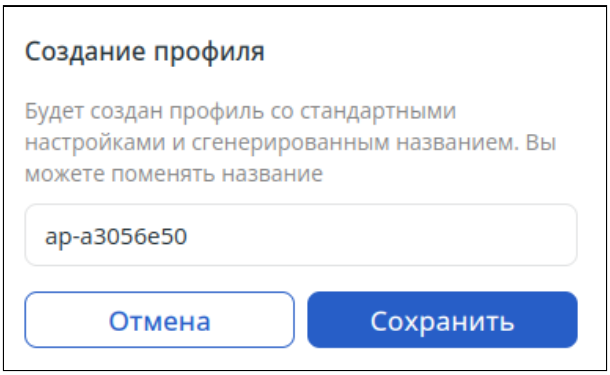
В заводской конфигурации уже создан профиль с названием «default-ap» со следующими параметрами:

- Описание: default_ap
- Формат пароля: Encrypted
- Пароль: 8CB5107EA7005AFF (password)
- SSH сервер: отключено
    - порт: 22
- Telnet сервер: отключено
    - порт: 23
- HTTP/HTTPS: отключено
    - HTTP порт: 80
    - HTTPS порт: 443
- SNMP: отключено
    - Пароль на чтение: public
    - Пароль на запись: private
    - Адрес для приема трапов v1: отсутствует
    - Адрес для приема трапов v2: отсутствует
    - Адрес для приёма сообщений Inform: отсутствует
- Syslog: отключено
    - Режим: Локальный файл
    - Адрес сервера: отсутствует
    - Порт сервера: 514
    - Размер файла, Кб: 1000
- Выгрузка лога на TFTP сервер: отключено
    - Адрес сервера: отсутствует
    - Максимальный размер файла: 10000
    - Период загрузки, с: 600
    - Количество попыток отправки: 3
- Настройки Trace: отключено у всех сервисов

⚠ В заводской конфигурации в профиле default-ap все сервисы **SSH/Telnet/HTTP/HTTPS/SNMP выключены.**

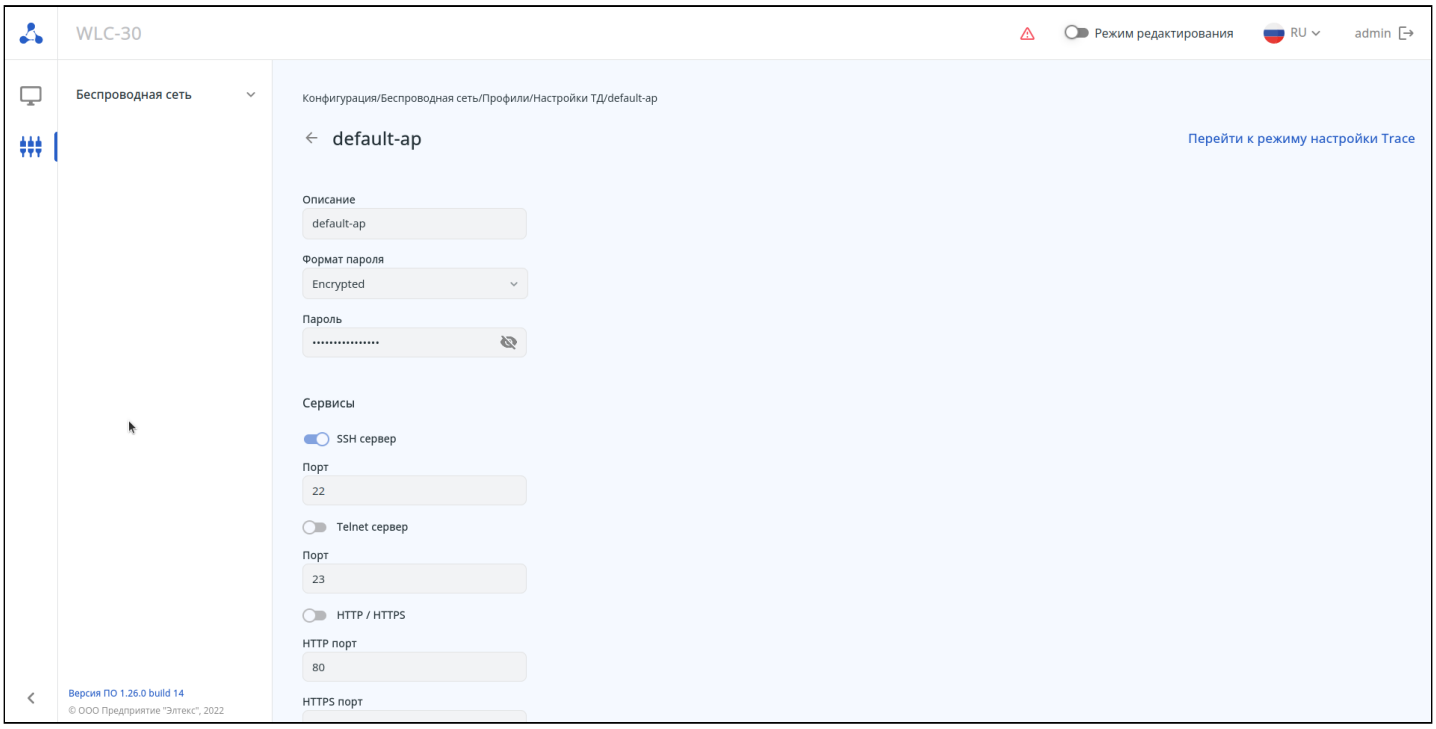
Для создания профиля «Настройки ТД» используйте кнопку «Создать профиль». Откроется окно с предложением создать профиль со стандартными настройками и сгенерированным названием, которое можно изменить самостоятельно. После нажатия кнопки «Сохранить» откроется страница профиля для

настройки параметров. При необходимости отмены создания нового профиля, используйте кнопку «Отмена».



Пароль является обязательным параметром и должен быть задан при создании профиля «Настройки ТД». Остальные параметры при отсутствии изменений будут созданы со значениями по умолчанию.
Более подробная информация описана в разделах «Профиль настроек ТД» и «Логирование сервисов ТД».

Профиль настроек ТД



Страница содержит следующие параметры:

- *Описание* – описание для профиля настроек точек доступа. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Формат пароля* – параметр, определяющий, в каком формате далее будет задан пароль для управления точкой доступа. Значение по умолчанию: Clear Text:
  Возможные значения:
  - Clear Text
  - Encrypted
- *Пароль* – пароль для управления точкой доступа. Значение по умолчанию: отсутствует;
  Возможные значения:
  - если выбран формат пароля Clear Text – пароль задаётся строкой от 8 до 64 символов;

- если выбран формат пароля Encrypted – задаётся хеш пароля по алгоритму sha512 строкой от 16 до 128 символов.

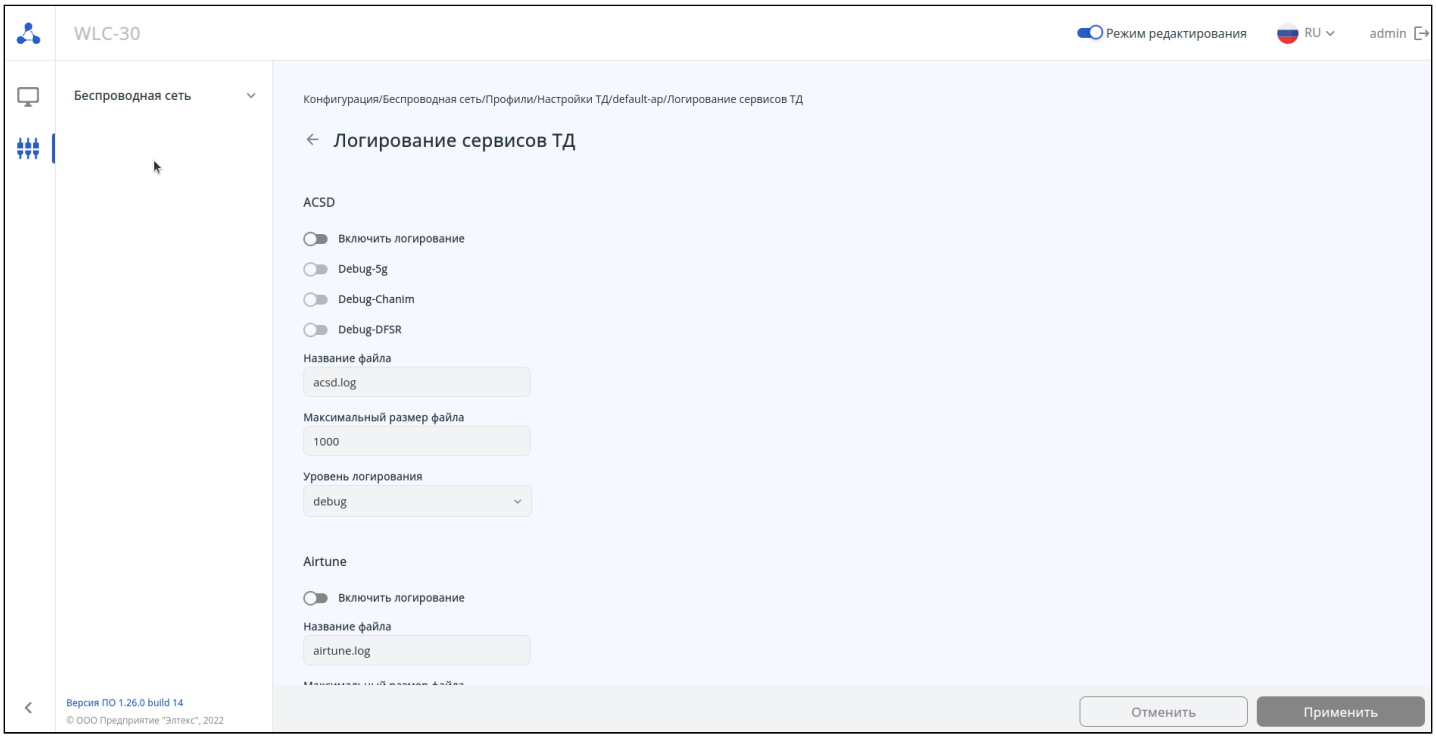
> ⚠ После сохранения конфигурации формат поля принудительно становится Encrypted и далее пароль будет отображаться и храниться в хешированном виде.

- *Сервисы:*
  - *SSH Сервер* – переключатель управляет возможностью подключения к точке доступа через протокол SSH. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
    - *Порт* – порт для подключения к точке доступа через протокол SSH. Значение по умолчанию: 22. Возможные значения: от 1 до 65535.
  - *Telnet сервер* – переключатель управляет возможностью подключения к точке доступа через протокол telnet. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
    - *Порт* – порт для подключения к точке доступа через протокол telnet. Значение по умолчанию: 23. Возможные значения: от 1 до 65535.
  - *HTTP/HTTPS* – переключатель управляет возможностью подключения к web-конфигуратору ТД через HTTP и HTTPS. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
    - *HTTP порт* – порт для подключения к web-конфигуратору ТД по HTTP. Значение по умолчанию: 80. Возможные значения: 80, от 1025 до 65535;
    - *HTTPS порт* – порт для подключения к web-конфигуратору ТД по HTTPS. Значение по умолчанию: 443. Возможные значения: 443, от 1025 до 65535.
  - *SNMP* – переключатель управляет работой сервиса SNMP на ТД. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
    - *Пароль на чтение* – параметр определяет community для доступа по протоколу SNMP в режиме "только для чтения". Значение по умолчанию: public. Возможные значения: строка от 1 до 128 символов;
    - *Пароль на запись* – параметр определяет community для доступа по протоколу SNMP в режиме "чтение и запись". Значение по умолчанию: private. Возможные значения: строка от 1 до 128 символов;
    - *Адрес для приёма трапов v1* – адрес хоста для работы с трапами протокола SNMP версии v1. Значение по умолчанию: отсутствует. Параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255;
    - *Адрес для приёма трапов v2* – адрес хоста для работы с трапами протокола SNMP версии v2. Значение по умолчанию: отсутствует. Параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255;
    - *Адрес для приёма сообщений Inform* – адрес хоста для работы с сообщениями типа Inform протокола SNMP. Значение по умолчанию: отсутствует. Параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255.
- *Syslog* – переключатель позволяет включить и выключить сервис syslog на точке доступа. Значение по умолчанию: включено. Возможные значения: включено/отключено:
  - *Режим* – выбор режима работы сервиса syslog на точках доступа. Значение по умолчанию: Локальный файл. Возможные значения:
    - *Локальный файл* – запись syslog будет производиться только в локальный файл на точке доступа в директории /var/log/;
    - *Сервер и файл* – syslog будет записываться в файл на точке доступа и отправляться на заданный syslog-сервер.
  - *Адрес сервера* – адрес syslog-сервера для отправки лога с точки доступа. Значение по умолчанию: отсутствует. Параметр задаётся в виде IP-адреса или доменного имени сервера;
  - *Порт сервера* – порт syslog-сервера для отправки лога с точки доступа. Значение по умолчанию: 514. Возможные значения: от 1 до 65535;
  - *Размер файла, Кб* – размер файла syslog на точке доступа, при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию. Значение по умолчанию: 1000 Кб. Возможные значения: от 1 до 1000 Кб.

- *Выгрузка лога на TFTP сервер* – переключатель позволяет включить и выключить автовыгрузку логов с точки доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
  - *Адрес сервера* – IP-адрес TFTP-сервера для автоматической выгрузки логов с точки доступа. Значение по умолчанию: отсутствует. Параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255;
  - *Максимальный размер файла* – пороговое значение размера папки с логами на точке доступа (/var/log/), при превышении которого логи будут автоматически выгружены на заданный TFTP-сервер при включенной выгрузке лога на TFTP-сервер. Значение по умолчанию: 10000 Кб. Возможные значения: от 0 до 20000 Кб;
  - *Период загрузки* – период отправки логов с точки доступа на TFTP-сервер при включенной выгрузке лога на TFTP-сервер. Значение по умолчанию: 600 с. Возможные значения: от 1 до 86400 с;
  - *Количество попыток отправки* – количество попыток повторной отправки логов с точки доступа на TFTP-сервер при включенной выгрузке лога на TFTP-сервер. Значение по умолчанию: 3. Возможные значения: от 0 до 5.

Логирование сервисов ТД

Страница настроек трассировки сервисов точек доступа открывается по ссылке «Перейти к режиму настройки Trace» в правом верхнем углу профиля настроек ТД.



В большинстве случаев сервисы ТД имеют одинаковые настройки логирования, но у некоторых сервисов есть и индивидуальные настройки. В общем случае настройка логирования любого сервиса содержит параметры:

- *Включить логирование* – переключатель позволяет включить и выключить логирование для каждого сервиса ТД. Значение по умолчанию: отключено у всех сервисов. Возможные значения: включено/отключено.
- *Название файла* – название файла лога сервиса. Файл создается на точке доступа при включении лога и находится в директории /var/log/. Возможные значения: название файла от 1 до 235 символов.
  Значение по умолчанию для каждого сервиса:
  ASCD – acsd.log
  Airtune – airtune.log
  Band Steer – bandsteerd.log
  Captive Portal – cportad.log

Captive Portal APBD – apbd.log
Captive Portal Tinyproxy – tinyproxy.log
ConfigD – configd.log
DMESG – dmesg.log
FTD – ftd.log
Hostapd – hostapd.log
MonitorD – monitord.log
Netconf – netconf.log
NetworkD – networkd.log
SNMP – snmp.log
WLC Service Activator – service-activator-wlc.log
WLC Service Activator Server – service-activator-server-wlc.log

- *Максимальный размер файла* – размер файла лога сервиса при превышении которого лог будет перезаписываться, чтобы обеспечить ротацию. Значение по умолчанию: 1000 Кб.
  Возможные значения: от 1 до 30000 Кб.
- *Уровень логирования* – уровень логирования сервиса. Параметр доступен для следующих сервисов ТД: **ACSD, Airtune, Band steer, Captive Portal, Captive Portal APBD, Hostapd, MonitorD, NetworkD.** Значение по умолчанию: debug.
  Возможные значения:
  error – лог будет записываться с уровнем error;
  warn – лог будет записываться с уровнем warning;
  info – лог будет записываться с уровнем info;
  debug – лог будет записываться с уровнем debug.

> У сервисов **Band Steer, Captive Portal** отсутствует логирование уровня **info.**

Индивидуальные настройки логирования сервисов:

- **ACSD**
  - **Debug-5g** – включает дополнительное логирование для модуля 5 GHz подсистемы автовыбора радиочастотного канала на точке доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено;
  - **Debug-Chanim** – включает дополнительное логирование для модуля chanim подсистемы автовыбора радиочастотного канала на точке доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено;
  - **Debug-DFSR** – включает дополнительное логирование для модуля DFSr подсистемы автовыбора радиочастотного канала на точке доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено.
- **Band Steer**
  - **Band Steer STA MAC** – параметр позволяет задать MAC-адрес клиентской станции Wi-Fi, для которой будет записываться лог подсистемы band steer на точке доступа. Значение по умолчанию: отсутствует. Возможные значения: MAC-адрес клиентской станции Wi-Fi в формате HH:HH:HH:HH:HH:HH
- **Captive Portal**
  - **Captive Portal Redirector Debug** – включает логирование модуля перенаправления запросов HTTP на точке доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено.

После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

Подробная информация по работе с конфигурацией устройства описана в разделе «Конфигурирование». После создания профиля, он отобразится в таблице профилей «Настройки ТД».

Радиопрофили

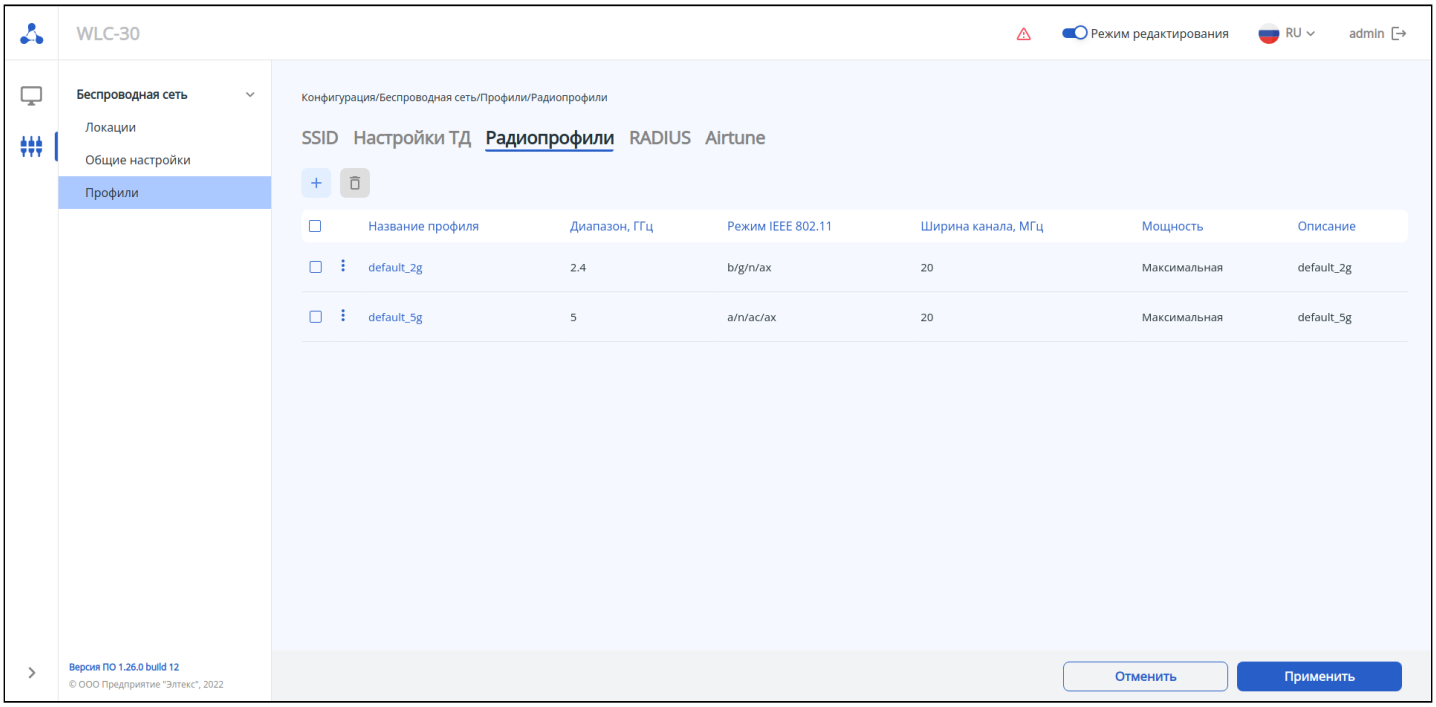
На странице в виде таблицы представлены профили настроек радиоинтерфейсов для точек доступа, имеющиеся в конфигурации.

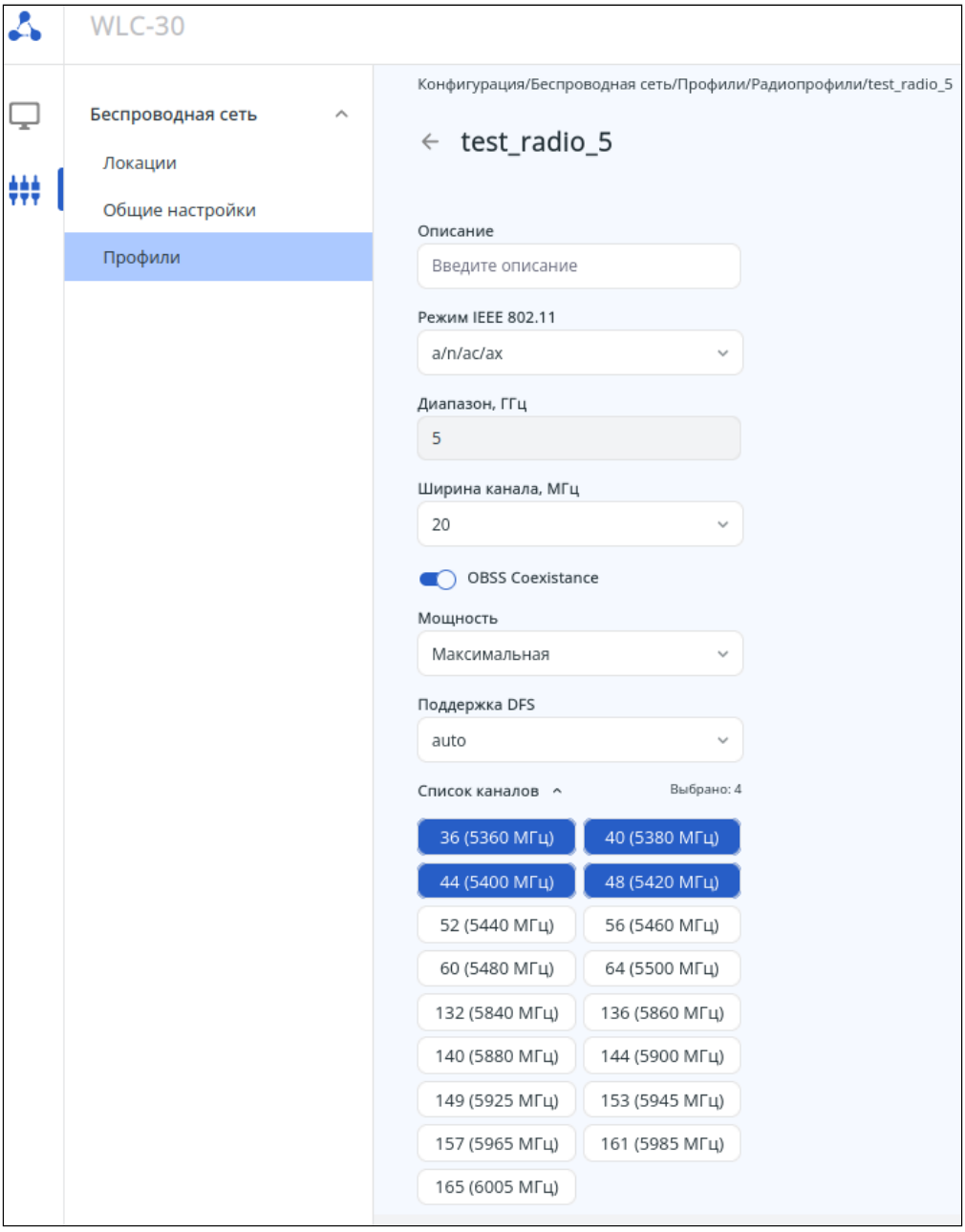
> Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

> Если в локацию добавлен Airtune-профиль, некоторые параметры радиоинтерфейсов точек доступа в данной локации будут находиться под управлением Airtune (если Airtune так же включен глобально на странице «Общие настройки»). Соответственно, когда Airtune включен в локации, менять параметры, связанные с мощностью и радиоканалами в радиопрофилях этой локации нецелесообразно, т.к. они не будут применены на точке доступа потому, что эти параметры автоматически настраиваются через Airtune. При необходимости изменить ширину канала или список каналов для автовыбора на точках доступа, необходимо сначала отключить Airtune, применить изменения, а затем снова включить Airtune для автоматического управления каналами в соответствии с новыми настройками.

В таблице содержатся основные настройки для каждого профиля, такие как:

- Название профиля
- Диапазон, ГГц
- Режим IEEE 802.11
- Ширина канала, МГц
- Мощность
- Описание профиля





В заводской конфигурации созданы радиопрофили с названиями «default_2g» для 2.4 ГГц и «default_5g» для 5 ГГц со следующими параметрами:

Профиль default_2g:

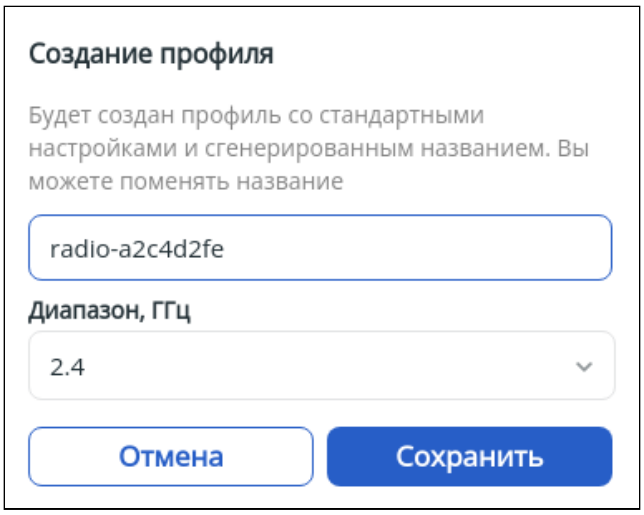
- Описание: default_2g
- Режим IEEE 802.11: b/g/n/ax
- Диапазон: 2,4 ГГц
- Ширина канала: 20 МГц
- Мощность: максимальная
- Список каналов: 1,6,11

Профиль default_5g

- Описание: default_5g
- Режим IEEE 802.11: a/n/ac/ax
- Диапазон: 5 ГГц
- Ширина канала: 20 МГц
- Мощность: максимальная
- Список каналов: 36,40,44,48,52,56,40,64

Для создания нового радиопрофиля используйте кнопку «Создать профиль».

Откроется окно с предложением создать профиль со стандартными настройками и сгенерированным названием, которое можно изменить самостоятельно. Необходимо сразу указать, для какого частотного диапазона создается профиль. После нажатия кнопки «Сохранить» откроется страница профиля для настройки параметров. При необходимости отмены создания нового профиля используйте кнопку «Отмена».



На страницах радиопрофилей представлены следующие параметры:

- *Описание* − описание для радиопрофиля. Значение по умолчанию: отсутствует. Возможные значения: произвольное описание задается строкой до 255 символов;
- *Режим IEEE 802.11* − режим работы радиоинтерфейса.
  Значения по умолчанию:
  - b/g/n/ax − для диапазона 2.4 ГГц;
  - a/n/ac/ax − для диапазона 5 ГГц.

  Возможные значения:
  - b/g, n/ax, b/g/n/ax − для диапазона 2.4 ГГц;
  - a/n/ac/ax − для диапазона 5 ГГц.
- *Диапазон, ГГц* − частотный диапазон радиоинтерфейса. Для каждого частотного диапазона (2.4 и 5 ГГц) создается отдельный радиопрофиль;
- *Ширина канала, МГц* − ширина полосы частот канала, на котором работает радиоинтерфейс точки доступа. Значение по умолчанию: 20 МГц.
  Возможные значения:
  - 20
  - 40L
  - 40U
  - 80 (только для 5 ГГц)
- *OBSS Coexistance* − переключатель управляет режимом автоматического уменьшения ширины канала на точке доступа при загруженном радиоэфире. Значение по умолчанию: отключено.
  Возможные значения: включено/отключено;
- *Мощность* − уровень мощности сигнала передатчика Wi-Fi для радиоинтерфейса. Значение по умолчанию: максимальная.
  Возможные значения:
  - максимальная
  - высокая
  - средняя
  - низкая
  - минимальная

Соответствие значений параметра мощности (указано в дБм) для каждого радиоинтерфейса ТД в зависимости от модели ТД представлены в таблицах:

	2,4 ГГц				
Модель ТД	**минимальная**	**низкая**	**средняя**	**высокая**	**максимальная**
WEP-1L	3	6	10	13	16
WEP-2L	3	6	10	13	16
WOP-2L	3	6	10	13	16
WOP-20L	8	10	12	14	16
WEP-200L	4	7	10	13	16
WEP-30L	0	4	8	12	16
WOP-30L	0	4	8	12	16
WOP-30LS	0	3	6	9	11
WEP-3ax	6	8	11	14	16
WEP-2ac	5	8	11	14	16
WEP-2ac Smart	5	8	11	14	16
WOP-2ac:rev.B/rev.C	5	8	11	14	16
	5 ГГц				
Модель ТД	**минимальная**	**низкая**	**средняя**	**высокая**	**максимальная**
WEP-1L	11	13	15	17	19
WEP-2L	11	13	15	17	19
WOP-2L	11	13	15	17	19
WOP-20L	11	13	15	17	19
WEP-200L	8	11	14	17	19
WEP-30L	0	5	10	15	19
WOP-30L	0	5	10	15	19
WOP-30LS	0	3	6	9	11
WEP-3ax	10	12	15	17	19
WEP-2ac	1	6	10	15	19
WEP-2ac Smart	11	13	15	17	19
WOP-2ac:rev.B/rev.C	1	6	10	15	19

- *Список каналов* – список радиоканалов для автоматического выбора в зависимости от радиоэфира.
  Значения по умолчанию:
  - 1, 6, 11 – для диапазона 2.4 ГГц;
  - 36, 40, 44, 48 – для диапазона 5 ГГц.

  Возможные значения:
  - 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 – для диапазона 2.4 ГГц;
  - 36, 40, 44, 48, 52, 56, 60, 64, 132, 136, 140, 144, 149, 153, 157, 161,165 – для диапазона 5 ГГц.

- *Поддержка DFS (только для диапазона 5 ГГц)* − параметр определяет режим динамического выбора частоты. Данный механизм требует от беспроводных устройств сканировать радиоэфир и избегать использования каналов, совпадающих с каналами, на которых работают радиолокационные системы в диапазоне 5 ГГц. Значение по умолчанию: auto.
  Возможные значения:
  - auto − механизм включен;
  - disabled − механизм выключен. DFS-каналы не доступны для выбора;
  - forced − механизм выключен. DFS-каналы доступны для выбора;

После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

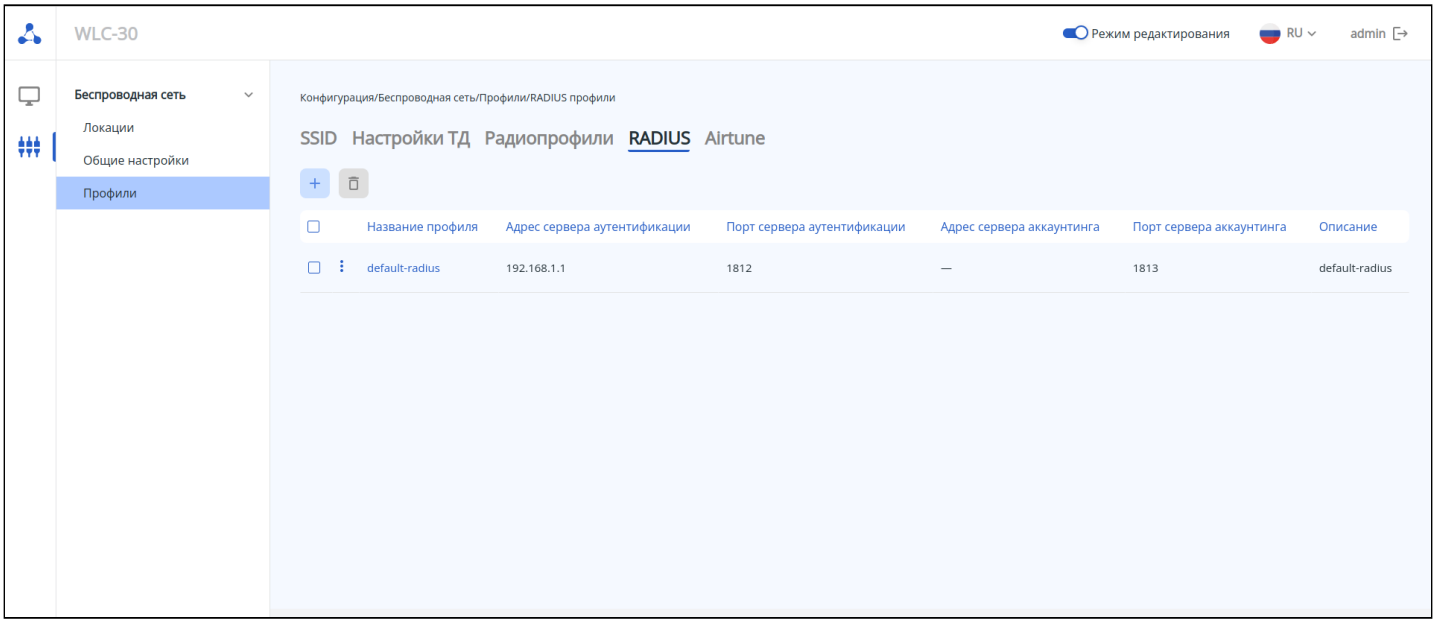
RADIUS

На странице представлены профили, описывающие параметры, необходимые для взаимодействия точки доступа с RADIUS-сервером при авторизации пользователей Wi-Fi, а также для сбора аккаунтинга.

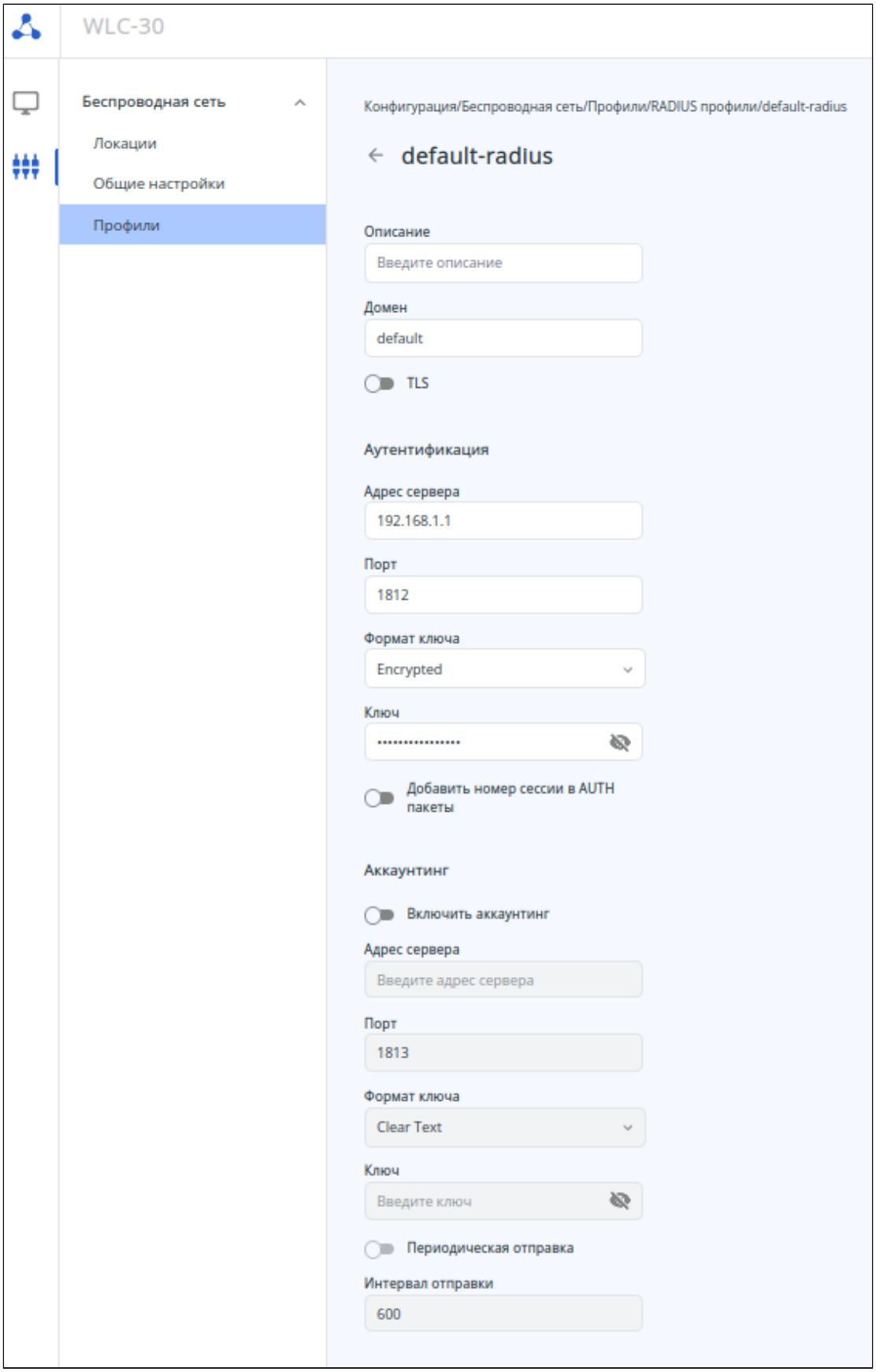
> Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

В таблице содержатся основные настройки для каждого RADIUS-профиля, такие как:

- Название профиля
- Адрес сервера аутентификации
- Порт сервера аутентификации
- Адрес сервера аккаунтинга
- Порт сервера аккаунтинга
- Описание профиля



Для того чтобы отредактировать существующий профиль, нажмите на его название. Откроется страница с настройками профиля.



В заводской конфигурации устройства создан RADIUS-профиль со следующими параметрами:

Общие:

- Описание: default-radius
- Домен: default
- TLS: отключено

Аутентификация:

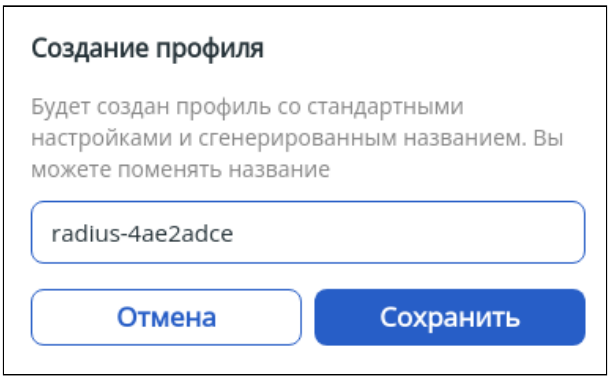
- Адрес сервера: 192.168.1.1
- Порт: 1812
- Ключ (хеш): 8CB5107EA7005AFF
- Добавить номер сессии в AUTH-пакеты: отключено

Аккаунтинг:

- Включить аккаунтинг: отключено.
- Адрес сервера: отсутствует
- Порт: 1813
- Ключ: отсутствует
- Периодическая отправка: отключено
- Интервал отправки: 600 с

Для создания нового RADIUS-профиля используйте кнопку «Создать профиль».

Откроется окно с предложением создать профиль со стандартными настройками и сгенерированным названием, которое можно изменить самостоятельно. После нажатия кнопки «Сохранить» откроется страница профиля для настройки параметров. При необходимости отмены создания нового профиля используйте кнопку «Отмена».



На странице настройки RADIUS-профиля представлены следующие параметры:
Общие:

- *Описание* – описание профиля. Значение по умолчанию: отсутствует. Возможные значения: произвольное описание задается строкой до 255 символов.
- *Домен* – домен пользователя. Значение по умолчанию: отсутствует. Возможные значения: формат доменного имени до 235 символов.
- *TLS* – переключатель, управляющий возможностью использования TLS при авторизации. Значение по умолчанию: отключено. Возможные значения: включено/отключено.

Аутентификация:

- *Адрес сервера* – адрес RADIUS-сервера аутентификации. Значение по умолчанию: отсутствует. Возможные значения: IP-адрес RADIUS-сервера в формате: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] или доменное имя RADIUS-сервера.

⚠ Адрес сервера авторизации является обязательным параметром при создании профиля.

- *Порт* – номер порта для обмена данными с RADIUS-сервером при выполнении аутентификации и авторизации. Значение по умолчанию: 1812. Возможные значения: от 1 до 65535;
- *Формат ключа* – определяет в каком виде будет указан ключ RADIUS-сервера, используемого для аутентификации и авторизации.
  Возможные значения:
  - Clear-Text
  - Encrypted
- *Ключ* – ключ для RADIUS-сервера, используемого для аутентификации и авторизации. Значение по умолчанию: отсутствует.

Возможные значения:
- если выбран формат ключа Clear-Text – ключ задаётся строкой от 8 до 63 символов
- если выбран формат ключа Encrypted – задается хеш ключа по алгоритму sha512 строкой от 16 до 126 символов

⚠ Ключ является обязательным параметром при создании RADIUS-профиля.

- *Добавить номер сессии в AUTH пакеты* – переключатель активирует передачу идентификатора сессии в запросах аккаунтинга. Значение по умолчанию: отключено.

Аккаунтинг:

- *Включить аккаунтинг* – переключатель активирует отправку аккаунтинга на RADIUS-сервер. Значение по умолчанию: отключено. Возможные значения: включено/отключено.
- *Адрес сервера* – адрес RADIUS-сервера для аккаунтинга. Значение по умолчанию: отсутствует. Возможные значения: IP-адрес RADIUS-сервера в формате: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255] или доменное имя RADIUS-сервера.
- *Порт* – порт RADIUS-сервера для отправки аккаунтинга. Значение по умолчанию: 1813. Возможные значения: от 1 до 65535.
- *Формат ключа* – определяет в каком виде будет указан ключ RADIUS-сервера, используемого для аккаунтинга.
  Возможные значения:
  - Clear-Text
  - Encrypted
- *Ключ* – ключ для RADIUS-сервера, используемого для аккаунтинга. Значение по умолчанию: отсутствует.
  Возможные значения:
  - если выбран формат ключа Clear-Text – ключ задаётся строкой от 8 до 63 символов
  - если выбран формат ключа Encrypted – задается хеш ключа по алгоритму sha512 строкой от 16 до 126 символов
- *Периодическая отправка* – переключатель активирует периодическую отправку аккаунтинга на RADIUS-сервер. Значение по умолчанию: отключено. Возможные значения: включено/отключено.
- *Интервал отправки* – период времени, через который осуществляется отправка аккаунтинга на RADIUS-сервер. Значение по умолчанию: 600 секунд. Возможные значения: от 1 до 86400 секунд.

После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

Airtune

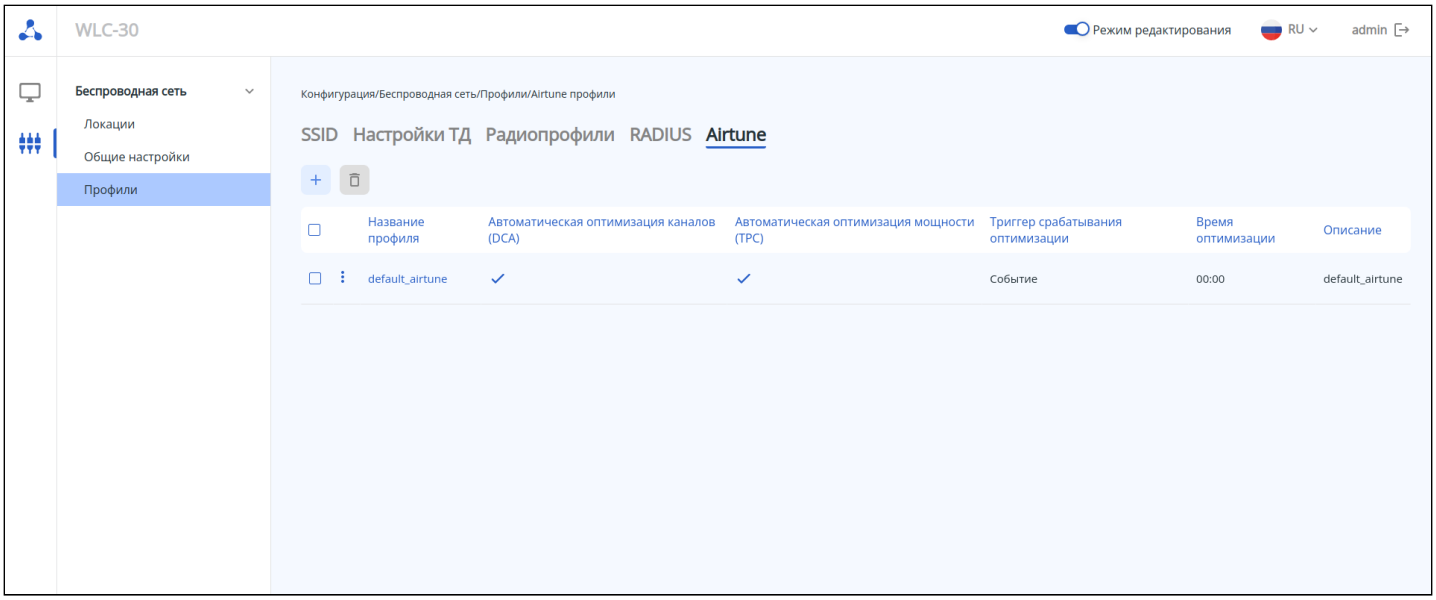
На странице представлены в виде таблицы профили Airtune, имеющиеся в конфигурации. Профили работы данного сервиса позволяют автоматически настраивать такие параметры радиоинтерфейсов точек доступа, как мощность и каналы, а так же позволяют управлять балансировкой клиентов и настройками роуминга.

ⓘ Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

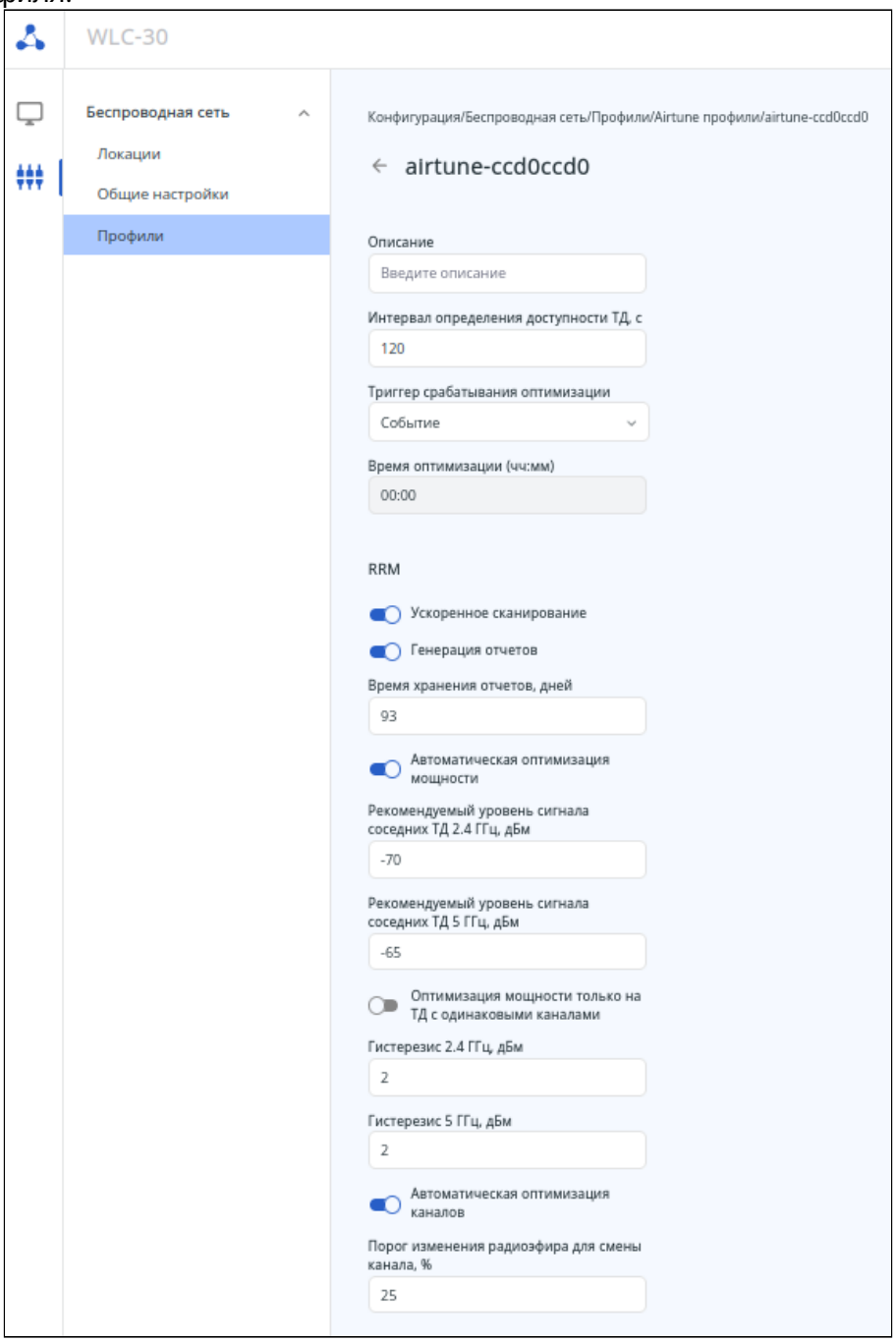
Если Airtune-профиль добавлен в локацию, некоторые параметры радиоинтерфейсов точек доступа в данной локации будут находиться под управлением airtune (если Airtune так же включен глобально на странице «Общие настройки»). Соответственно, когда Airtune включен в локации, менять параметры, связанные с мощностью и радиоканалами в радиопрофилях этой локации нецелесообразно, т.к. они не будут применены на точки доступа потому, что эти параметры автоматически настраиваются через Airtune. При необходимости изменить ширину канала или список каналов для автовыбора на точках доступа, необходимо сначала отключить Airtune, применить изменения, а затем снова включить Airtune для автоматического управления каналами в соответствии с новыми настройками.

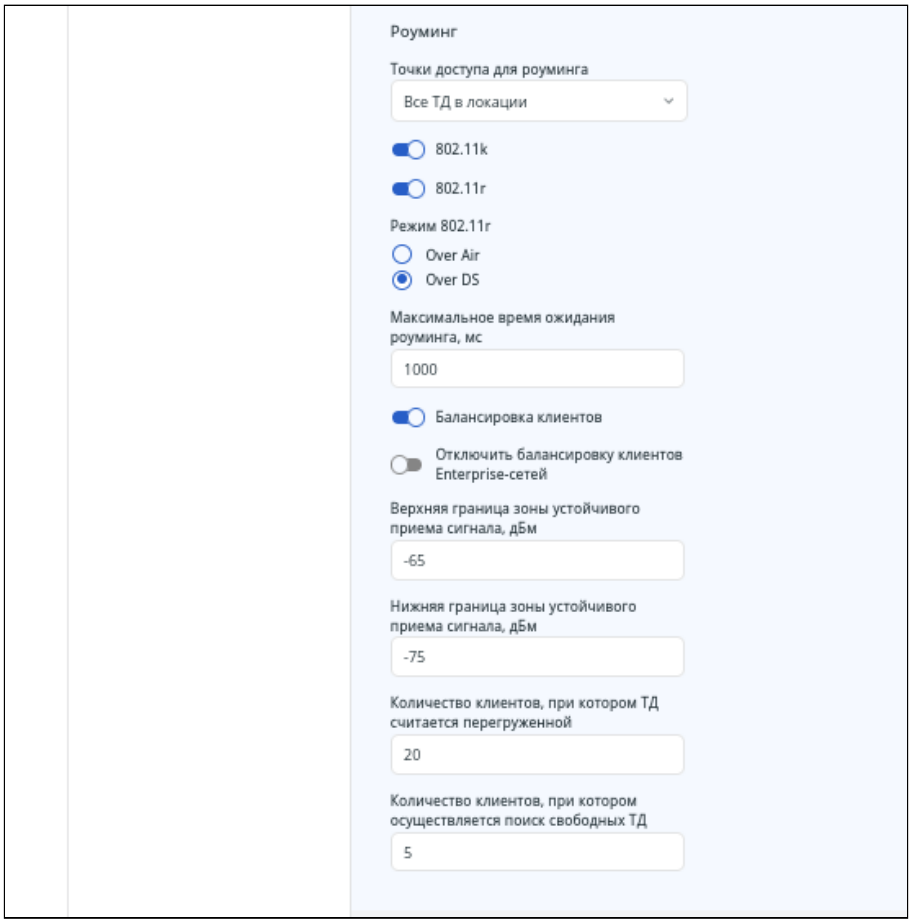
В таблице содержатся основные параметры для каждого профиля, такие как:

- Название профиля
- Статус работы автоматической оптимизации каналов (DCA)
- Статус работы автоматической оптимизации мощности (TCP)
- Триггер срабатывания оптимизации
- Время, заданное для оптимизации
- Описание профиля



Для того чтобы отредактировать существующий профиль, нажмите на его название. Откроется страница с настройками профиля.





В заводской конфигурации создан профиль с названием «default-airtune» со следующими параметрами:

Общие:

- Описание: default-airtune
- Интервал определения доступности ТД: 100 с
- Триггер срабатывания оптимизации: событие
- Время оптимизации: 00:00

RRM:

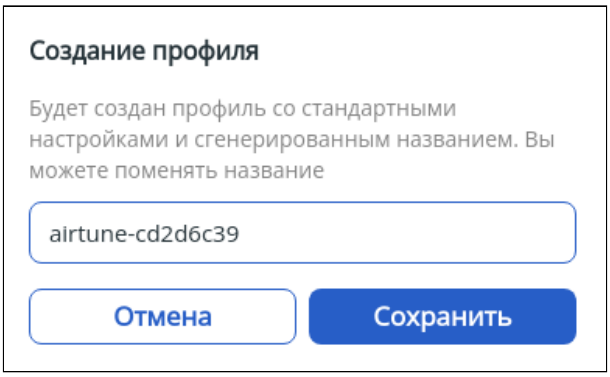
- Ускоренное сканирование: включено
- Генерация отчетов: включено
- Время хранения отчетов: 93 дня
- Автоматическая оптимизация мощности: включено
- Рекомендуемый уровень сигнала соседних ТД 2.4 ГГц: -70 дБм
- Рекомендуемый уровень сигнала соседних ТД 5ГГц: -65 дБм
- Оптимизация мощности только на ТД с одинаковыми каналами: отключено
- Гистерезис 2.4 ГГц: 2 дБм
- Гистерезис 5 ГГц: 2 дБм
- Автоматическая оптимизация каналов: включено
- Порог изменения радиоэфира для смены канала: 25%

Роуминг:

- Точки доступа для роуминга: все ТД в локации
- 802.11k: включено
- 802.11r: включено
- Режим 802.11r: Over DS
- Максимальное время ожидания роуминга: 1000 мс
- Балансировка клиентов: включено
- Отключить балансировку клиентов Enterprise-сетей: отключено
- Верхняя страница зоны устойчивого приёма сигнала: -65 дБм

- Нижняя граница зоны устойчивого приёма сигнала: -75 дБм
- Количество клиентов, при котором ТД считается перегруженной: 20
- Количество клиентов, при котором осуществляется поиск свободных ТД: 5

Для создания нового профиля Airtune используйте кнопку «Создать профиль». Откроется окно с предложением создать профиль со стандартными настройками и сгенерированным названием, которое можно изменить самостоятельно. После нажатия кнопки «Сохранить» откроется страница профиля для настройки параметров. При необходимости отмены создания нового профиля используйте кнопку «Отмена».



На странице профиля Airtune представлены следующие параметры:
Общие:

- *Описание* – описание профиля. Значение по умолчанию: отсутствует. Возможные значения: произвольное описание задается строкой до 255 символов.
- *Интервал определения доступности ТД* – защитный интервал для определения доступности ТД сервером, то есть допустимое время ожидания ТД в случае потери связи, по истечении которого сервис будет считать ТД отключенной от сервиса. Значение по умолчанию: 120 секунд. Возможные значения: от 10 до 3600 секунд.
- *Триггер срабатывания оптимизации* – выбор параметра, по которому будет срабатывать оптимизация. Значение по умолчанию: событие.
  Возможные значения:
  - *Событие* – включение функционала оптимизации по событию:
    - Добавление новой ТД в домен;
    - Удаление ТД из домена;
    - Пропадание связи до одной из ТД более 5 минут.
  - *Время* – включение функционала оптимизации по указанному времени;
  - *Событие и время* – включение функционала оптимизации и по событию, и по указанному времени;
  - *Отключить* – выключение функционала оптимизации.
- *Время оптимизации* – время, в которое будет срабатывать оптимизация, когда установлен триггер, содержащий время. Значение по умолчанию: 00:00. Возможные значения: время в формате чч:мм, где первые две цифры – это часы, вторые – минуты.

RRM:

- *Ускоренное сканирование* – переключатель активирует ускоренное сканирование для точек доступа Eltex. С включенным параметром точки доступа в один момент времени обмениваются специальными Action-фреймами в определенном частотном канале, который сообщил им сервис. По окончанию обмена передают сообщение на сервис с полученными результатами. Весь процесс оптимизации в таком режиме будет занимать не более пары минут вне зависимости от количества ТД в домене. В случае отключенного параметра ТД по очереди сканируют все каналы, учитывают влияние конкурентных ТД. В данном случае время, требуемое для оптимизации, будет увеличиваться при увеличении количества ТД (на 1 ТД – 50-60 секунд). Значение по умолчанию: включено. Возможные значения: включено/отключено.
- *Генерация отчетов* – переключатель активирует генерацию отчетов работы RRM. Значение по умолчанию: включено. Возможные значения: включено/отключено.

- *Время хранения отчетов* – время хранения отчётов по оптимизации RRM. Значение по умолчанию: 93.Возможные значения: допустимы значения от 1 до 365 дней.

> ⚠ Выполненные отчеты доступны в меню «Мониторинг/Беспроводная сеть/Локации/<Название локации>/Отчеты RRM». Отчеты можно посмотреть за период до 7 дней. При необходимости отчет можно выгрузить.

- *Автоматическая оптимизация мощности* – переключатель позволяет активировать автоматическое управление мощностью на ТД в локации. Значение по умолчанию: включено. Возможные значения: включено/отключено.
- *Рекомендуемый уровень сигнала соседних ТД 2.4 ГГц* – уровень сигнала, с которым соседние ТД должны видеть друг друга в диапазоне 2.4 ГГц. В зависимости от полученного уровня RSSI от соседней ТД, сервер будет сравнивать его с указанным в данном параметре уровнем и рекомендовать уменьшить (если RSSI от ТД больше) либо увеличить мощность передатчика ТД (если RSSI от ТД меньше). Значение по умолчанию: -70 дБм. Возможные значения: от -100 до -1 дБм.
- *Рекомендуемый уровень сигнала соседних ТД 5 ГГц* – уровень сигнала, с которым соседние ТД должны видеть друг друга в диапазоне 5 ГГц. В зависимости от полученного уровня RSSI от соседней ТД, сервер будет сравнивать его с указанным в данном параметре уровнем и рекомендовать уменьшить (если RSSI от ТД больше) либо увеличить мощность передатчика ТД (если RSSI от ТД меньше). Значение по умолчанию: -65 дБм. Возможные значения: от -100 до -1 дБм.
- *Оптимизация мощности только на ТД с одинаковыми каналами* – переключатель активирует режим автоматической оптимизации мощности (TPC-HD) только на ТД, работающих на одинаковых каналах. Значение по умолчанию: отключено. Возможные значения: включено/отключено.
- *Гистерезис 2.4 ГГц* – допустимая погрешность для частотного диапазона 2.4 ГГц. Если полученный сигнал лежит в диапазоне рекомендуемого уровня сигнала плюс или минус значение гистерезиса, оптимизацию по мощности проводить не следует. Значение по умолчанию: 2 дБм. Возможные значения: от 1 до 10 дБм.
- *Гистерезис 5 ГГц* – допустимая погрешность для частотного диапазона 5 ГГц. Если полученный сигнал лежит в диапазоне рекомендуемого уровня сигнала плюс или минус значение гистерезиса, оптимизацию по мощности проводить не следует. Значение по умолчанию: 2 дБм. Возможные значения: от 1 до 10 дБм.
- *Автоматическая оптимизация каналов* – переключатель активирует использование алгоритма автоматического распределения частотных каналов каждой точки доступа в локации, чтобы избежать интерференции между ними. Значение по умолчанию: включено. Возможные значения: включено/отключено.
- *Порог изменения радиоэфира для смены канала* – порог изменения радиоэфира при динамическом распределении каналов, необходимый для смены каналы. Значение по умолчанию: 25 %. Возможные значения: от 0 до 99 %.

Роуминг:

- *Точки доступа для роуминга* – выбор ТД для роуминга. Значение по умолчанию: все ТД в локации.
  Возможные значения:
  - *Соседствующие ТД* – ТД будут сканировать эфир и определять какие ТД являются соседями, чтобы балансировать клиентов и осуществлять роуминг только между рядом стоящими ТД (меньше лишнего трафика в проводной сети, но больше в радиосреде);
  - *Все ТД в локации* – сервис использует функционал в рамках всего домена, даже если ТД находятся на большом расстоянии друг от друга (больше трафика в проводной сети, меньше в радиосреде).
- *802.11k* – переключатель активирует синхронизацию списков для роуминга стандарта 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, которое клиент затрачивает на поиск другой сети при роуминге, так как клиенту не нужно производить сканирование каналов, на которых нет целевых точек доступа, доступных для переключения. Данный вид роуминга возможен только для тех клиентских устройств, которые поддерживают 802.11k. Значение по умолчанию: включено. Возможные значения: включено/отключено.

- *802.11r* – переключатель активирует отправку ключей для роуминга стандарта 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 PSK и WPA2/WPA3 Enterprise. Значение по умолчанию: включено. Возможные значения: включено/отключено.
- *Режим 802.11r* – выбор режима взаимодействия с целевой точкой доступа для роуминга 802.11r. Значение по умолчанию: Over-DS.
  Возможные значения:
  - Over-DS
  - Over-Air
- *Максимальное время ожидания роуминга* – максимальный период времени, в течение которого ТД должны обменяться данными о попытке роуминга клиента (RRB-пакеты). Если ответ на запрос по истечению таймаута не пришел, RRB-запрос на бесшовный роуминг считается неуспешным. Значение по умолчанию: 1000 мс. Возможные значения: от 1000 до 268431360 мс.

⚠ Нижеописанные параметры актуальны для точек доступа WEP-2ac, WEP-2ac Smart, WOP-2ac:revB и WOP-2ac:rev.C.

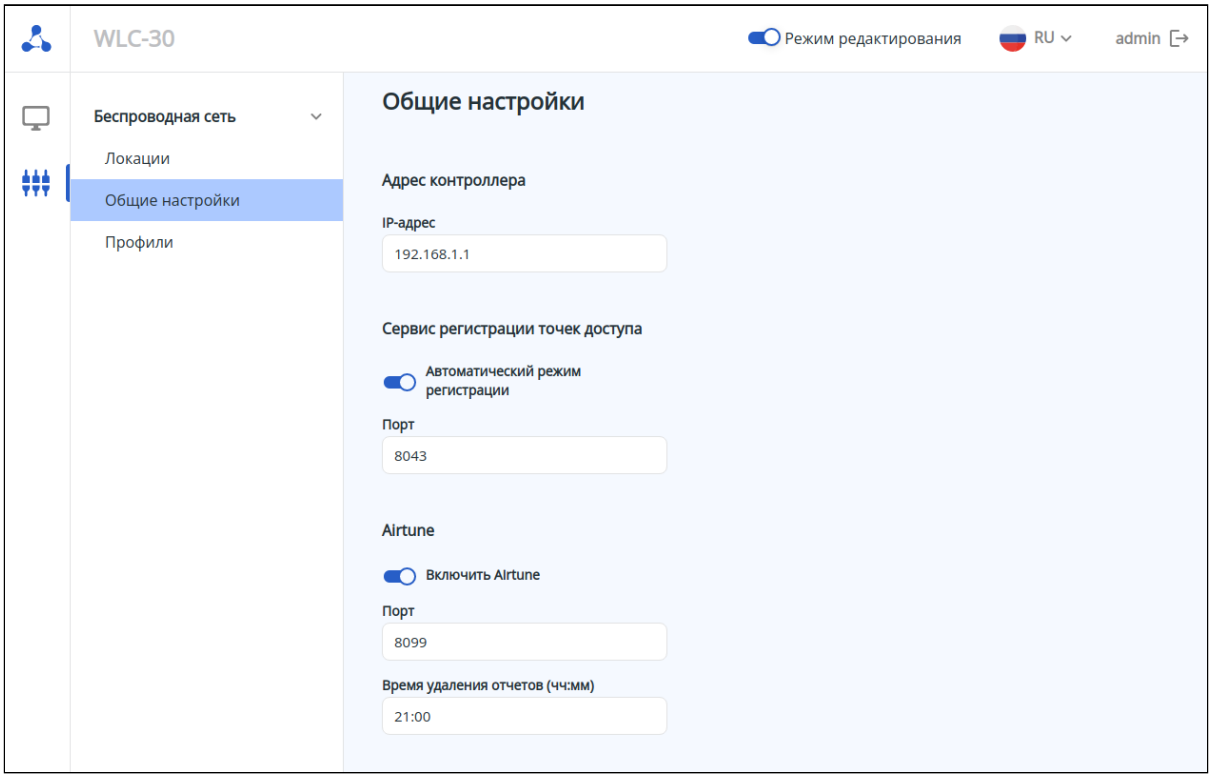
- *Балансировка клиентов* – переключатель активирует балансировку клиентов по всем ТД в домене, независимо от их фактического расположения. Функционал нужен для равномерного распределения клиентов между ТД, чтобы избежать перегрузки одной из ТД, если в зоне видимости клиента есть более свободная ТД. Значение по умолчанию: включено. Возможные значения: включено/отключено.
- *Отключить балансировку клиентов Enterprise-сетей* – отключение балансировки клиентов enterprise-сетей между ТД. Значение по умолчанию: отключено. Возможные значения: включено/отключено.
- *Верхняя страница зоны устойчивого приёма сигнала* – верхняя граница окончания зоны устойчивого приема сигнала от клиента, то есть порог уровня RSSI от клиента, при превышении которого подключенный клиент будет считаться в "уверенной" зоне и поиск новой ТД не начнется в случае, если ТД не перегружена. Значение по умолчанию: -65 дБм. Возможные значения: от -100 до 1 дБм.
- *Нижняя граница зоны устойчивого приёма сигнала* – нижняя граница окончания зоны устойчивого приема сигнала от клиента, то есть порог уровня RSSI от клиента. В случае если RSSI от клиента меньше указанного в данном параметре, клиент считается находящимся в "неуверенной" зоне. Сервис будет пытаться найти для клиента ТД с "уверенным" приемом для последующего переключения клиента на целевую ТД. Значение по умолчанию: -75 дБм. Возможные значения: от -100 до 1 дБм.
- *Количество клиентов, при котором ТД считается перегруженной* – порог количества подключенных клиентов на радиоинтерфейсе, при превышении которого точка будет считаться перегруженной. Значения по умолчанию: 20. Возможные значения: от 1 до 100 клиентов.
- *Количество клиентов, при котором осуществляется поиск свободных ТД* – порог количества подключенных клиентов на радиоинтерфейсе, при превышении которого сервис будет искать для новых клиентов более свободную ТД (если таковая не найдется, клиент продолжит работу на текущей точке доступа). Если количество клиентов меньше текущего порога – точка доступа считается свободной. Значения по умолчанию: 5. Возможные значения: от 1 до 100 клиентов.

После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

Подменю «Общие настройки»

В разделе задаются общие настройки контроллера, режим регистрации точек доступа и общие настройки сервиса Airtune.

> Для редактирования общих настроек должен быть включен режим редактирования.



В заводской конфигурации общие настройки имеют следующие значения:

- IP-адрес контроллера: 192.168.1.1
- Автоматический режим регистрации: включен
- Порт сервиса регистрации: 8043
- Сервис Airtune: включен
- Порт Airtune: 8099
- Время удаления отчетов: 21:00

На странице профиля представлены следующие параметры:

Адрес контроллера:

- *IP-адрес* – IP-адрес контроллера, по которому точки доступа будут взаимодействовать с WLC. Значение по умолчанию: отсутствует. Параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255.

Сервис регистрации точек доступа:

- *Автоматический режим регистрации* – переключатель активирует режим, при котором пришедшие на контроллер точки доступа не будут ожидать действий администратора для регистрации, т.е. регистрация произойдет в автоматическом режиме. Если переключатель выключен, администратор самостоятельно выполняет регистрацию точек доступа, находящихся на вкладке «Мониторинг/Беспроводная сеть/Точки доступа/Новые точки доступа» с помощью соответствующей кнопки «Зарегистрировать все» или с помощью контекстного меню для каждой обнаруженной точки доступа. Значение по умолчанию: отключено. Возможные значения: включено/отключено;
- *Порт* – порт, на котором работает сервис регистрации точек доступа. Значение по умолчанию: 8043. Возможные значения: от 1024 до 65535.

Airtune:

- *Включить Airtune* – глобальная активация работы сервиса Airtune. Значение по умолчанию: отключено;
- *Порт* – порт, на котором работает сервис Airtune. Значение по умолчанию: 8099. Возможные значения: от 1024 до 65535;
- *Время удаления отчетов (чч:мм)* – время, в которое отчеты оптимизации будут удаляться. Задается в формате чч:мм, где первые две цифры – это часы, вторые – минуты. Значение по умолчанию: 21:00.

После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

11 Управление туннелированием

Алгоритм и примеры настройки функций управления туннелированием см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

12 Управление функциями второго уровня (L2)

Алгоритм и примеры настройки управления функциями второго уровня (L2) см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

13 Управление QoS

Управление технологией Quality of Service (QoS) описано в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

14 Управление маршрутизацией

Алгоритм и примеры настройки функций управления маршрутизацией см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

15 Управление технологией MPLS

Управление технологией MPLS описано в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

16 Управление безопасностью

Алгоритм и примеры настройки функций управления безопасностью см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

17 Управление резервированием

Алгоритм и примеры настройки функций управления резервированием см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

18 Управление удаленным доступом

Алгоритм и примеры настройки функций управления удаленным доступом см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

19 Управление сервисами

Алгоритм и примеры настройки функций управления сервисами см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

20 Мониторинг

Данный раздел см. в документации ESR.

> ⚠ Значения параметров для WLC-15/30/3200 идентичны значениям для ESR-15/15R/30/3200 соответственно.

21 Управление BRAS (Broadband Remote Access Server)

Активируется лицензией BRAS.

21.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Добавить RADIUS-сервер в список используемых серверов и перейти в режим его конфигурирования.	**wlc(config)# radius-server host { <IP-ADDR> | <IPV6-ADDR> } [vrf <VRF>]** **wlc(config-radius-server)#**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF]; <VRF> – имя экземпляра VRF, задается строкой до 31 символа.
2	Задать пароль для аутентификации на удаленном RADIUS-сервере.	**wlc(config-radius-server)# key ascii-text { <TEXT> | encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
3	Создать профиль AAA.	**wlc(config)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
4	В профиле AAA указать RADIUS-сервер.	**wlc(config-aaa-radius-profile)# radius-server host { <IP-ADDR> | <IPV6-ADDR> }**	<IP-ADDR> – IP-адрес RADIUS-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255]; <IPV6-ADDR> – IPv6-адрес RADIUS-сервера, задаётся в виде X:X:X:X::X, где каждая часть принимает значения в шестнадцатеричном формате [0..FFFF].
5	Создать DAS-сервер.	**wlc(config)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
6	Задать пароль для аутентификации на удаленном DAS-сервере.	**wlc(config-das-server)# key ascii-text {<TEXT>|encrypted <ENCRYPTED-TEXT> }**	<TEXT> – строка [8..16] ASCII-символов; <ENCRYPTED-TEXT> – зашифрованный пароль, размером [8..16] байт, задаётся строкой [16..32] символов.
7	Создать AAA DAS-профиль.	**wlc(config)# aaa das-profile <NAME>**	<NAME> – имя DAS-профиля, задается строкой до 31 символа.
8	Указать DAS-сервер в DAS-профиле.	**wlc(config-aaa-das-profile)# das-server <NAME>**	<NAME> – имя DAS-сервера, задается строкой до 31 символа.
9	Сконфигурировать BRAS.	**wlc(config)# subscriber-control [vrf <VRF>]**	<VRF> – имя экземпляра VRF, задается строкой до 31 символа, в рамках которого будет работать контроль пользователей.
10	Выбрать профиль серверов динамической авторизации (DAS), на которые будут приходить CoA-запросы от PCRF.	**wlc(config-subscriber-control)# aaa das-profile <NAME>**	<NAME> – имя профиля серверов динамической авторизации (DAS), задается строкой до 31 символа.
11	Выбрать профиль RADIUS-серверов для получения параметров сервисов пользователя.	**wlc(config-subscriber-control)# aaa services-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.

Шаг	Описание	Команда	Ключи
12	Выбрать профиль RADIUS-серверов для получения параметров сессии пользователя.	**wlc(config-subscriber-control)# aaa sessions-radius-profile <NAME>**	<NAME> – имя профиля RADIUS-серверов, задается строкой до 31 символа.
13	Определить IP-адрес контроллера, который будет использоваться в качестве IP-адреса источника в отправляемых RADIUS-пакетах.	**wlc(config-subscriber-control)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
14	Включить аутентификацию сессий по MAC-адресу (не обязательно).	**wlc(config-subscriber-control)# session mac-authentication**	
15	Организовать прозрачное пропускание служебного трафика (DHCP, DNS и т.д.) на основе фильтров.	**wlc(config-subscriber-control)# bypass-traffic-a c l <NAME>**	<NAME> – имя привязываемого ACL, задается строкой до 31 символа.
16	Перейти в режим конфигурирования сервиса по умолчанию.	**wlc(config-subscriber-control)# default-service**	
17	Привязать указанный QoS-класс к сервису по умолчанию.	**wlc(config-subscriber-default-service)# class-map <NAME>**	<NAME> – имя привязываемого класса, задается строкой до 31 символа.
18	Указать имя списка URL, который будет использоваться для фильтрации HTTP/HTTPS-трафика не аутентифицированных пользователей.	**wlc(config-subscriber-default-service)# filter-name { local<LOCAL-NAME>** | **remote<REMOTE-NAME> }**	<LOCAL-NAME> – имя профиля URL, задаётся строкой до 31 символа; <REMOTE-NAME> – имя списка URL на удаленном сервере, задаётся строкой до 31 символа.
19	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых входит в список URL, назначенных командой «filter-name».	**wlc(config-subscriber-default-service)# filter-action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается. redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.

Шаг	Описание	Команда	Ключи
20	Указать действия, которые должны быть применены для HTTP/HTTPS-пакетов, URL которых не входит в список URL, назначенных командой «filter-name».	**wlc(config-subscriber-default-service)# default -action<ACT>**	<ACT> – назначаемое действие: • **permit** – прохождение трафика разрешается; • **deny** – прохождение трафика запрещается. redirect <URL> – будет выполнен редирект на указанный URL, задается строкой до 255 символов.
21	Активировать профиль контроля пользователей.	**wlc(config-subscriber-control)# enable**	
22	Изменить идентификатор сетевого интерфейса (физического, саб-интерфейса или сетевого моста) (не обязательно).	**wlc(config-if)# location <ID>**	<ID> – идентификатор сетевого интерфейса, задаётся строкой до 220 символов.
23	Включить контроль пользователей на интерфейсе.	**wlc(config-if-gi)# service-subscriber-control {any| object-group <NAME>}**	<NAME> – имя профиля IP-адресов, задаётся строкой до 31 символа.
24	Включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени (не обязательно).	**wlc(config-subscriber-control)# quota-expired-reauth**	
25	Включить аутентификацию сессий по IP-адресу (не обязательно).	**wlc(config-subscriber-control)# session ip-authentication**	
26	Включить прозрачное пропускание трафика в состоянии backup для BRAS (не обязательно).	**wlc(config-subscriber-control)# backup traffic-processing transparent**	
27	Задать интервал, по истечении которого с устройства будут удалены неиспользуемые в текущий момент списки URL (не обязательно).	**wlc(config)# subscriber-control unused-filters-remove-delay <DELAY>**	<DELAY> – временной интервал в секундах, принимает значения [10800..86400].
28	Задать интервал, по истечении которого, если не было пакетов от пользователя, сессия считается устаревшей и удаляется с устройства (не обязательно).	**wlc(config-subscriber-default-service)# session-timeout <SEC>**	<SEC> – период времени в секундах, принимает значения [120..3600].

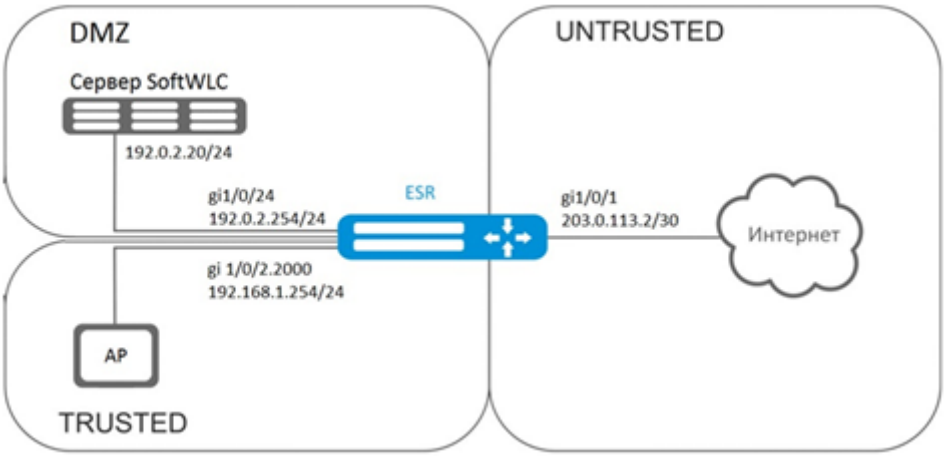
Шаг	Описание	Команда	Ключи
29	Определить VRRP-группу, на основе которой определяется состояние сервиса контроля абонентов (основной/резервный) (не обязательно).	**wlc(config-subscriber-control)# vrrp-group <GRID>**	<GRID> – идентификатор группы VRRP-контроллера, принимает значения [1..32].
30	Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTP Proxy-сервер контроллера (не обязательно).	**wlc(config-subscriber-control)# ip proxy http listen-ports <NAME>**	<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.
31	Определить порт HTTP Proxy-сервера на контроллере (не обязательно).	**wlc(config-subscriber-control)# ip proxy http redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535].
32	Определить с каких TCP-портов назначения трафик будет перенаправлен на HTTPS Proxy-сервер контроллера (не обязательно).	**wlc(config-subscriber-control)# ip proxy https listen-ports <NAME>**	<NAME> – имя профиля TCP/UDP-портов, задаётся строкой до 31 символа.
33	Определить порт HTTPS Proxy-сервера на контроллере (не обязательно).	**wlc(config-subscriber-control)# ip proxy https redirect-port <PORT>**	<PORT> – номер порта, указывается в диапазоне [1..65535].
34	Определить IP-адрес контроллера, который будет использоваться в качестве IP-адреса источника в отправляемых Proxy-сервером HTTP/HTTPS пакетах (не обязательно).	**wlc(config-subscriber-control)# ip proxy source-address <ADDR>**	<ADDR> – IP-адрес источника, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
35	Задать URL-адрес сервера, предоставляющего списки приложений для фильтрации трафика (не обязательно).	**wlc(config)# subscriber-control apps-server-url <URL>**	<URL> – адрес ссылки, задаётся строкой от 8 до 255 символов.
36	Включить контроль приложений на интерфейсе (не обязательно).	**wlc(config-if-gi)# subscriber-control application-filter <NAME>**	<NAME> – имя профиля приложений, задаётся строкой до 31 символа.
37	Установить/сбросить верхнюю границу количества сессий BRAS (не обязательно).	**wlc(config-subscriber-control)# thresholds sessions-number high <Threshold>**	<Threshold> – количество сессий BRAS: • [0-10000] – для WLC-3200

Шаг	Описание	Команда	Ключи
38	Установить/сбросить нижнюю границу количества сессий BRAS (не обязательно).	**wlc(config-subscriber-control)# thresholds sessions-number low <Threshold>**	<Threshold> – количество сессий BRAS: • [0-10000] – для WLC-3200

21.2 Пример настройки с SoftWLC

Задача:

Предоставлять доступ до ресурсов сети Интернет, только для авторизованных пользователей.



Решение:

За хранение учетных данных пользователей и параметров тарифных планов отвечает сервер SoftWLC. Информацию по установке и настройке сервера SoftWLC можно найти по ссылкам ниже:

Общая статья о SoftWLC;

Установка SoftWLC из репозиториев.

Для контроллера необходимо наличие лицензии BRAS, после ее активации можно переходить к конфигурированию устройства.

Создадим три зоны безопасности на устройстве, согласно схеме сети:

```
wlc# configure
wlc(config)# security zone trusted
wlc(config-zone)# exit
wlc(config)# security zone untrusted
wlc(config-zone)# exit
wlc(config)# security zone dmz
wlc(config-zone)# exit
```

Сконфигурируем параметры публичного порта и сразу пропишем шлюз по умолчанию:

```
wlc(config)# interface gigabitethernet 1/0/1
wlc(config-if-gi)# security-zone untrusted
wlc(config-if-gi)# ip address 203.0.113.2/30
wlc(config-if-gi)# service-policy dynamic upstream
wlc(config-if-gi)# exit
wlc(config)# ip route 0.0.0.0/0 203.0.113.1
```

Сконфигурируем порт в сторону сервера SoftWLC:

```
wlc(config)# interface gigabitethernet 1/0/24
wlc(config-if-gi)# security-zone dmz
wlc(config-if-gi)# ip address 192.0.2.1/24
wlc(config-if-gi)# exit
```

Сконфигурируем порт для подключения Wi-Fi точки доступа:

```
wlc(config)# bridge 2
wlc(config-bridge)# security-zone trusted
wlc(config-bridge)# ip address 192.168.0.254/24
wlc(config-bridge)# ip helper-address 192.0.2.20
wlc(config-bridge)# service-subscriber-control object-group users
wlc(config-bridge)# location ssid1
wlc(config-bridge)# enable
wlc(config-bridge)# exit
wlc(config)# interface gigabitethernet 1/0/2.2000
wlc(config-subif)# bridge-group 1
wlc(config-subif)# exit
wlc(config)# interface gigabitethernet 1/0/2
wlc(config-if-gi)# service-policy dynamic downstream
esr (config-if-gi)# exit
```

Подключать клиентов необходимо через саб-интерфейсы в бриджи, причем от параметра location (смотри конфигурацию bridge 2) зависит выбор тарифного плана.

Модуль, отвечающий за AAA-операции, основан на eltex-radius и доступен по IP-адресу сервера SoftWLC. Номера портов для аутентификации и аккаунтинга в нашем примере – это значения по умолчанию для SoftWLC.

Зададим параметры для взаимодействия с этим модулем:

```
wlc(config)# radius-server host 192.0.2.20
wlc(config-radius-server)# key ascii-text password
wlc(config-radius-server)# auth-port 31812
wlc(config-radius-server)# acct-port 31813
wlc(config-radius-server)# exit
```

Создадим профиль AAA:

```
wlc(config)# aaa radius-profile RADIUS
wlc(config-aaa-radius-profile)# radius-server host 192.0.2.20
wlc(config-aaa-radius-profile)# exit
```

Укажем параметры доступа к DAS (Direct-attached storage)-серверу:

```
wlc(config)# object-group network server
wlc(config-object-group-network)# ip address-range 192.0.2.20
wlc(config-object-group-network)# exit
wlc(config)# das-server CoA
wlc(config-das-server)# key ascii-text password
wlc(config-das-server)# port 3799
wlc(config-das-server)# clients object-group server
wlc(config-das-server)# exit
wlc(config)# aaa das-profile CoA
wlc(config-aaa-das-profile)# das-server CoA
wlc(config-aaa-das-profile)# exit
```

До аутентификации весь трафик из зоны trusted блокируется, в том числе DHCP- и DNS-запросы. Необходимо настроить разрешающие правила для пропуска DHCP- и DNS-запросов:

```
wlc(config)# ip access-list extended DHCP
wlc(config-acl)# rule 10
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol udp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port 68
wlc(config-acl-rule)# match destination-port 67
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# rule 11
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol udp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 53
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
wlc(config)# ip access-list extended WELCOME
wlc(config-acl)# rule 10
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol any
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# exit
wlc(config)# ip access-list extended INTERNET
wlc(config-acl)# rule 10
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol any
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# exit
```

Зададим web-ресурсы доступные без авторизации:

```
wlc(config)# object-group url defaultservice
wlc(config-object-group-url)# url http://eltex.nsk.ru
wlc(config-object-group-url)# exit
```

Списки фильтрации по URL находятся на сервере SoftWLC (меняется только IP-адрес сервера SoftWLC, если используется адресация отличная от данного примера, все остальное в URL следует оставить без изменения):

```
wlc(config)# subscriber-control filters-server-url http://192.0.2.20:7070/Filters/file/
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с SoftWLC, в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/24:

```
wlc(config)# subscriber-control
wlc(config-subscriber-control)# aaa das-profile CoA
wlc(config-subscriber-control)# aaa sessions-radius-profile RADIUS
wlc(config-subscriber-control)# nas-ip-address 192.0.2.1
wlc(config-subscriber-control)# session mac-authentication
wlc(config-subscriber-control)# bypass-traffic-acl DHCP
wlc(config-subscriber-control)# default-service
wlc(config-subscriber-default-service)# class-map INTERNET
wlc(config-subscriber-default-service)# filter-name local defaultservice
wlc(config-subscriber-default-service)# filter-action permit
wlc(config-subscriber-default-service)# default-action redirect http://192.0.2.20:8080/
eltex_portal/
wlc(config-subscriber-default-service)# session-timeout 3600
wlc(config-subscriber-default-service)# exit
wlc(config-subscriber-control)# enable
wlc(config-subscriber-control)# exit
```

Далее необходимо сконфигурировать правила перехода между зонами безопасности:

```
wlc(config)# object-group service telnet
wlc(config-object-group-service)# port-range 23
wlc(config-object-group-service)# exit
wlc(config)# object-group service ssh
wlc(config-object-group-service)# port-range 22
wlc(config-object-group-service)# exit
wlc(config)# object-group service dhcp_server
wlc(config-object-group-service)# port-range 67
wlc(config-object-group-service)# exit
wlc(config)# object-group service dhcp_client
wlc(config-object-group-service)# port-range 68
wlc(config-object-group-service)# exit
wlc(config)# object-group service ntp
wlc(config-object-group-service)# port-range 123
wlc(config-object-group-service)# exit
```

Разрешим доступ в Интернет из зон trusted и dmz:

```
wlc(config)# security zone-pair trusted untrusted
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol any
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair dmz untrusted
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol any
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
wlc(config)# security zone-pair dmz trusted
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol any
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
```

Разрешим прохождение DHCP из trusted в dmz:

```
wlc(config)# security zone-pair trusted dmz
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol udp
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# match source-port dhcp_client
wlc(config-zone-pair-rule)# match destination-port dhcp_server
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# exit
```

Разрешим прохождение ICMP к устройству, для работы BRAS необходимо открыть порты для веб-проксирования – TCP 3129/3128 (NetPort Discovery Port/Active API Server Port):

```
wlc(config)# object-group service bras
wlc(config-object-group-service)# port-range 3129
wlc(config-object-group-service)# port-range 3128
wlc(config-object-group-service)# exit
wlc(config)# security zone-pair trusted self
wlc(config-zone-pair)# rule 10
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# match source-port any
wlc(config-zone-pair-rule)# match destination-port bras
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 20
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol icmp
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair-rule)# exit
wlc(config)# security zone-pair dmz self
wlc(config-zone-pair)# rule 20
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol icmp
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair-rule)# exit
wlc(config)# security zone-pair untrusted self
wlc(config-zone-pair)# rule 20
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol icmp
wlc(config-zone-pair-rule)# match source-address any
wlc(config-zone-pair-rule)# match destination-address any
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair-rule)# exit
```

Активируем DHCP-Relay:

```
wlc(config)# ip dhcp-relay
```

Настроим SNAT в порт gigabitethernet 1/0/1:

```
wlc(config)# nat source
wlc(config-snat)# ruleset inet
wlc(config-snat-ruleset)# to interface gigabitethernet 1/0/1
wlc(config-snat-ruleset)# rule 10
wlc(config-snat-rule)# match source-address any
wlc(config-snat-rule)# action source-nat interface
wlc(config-snat-rule)# enable
wlc(config-snat-rule)# end
```

21.3 Пример настройки без SoftWLC

Задача:

Настроить BRAS без поддержки SoftWLC.

Дано:

Подсеть с клиентами 10.10.0.0/16, подсеть для работы с FreeRADIUS-сервером 192.168.1.1/24.

Решение:

Шаг 1:

Настройка RADIUS-сервера.

Для FreeRADIUS-сервера нужно задать подсеть, из которой могут приходить запросы и добавить список пользователей. Для этого в файл users в директории с файлами конфигурации FreeRADIUS-сервера нужно добавить:

Профиль пользователя:

```
<MACADDR> Cleartext-Password := <MACADDR>
```

Имя пользователя:

```
User-Name = <USER_NAME>,
```

Максимальное время жизни сессии:

```
Session-Timeout = <SECONDS>,
```

Максимальное время жизни сессии при бездействии пользователя:

```
Idle-Timeout = <SECONDS>,
```

Время на обновление статистики по сессии:

```
Acct-Interim-Interval = <SECONDS>,
```

Имя сервиса для сессии (A – сервис включен, N – сервис выключен):

```
Cisco-Account-Info = "{A|N}<SERVICE_NAME>"
```

Профиль сервиса:

```
<SERVICE_NAME> Cleartext-Password := <MACADDR>
```

Соответствует имени class-map в настройках ESR:

```
Cisco-AVPair = "subscriber:traffic-class=<CLASS_MAP>",
```

Действие, которое применяет ESR к трафику (permit, deny, redirect):

```
 Cisco-AVPair = "subscriber:filter-default-action=<ACTION>",
```

Возможность прохождения IP-потоков (enabled-uplink, enabled-downlink, enabled, disabled):

```
 Cisco-AVPair = "subscriber:flow-status=<STATUS>"
```

В файл clients.conf нужно добавить подсеть, в которой находится ESR:

```
client ESR {
ipaddr = <SUBNET>
secret = <RADIUS_KEY>
}
```

В нашем случае настройка RADIUS-сервера будет выглядеть так:

В файл «clients.conf» добавляем строки:

```
client BRAS {
ipaddr = 192.168.1.1
secret = password
}
```

В файл «users» добавляем строки (вместо <MAC> нужно указать MAC-адрес клиента):

```
"54-E1-AD-8F-37-35" Cleartext-Password := "54-E1-AD-8F-37-35"
User-Name = "Bras_user",
Session-Timeout = 259200,
Idle-Timeout = 259200,
Cisco-AVPair += "subscriber:policer-rate-in=1000",
Cisco-AVPair += "subscriber:policer-rate-out=1000",
Cisco-AVPair += "subscriber:policer-burst-in=188",
Cisco-AVPair += "subscriber:policer-burst-out=188",
Cisco-Account-Info = "AINTERNET"
INTERNET Cleartext-Password := "INTERNET"
User-Name = "INTERNET",
Cisco-AVPair = "subscriber:traffic-class=INTERNET",
Cisco-AVPair += "subscriber:filter-default-action=permit"
```

Шаг 2:

Настройка ESR.

Для настройки функционала BRAS необходимо наличие лицензии BRAS:

```
wlc(config)# do sh licence
Licence information
-------------------
Name:    Eltex
Version: 1.0
Type:    ESR-X
S/N:     NP00000000
MAC:     XX:XX:XX:XX:XX:XX
Features:
  BRAS - Broadband Remote Access Server
```

Настройка параметров для взаимодействия с RADIUS-сервером:

```
wlc(config)# radius-server host 192.168.1.2
wlc(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
wlc(config-radius-server)# source-address 192.168.1.1
wlc(config-radius-server)# exit
```

Создадим профиль AAA:

```
wlc(config)#  aaa radius-profile bras_radius
wlc(config-aaa-radius-profile)# radius-server host 192.168.1.2
wlc(config-aaa-radius-profile)#  exit
wlc(config)#  aaa radius-profile bras_radius_servers
wlc(config-aaa-radius-profile)#  radius-server host 192.168.1.2
wlc(config-aaa-radius-profile)#  exit
```

Укажем параметры к DAS-серверу:

```
wlc(config)# das-server das
wlc(config-das-server)# key ascii-text encrypted 8CB5107EA7005AFF
wlc(config-das-server)#  exit
wlc(config)#  aaa das-profile bras_das
wlc(config-aaa-das-profile)#  das-server das
wlc(config-aaa-das-profile)# exit
wlc(config)#  vlan 10
wlc(config-vlan)#  exit
```

Далее создаем правила для редиректа на портал и пропуска трафика в Интернет:

```
wlc(config)# ip access-list extended BYPASS
wlc(config-acl)# rule 1
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol udp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port 68
wlc(config-acl-rule)# match destination-port 67
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# rule 2
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol udp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 53
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config)# ip access-list extended INTERNET
wlc(config-acl)# rule 1
wlc(config-acl-rule)#  action permit
wlc(config-acl-rule)# match protocol any
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config)# ip access-list extended WELCOME
wlc(config-acl)# rule 10
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol tcp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 443
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# rule 20
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol tcp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 8443
```

```
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# rule 30
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol tcp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 80
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# rule 40
wlc(config-acl-rule)# action permit
wlc(config-acl-rule)# match protocol tcp
wlc(config-acl-rule)# match source-address any
wlc(config-acl-rule)# match destination-address any
wlc(config-acl-rule)# match source-port any
wlc(config-acl-rule)# match destination-port 8080
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
```

Настройка действия фильтрации по URL обязательно, а именно, необходимо настроить фильтрацию http-proxy на BRAS для неавторизованных пользователей:

```
wlc(config)# object-group url defaultserv
wlc(config-object-group-url)# url http://eltex.nsk.ru
wlc(config-object-group-url)# url http://ya.ru
wlc(config-object-group-url)# url https://ya.ru
wlc(config-object-group-url)# exit
```

Сконфигурируем и включим BRAS, в качестве NAS IP указываем адрес интерфейса на стыке с RADIUS-сервером в данном примере – это IP-адрес интерфейса gigabitethernet 1/0/2:

```
wlc(config)# subscriber-control
wlc(config-subscriber-control)# aaa das-profile bras_das
wlc(config-subscriber-control)# aaa sessions-radius-profile bras_radius
wlc(config-subscriber-control)# aaa services-radius-profile bras_radius_servers
wlc(config-subscriber-control)# nas-ip-address 192.168.1.1
wlc(config-subscriber-control)# session mac-authentication
wlc(config-subscriber-control)# bypass-traffic-acl BYPASS
wlc(config-subscriber-control)# default-service
wlc(config-subscriber-default-service)# class-map BYPASS
wlc(config-subscriber-default-service)# filter-name local defaultserv
wlc(config-subscriber-default-service)# filter-action permit
wlc(config-subscriber-default-service)# default-action redirect http://192.
168.1.2:8080/eltex_portal
wlc(config-subscriber-default-service)# session-timeout 121
wlc(config-subscriber-default-service)# exit
wlc(config-subscriber-control)# enable
wlc(config-subscriber-control)# exit
```

На интерфейсах, для которых требуется работа BRAS, произвести настройку (для успешного запуска требуется как минимум один интерфейс):

```
wlc(config)# bridge 10
wlc(config-bridge)# vlan 10
wlc(config-bridge)# ip firewall disable
wlc(config-bridge)# ip address 10.10.0.1/16
wlc(config-bridge)# ip helper-address 192.168.1.2
wlc(config-bridge)# service-subscriber-control any
wlc(config-bridge)# location USER
wlc(config-bridge)# protected-ports
wlc(config-bridge)# protected-ports exclude vlan
wlc(config-bridge)# enable
wlc(config-bridge)# exit
```

Сконфигурируем порт в сторону RADIUS-сервера:

```
wlc(config)# interface gigabitethernet 1/0/2
wlc(config-if-gi)# ip firewall disable
wlc(config-if-gi)# ip address 192.168.1.1/24
wlc(config-if-gi)# exit
```

Порт в сторону клиента:

```
wlc(config)# interface gigabitethernet 1/0/3.10
wlc(config-subif)# bridge-group 10
wlc(config-subif)# ip firewall disable
wlc(config-subif)# exit
```

Настройка SNAT в порт gigabitethernet 1/0/2:

```
wlc(config)# nat source
wlc(config-snat)# ruleset factory
wlc(config-snat-ruleset)# to interface gigabitethernet 1/0/2
wlc(config-snat-ruleset)# rule 10
wlc(config-snat-rule)# description "replace 'source ip' by outgoing interface ip address"
wlc(config-snat-rule)# match protocol any
wlc(config-snat-rule)# match source-address any
wlc(config-snat-rule)# match destination-address any
wlc(config-snat-rule)# action source-nat interface
wlc(config-snat-rule)# enable
wlc(config-snat-rule)# exit
wlc(config-snat-ruleset)# exit
wlc(config-snat)# exit
wlc(config)# ip route 0.0.0.0/0 192.168.1.2
```

Изменения конфигурации вступят в действие после применения:

```
wlc(config) # do commit
wlc(config) # do confirm
```

Для просмотра информации и статистики по сессиям контроля пользователей – можно воспользоваться командой:

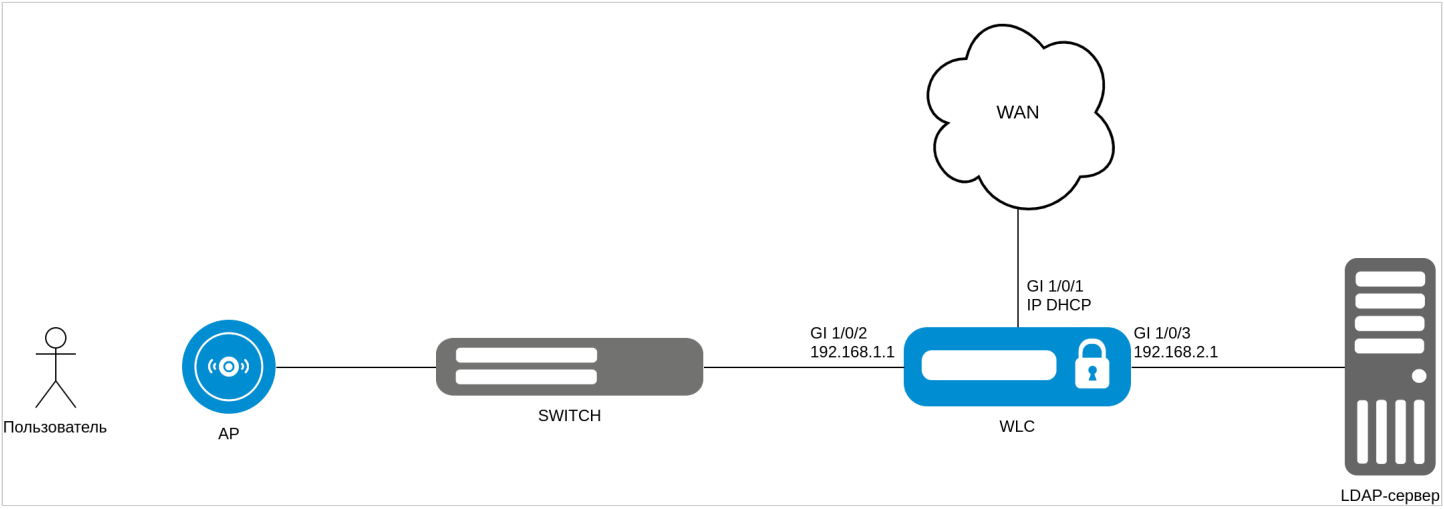
```
wlc# sh subscriber-control sessions status

Session id       User name     IP address       MAC address        Interface           Domain
--------------------   ---------------   ----------------   ------------------
1729382256910270473     Bras_user    10.10.0.3  54:e1:ad:8f:37:35     gi1/0/3.10      --
```

22 Статьи

22.1 LDAP-авторизация

22.1.1 Настройка LDAP-авторизации

> В текущей версии реализована работа LDAP-авторизации только в режиме хранения учетных данных пользователей на LDAP-сервере в открытом виде.



Для настройки LDAP-авторизации пользователей Wi-Fi понадобится предварительно настроенный LDAP-сервер (например, OpenLDAP) со следующими параметрами:

1. Создана хотя бы одна группа пользователей OU, например Users;
2. Создан хотя бы один пользователь, например user.

Перед включением функции LDAP-авторизации пользователей необходимо настроить параметры ldap-server:

```
wlc(config)# ldap-server bind authenticate root-dn "cn=admin,dc=eltex,dc=ru"
wlc(config)# ldap-server bind authenticate root-password ascii-text <пароль Администратора>
wlc(config)# ldap-server host <адрес LDAP-сервера>
wlc(config-ldap-server)# exit
```

Параметры root-dn и root-password – это параметры, с которыми создавался пользователь "Администратор" LDAP-сервера: доменное имя и пароль соответственно. Ldap-server host – адрес хоста, на котором установлен LDAP-сервер.

Далее необходимо настроить ldap-profile:

```
wlc(config)# aaa ldap-profile tester
wlc(config-aaa-ldap-profile)# base-dn "ou=Users,dc=eltex,dc=ru"
wlc(config-aaa-ldap-profile)# ldap-server host <адрес LDAP-сервера>
wlc(config-aaa-ldap-profile)# exit
wlc(config)#
```

Параметр base-dn в данном случае является доменным именем пользователя, которое задается при его создании в LDAP.

Далее необходимо указать данный профиль в настройках локального радиуса:

```
wlc(config)# radius-server local
wlc(config-radius)# virtual-server default
wlc(config-radius-vserver)# ldap-mode
wlc(config-radius-vserver)# enable
wlc(config-radius-vserver)# exit
wlc(config-radius)# ldap-profile tester
```

Примените и подтвердите конфигурацию:

```
wlc# commit
wlc# confirm
```

Для проверки к WLC должна быть подключена точка доступа и настроен SSID с Enterprise-авторизацией.

22.2 RADIUS-сервер

22.2.1 Настройка локального RADIUS-сервера

```
wlc(config)# radius-server local
```

Настраиваем **NAS ap**, который содержит подсети точек доступа, которые будут обслуживаться локальным RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:

```
wlc(config-radius)# nas ap
wlc(config-radius-nas)# key ascii-text password
wlc(config-radius-nas)# network 192.168.1.0/24
wlc(config-radius-nas)# exit
```

Настраиваем **NAS local**. Используется при обращении WLC к локальному RADIUS-серверу при построении SoftGRE-туннелей:

```
wlc(config-radius)# nas local
wlc(config-radius-nas)# key ascii-text password
wlc(config-radius-nas)# network 127.0.0.1/32
wlc(config-radius-nas)# exit
```

Создаем домен для пользователей:

```
wlc(config-radius)# domain default
```

В этом домене создаем учетную запись пользователя Wi-Fi для подключения к Enterprise SSID:

```
wlc(config-radius-domain)# user name1
wlc(config-radius-user)# password ascii-text password1
wlc(config-radius-user)# exit
wlc(config-radius-domain)# exit
```

В заводской конфигурации учетная запись пользователя не настроена в целях безопасности, поэтому для подключения к Enterprise SSID в заводской конфигурации необходимо создать учетную запись.

Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга, настройки проксирования на внешний RADIUS-сервер. Использование стандартных портов (1812 для аутентификации и 1813 для аккаунтинга) не требует настройки. В случае настройки локального RADIUS-сервера достаточно просто включения виртуального сервера (enable).

```
wlc(config-radius)# virtual-server default
wlc(config-radius-vserver)# enable

wlc(config-radius-vserver)# exit
wlc(config-radius)# enable
wlc(config)# exit
```

Определим параметры для взаимодействия с RADIUS-сервером: IP-адрес и ключ.
Так как RADIUS-сервер находится локально на контроллере, в качестве адреса хоста задаем 127.0.0.1.
Ключ должен совпадать с ключом, указанным для **nas local**, который мы задали в **radius-server local**.

```
wlc(config)# radius-server host 127.0.0.1
wlc(config-radius-server)# key ascii-text password
wlc(config-radius-server)# exit
```

Добавляем профиль AAA, указываем адрес сервера, который будет использоваться:

```
wlc(config)# aaa radius-profile default_radius
wlc(config-aaa-radius-profile)# radius-server host 127.0.0.1
wlc(config-aaa-radius-profile)# exit
```

Настраиваем и включаем функционал автоматического поднятия SoftGRE-туннелей:

```
wlc(config)# softgre-controller
```

RADIUS-сервер находится локально на контроллере, поэтому указываем nas-ip-address 127.0.0.1:

```
wlc(config-softgre)# nas-ip-address 127.0.0.1
```

Выбираем режим создания data SoftGRE туннелей – WLC:

```
wlc(config-softgre)# data-tunnel configuration wlc
```

Указываем пользовательский vlan:

```
wlc(config-softgre)# service-vlan add 3
```

Указываем созданный ранее AAA-профиль:

```
wlc(config-softgre)# aaa radius-profile default_radius
wlc(config-softgre)# keepalive-disable
wlc(config-softgre)# enable
wlc(config-softgre)# exit
```

Переходим к настройкам модуля управления конфигурацией точек доступа:

```
wlc(config)# wlc
```

Настраиваем профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi:

```
wlc(config-wlc)# radius-profile default-radius
```

RADIUS-сервер находится локально на контроллере, указываем адрес контроллера в подсети точек доступа:

```
wlc(config-wlc-radius-profile)# auth-address 192.168.1.1
```

Ключ RADIUS-сервера должен совпадать с ключом, указанным для **NAS ap**, который мы указали в **radius-server local**:

```
wlc(config-wlc-radius-profile)# auth-password ascii-text password
```

Указываем домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные записи пользователей Enterprise, который располагается в **radius-server local:**

```
wlc(config-wlc-radius-profile)# domain default
wlc(config-wlc-radius-profile)# exit
```

Профиль SSID содержит настройки SSID точки доступа:

```
wlc(config-wlc)# ssid-profile default-ssid
```

Указываем в **ssid-profile** ранее настроенный профиль настроек RADIUS-сервера, который будет использоваться для авторизации пользователей Wi-Fi и пользовательский vlan:

```
wlc(config-wlc-ssid-profile)# radius-profile default-radius

wlc(config-wlc-ssid-profile)# vlan-id 3
```

22.2.2 Настройка проксирования на внешний RADIUS

Настраиваем локальный RADIUS-сервер

```
wlc# configure
wlc(config)# radius-server local
```

Настраиваем **NAS ap**, который содержит подсети точек доступа, которые будут обслуживаться локальным RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi:

```
wlc(config-radius)# nas ap
wlc(config-radius-nas)# key ascii-text password
wlc(config-radius-nas)# network 192.168.1.0/24
wlc(config-radius-nas)# exit
```

Настройки виртуального сервера содержат номера портов для аутентификации и аккаунтинга, настройки проксирования на внешний RADIUS server. Использование стандартных портов (1812 для аутентификации и 1813 для аккаунтинга) не требует настройки. Для проксирования RADIUS-запросов на внешний сервер необходимо включить proxy-mode:

Типы upstream серверов
Server-type auth — используется для проксирования только запросов аутентификации. Запросы будут проксироваться на порт, указанный в параметре port (по умолчанию – 1812).
Server-type acct — используется для проксирования только аккаунтинга. Проксирование осуществляется на порт, указанный в параметре port (по умолчанию – 1812). При необходимости измените его (стандартный порт для аккаунтинга – 1813).
Server-type all — используется для проксирования запросов аутентификации и аккаунтинга. Запросы аутентификации будут проксироваться на порт, указанный в параметре port (по умолчанию – 1812), а аккаунтинг будет проксироваться на порт = 'port'+1 (то есть по умолчанию – 1813).

Настраиваем внешний сервер (virtual-server), указывая его адрес, тип (server-type) и ключ, также можно указать порт. По умолчанию выставлен сервер для аутентификации (server-type auth) и порт 1812, если нет необходимости менять эти настройки, тогда достаточно настроить адрес и ключ для сервера:

```
wlc(config-radius)# virtual-server default
wlc(config-radius-vserver)# enable
wlc(config-radius-vserver)# proxy-mode
wlc(config-radius-vserver)# upstream-server eltex
wlc(config-radius-upstream-server)# host 10.10.10.12
wlc(config-radius-upstream-server)# server-type all
wlc(config-radius-upstream-server)# key ascii-text password
wlc(config-radius-vserver)# exit
```

```
wlc(config-radius)# enable
wlc(config)# exit
```

Переходим к настройкам модуля управления конфигурацией точек доступа:

```
wlc(config)# wlc
```

Настраиваем профиль RADIUS-сервера, который будет использоваться для аутентификации беспроводных клиентов Enterprise SSID точек доступа Wi-Fi:

```
wlc(config-wlc)# radius-profile default-radius
```

Поскольку мы настраиваем проксирование запросов аутентификации и аккаунтинга, то указываем адрес контроллера локального RADIUS-сервера в подсети точек доступа.
Ключ RADIUS-сервера должен совпадать с ключом, указанным для **NAS ap**, который мы указали в **radius-server local.**

```
wlc(config-wlc-radius-profile)# auth-address 192.168.1.1
wlc(config-wlc-radius-profile)# auth-password ascii-text password
```

Если вы используете проксирование на SoftWLC, укажите домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные записи пользователей Enterprise на SoftWLC.

wlc(config-wlc-radius-profile)# domain root

Указываем IP-адрес RADIUS-сервера подсети точек доступа, используемого для аккаунтинга и ключ RADIUS-сервера:

```
wlc(config-wlc-radius-profile)# acct-address 192.168.1.1
wlc(config-wlc-radius-profile)# acct-password ascii-text password
```

Активируем отправку аккаунтинга на RADIUS-сервер:

```
wlc(config-wlc-radius-profile)# acct-enable
```

Настройки SSID точки доступа.

```
wlc(config-wlc)# ssid-profile default-ssid
```

Указываем в **ssid-profile** ранее настроенный профиль настроек RADIUS-сервера, который будет использоваться для авторизации пользователей Wi-Fi:

```
wlc(config-wlc-ssid-profile)# radius-profile default-radius
```

Для настройки внешнего RADIUS-сервера необходимо записать в таблицу NAS внешнего RADIUS-сервера адрес и ключ локального RADIUS-сервера WLC-30.

Пример конфигурации:

```
 radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  virtual-server default
    proxy-mode
    upstream-server eltex
      host 10.10.10.12
      server-type all
      key ascii-text encrypted 8CB5107EA7005AFF
    exit
    enable
  exit
  enable
exit



wlc
 radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    acct-enable
    acct-address 192.168.1.1
    acct-password ascii-text encrypted 8CB5107EA7005AFF
exit
```

22.3 TLS-авторизация

22.3.1 Настройка TLS-авторизации

Для настройки TLS-авторизации необходимо:

1. Сгенерировать клиентский сертификат;
2. Настроить radius-server local;
3. Загрузить и установить созданный сертификат на клиентское устройство.

Генерация клиентского сертификата

Для генерации сертификата клиента нужно создать private-key, сгенерировать csr, выпустить сертификат клиента и создать контейнер pkcs12.

Генерация private-key

Для каждого сертификата клиента необходимо создать private-key. Используется алгоритм RSA, размер ключа в битах задается в диапазоне от 1024 до 4096 (необязательный параметр, по умолчанию – 2048 бит).

Команда имеет вид:

```
crypto generate private-key rsa [размер ключа 1024-4096] filename <Имя файла для ключа .pem>
```

Если ввести знак "?" после **filename**, то в подсказке будет показан список файлов с ключами в директории **crypto:private-key/.**

```
wlc# crypto generate private-key rsa filename ?
  WORD(1-31)  Name of file

  ----FILE----
  default_ca_key.pem
  default_cert_key.pem
  tester.pem
  wlc-sa.key
```

Можно выбрать файл, который уже существует и перезаписать его:

```
wlc# crypto generate private-key rsa 1024 filename tester.pem
Destination file already exists.
Do you really want to overwrite it? (y/N): y
..........++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..................++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Если файлов слишком много, то в списке будет присутствовать только часть сертификатов:

```
wlc# crypto generate cert csr tester.csr ca ?
  CRYPTO FILES  Select file:

  ----FILE----
  E828C1000002.pem                  E828C1000004.pem                  E828C1000006.pem
  E828C1000008.pem                  E828C100000A.pem                  E828C100000C.pem
  E828C100000E.pem                  E828C1000010.pem                  E828C1000012.pem
  E828C1000014.pem                  E828C1000016.pem                  E828C1000018.pem
  E828C100001A.pem                  E828C100001C.pem                  E828C100001E.pem
  E828C1000020.pem                  E828C1000022.pem                  E828C1000024.pem
  E828C1000026.pem                  E828C1000028.pem                  E828C100002A.pem
  E828C100002C.pem                  E828C100002E.pem                  E828C1000030.pem
  E828C1000032.pem                  E828C1000034.pem                  E828C1000036.pem
  E828C1000038.pem                  E828C100003A.pem                  E828C100003C.pem
  E828C100003E.pem                  E828C1000040.pem                  E828C1000042.pem
  E828C1000044.pem                  E828C1000046.pem                  E828C1000048.pem
  E828C100004A.pem                  E828C100004C.pem                  E828C100004E.pem
  E828C1000050.pem                  E828C1000052.pem                  E828C1000054.pem
  E828C1000056.pem                  E828C1000058.pem                  E828C100005A.pem
  E828C100005C.pem                  E828C100005E.pem                  E828C1000060.pem
  E828C1000062.pem                  E828C1000064.pem                  E828C1000066.pem
  E828C1000068.pem                  E828C100006A.pem                  E828C100006C.pem
  E828C100006E.pem                  E828C1000070.pem                  E828C1000072.pem
  E828C1000074.pem                  E828C1000076.pem                  E828C1000078.pem
  E828C100007A.pem                  E828C100007C.pem                  E828C100007E.pem
  E828C1000080.pem                  E828C1000082.pem                  E828C1000084.pem
  E828C1000086.pem                  E828C1000088.pem                  E828C100008A.pem
  ...
```

В этом случае можно ввести часть слова и знак "?", чтобы увидеть отфильтрованные записи:

```
wlc# crypto generate cert csr tester.csr ca d?
  CRYPTO FILES  Select file:

  ----FILE----
  default_ca.pem                    default_cert.pem
```

Работа с файлами аналогична в остальных командах генерации сертификата.

Пример генерации private-key

```
wlc# crypto generate private-key rsa 4096 filename tester.pem
.+...+..................+....+...+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++
+++++++*...+.+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.............
+...........+....................+.....+....+..
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Генерация csr

При генерации csr нужно выбрать **private-key** (файл, сгенерированный на предыдущем шаге), указать **common-name** в формате <имя пользователя>@<домен> и выбрать файл для сохранения csr **(filename).** Рекомендуется использовать реальные имя пользователя и домен в **common name.**

Помимо обязательных параметров существуют опциональные параметры:

- alternative-name – альтернативное имя пользователя (5–255 символов);
- country – код страны (2 символа);

- email-address – адрес электронной почты (3–64 символа);
- locality – местонахождение клиента (1–128 символов);
- organization – название организации (1–64 символа);
- organizational-unit – название структурного подразделения организации (1–64 символа);
- state – название региона/области (1–128 символов).

Пример генерации csr с минимальным количеством заполненных полей

```
wlc# crypto generate csr private-key tester.pem common-name tester@wlc.root filename tester.csr
```

Пример генерации csr со всеми заполненными полями

```
crypto generate csr private-key tester.pem alternative-name IP:10.10.10.10 common-name
tester@wlc.root country ru email-address test@test.com locality 4_floor organization ELTEX
organizational-unit wireless state Novosibirsk_oblast filename tester.csr
```

Посмотреть созданный csr можно с помощью команды **show crypto certificates csr <имя файла>**:

Пример созданного сертификата

```
wlc# show crypto certificates csr tester.csr
Version:                                1
Subject name:
    C(countryName):                     ru
    ST(stateOrProvinceName):            Novosibirsk_oblast
    L(localityName):                    4_floor
    O(organizationName):                ELTEX
    OU(organizationalUnitName):         wireless
    CN(commonName):                     tester@wlc.root
    emailAddress(emailAddress):         test@test.com
Signature:
    Algorithm:                          sha256WithRSAEncryption
    Value:                              32:DE:27:BE:38:E0:B4:1A:BE:57:0C:50:5E:05:D5:9F:3D:ED:
                                        12:EC:27:3F:42:17:3D:36:EC:72:4A:52:AF:0C:C1:FB:6A:CA:
                                        12:27:E7:C2:31:0A:5A:2D:5D:C3:5D:6B:80:6E:86:D1:66:06:
                                        4F:21:AC:A9:40:E7:1F:CC:FD:D0:9B:C4:D7:F0:56:84:19:07:
                                        1E:D4:28:0F:C9:36:26:D6:D1:9F:25:F6:73:04:DB:9A:31:94:
                                        79:BE:8D:8E:97:05:0E:F8:A7:CD:A7:F8:80:6E:E1:A2:7B:D5:
                                        D7:1F:73:8E:D0:C3:2E:F3:D2:EF:87:E0:9A:F8:F3:6B:A6:4D:
                                        E3:6C:5A:B7:6E:2A:61:DE:BF:8E:FB:94:D5:DC:40:15:39:70:
                                        43:AA:9B:B1:76:43:BA:7E:52:FD:46:6F:E3:1B:C0:19:09:86:
                                        6E:71:9B:37:BD:A5:B9:0C:E8:66:4E:8E:DF:E0:9B:70:07:48:
                                        15:CD:6F:8E:80:87:56:89:74:17:9D:C3:D5:2A:92:C4:BB:16:
                                        D9:09:E7:8A:EB:D0:3B:C4:A8:74:92:92:C3:39:40:3D:8E:62:
                                        7D:A7:B6:22:D9:5D:50:5D:BB:CD:B5:0D:47:D2:F6:C1:D6:FF:
                                        FA:18:58:15:A9:52:B1:D3:3C:94:A4:40:4B:15:D1:48:F8:53:
                                        E8:A8:3A:35
Subject Public Key Info:
    Algorithm:                          RSA
    Key size:                           2048
    Exponent:                           65537
    Modulus:                            00:AE:90:97:89:02:4D:49:6F:D7:45:9F:19:8D:4B:F7:30:6B:
                                        5C:DF:FE:2B:D0:E4:85:66:45:2E:2E:98:20:E8:B8:A2:42:29:
                                        C1:1A:A1:44:B4:DD:B1:BE:93:45:1F:0E:7A:A6:A9:C1:5B:D6:
                                        DD:74:4C:E6:DE:D2:B9:12:5A:8F:33:DE:21:64:08:BE:1B:D5:
                                        1B:C2:2C:07:AB:4D:40:3F:87:C7:60:41:EC:9C:48:35:D0:16:
                                        70:DD:A7:28:26:34:A4:54:E4:55:14:72:2A:0A:39:A8:39:E5:
                                        4A:CA:1F:D9:10:4C:7B:BC:BE:F4:08:64:CE:A0:43:7D:FA:EB:
                                        B4:7C:F7:0B:D6:AF:C9:AA:37:B9:9A:10:6F:3D:2F:D7:71:FC:
                                        DB:6C:76:E5:9F:25:DC:80:D6:BB:71:E7:9C:31:42:F8:A3:D4:
                                        67:E3:5D:F8:FB:9A:EF:44:E4:E3:C1:8C:00:23:9D:C0:37:76:
                                        23:9D:B5:B3:C4:45:D7:84:C9:10:4D:26:56:CF:6D:AA:F3:10:
                                        34:AC:C4:AC:7B:7A:CA:D1:BC:D6:D6:84:74:AB:42:FB:AE:56:
                                        EC:26:09:DF:A1:2B:B1:AD:D5:F7:78:8C:89:0D:B1:5F:A9:D1:
                                        23:63:8E:8E:BF:AE:26:F8:EC:39:8A:4C:45:5C:3B:AB:BE:40:
                                        23:7D:73:F2:A7
X509v3 Subject Alternative Name:
    Names:                              IP Address:10.10.10.10
    Critical:                           No
```

Генерация сертификата, подписанного CA от RADIUS

После генерации csr клиента нужно подписать его с помощью CA-сертификата от RADIUS-сервера.

Пример CA-сертификата

```
wlc# sh crypto certificates cert default_ca.pem
Version:                                3
Serial:                                 43:60:5B:D5:8E:6B:0A:56:39:0D:0D:D2:6E:25:CF:31:37:F3:
                                        EB:24
Subject name:
    C(countryName):                     RU
    ST(stateOrProvinceName):            Russia
    L(localityName):                    Novosibirsk
    O(organizationName):                Eltex Enterprise Ltd
    CN(commonName):                     Eltex default certificate authority
Issuer name:
    C(countryName):                     RU
    ST(stateOrProvinceName):            Russia
    L(localityName):                    Novosibirsk
    O(organizationName):                Eltex Enterprise Ltd
    CN(commonName):                     Eltex default certificate authority
Validity period:
    Valid after:                        25.12.2023 09:32:54
    Invalid after:                      01.12.2123 09:32:54
Signature:
    Algorithm:                          sha256WithRSAEncryption
    Value:                              3C:7B:5B:A1:E9:E4:61:67:86:09:F0:54:BF:1F:18:47:7D:D3:
                                        F6:F0:B2:96:24:AC:88:41:EE:ED:69:43:1D:45:BD:5F:00:85:
                                        CE:6D:02:90:80:38:CC:1D:78:EE:58:6B:22:1D:D4:62:A0:6D:
                                        FB:1A:AB:E7:5C:29:99:1F:4E:FD:0D:92:85:35:6C:0E:22:78:
                                        3F:37:26:41:E3:6B:74:21:5F:AC:EF:2C:55:19:5E:44:AA:63:
                                        FE:40:6C:76:C4:29:F2:DB:35:E1:7B:CA:7C:E0:0B:D1:26:2E:
                                        D5:33:46:0A:F4:B0:E3:03:7D:0D:93:7E:D3:86:77:90:C9:EB:
                                        58:31:51:A7:09:76:D5:06:B1:70:14:E9:04:0B:5C:D1:1B:B0:
                                        44:45:41:6C:DC:CD:E6:B4:0A:85:04:1C:4A:31:63:3C:03:AE:
                                        3C:84:CB:01:C3:20:97:74:C8:42:63:A2:F1:B1:68:92:2F:9D:
                                        35:3E:61:97:37:4E:97:CD:75:78:72:C5:D1:B7:8F:5F:78:E0:
                                        B3:96:BA:0D:DB:4D:E5:B0:43:BC:D1:94:42:02:FD:5B:A6:7A:
                                        CC:33:B5:4E:CF:8C:2C:91:16:E8:3E:14:2C:ED:48:5A:2C:CD:
                                        E4:1C:B6:3D:F7:B4:5D:C8:F9:89:6B:E4:DC:31:CD:C8:27:C5:
                                        6C:1F:B4:DA
Public key info:
    Algorithm:                          RSA
    Key size:                           2048
    Exponent:                           65537
    Modulus:                            00:B7:D2:A2:88:E1:4D:80:62:26:43:09:82:85:4B:5F:7C:B3:
                                        77:0E:D5:E3:7C:62:F5:5A:12:16:71:4E:DA:48:A3:B5:6A:3F:
                                        83:F2:9B:BA:89:E7:0F:52:C5:F1:F2:DD:D2:7E:42:3A:F1:8A:
                                        AF:EC:0D:3C:47:C2:9A:7E:DC:27:B6:AA:4C:B0:3F:AE:5D:4F:
                                        93:17:A9:9F:60:B3:29:3B:46:7C:BA:F7:6C:73:95:F2:0E:BC:
                                        71:00:D7:47:BC:5E:4F:FB:8F:B8:E2:50:91:41:30:CE:73:DA:
                                        1F:17:2D:94:21:02:24:D5:FA:EA:1A:18:C6:1C:DB:9F:B2:2A:
                                        27:0B:2F:65:35:A7:FB:1E:32:40:28:85:CD:F8:B1:46:68:48:
                                        AB:7E:E7:5F:4E:B7:0D:8D:40:1A:03:76:24:A2:63:10:0A:C2:
                                        69:CD:DA:3E:E3:A0:C0:EF:9F:BA:B4:D5:37:89:F7:E8:9E:79:
                                        C2:8E:1A:65:45:4B:7F:1D:F5:44:C5:BD:C8:D9:81:C3:6B:C2:
                                        A0:1A:C7:A0:78:B1:D3:F3:C4:9A:A2:A1:25:82:94:EC:56:B9:
                                        F2:45:60:EC:24:B2:3B:1A:32:C9:B5:47:8F:B9:DC:24:CC:2D:
                                        89:67:05:0D:8C:50:4F:D8:6B:A1:48:57:30:71:16:95:0A:49:
                                        5C:48:41:0B:15
X509v3 Subject key identifier:
    ID:                                 CE:26:E0:9F:6B:39:95:5F:2C:AC:99:87:70:EA:90:7D:7E:C7:
                                        86:40
```

```
    Critical:                           No
X509v3 Authority key identifier:
    ID:                                 CE:26:E0:9F:6B:39:95:5F:2C:AC:99:87:70:EA:90:7D:7E:C7:
                                        86:40
    Critical:                           No
X509v3 Basic Constraints:
    CA:                                 Yes
    Critical:                           Yes
```

Команда генерации сертификата имеет вид:

```
crypto generate cert csr <имя csr-файла> ca <Имя файла CA-сертификата> private-key <Имя файла ключа CA-сертификата> filename <имя crt-файла для сохранения>
```

Пример генерации сертификата клиента

```
wlc# crypto generate cert csr tester.csr ca default_ca.pem private-key default_ca_key.pem
filename tester.crt
Certificate request self-signature ok
subject=C = ru, ST = Novosibirsk_oblast, L = 4_floor, O = ELTEX, OU = wireless, CN = tester@wlc.
root, emailAddress = test@test.com
```

Пример сгенерированного сертификата

```
wlc# sh crypto certificates cert tester.crt
Version:                                1
Serial:                                 56:5D:6F:19:3F:AB:17:5A:B5:7A:81:0F:0A:2A:AD:7F:9B:20:
                                        87:41
Subject name:
    C(countryName):                     ru
    ST(stateOrProvinceName):            Novosibirsk_oblast
    L(localityName):                    4_floor
    O(organizationName):                ELTEX
    OU(organizationalUnitName):         wireless
    CN(commonName):                     tester@wlc.root
    emailAddress(emailAddress):         test@test.com
Issuer name:
    C(countryName):                     RU
    ST(stateOrProvinceName):            Russia
    L(localityName):                    Novosibirsk
    O(organizationName):                Eltex Enterprise Ltd
    CN(commonName):                     Eltex default certificate authority
Validity period:
    Valid after:                        25.12.2023 09:40:47
    Invalid after:                      01.12.2123 09:40:47
Signature:
    Algorithm:                          sha256WithRSAEncryption
    Value:                              B5:8A:92:2A:A8:F0:82:0A:97:0D:D5:D1:5D:33:5F:F3:E2:A1:
                                        EE:3D:3D:F6:87:09:D0:4A:1F:E4:43:D8:E8:36:E5:A0:88:E2:
                                        80:80:59:EA:24:57:02:3D:3D:0A:21:4C:9C:FC:D8:88:27:3E:
                                        DF:96:75:A5:48:26:64:61:CE:ED:C9:91:AA:F4:10:63:2A:2D:
                                        95:8A:85:7E:55:68:8D:F3:08:F7:F4:08:61:1E:78:D5:51:75:
                                        89:23:E7:B5:49:18:55:E5:57:25:4C:3D:7E:65:73:60:AF:DC:
                                        50:72:2B:69:C8:A7:E7:03:7B:D7:C9:FF:5F:B2:17:3E:F0:71:
                                        46:E0:7F:14:77:00:D1:BB:B3:01:0F:4E:D0:F4:20:06:72:C2:
                                        62:53:D4:4C:84:E1:FD:95:3A:FE:18:77:AE:D8:ED:83:6C:47:
                                        4C:43:41:64:8E:60:38:8F:04:99:97:BE:C3:CB:DB:20:85:90:
                                        A9:0E:88:3D:D0:47:65:1D:CB:F5:9B:D9:87:36:9C:9B:CA:02:
                                        43:3F:45:34:F0:82:63:DA:A4:D3:88:07:10:E9:BD:F5:0C:BD:
                                        3C:E1:8A:2B:33:B9:07:F6:32:2A:D7:ED:91:8F:C3:F7:B2:C2:
                                        D1:B4:2A:F5:30:56:F2:5D:FF:DC:AC:03:C8:75:BA:D2:3F:3D:
                                        39:BD:59:2F
Public key info:
    Algorithm:                          RSA
    Key size:                           1024
    Exponent:                           65537
    Modulus:                            00:B0:52:66:23:B2:31:DE:EB:9F:44:BF:62:58:86:67:71:F0:
                                        79:A0:77:42:11:75:A3:F3:36:69:47:B5:5A:AD:64:98:9C:D4:
                                        29:E8:5D:89:E0:BB:90:6C:69:19:75:FC:B9:3F:B8:A5:D0:2E:
                                        47:59:A9:59:A1:6A:55:2E:70:3E:B3:AD:A8:FE:9B:33:C6:6C:
                                        90:B7:BD:4F:8D:C3:5C:6F:D5:39:9C:87:A1:54:C6:D2:E6:AC:
                                        F1:6A:23:77:36:6F:65:96:41:F5:06:08:EE:EA:C7:4C:C6:DA:
                                        F9:CA:9B:C5:69:3D:FF:18:09:8E:C9:E6:FE:3B:68:85:7B:F2:
                                        88:85:01
```

Создание контейнера PKCS #12 с ключом и сертификатами

Формат .p12, также известный как PKCS #12, является стандартным форматом контейнера, который используется для хранения и обмена зашифрованными или подписанными данными. Он может содержать закрытые ключи, сертификаты, цепочки сертификации, а также другую смежную информацию. Рекомендуется использовать именно формат .p12, так как он поддерживается

практически всеми операционными системами, программным обеспечением и устройствами, включая Windows, macOS, Linux, Android и iOS. Контейнеры формата .p12 могут быть защищены паролем, что обеспечивает дополнительный уровень безопасности. Пароль может быть использован для шифрования закрытых ключей и сертификатов, что делает их доступными только авторизованным пользователям. В формате .p12 можно хранить не только сертификаты, но и целую цепочку сертификации, что упрощает процесс установки и обновления сертификатов на различных устройствах.

Команда генерации контейнера имеет вид:

```
crypto generate pfx private-key <Имя файла ключа от клиентского сертификата> cert <Имя файла клиентского сертификата> ca <Имя файла CA> password ascii-text <Пароль от контейнера> filename <Имя файла для сохранения сертификата (.p12)>
```

Пример генерации контейнера

```
wlc# crypto generate pfx private-key tester.pem cert tester.crt ca default_ca.pem password ascii-text 12345678 filename tester.p12
```

Настройка radius-server local

В настройках **radius-server local** необходимо включить **tls mode domain** в выбранном домене:

```
wlc(config-radius)# domain default
wlc(config-radius-domain)# tls mode domain
```

Настройка SSID и RADIUS-профиля

Для корректной работы TLS-авторизации необходимо настроить RADIUS-профиль и SSID-профиль на работу с нужным доменом:

```
configure
    wlc
        ssid-profile default-ssid
            description default-ssid
            ssid wlc_tls_ssid
            radius-profile tls-radius
        exit
        radius-profile tls-radius
            auth-address 192.168.1.1
            auth-password ascii-text encrypted 8CB5107EA7005AFF
            domain wlc.root
        exit
```

Настройка пользователя

Для завершения настройки WLC нужно указать сгенерированный сертификат в настройках пользователя, для которого этот сертификат сгенерирован. В примере common-name tester@wlc.root, поэтому нужно перейти к настройкам пользователя tester в домене wlc.root и указать название файла с сертификатом этого пользователя командой:

```
crypto cert <имя файла>
```

Пример:

```
wlc# configure
wlc(config)# radius-server local
wlc(config-radius)# domain wlc.root
wlc(config-radius-domain)# user tester
wlc(config-radius-user)# crypto cert tester.crt
```

После настройки необходимо применить изменения:

```
wlc# commit
wlc# confirm
```

Пример конфигурации radius-server local:

```
radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  domain default
  exit
  domain wlc.root
    user tester
      password ascii-text encrypted 8CB5107EA7005AFF
      crypto cert tester.crt
    exit
  exit
  virtual-server default
    no proxy-mode
    auth-port 1812
    acct-port 1813
    enable
  exit
  enable
  tls mode domain
  crypto private-key default_cert_key.pem
  crypto cert default_cert.pem
  crypto ca default_ca.pem
exit
```

22.3.2 Установка клиентского сертификата

Экспорт сертификата

Для установки сертификата на устройство клиента нужно экспортировать его с WLC. Это можно сделать с помощью команды **copy** с использованием протоколов ftp, http, https, scp, sftp, tftp, а также на USB- и MMC-устройства. Команда передачи контейнера с сертификатом имеет вид:

```
copy crypto:pfx/<Имя контейнера> <DESTINATION>
```

где <DESTINATION> – путь для копирования. Подробнее о команде **copy** можно прочитать по ссылке.

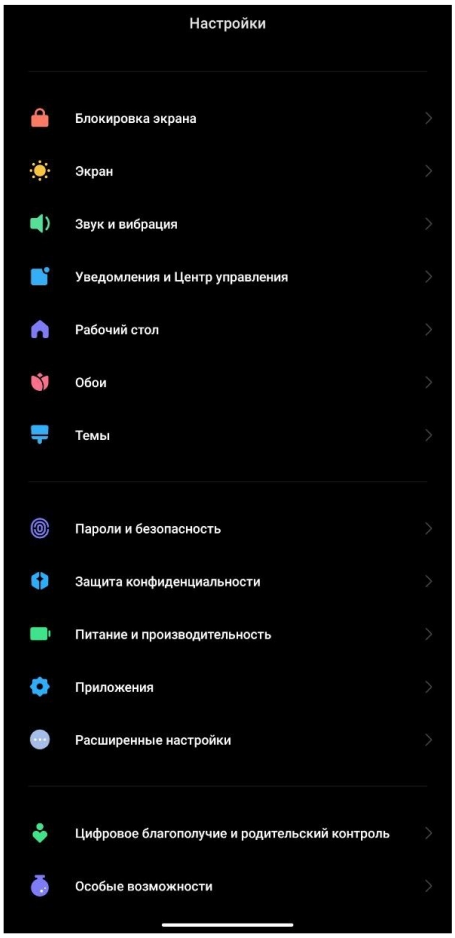
Пример команды экспорта сертификата с помощью tftp

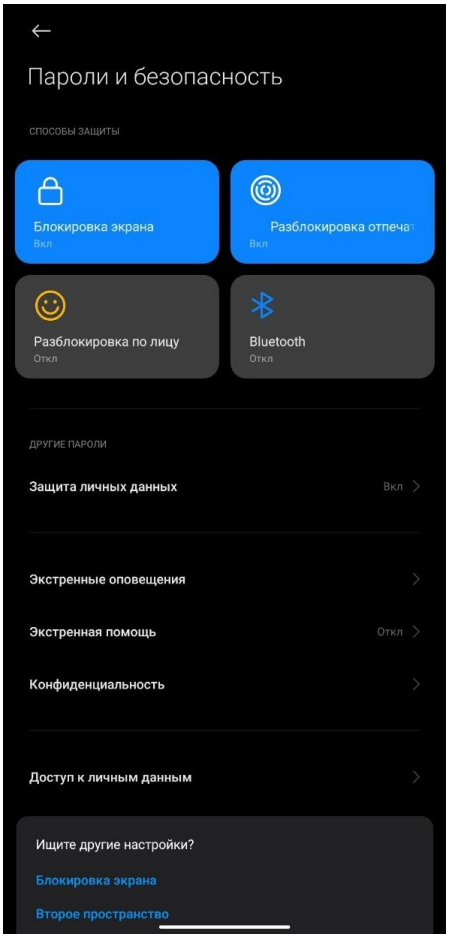
```
wlc# copy crypto:pfx/tester.p12 tftp://100.110.1.79:/tester.p12
|****************************************| 100% (2861B) Success!
```

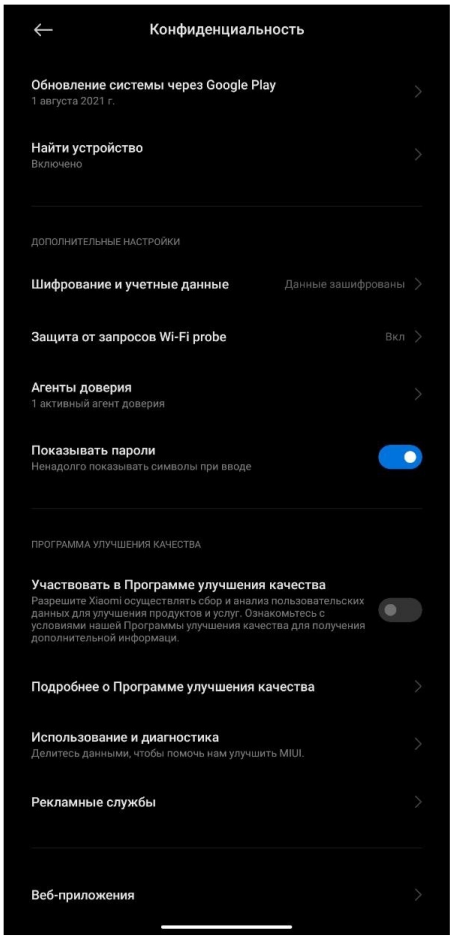
Установка сертификата для устройств с Android версии 11 и выше

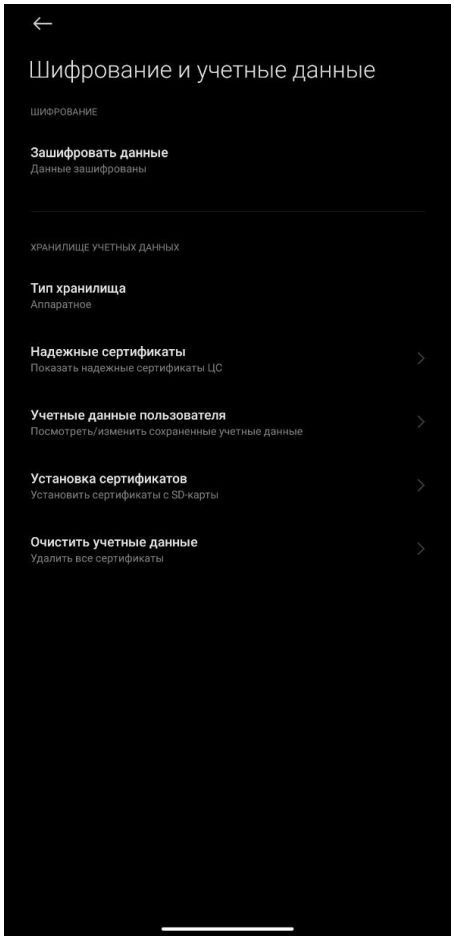
Для установки сертификата на устройство с Android скопируйте содержимое архива на клиентское устройство.

1. Зайдите в настройки устройства и откройте раздел "Пароли и безопасность" → "Конфиденциальность" → "Шифрование и учетные данные";

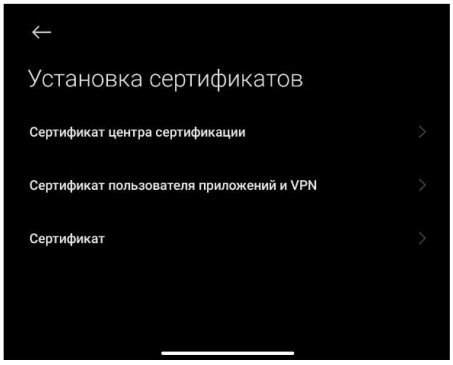






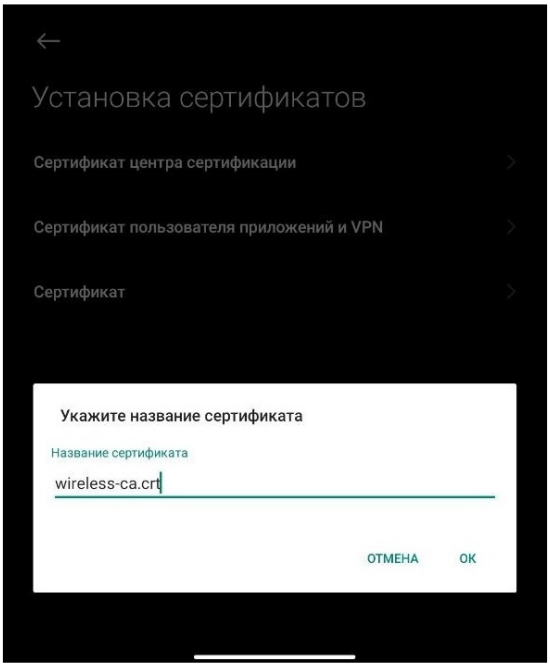


4. Если имеются старые сертификаты, то их можно удалить кнопкой "Очистить учетные данные";
5. Для загрузки новых сертификатов нажмите кнопку "Установка сертификатов";
6. Корневой и пользовательский сертификаты устанавливаются нажатием кнопки "Сертификат".

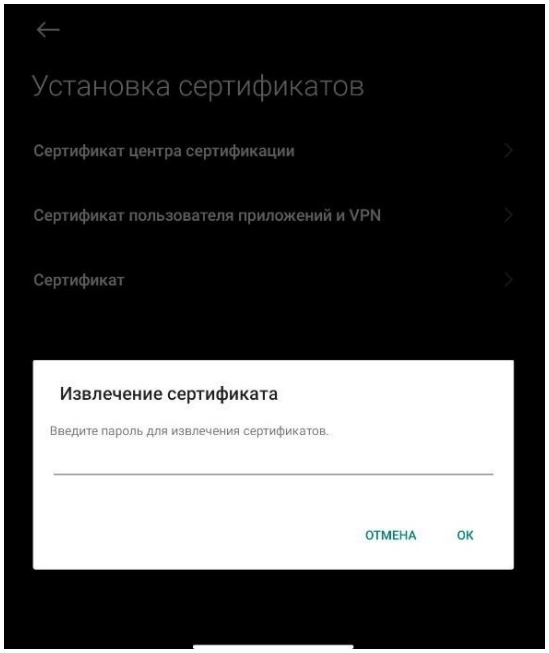


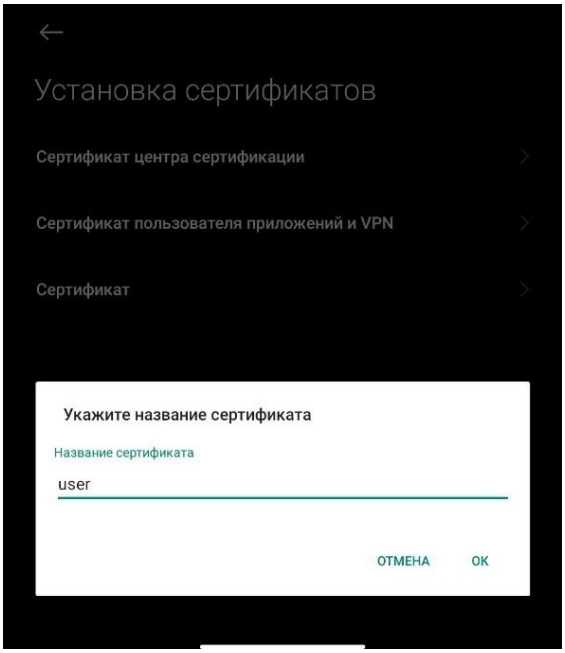
7. Выберите расположение распакованного архива;

8. Для загрузки корневого сертификата выберите файл "wireless-ca.crt", затем введите его название;



9. Для загрузки пользовательского сертификата выберите файл "user.p12", затем введите пароль, указанный в сертификате, и название.



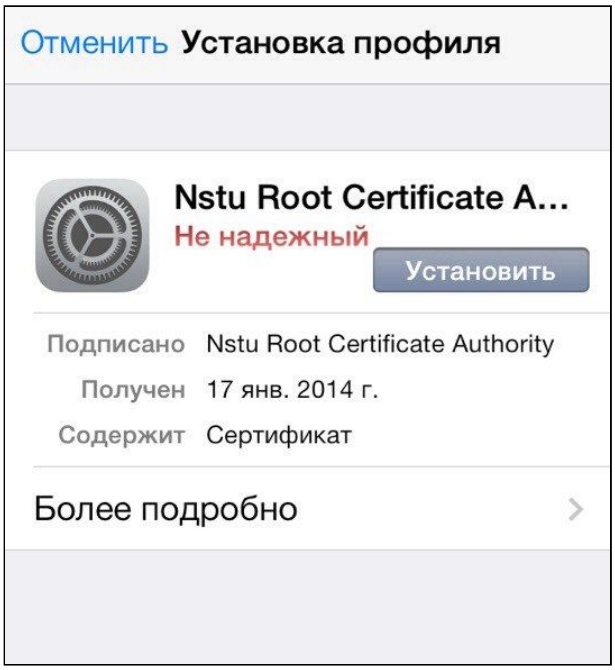


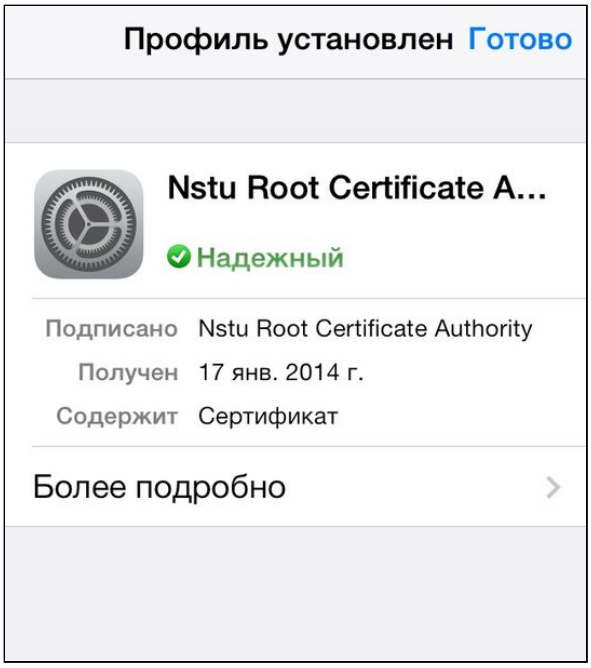
Установка сертификата в iOS

Для установки сертификата на устройство с iOS отправьте файлы с сертификатами (*.crt и *.p12) почтой на свой e-mail и откройте их на телефоне. Также можно загрузить файлы на свой телефон через usb.

Установка корневого сертификата

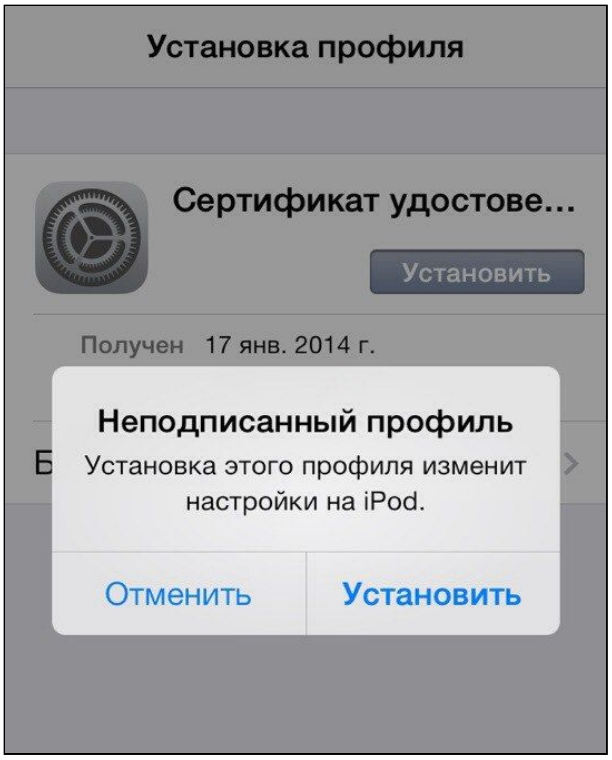
Открыв письмо с вложенным файлом стандартными приложениями iOS (Safari, Mail), нажмите на файл с расширением *.crt. При установке сертификата система будет предупреждать о ненадежности профиля, разрешите установку и сертификат будет успешно установлен.

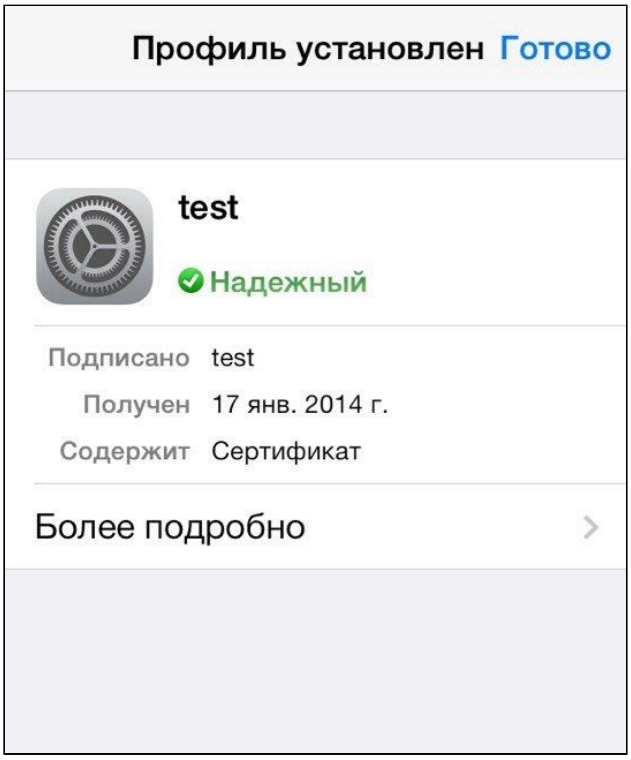


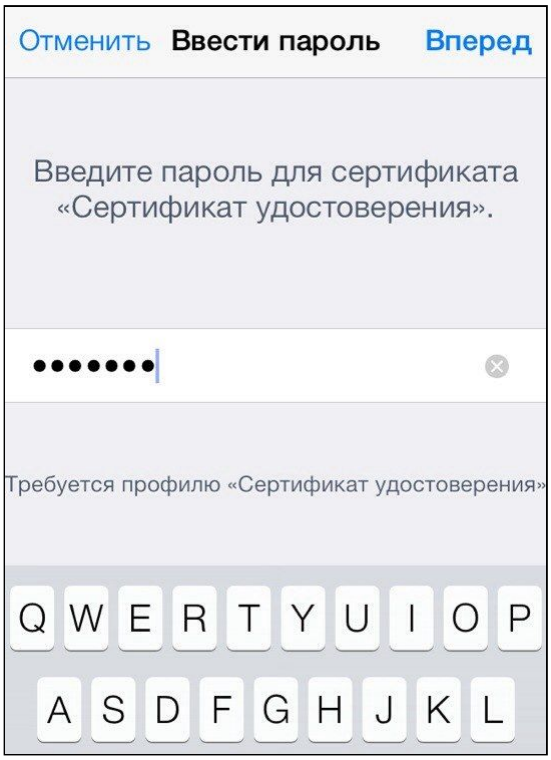


Установка пользовательского сертификата

Установка пользовательского сертификата происходит аналогично установке корневого сертификата. Далее необходимо ввести пароль сертификата. Пароль соответствует параметру сертификата Password, который находится в файле .txt.

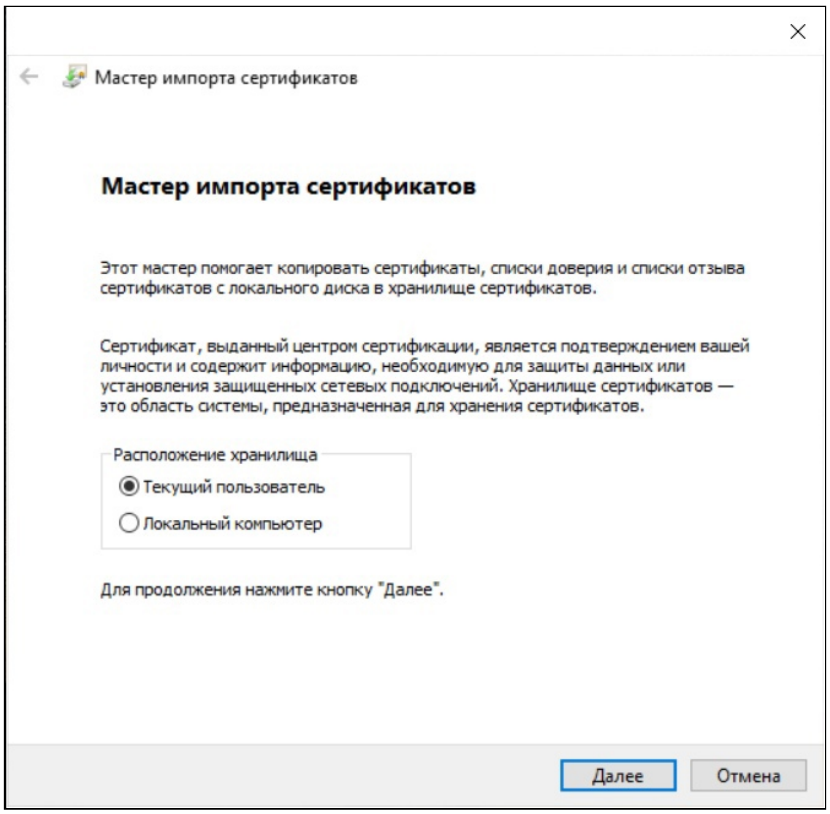

Установка профиля
Сертификат удостове...
Установить
Получен 17 янв. 2014 г.
Неподписанный профиль
Установка этого профиля изменит настройки на iPod.
Отменить
Установить


Профиль установлен
Готово
test
Надежный
Подписано test
Получен 17 янв. 2014 г.
Содержит Сертификат
Более подробно

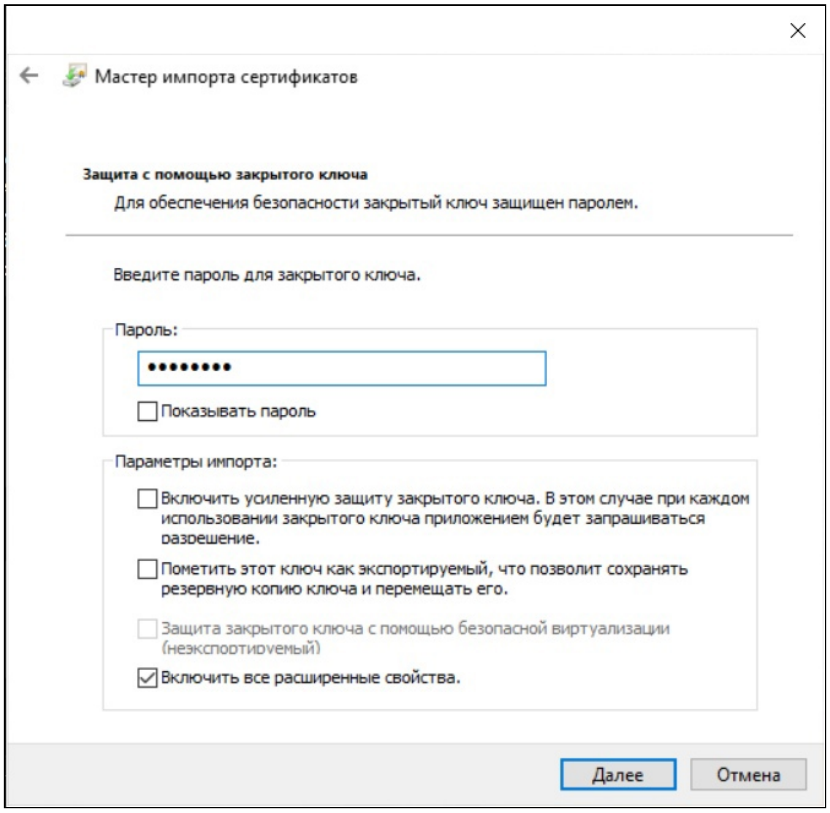

Отменить
Ввести пароль
Вперед
Введите пароль для сертификата «Сертификат удостоверения».
Требуется профилю «Сертификат удостоверения»
Q W E R T Y U I O P
A S D F G H J K L

Установка сертификата в Windows

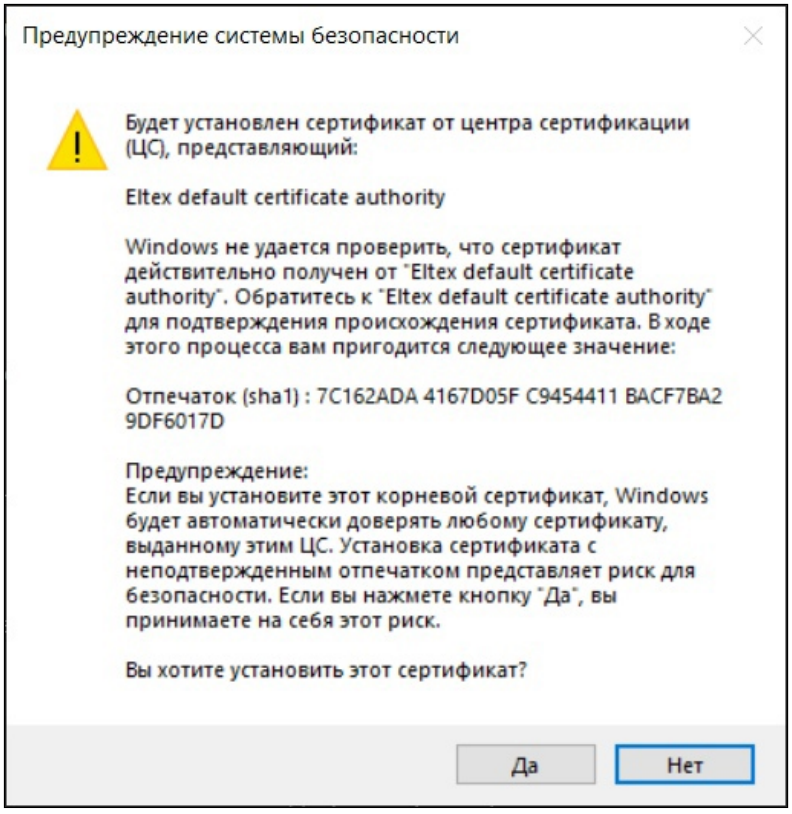
1. Откройте файл .p12. Параметры менять не нужно. Нажмите "Далее".



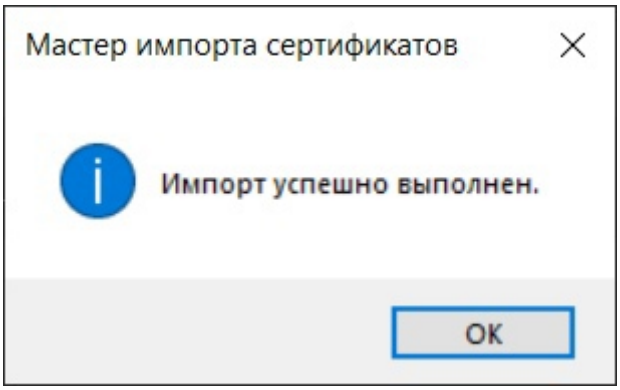
2. Введите пароль. Он соответствует параметру сертификата Password, который вы указали при генерации контейнера на wlc.



3. Подтвердите установку пользовательского сертификата.



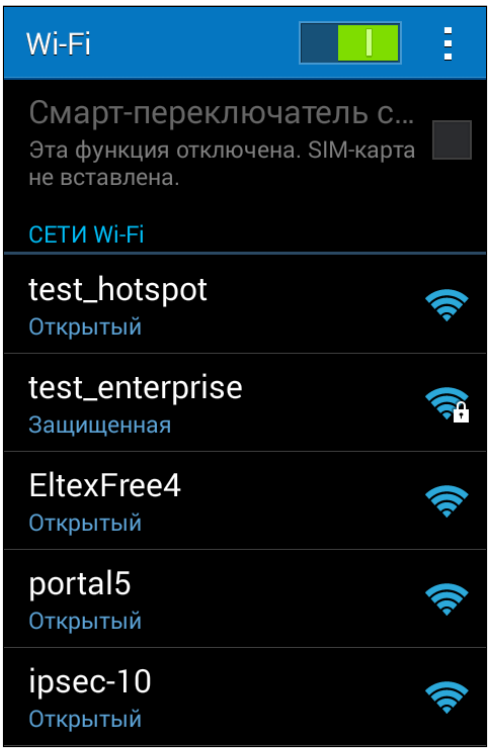
4. При успешной установке пользовательского и корневого сертификата отобразится следующий экран.



22.3.3 Подключение к SSID с поддержкой TLS

Подключение с Android

1. В меню Wi-Fi найдите созданный ранее SSID test_enterprise.



2. Задайте параметры подключения к сети:

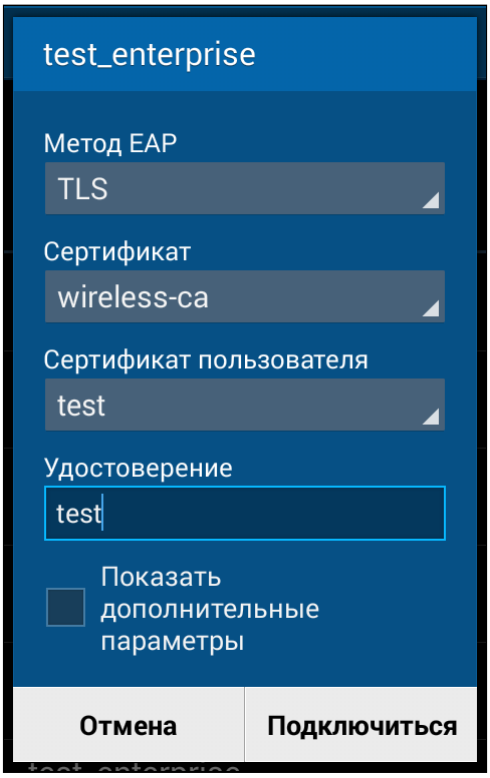
   Метод EAP: TLS

   Сертификат: wireless-ca

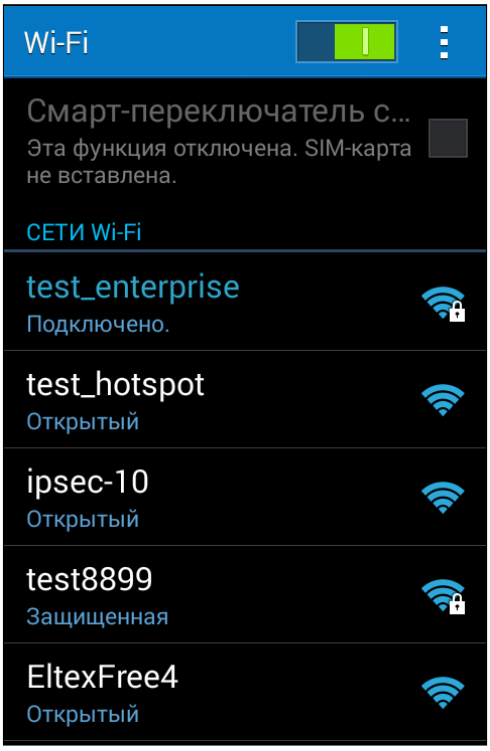
   Сертификат пользователя: test

   Удостоверение: test

   Значение параметра "Удостоверение" задается в соответствии с именем пользователя в сертификате.

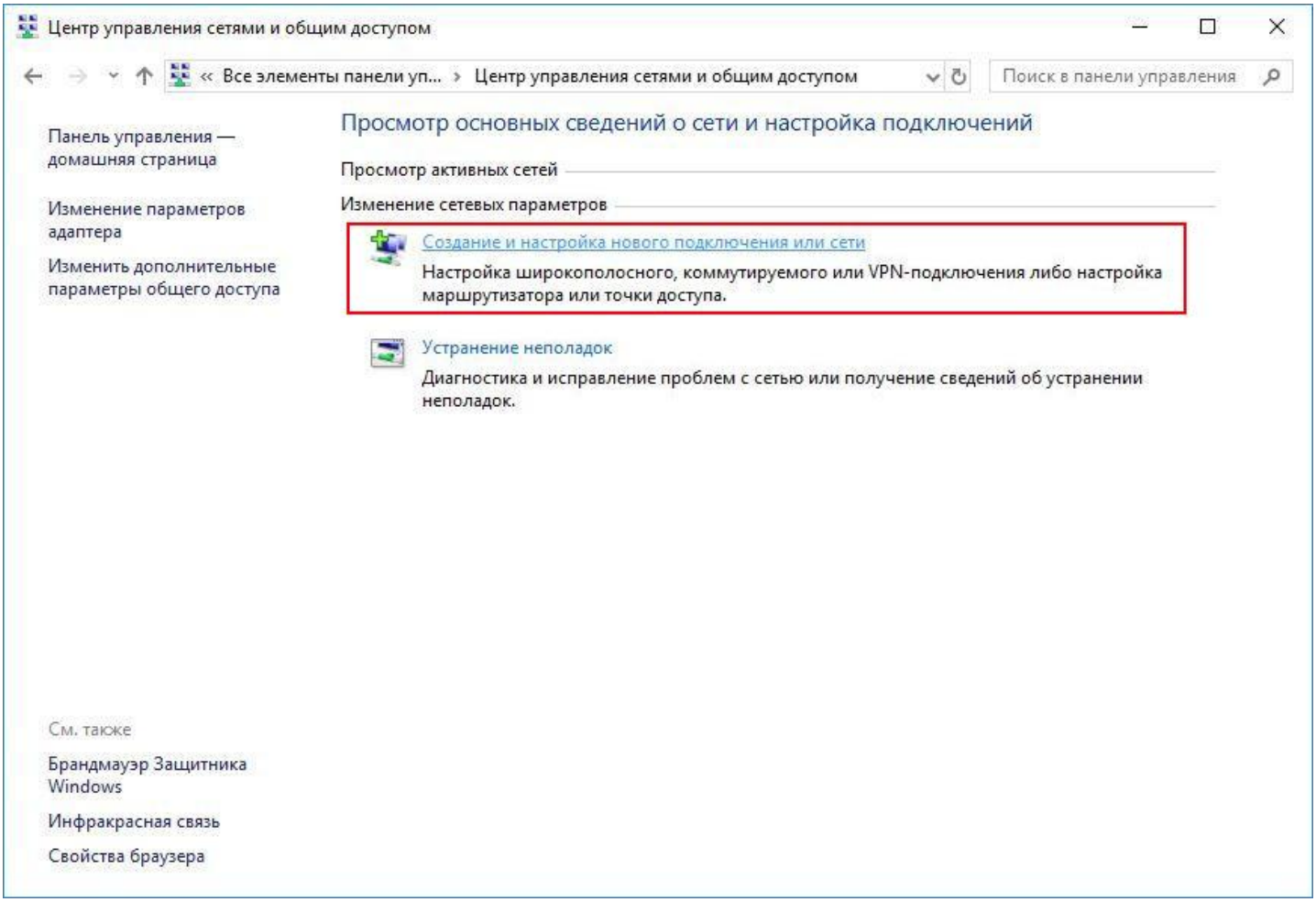


3. Если параметры введены верно, авторизация пройдет успешно.

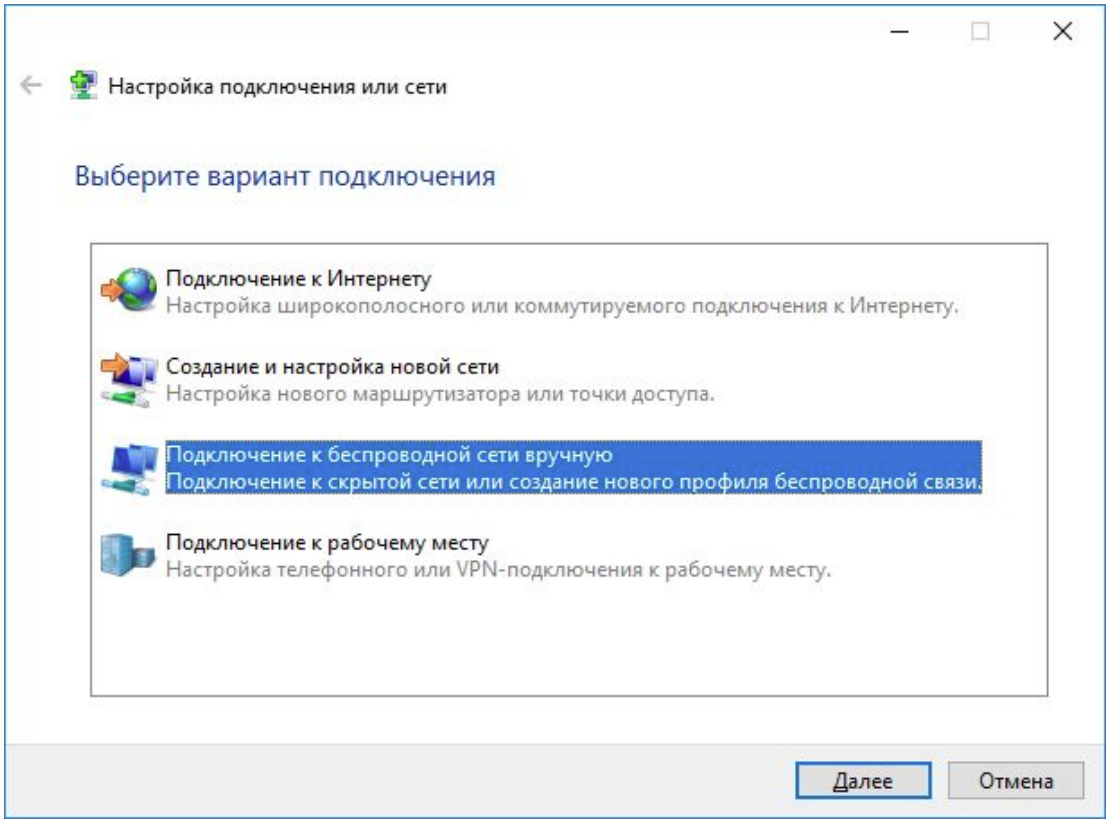


Подключение с Windows

Для создания и настройки нового подключения перейдите в "Центр управления сетями и общим доступом" → "Создание и настройка нового подключения или сети".



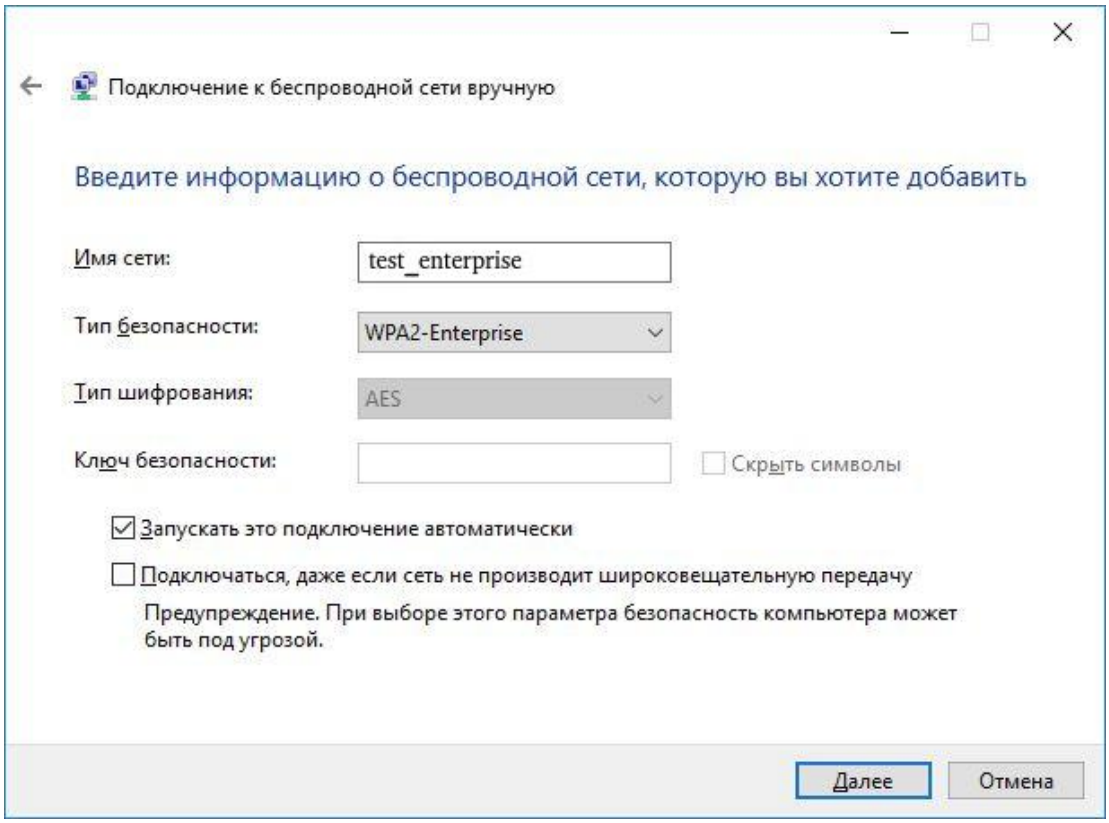
В открывшемся окне выберите пункт "Подключение к беспроводной сети вручную" и нажмите "Далее".



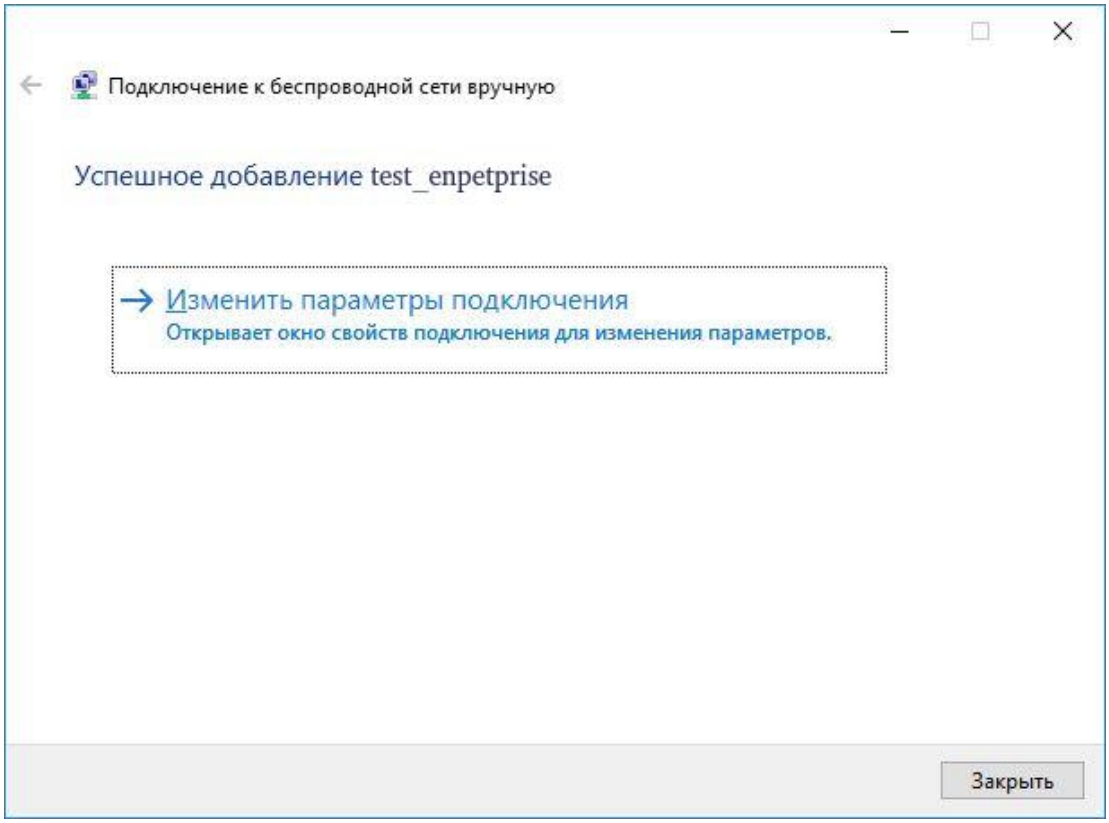
Введите информацию о беспроводной сети:

- Имя сети;
- Тип безопасности: WPA2-Enterprise.

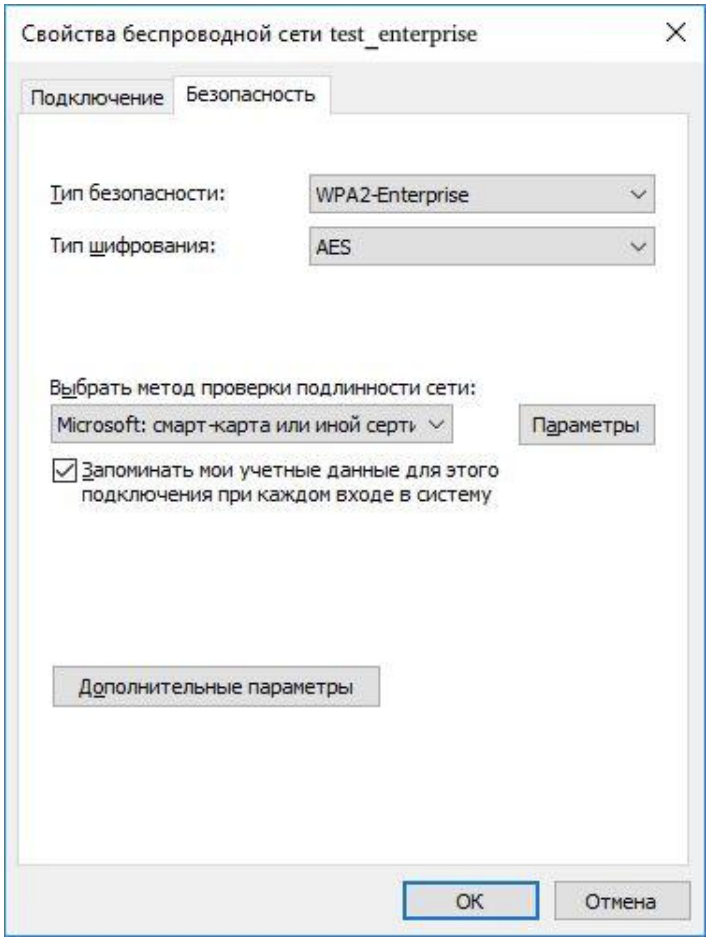
Установите флаг "Запускать это подключение автоматически". Нажмите "Далее".



Сеть успешно добавлена. Далее необходимо настроить параметры подключения.



Откройте раздел "Безопасность", выберите метод проверки подлинности "Microsoft: смарт-карта или иной сертификат". Нажмите кнопку "Параметры".

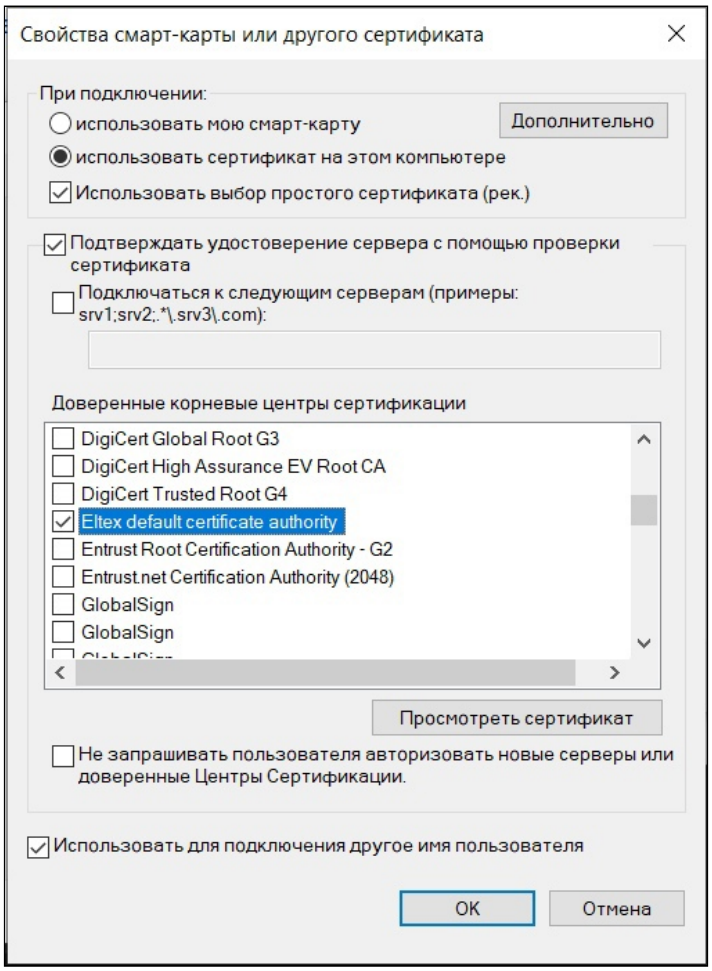


Установите следующие флаги:

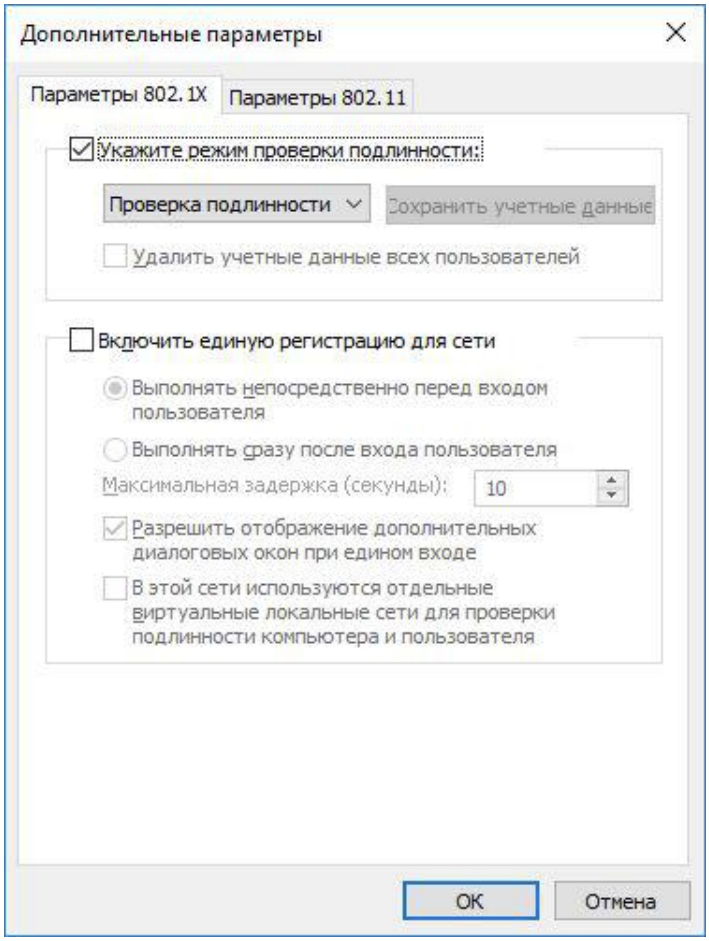
- Использовать сертификат на этом компьютере;
- Использовать выбор простого сертификата;
- Подтверждать удостоверение сервера с помощью проверки сертификата;
- Использовать для подключения другое имя пользователя.

В списке "Доверенных корневых центров сертификации" выберите корневой сертификат "**Eltex default certificate authority**". Это сертификат УЦ, который установился при установке клиентского сертификата.

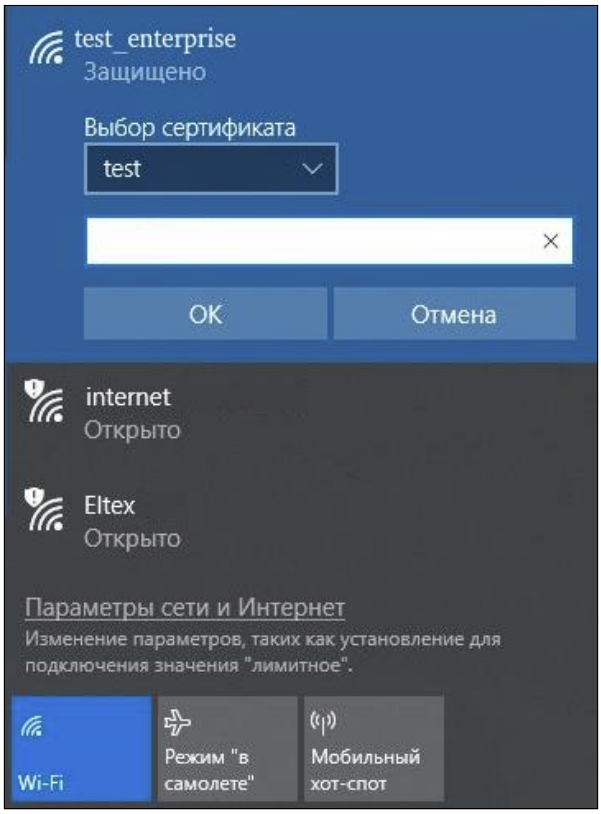
Нажмите кнопку "ОК". В открывшемся окне выберите "Дополнительные параметры".



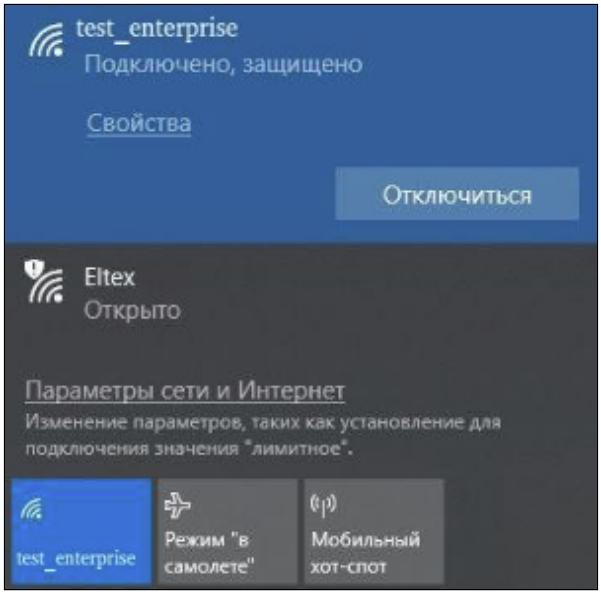
Укажите режим проверки подлинности – "Проверка подлинности пользователя". Нажмите "ОК".



Найдите нужную сеть и нажмите "Подключиться". Выберите пользовательский сертификат для подключения к сети и введите логин пользователя. Нажмите "ОК".

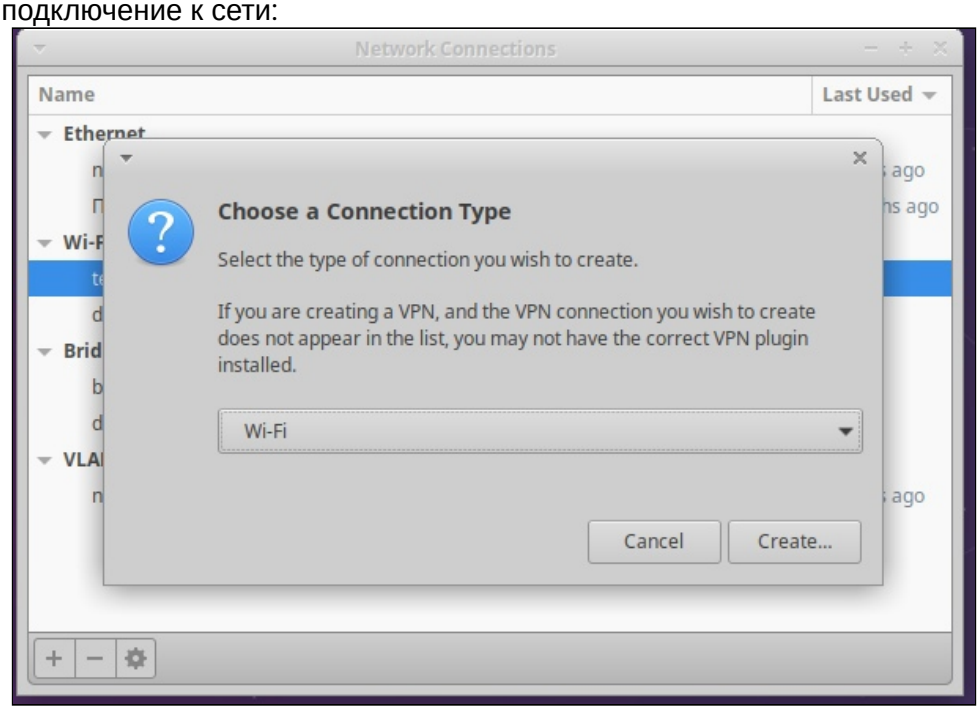


Если параметры введены верно, подключение пройдет успешно.

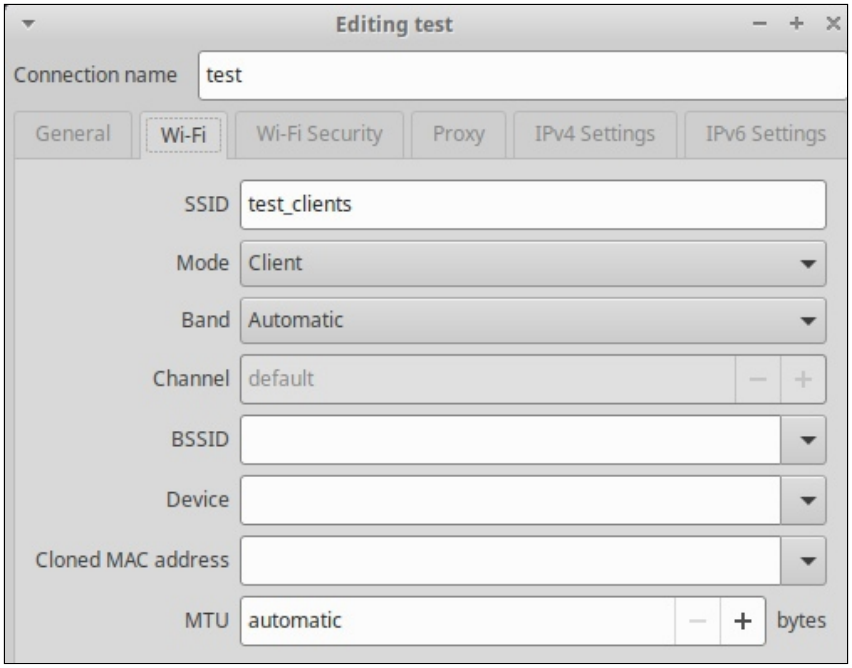


Подключение с Ubuntu

Создайте новое подключение к сети:

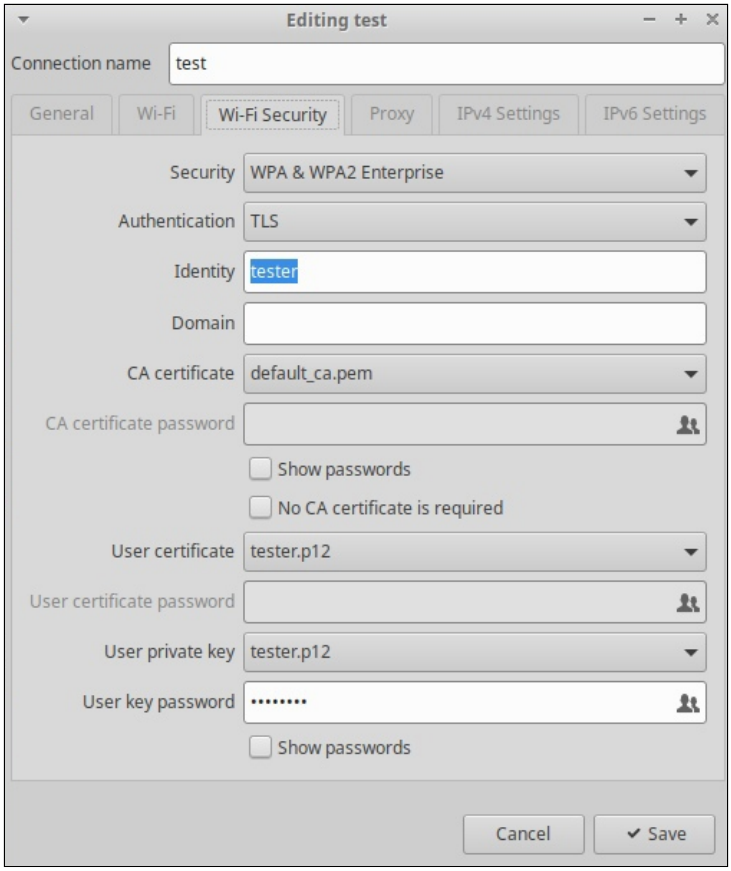


Укажите ssid:



Введите параметры для подключения к сети:

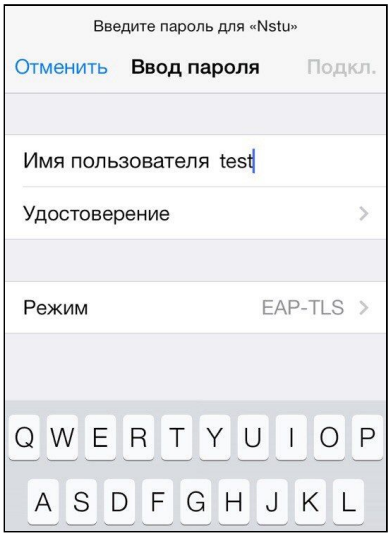
- Security – WPA & WPA2 Enterprice;
- Authentication – TLS;
- Identity – имя пользователя на радиус сервере;
- CA certificate – сертификат УЦ (скачивается с wlc отдельно);
- User certificate – контейнер с сертификатом клиента;
- User private key – контейнер с сертификатом клиента (он также содержит ключ);
- User key password – пароль импорта, заданный при генерации контейнера.

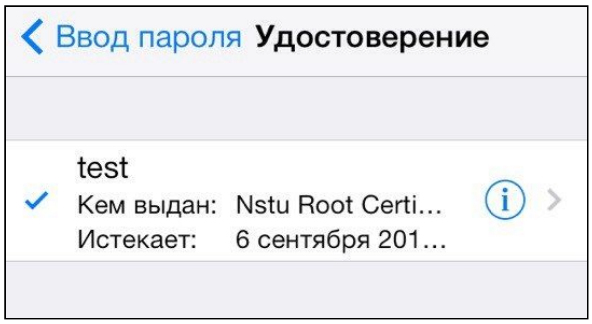


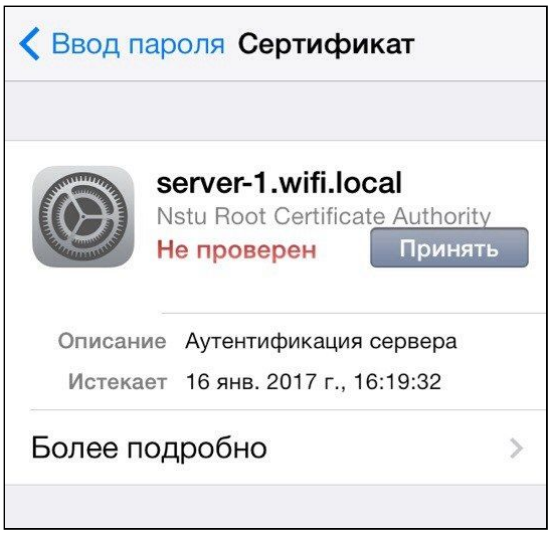
Если параметры введены верно, подключение пройдет успешно.

Подключение с iOS

В меню настройки Wi-Fi найдите необходимую сеть. При подключении к сети введите свой личный логин, выберите режим EAP-TLS. Нажмите на пункт "Удостоверение" и выберите сертификат. Вернитесь назад к вводу пароля и нажмите "Подключиться". В появившемся окне нажмите кнопку "Принять".







22.3.4 Обновление и замена серверного сертификата

Существуют команды для обновления дефолтного **CA-сертификата** и/или сертификата сервера:

```
wlc# update crypto default ca
wlc# update crypto default cert
```

Для замены сертификата сервера нужно загрузить новый сертификат, CA-сертификат и ключ от сертификата сервера и поместить их в директории *crypto:cert/* и *crypto:private-key/*. После загрузки файлов следует указать сертификаты сервера и CA, а также ключ от сертификата сервера в настройках **radius-server local.** По умолчанию указан дефолтный сертификат.

Установка сертификатов в настройках radius server

```
configure
    radius-server local
        crypto private-key my_cert_key.pem
        crypto cert my_cert.pem
        crypto ca my_ca.pem
```

После обновления или замены сертификатов нужно перезагрузить WLC или перезапустить RADIUS-сервер:

Перезапуск radius-server local

```
wlc(config)# radius-server local
wlc(config-radius)# no enable
wlc(config-radius)# do commit
wlc(config-radius)# do restore
wlc(config-radius)# do rollback
```

После обновления или замены серверного сертификата нужно перевыпустить клиентские сертификаты.

22.4 Активация функционала по лицензии

Функционал WLC можно активировать с помощью лицензии на ESR-15, ESR-15R и ESR-3200. Для всех устройств с функционалом WLC доступно увеличение максимального числа точек доступа по лицензии WLC-AP-N (с лимитами можно ознакомиться в кратком техническом описании).

Для загрузки лицензии введите следующую команду. В качестве параметра *<server>* должен быть указан IP-адрес используемого сервера. Для обновления с FTP- или SCP-сервера потребуется ввести имя пользователя (параметр *<user>*) и пароль (параметр *<password>*). В качестве параметра *<file_name>* укажите имя файла лицензии, помещенного на сервер (при использовании SCP нужно указать полный путь – параметр *<folder>*). После ввода команды устройство скопирует файл во внутреннюю память, проверит целостность данных и сохранит его.

TFTP:

```
esr# copy tftp://<server>:/<file_name> system:licence
```

FTP:

```
esr# copy ftp://[<user>[:<password>]@]<server>:/<file_name> system:licence
```

SCP:

```
esr# copy scp://[<user>[:<password>]@]<server>://<folder>/<file_name> system:licence
```

SFTP:

```
esr# copy sftp://[<user>[:<password>]@]<server>:/<file_name> system:licence
```

Пример загрузки лицензии через SCP:

```
esr# copy scp://adm:password123@192.168.16.168://home/tftp/licence system:licence
```

Для активации лицензии необходимо перезагрузить устройство:

```
esr# reload system
```

После перезагрузки проверьте, что лицензия активирована:

```
esr# show licence
Feature                          Value                            Valid from
Expiries
-------------------------------  -------------------------------
-------------------------------  -------------------------------
BRAS                             true                             --
--
WLC-AP                           300                              --
--
WLC                              true                             --
--

After reboot:
Feature                          Value                            Valid from
Expiries
-------------------------------  -------------------------------
-------------------------------  -------------------------------
BRAS                             true                             --
--
WLC-AP                           300                              --
--
WLC                              true                             --
--
```

Загружаемая лицензия перезаписывает активную лицензию. В случае, если в загружаемой лицензии отсутствует функционал, который был в уже активной лицензии, то после перезагрузки этот функционал перестанет работать:

```
esr# show licence
Feature                          Value                            Valid from
Expiries
-------------------------------  -------------------------------
-------------------------------  -------------------------------
BRAS                             true                             --
--
WLC-AP                           200                              --
--
WLC                              true                             --
--

After reboot:
Feature                          Value                            Valid from
Expiries
-------------------------------  -------------------------------
-------------------------------  -------------------------------
WLC-AP                           200                              --
--
WLC                              true                             --
--
```

В примере выше после перезагрузки устройства будет заблокирован доступ к функционалу под лицензией BRAS и все текущие настройки в конфигурации, связанные с BRAS, перестанут быть активными.

В случае расширения списка доступного функционала, при обращении в техническую поддержку или коммерческий отдел компании ЭЛТЕКС необходимо сообщать информацию **show system** и **show licence.**

22.5 Настройка MAC-авторизации пользователей

- Настройка mac-auth по локальным спискам
- Настройка mac-auth по спискам на локальном RADIUS-сервере

Поддержано начиная с версий:
Устройства: WLC-15/30/3200, ESR-15/15R/30/3200
Версия ПО WLC: 1.26.0
Устройства: WEP-1L/2L/30L/30L-Z/200L и WOP-2L/20L/30L/30LS
Версия ПО ТД: 2.5.0
Устройства: WEP-3ax
Версия ПО ТД: 1.8.0 (для работы с WLC нужно использовать актуальную версию ПО 1.12.0 или выше)

Настройка осуществляется в рамках настройки SSID-профиля. Существует 2 режима работы mac-auth:

- По локальным спискам;
- По записям в RADIUS server.

```
wlc(config-wlc-ssid-profile)# mac-auth mode
  local   Set MAC authentication local mode
  radius  Set MAC authentication radius mode
```

22.5.1 Настройка mac-auth по локальным спискам

Для авторизации по локальным спискам требуется:

1. Создать object-group mac и указать в данной группе MAC-адреса клиентов.

```
wlc# configure
wlc(config)# object-group mac test_mac_auth
wlc(config-object-group-mac)# mac address 11:11:11:11:11:11
wlc(config-object-group-mac)# mac address 22:22:22:22:22:22
wlc(config-object-group-mac)# exit
```

2. Перейти в настройки SSID-профилей (WLC → SSID-PROFILE <NAME>) и добавить правило, необходимое для работы mac-auth. Пример ниже приведён для ssid-profile default-ssid.

```
wlc(config)# wlc
wlc(config-wlc)# ssid-profile default-ssid
wlc(config-wlc-ssid-profile)# mac-auth mode local policy permit test_mac_auth
wlc(config-wlc-ssid-profile)# end
```

3. Применить изменения.

```
wlc# commit
wlc# confirm
```

⚠ В данном примере будет разрешено подключение к default-ssid для устройств, у которых MAC-адрес указан в профиле MAC-адресов test_mac_auth. Помимо этого можно настроить следующие варианты:
mac-auth mode local policy permit any – разрешить доступ всем
mac-auth mode local policy deny any – запретить доступ всем
mac-auth mode local policy deny test_mac_auth – запретить доступ для устройств, у которых MAC-адрес указан в object group test_mac_auth.

22.5.2 Настройка mac-auth по спискам на локальном RADIUS-сервере

Для авторизации по записям на RADIUS-сервере требуется:

1. Добавить адрес пользователя на RADIUS-сервер в домен, который будет использоваться для авторизации. В данном примере запись создаётся в domain default.

```
wlc# configure
wlc(config)# radius-server local
wlc(config-radius)# domain default
wlc(config-radius-domain)# user 11-11-11-11-11-11
wlc(config-radius-user)# password ascii-text NOPASSWORD
wlc(config-radius-user)# ex
wlc(config-radius-domain)# ex
wlc(config-radius)# ex
```

В поле "user" необходимо вводить MAC-адрес в формате: *AA-BB-CC-DD-EE-FF*
В поле "password" необходимо вводить: *NOPASSWORD*

2. Перейти в настройки SSID-профилей (WLC → SSID-PROFILE <NAME>) и добавить правило, необходимое для работы mac-auth. Пример ниже приведён для ssid-profile default-ssid. Настройка проксирования на внешний RADIUS.

```
wlc(config)# wlc
wlc(config-wlc)# ssid-profile default-ssid
wlc(config-wlc-ssid-profile)# mac-auth mode radius policy permit
```

3. Применить изменения.

```
wlc# commit
wlc# confirm
```

⚠ Логика работы по записям на RADIUS-сервере отличается от логики работы по локальным спискам.
Если для правила *mac-auth mode radius policy permit* не создать записи на сервере, то доступ будет запрещён всем, так как записей, для которых необходимо открыть доступ – нет.
Аналогично и для *mac-auth mode radius policy deny* – если записей не создано, то разрешается доступ всем.

Если список пользователей находится на внешнем сервере, необходимо настроить проксирование по статье "Настройка проксирования на внешний RADIUS".

22.6 Обновление точек доступа

✓ Всегда загружайте актуальную версию ПО точек доступа на контроллер для обновления новых точек при их подключении. Это требуется для корректной работы, т.к. управление контроллером поддерживается не на всех версиях ПО точек доступа.

Важные моменты:

- Версия, которая загружена на контроллер, считается приоритетно актуальной. При подключении новой точки доступа, она обновится на данную версию, независимо от того, какая установлена на ней (старше или младше).
- Если на контроллер загружено несколько версий ПО для одной модели точки доступа, то актуальным будет считаться ПО старшее по номеру. Например, если загружены версии ПО:
  - WEP-1L-1.5.0_build_100.tar.gz,
  - WEP-1L-1.6.0_build_50.tar.gz

  актуальным будет ПО 1.6.0_build_50.tar.gz.

22.6.1 Загрузка ПО на контроллер

Для загрузки прошивки используйте команду:

```
wlc# copy tftp://192.168.1.2:/WEP-1L-1.6.0_build_75.tar.gz system:access-points-firmwares
# где
# IP-адрес TFTP-сервера: 192.168.1.2,
# название файла ПО: WEP-1L-1.6.0_build_75.tar.gz.
```

Для просмотра списка загруженных файлов используйте команду:

```
wlc# dir system:access-points-firmwares
# Пример вывода
Name                                                    Type         Size
------------------------------------------------------  ----------   --------   --
WEP-1L-1.5.0_build_59.tar.gz                            File         9.07       MB
WEP-1L-1.6.0_build_75.tar.gz                            File         9.08       MB
```

Для удаления файлов ПО с контроллера используйте команду:

```
# Удаление всех файлов ПО. Команда требует подтверждения
wlc# delete system:access-points-firmwares
Do you really want to clear directory? (y/N): y

# Удаление конкретного файла
wlc# delete system:access-points-firmwares/WEP-1L-1.5.0_build_59.tar.gz
```

22.6.2 Алгоритм запуска обновлений

Настройка по умолчанию

Настройка по умолчанию работает следующим образом: когда подключается новая точка доступа, она сразу автоматически обновляется на прошивку, которая загружена на WLC. Если точка доступа уже находится под управлением WLC, то она обновится на актуальную прошивку сразу после ее загрузки, если менеджер обновления отключен.

Настройка менеджера обновлений по расписанию

В конфигурации WLC для того, чтобы избежать прерывание сервиса во время обновления, предусмотрен менеджер обновлений – update-mgr, который позволяет установить временной интервал, в течение которого может быть запущено обновление. Настройка состоит из трех параметров:

- start-time – начало интервала времени, в который производится обновление. Значение по умолчанию: 03:00;
- end-time – окончание интервала времени, в который производится обновление. Значение по умолчанию: 04:00;
- scheduled – включение менеджера обновлений по расписанию. Значение по умолчанию: no scheduled (выключен).

При включенном менеджере, обновление по расписанию будет выполняться только для точек доступа, которые уже находятся под управлением контроллера.

При подключении новой точки, которая имеет версию ПО, отличную от загруженной на контроллер, обновление произойдет сразу, независимо от расписания.

Пример настройки

```
# Настройка менеджера обновления по расписанию. Интервал для обновлений: 00:00 – 01:00
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# update-manager
wlc(config-wlc-update-mgr)# start-time 00:00
wlc(config-wlc-update-mgr)# end-time 01:00
wlc(config-wlc-update-mgr)# scheduled

# Применение и сохранение конфигурации
wlc(config-wlc-update-mgr)# do commit
wlc(config-wlc-update-mgr)# do confirm

# Просмотр конфигурации
wlc# show run wlc update-manager
  update-manager
    scheduled
    start-time 00:00
    end-time 01:00
  exit
wlc#
```

При такой настройке обновление точек доступа, которые уже находятся под управлением контроллера, на актуальную загруженную версию произойдет в интервале времени 00:00–01:00.

Если точка доступа пришла на контроллер с устаревшей версией ПО, (работа с которой не поддержана на контроллере), при этом актуальная версия ПО не добавлена на контроллер для обновления, точка доступа не будет работать под управлением контроллера.
В логе будет ошибка:

```
2024-01-18T14:16:57+07:00 %WLC-E-ERROR: SA:[e8:28:c1:da:c9:b0]:AP with board type
'WEP-1L' with unsupported firmware version '2.2.0 build 352', no firmware image for
 upgrade
```

Версии ПО точек доступа, для которых поддержано взаимодействие с контроллером WLC версий 1.26.0 указаны в таблице ниже:

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-1L	2.5.2	2.5.x
WEP-2L	2.5.2	2.5.x
WEP-200L	2.5.2	2.5.x
WEP-30L	2.5.2	2.5.x
WEP-30L-Z	2.5.2	2.5.x
WEP-3ax	1.12.0	1.12.x
WOP-2L	2.5.2	2.5.x
WOP-20L	2.5.2	2.5.x
WOP-30L	2.5.2	2.5.x
WOP-30LS	2.5.2	2.5.x

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-2ac	1.25.0	1.25.x
WEP-2ac Smart	1.25.0	1.25.x
WOP-2ac	1.25.0	1.25.x
WOP-2ac:rev.B	1.25.0	1.25.x
WOP-2ac:rev.C	1.25.0	1.25.x

Версии ПО точек доступа, для которых поддержано взаимодействие с контроллером WLC версий 1.19.2 указаны в таблице ниже:

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-1L	2.3.2	2.3.x
WEP-200L	2.3.2	2.3.x
WEP-2L	2.3.2	2.3.x
WEP-3ax	1.11.0	1.11.x
WOP-20L	2.3.2	2.3.x
WOP-2L	2.3.2	2.3.x
WEP-30L	2.3.2	2.3.x
WOP-30L	2.3.2	2.3.x
WOP-30LS	2.3.2	2.3.x

Версии ПО точек доступа, для которых поддержано взаимодействие с контроллером WLC версий 1.15.3-1.19.1 включительно, указаны в таблице ниже:

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-1L	1.6.0	2.2.x
WEP-200L	1.6.0	2.2.x
WEP-2L	1.6.0	2.2.x
WEP-3ax	1.7.0	1.10.x
WOP-20L	1.6.0	2.2.x
WOP-2L	1.6.0	2.2.x
WEP-30L	2.1.0	2.2.x
WOP-30L	2.1.0	2.2.x

22.7 Портальная авторизация

22.7.1 Авторизация через RADIUS

Алгоритм работы

Поддержано начиная с версий:
Устройства: WLC-15/30/3200, ESR-15/15R/30/3200
Версия ПО WLC: 1.26.0
Устройства: WEP-1L/2L/30L/30L-Z/200L и WOP-2L/20L/30L/30LS
Версия ПО ТД: 2.5.0

На ТД поддержан способ портальной авторизации через RADIUS.

Клиент подключается к открытому SSID. При первом подключении клиента для него пока отсутствует учетная запись во внешней системе (в RADIUS-сервере), поэтому весь клиентский трафик блокируется, кроме:

- DHCP
- DNS
- Запросов на адрес портала
- Запросов URL/IP из белого списка

После подключения клиента ТД пытается провести MAB-авторизацию (MAC Authentication Bypass) на RADIUS-сервере, подставляя MAC-адрес клиента в атрибуты User-Name и User-Password в запросе Access-Request к RADIUS-серверу. Так как на RADIUS-сервере учетная запись с такими параметрами на данный момент отсутствует, сервер отправляет Access-Reject.

Далее клиент обращается на HTTP-ресурс. ТД перехватывает запрос и перенаправляет клиента на гостевой портал, который был задан в настройках SSID (portal-profile). Клиент переходит на портал по полученному URL, который содержит в себе:

- switch_url – URL для перенаправления клиента после авторизации на портале
- ap_mac – MAC-адрес ТД, к которой подключен клиент
- client_mac – MAC-адрес клиента
- wlan – название SSID, к которому подключен клиент
- redirect – URL, который клиент запрашивал первоначально

Пример URL:

```
https://eltex-co.ru/?switch_url=http://redirect.loc:10081&ap_mac=68:13:E2:35:1F:
30&client_mac=38:d5:7a:e1:e0:13&wlan=Portal-SSID&redirect=http://www.msftconnecttest.com/
connecttest.txt
```

Далее пользователь проходит саморегистрацию на гостевом портале и через форму портала ему возвращается URL редиректа на ТД, который содержит параметры:

- username – имя пользователя;
- password – пароль пользователя;

- redirect_url – URL, который клиент запрашивал первоначально, т.к. портал, возможно, подменил адрес. В нашем примере клиент пытался подключиться к http://www.msftconnecttest.com, но его перенаправили на https://eltex-co.ru;
- error_url – URL для перенаправления клиента в случае ошибки авторизации. В нашем примере этот параметр не используется.

> ⓘ Названия параметров можно переопределить в конфигурации ap-profile.

Пример URL:

```
http://redirect.loc:10081/?
username=60336144&password=3hMYEPEW0tdb&buttonClicked=4&redirect_url=https://eltex-co.ru/
```

На устройстве клиента открывается URL редиректа, полученный от портала. ТД вычитывает из него username и password, подставляет их в атрибуты User-Name и User-Password в запросе Access-Request и отправляет запрос на RADIUS-сервер. После успешной авторизации клиента на RADIUS-сервере, ТД снимает ограничения на доступ и перенаправляет клиента на URL, указанный в redirect_url. После регистрации пользователя его учетная запись для MAB-авторизации создается в БД RADIUS.

В случае переподключения клиента к ТД или подключения к другой ТД (к тому же SSID) авторизация будет проходить по MAC-адресу; на запрос Access-Request MAB-авторизации вернется Access-Accept, так как на RADIUS-сервере уже есть соответствующая учетная запись клиента (MAB-авторизация запрашивается при подключение клиента к ТД, если ТД не "помнит" клиента). Перенаправление клиента на портал происходить не будет до тех пор, пока MAC-адрес клиента не будет удален из БД.

Конфигурация WLC

Пример настроек будет выполнен на factory конфигурации WLC.

Порядок настройки:

1. Создаем белый список URL
2. Создаем белый список IP-адресов
3. Создаем portal-profile
4. Создаем radius-profile
5. Создаем ssid-profile
6. Добавляем ssid-profile в ap-location

Белые списки предназначены для того, чтобы в случае необходимости предоставить пользователю доступ к определенным ресурсам до авторизации. Список этих ресурсов можно задать через URL, RegExp или подсеть IP. Белые списки не являются обязательными. Адрес портала добавляется в белый список автоматически, поэтому задавать его не требуется.

1. Создаем белый список URL, он может содержать URL и/или RegExp. Доступ к указанным адресам будет разрешён до авторизации.

   ```
   object-group url white_url
     url eltex-co.ru
     regexp '(.+\.)eltex-co\.com'
   exit
   ```

2. Создаем белый список IP-адресов, доступ к указанным адресам будет разрешён до авторизации. В белый список можно добавлять адреса подсетей, которые нужны для авторизации.

   ```
   object-group network white_ip
     ip prefix 192.168.0.0/24
   exit
   ```

3. Создаем portal-profile.
   Описание параметров:
   redirect-url – адрес портала;
   age-timeout – временной интервал, в течение которого точка доступа "помнит" клиента и не проводит MAB-авторизацию;
   verification-mode – режим работы портала;
   white-list domain – белый список URL;
   white-list address – белый список IP-адресов.

```
wlc
  portal-profile portal-pr
    redirect-url https://eltex-co.ru
    age-timeout 10
    verification-mode external-portal
    white-list domain white_url
    white-list address white_ip
  exit
exit
```

   При режиме verification-mode external-portal к указанному URL в redirect-url автоматически добавляются параметры таким образом, что результирующий URL имеет вид:

```
https://eltex-co.ru/?
switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID>&redirec
t=<ORIGINAL_URL>
```

   Если необходимо изменить названия параметров **switch_url, ap_mac, client_mac, wlan**, **redirect** можно задать строку самостоятельно через параметр redirect-url-custom, например:

```
redirect-url-custom https://eltex-co.ru/?
action_url=<SWITCH_URL>&ap_addr=<AP_MAC>&client_addr=<CLIENT_MAC>&ssid_name=<SSID>&
red_url=<ORIGINAL_URL>&nas=<NAS_ID>
```

   В примере в строку был добавлен <NAS_ID> и были изменены следующие названия параметров:
   - switch_url → action_url
   - ap_mac → ap_addr
   - client_mac →client_addr
   - wlan →ssid_name
   - redirect →red_url

   Строка редиректа может содержать плейсхолдеры:
   - <NAS_ID>
   - <SWITCH_URL>
   - <AP_MAC>
   - <CLIENT_MAC>
   - <SSID>
   - <ORIGINAL_URL>

4. Создаем radius-profile.

```
wlc
  radius-profile portal_radius
    auth-address 192.168.4.5
    auth-password ascii-text encrypted 92BB3C7EB50C5AFE80
    auth-acct-id-send
    acct-enable
    acct-address 192.168.4.5
    acct-password ascii-text encrypted 92BB3C7EB50C5AFE80
    acct-periodic
    acct-interval 300
  exit
exit
```

5. Создаем ssid-profile.

```
wlc
  ssid-profile portal_test
    ssid portal_test
    radius-profile portal_radius
    portal-enable
    portal-profile portal-pr
    vlan-id 3
    band 5g
    enable
  exit
exit
```

6. Добавляем ssid-profile в ap-location.

```
wlc
  ap-location default-location
    description default-location
    mode tunnel
    ap-profile default-ap
    ssid-profile portal_test
  exit
exit
```

Полная конфигурация

```
#!/usr/bin/clish
#260
#1.26.1
#02/07/2024
#21:56:21
object-group service airtune
  port-range 8099
exit
object-group service dhcp_client
  port-range 68
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dns
  port-range 53
exit
object-group service netconf
  port-range 830
exit
object-group service ntp
  port-range 123
exit
object-group service radius_auth
  port-range 1812
exit
object-group service sa
  port-range 8043-8044
exit
object-group service ssh
  port-range 22
exit
object-group service web
  port-range 443
exit

object-group network white_ip
  ip prefix 192.168.0.0/24
  ip prefix 192.168.1.0/24
  ip prefix 100.110.0.0/23
exit

object-group url white_url
  url eltex-co.ru
  regexp '(.+\.)eltex-co\.com'
exit

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit

radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
```

```
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  domain default
  exit
  virtual-server default
    enable
  exit
  enable
exit
username admin
  password encrypted $6$mxcmBjMFhD3le5vZ$3qVKBN4Y6Uh126nuH/
9VWOiH5m1pMWI1KvRTrrie5ZgmKaYxxZgeinS6Y210.3P2n.ZhlVHbaCcLKlfbOJzEG.
exit

radius-server host 127.0.0.1
  key ascii-text encrypted 8CB5107EA7005AFF
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit

boot host auto-config
boot host auto-update

vlan 3
  force-up
exit
vlan 2
exit

no spanning-tree

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone users
exit

bridge 1
  vlan 1
  security-zone trusted
  ip address 192.168.1.1/24
  no spanning-tree
  enable
exit
bridge 2
  vlan 2
  security-zone untrusted
  ip address dhcp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
```

```
  ip address 192.168.2.1/24
  no spanning-tree
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 1/0/2
  mode switchport
exit
interface gigabitethernet 1/0/3
  mode switchport
exit
interface gigabitethernet 1/0/4
  mode switchport
exit
interface tengigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 1/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

security zone-pair trusted self
  rule 10
    action permit
    match protocol tcp
    match destination-port object-group ssh
    enable
  exit
  rule 20
    action permit
    match protocol icmp
    enable
  exit
  rule 30
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_server
    enable
  exit
  rule 40
    action permit
    match protocol udp
    match destination-port object-group ntp
    enable
  exit
  rule 50
    action permit
    match protocol tcp
```

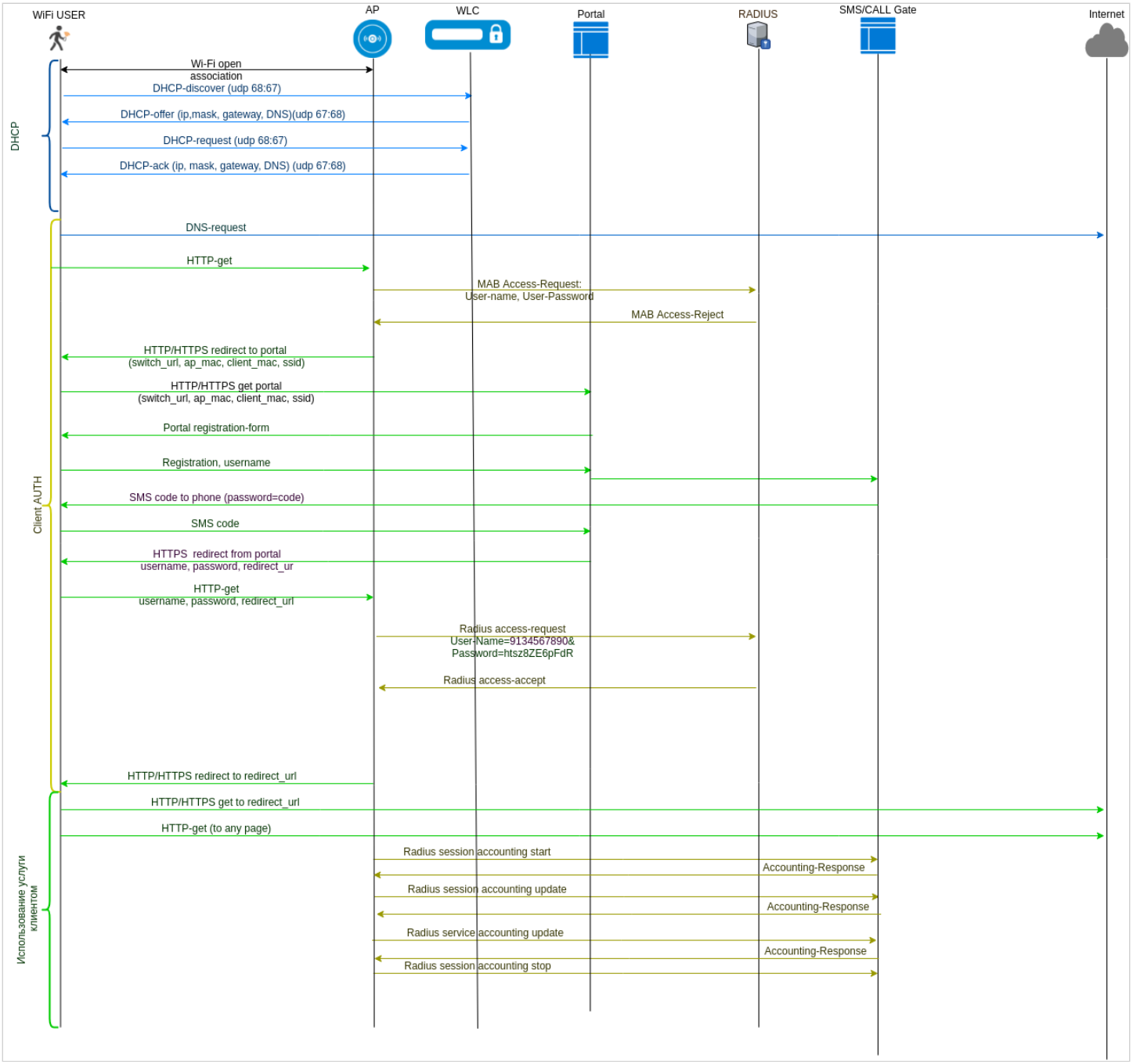
```
    match destination-port object-group dns
    enable
  exit
  rule 60
    action permit
    match protocol udp
    match destination-port object-group dns
    enable
  exit
  rule 70
    action permit
    match protocol tcp
    match destination-port object-group netconf
    enable
  exit
  rule 80
    action permit
    match protocol tcp
    match destination-port object-group sa
    enable
  exit
  rule 90
    action permit
    match protocol udp
    match destination-port object-group radius_auth
    enable
  exit
  rule 100
    action permit
    match protocol gre
    enable
  exit
  rule 110
    action permit
    match protocol tcp
    match destination-port object-group airtune
    enable
  exit
  rule 120
    action permit
    match protocol tcp
    match destination-port object-group web
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
```

```
    match source-port object-group dhcp_server
    match destination-port object-group dhcp_client
    enable
  exit
exit
security zone-pair users self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
  rule 20
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_server
    enable
  exit
  rule 30
    action permit
    match protocol tcp
    match destination-port object-group dns
    enable
  exit
  rule 40
    action permit
    match protocol udp
    match destination-port object-group dns
    enable
  exit
exit
security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit

security passwords default-expired

nat source
  ruleset factory
    to zone untrusted
    rule 10
      description "replace 'source ip' by outgoing interface ip address"
      action source-nat interface
      enable
    exit
  exit
exit

ip dhcp-server
ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.2-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043"
```

```
  exit
exit
ip dhcp-server pool users-pool
  network 192.168.2.0/24
  address-range 192.168.2.2-192.168.2.254
  default-router 192.168.2.1
  dns-server 192.168.2.1
exit

softgre-controller
  nas-ip-address 127.0.0.1
  data-tunnel configuration wlc
  aaa radius-profile default_radius
  keepalive-disable
  service-vlan add 3
  enable
exit

wlc
  outside-address 192.168.1.1
  service-activator
    aps join auto
  exit
  airtune
    enable
  exit
  ap-location default-location
    description default-location
    mode tunnel
    ap-profile default-ap
    airtune-profile default_airtune
    ssid-profile default-ssid
    ssid-profile portal_test
  exit
  airtune-profile default_airtune
    description default_airtune
  exit
  ssid-profile default-ssid
    description default-ssid
    ssid default-ssid
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    band 5g
    enable
  exit
  ssid-profile portal_test
    ssid portal_test
    radius-profile portal_radius
    portal-enable
    portal-profile portal-pr
    vlan-id 3
    band 5g
    enable
  exit
  radio-2g-profile default_2g
    description default_2g
  exit
  radio-5g-profile default_5g
```

```
    description default_5g
  exit
  ap-profile default-ap
    description default-ap
    password ascii-text encrypted 8CB5107EA7005AFF
  exit
  portal-profile portal-pr
    redirect-url https://eltex-co.ru
    age-timeout 10
    verification-mode external-portal
    white-list domain white_url
    white-list address white_ip
  exit
  radius-profile default-radius
    description default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    domain default
  exit
  radius-profile portal_radius
    auth-address 192.168.4.5
    auth-password ascii-text encrypted 92BB3C7EB50C5AFE80
    auth-acct-id-send
    acct-enable
    acct-address 192.168.4.5
    acct-password ascii-text encrypted 92BB3C7EB50C5AFE80
    acct-periodic
    acct-interval 300
  exit
  ip-pool default-ip-pool
    description default-ip-pool
    ap-location default-location
  exit
  enable
exit

wlc-journal all
  limit days 365
exit

ip ssh server

ntp enable
ntp broadcast-client enable

ip https server
```

Диаграмма подключения



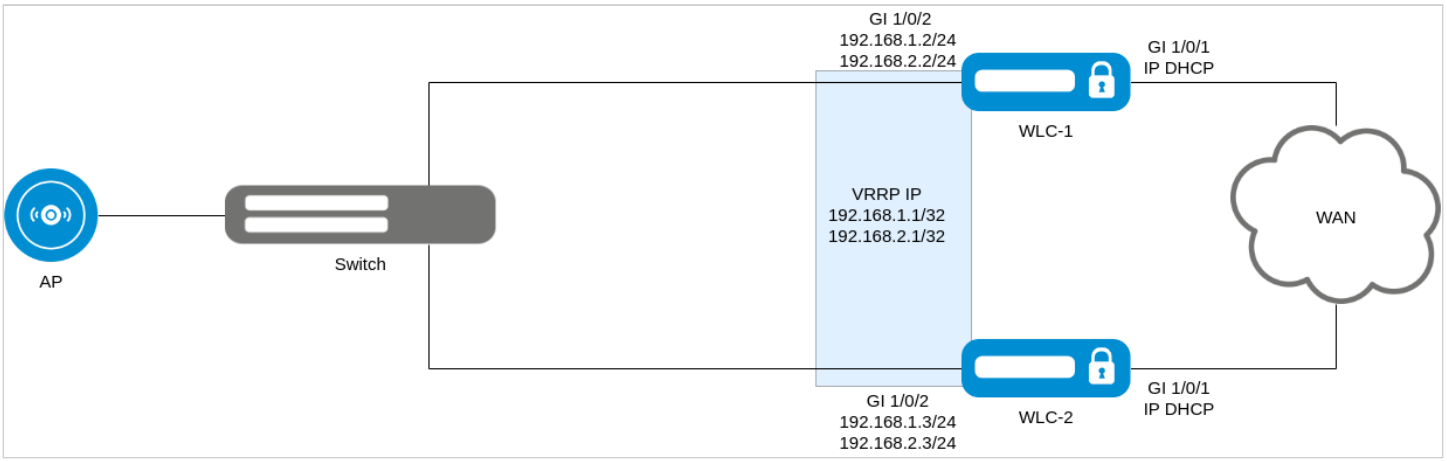
22.8 Резервирование WLC

22.8.1 Описание

Два WLC резервируют себя через протокол VRRP, интерфейс в сторону точек доступа подключен к коммутатору.

> ⚠ **Резервирование и организация Uplink не рассматриваются в данной статье.**

22.8.2 Схема включения



22.8.3 Задача

Организовать резервирование контроллера WLC.

22.8.4 Решение

Настройка будет выполнена на базе заводской конфигурации (Factory). Интерфейс gi 1/0/1 смотрит в сторону Uplink, gi 1/0/2 — в сторону точек доступа.

Для решения поставленной задачи на каждом WLC необходимо:

- Создать object-group для настройки firewall
- Настроить VRRP на интерфейсах
- Настроить Crypto-Sync для синхронизации сертификатов
- Настроить WLC для синхронизации состояния точек доступа
- Настроить Softgre-Controller для синхронизации туннелей
- Настроить Firewall, разрешить обмен VRRP-анонсами и отрыть порты для синхронизации туннелей, сертификатов и состояния WLC
- Настроить DHCP-сервер в режиме Active-Standby
- Настроить DHCP failover
- Настроить NTP-сервер

На интерфейсах, где включен vrrp необходимо включить:

```
vrrp timers garp refresh 60
```

Данная команда определяет интервал, по истечении которого будет происходить периодическая отправка Gratuituous ARP-сообщения(ий), пока маршрутизатор находится в состоянии Master.

Адресация:

Интерфейс	VLAN	WLC-1 IP	WLC-2 IP	VRRP IP	Описание
Birdge 1	2449	192.168.1.2/24	192.168.1.3/24	192.168.1.1/32	Интерфейс для сети управления
Bridge 3	3	192.168.2.2/24	192.168.2.3/24	192.168.2.1/32	Интерфейс для клиентов Wi-Fi

Порты и протоколы, для которых нужно настроить Firewall:

Сервис	Протокол	Порт	Описание
softgre-controller	TCP	1337	Используется для синхронизации softgre-туннелей
crypto-sync	TCP	873	Используется для синхронизации сертификатов и состояния ТД
VRRP	VRRP	-	Используется для резервирования

Пример настройки WLC-1

Подключаемся к WLC и переходим в режим конфигурирования:

```
wlc# config
```

Меняем имя устройства:

```
hostname WLC-1
```

Создаем vlan 2449:

```
vlan 2449
  force-up
exit
```

Настраиваем интерфейс gi 1/0/2 для приема тегированного трафика в VLAN 3 и 2449:

```
interface gigabitethernet 1/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
```

Создаем object-group для настройки Firewall:

```
object-group service sync
  port-range 873
exit
object-group service softgre_controller
  port-range 1337
exit
```

Меняем адресацию и настраиваем VRRP на Bridge:

```
no bridge 1
no bridge 3

bridge 1
  vlan 2449
  security-zone trusted
  ip address 192.168.1.2/24
  vrrp priority 120
  vrrp id 1
  vrrp ip 192.168.1.1/32
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.2/24
  vrrp priority 120
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
```

Указываем адресацию резервируемых контроллеров и назначаем им группу:

```
ip failover
  local-address 192.168.1.2
  remote-address 192.168.1.3
  vrrp-group 1
exit
```

Настраиваем Crypto-Sync для синхронизации сертификатов:

```
crypto-sync
crypto-sync remote-delete
```

Настраиваем Softgre-Controller для синхронизации туннелей SoftGRE:

```
softgre-controller
  failover
exit
```

Настраиваем WLC для синхронизации точек доступа

```
wlc
  failover
exit
```

Настраиваем правила Firewall, разрешаем протокол VRRP и порты для синхронизации туннелей и сертификатов:

```
security zone-pair trusted self
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
  rule 12
    action permit
    match protocol tcp
    match destination-port object-group softgre_controller
    enable
  exit
  rule 13
    action permit
    match protocol tcp
    match destination-port object-group sync
    enable
  exit
exit
security zone-pair users self
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Настраиваем DHCP-сервер:

```
no ip dhcp-server pool users-pool
no ip dhcp-server pool ap-pool

ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.4-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043"
  exit
exit
ip dhcp-server pool users-pool
  network 192.168.2.0/24
  address-range 192.168.2.4-192.168.2.254
  default-router 192.168.2.1
  dns-server 192.168.2.1
exit
```

Настраиваем DHCP Failover:

```
ip dhcp-server failover
  mode active-standby
  enable
exit
```

Настраиваем NTP-сервер. Время на устройствах должно быть синхронизировано для корректной работы синхронизации:

```
no ntp broadcast-client enable

ntp enable
ntp server 100.110.0.65
exit
```

Создаем пользователя в локальном Radius-сервере:

```
radius-server local
  domain default
    user test
      password ascii-text 12345678
    exit
  exit
exit
```

Применяем и подтверждаем конфигурацию:

```
wlc-1# commit
wlc-1# confirm
```

Полная конфигурация WLC-1

```
#!/usr/bin/clish
#260
#1.26.x
#01/05/2024
#11:54:29
hostname WLC-1

object-group service airtune
  port-range 8099
exit
object-group service dhcp_client
  port-range 68
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dns
  port-range 53
exit
object-group service netconf
  port-range 830
exit
object-group service ntp
  port-range 123
exit
object-group service radius_auth
  port-range 1812
exit
object-group service sa
  port-range 8043-8044
exit
object-group service ssh
  port-range 22
exit
object-group service sync
  port-range 873
exit
object-group service softgre_controller
  port-range 1337
exit

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit

radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  domain default
    user test
```

```
      password ascii-text encrypted CDE65039E5591FA3
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text encrypted 8CB5107EA7005AFF
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit

boot host auto-config
boot host auto-update

vlan 3
  force-up
exit
vlan 2449
  force-up
exit
vlan 2
exit

no spanning-tree

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone users
exit

bridge 1
  vlan 2449
  security-zone trusted
  ip address 192.168.1.2/24
  vrrp id 1
  vrrp ip 192.168.1.1/32
  vrrp priority 120
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 2
  vlan 2
  security-zone untrusted
  ip address dhcp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
```

```
  mtu 1458
  security-zone users
  ip address 192.168.2.2/24
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp priority 120
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 1/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 1/0/3
  mode switchport
exit
interface gigabitethernet 1/0/4
  mode switchport
exit
interface tengigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 1/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address 192.168.1.2
  remote-address 192.168.1.3
  vrrp-group 1
exit

security zone-pair trusted self
  rule 10
    action permit
    match protocol tcp
    match destination-port object-group ssh
    enable
  exit
  rule 11
    action permit
    match protocol vrrp
    enable
```

```
exit
rule 12
  action permit
  match protocol tcp
  match destination-port object-group softgre_controller
  enable
exit
rule 13
  action permit
  match protocol tcp
  match destination-port object-group sync
  enable
exit
rule 20
  action permit
  match protocol icmp
  enable
exit
rule 30
  action permit
  match protocol udp
  match source-port object-group dhcp_client
  match destination-port object-group dhcp_server
  enable
exit
rule 40
  action permit
  match protocol udp
  match destination-port object-group ntp
  enable
exit
rule 50
  action permit
  match protocol tcp
  match destination-port object-group dns
  enable
exit
rule 60
  action permit
  match protocol udp
  match destination-port object-group dns
  enable
exit
rule 70
  action permit
  match protocol tcp
  match destination-port object-group netconf
  enable
exit
rule 80
  action permit
  match protocol tcp
  match destination-port object-group sa
  enable
exit
rule 90
  action permit
  match protocol udp
  match destination-port object-group radius_auth
  enable
exit
```

```
  rule 100
    action permit
    match protocol gre
    enable
  exit
  rule 110
    action permit
    match protocol tcp
    match destination-port object-group airtune
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
    match source-port object-group dhcp_server
    match destination-port object-group dhcp_client
    enable
  exit
exit
security zone-pair users self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
  rule 20
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_server
    enable
  exit
  rule 30
    action permit
    match protocol tcp
    match destination-port object-group dns
    enable
  exit
  rule 40
    action permit
    match protocol udp
    match destination-port object-group dns
```

```
    enable
  exit
exit
security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit

security passwords default-expired

nat source
  ruleset factory
    to zone untrusted
    rule 10
      description "replace 'source ip' by outgoing interface ip address"
      action source-nat interface
      enable
    exit
  exit
exit

ip dhcp-server
ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.4-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043"
  exit
exit
ip dhcp-server pool users-pool
  network 192.168.2.0/24
  address-range 192.168.2.4-192.168.2.254
  default-router 192.168.2.1
  dns-server 192.168.2.1
exit
ip dhcp-server failover
  mode active-standby
  enable
exit

softgre-controller
  nas-ip-address 127.0.0.1
  failover
  data-tunnel configuration wlc
  aaa radius-profile default_radius
  keepalive-disable
  service-vlan add 3
  enable
exit

wlc
  outside-address 192.168.1.1
  service-activator
    aps join auto
  exit
```

```
  airtune
    enable
  exit
  failover
  ap-location default-location
    description default-location
    mode tunnel
    ap-profile default-ap
    ssid-profile default-ssid
  exit
  ssid-profile default-ssid
    description default-ssid
    ssid default-ssid
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    band 5g
    enable
  exit
  ap-profile default-ap
    password ascii-text encrypted 8CB5107EA7005AFF
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    domain default
  exit
  ip-pool default-ip-pool
    description default-ip-pool
    ap-location default-location
  exit
  enable
exit

ip ssh server

ntp enable
ntp server 100.110.0.65
exit

crypto-sync
crypto-sync remote-delete
```

Пример настройки WLC-2

Подключаемся к WLC и переходим в режим конфигурирования:

```
wlc# config
```

Меняем имя устройства:

```
hostname WLC-2
```

Создаем vlan 2449:

```
vlan 2449
  force-up
exit
```

Настраиваем интерфейс gi 1/0/2 для приема тегированного трафика в VLAN 3 и 2449:

```
interface gigabitethernet 1/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
```

Создаем object-group для настройки Firewall:

```
object-group service sync
  port-range 873
exit
object-group service softgre_controller
  port-range 1337
exit
```

Меняем адресацию и настраиваем VRRP на Bridge:

```
no bridge 1
no bridge 3

bridge 1
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24
  vrrp priority 110
  vrrp id 1
  vrrp ip 192.168.1.1/32
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.3/24
vrrp priority 110
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
```

Указываем адресацию резервируемых контроллеров и назначаем им группу:

```
ip failover
  local-address 192.168.1.3
  remote-address 192.168.1.2
  vrrp-group 1
exit
```

Настраиваем Crypto-Sync для синхронизации сертификатов:

```
crypto-sync
crypto-sync remote-delete
```

Настраиваем Softgre-Controller для синхронизации туннелей SoftGRE:

```
softgre-controller
  failover
exit
```

Настраиваем WLC для синхронизации точек доступа:

```
wlc
  failover
exit
```

Настраиваем правила Firewall, разрешаем протокол VRRP и порты для синхронизации туннелей и сертификатов:

```
security zone-pair trusted self
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
  rule 12
    action permit
    match protocol tcp
    match destination-port object-group softgre_controller
    enable
  exit
  rule 13
    action permit
    match protocol tcp
    match destination-port object-group sync
    enable
  exit
exit
security zone-pair users self
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
exit
```

Настраиваем DHCP-сервер:

```
no ip dhcp-server pool users-pool
no ip dhcp-server pool ap-pool

ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.4-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043"
  exit
exit
ip dhcp-server pool users-pool
  network 192.168.2.0/24
  address-range 192.168.2.4-192.168.2.254
  default-router 192.168.2.1
  dns-server 192.168.2.1
exit
```

Настраиваем DHCP Failover:

```
ip dhcp-server failover
  mode active-standby
  enable
exit
```

Настраиваем NTP-сервер. Время на устройствах должно быть синхронизировано для корректной работы синхронизации:

```
no ntp broadcast-client enable

ntp enable
ntp server 100.110.0.65
exit
```

Создаем пользователя в локальном Radius-сервере:

```
radius-server local
  domain default
    user test
      password ascii-text 12345678
    exit
  exit
exit
```

Применяем и подтверждаем конфигурацию:

```
wlc-2# commit
wlc-2# confirm
```

Полная конфигурация WLC-2

```
#!/usr/bin/clish
#260
#1.26.x
#01/05/2024
#11:54:29
hostname WLC-2

object-group service airtune
  port-range 8099
exit
object-group service dhcp_client
  port-range 68
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dns
  port-range 53
exit
object-group service netconf
  port-range 830
exit
object-group service ntp
  port-range 123
exit
object-group service radius_auth
  port-range 1812
exit
object-group service sa
  port-range 8043-8044
exit
object-group service ssh
  port-range 22
exit
object-group service sync
  port-range 873
exit
object-group service softgre_controller
  port-range 1337
exit

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit

radius-server local
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  domain default
    user test
```

```
      password ascii-text encrypted CDE65039E5591FA3
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text encrypted 8CB5107EA7005AFF
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit

boot host auto-config
boot host auto-update

vlan 3
  force-up
exit
vlan 2449
  force-up
exit
vlan 2
exit

no spanning-tree

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone users
exit

bridge 1
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24
  vrrp id 1
  vrrp ip 192.168.1.1/32
  vrrp priority 110
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 2
  vlan 2
  security-zone untrusted
  ip address dhcp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
```

```
  mtu 1458
  security-zone users
  ip address 192.168.2.3/24
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp priority 110
  vrrp group 1
  vrrp preempt disable
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 1/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 1/0/3
  mode switchport
exit
interface gigabitethernet 1/0/4
  mode switchport
exit
interface tengigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 1/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address 192.168.1.3
  remote-address 192.168.1.2
  vrrp-group 1
exit

security zone-pair trusted self
  rule 10
    action permit
    match protocol tcp
    match destination-port object-group ssh
    enable
  exit
  rule 11
    action permit
    match protocol vrrp
    enable
```

```
exit
rule 12
  action permit
  match protocol tcp
  match destination-port object-group softgre_controller
  enable
exit
rule 13
  action permit
  match protocol tcp
  match destination-port object-group sync
  enable
exit
rule 20
  action permit
  match protocol icmp
  enable
exit
rule 30
  action permit
  match protocol udp
  match source-port object-group dhcp_client
  match destination-port object-group dhcp_server
  enable
exit
rule 40
  action permit
  match protocol udp
  match destination-port object-group ntp
  enable
exit
rule 50
  action permit
  match protocol tcp
  match destination-port object-group dns
  enable
exit
rule 60
  action permit
  match protocol udp
  match destination-port object-group dns
  enable
exit
rule 70
  action permit
  match protocol tcp
  match destination-port object-group netconf
  enable
exit
rule 80
  action permit
  match protocol tcp
  match destination-port object-group sa
  enable
exit
rule 90
  action permit
  match protocol udp
  match destination-port object-group radius_auth
  enable
exit
```

```
  rule 100
    action permit
    match protocol gre
    enable
  exit
  rule 110
    action permit
    match protocol tcp
    match destination-port object-group airtune
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair untrusted self
  rule 1
    action permit
    match protocol udp
    match source-port object-group dhcp_server
    match destination-port object-group dhcp_client
    enable
  exit
exit
security zone-pair users self
  rule 10
    action permit
    match protocol icmp
    enable
  exit
  rule 11
    action permit
    match protocol vrrp
    enable
  exit
  rule 20
    action permit
    match protocol udp
    match source-port object-group dhcp_client
    match destination-port object-group dhcp_server
    enable
  exit
  rule 30
    action permit
    match protocol tcp
    match destination-port object-group dns
    enable
  exit
  rule 40
    action permit
    match protocol udp
    match destination-port object-group dns
```

```
    enable
  exit
exit
security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit

security passwords default-expired

nat source
  ruleset factory
    to zone untrusted
    rule 10
      description "replace 'source ip' by outgoing interface ip address"
      action source-nat interface
      enable
    exit
  exit
exit

ip dhcp-server
ip dhcp-server pool ap-pool
  network 192.168.1.0/24
  address-range 192.168.1.4-192.168.1.254
  default-router 192.168.1.1
  dns-server 192.168.1.1
  option 42 ip-address 192.168.1.1
  vendor-specific
    suboption 12 ascii-text "192.168.1.1"
    suboption 15 ascii-text "https://192.168.1.1:8043"
  exit
exit
ip dhcp-server pool users-pool
  network 192.168.2.0/24
  address-range 192.168.2.4-192.168.2.254
  default-router 192.168.2.1
  dns-server 192.168.2.1
exit
ip dhcp-server failover
  mode active-standby
  enable
exit

softgre-controller
  nas-ip-address 127.0.0.1
  failover
  data-tunnel configuration wlc
  aaa radius-profile default_radius
  keepalive-disable
  service-vlan add 3
  enable
exit

wlc
  outside-address 192.168.1.1
  service-activator
    aps join auto
  exit
```

```
  airtune
    enable
  exit
  failover
  ap-location default-location
    description default-location
    mode tunnel
    ap-profile default-ap
    ssid-profile default-ssid
  exit
  ssid-profile default-ssid
    description default-ssid
    ssid default-ssid
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    band 5g
    enable
  exit
  ap-profile default-ap
    password ascii-text encrypted 8CB5107EA7005AFF
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    domain default
  exit
  ip-pool default-ip-pool
    description default-ip-pool
    ap-location default-location
  exit
  enable
exit

ip ssh server

ntp enable
ntp server 100.110.0.65
exit

crypto-sync
crypto-sync remote-delete
```

22.8.5 Проверка

Для проверки синхронизации туннелей, WLC, DHCP можно посмотреть вывод:

```
WLC-1# show high-availability state
VRRP role:                          Master
AP Tunnels:
    State:                          Successful synchronization
    Last synchronization:           06:18:03 25.09.2023
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
VRF:                                --
    State:                          Successful synchronization
crypto-sync:
    State:                          Successful synchronization
    Last synchronization:           06:18:03 25.09.2023
Firewall:
    State:                          Disabled
    Last state change:              --
WLC:
    State:                          Successful synchronization
    Last synchronization:           06:18:03 25.09.2023
```

23 Часто задаваемые вопросы

Не удалось получить маршруты по BGP и/или OSPF, сконфигурированных в VRF. Соседство успешно устанавливается, но в записи маршрутов в RIB отказано %ROUTING-W-KERNEL: Can not install route. Reached the maximum number of BGP routes in the RIB

Необходимо выделить ресурс RIB для VRF, по умолчанию он равен нулю. Делаем это в режиме конфигурирования VRF:

```
wlc(config)# ip vrf <NAME>
wlc(config-vrf)# ip protocols ospf max-routes 12000
wlc(config-vrf)# ip protocols bgp max-routes 1200000
wlc(config-vrf)# end
```

Закрываются сессии SSH/Telnet, проходящие через контроллер WLC

Для поддержания сессии активной необходимо настроить передачу keepalive-пакетов. Опция отправки keepalive настраивается в клиенте SSH, например, для клиента PuTTY раздел “Соединение”.

В свою очередь, на контроллере можно выставить время ожидания до закрытия неактивных сессий TCP (в примере выставлен 1 час):

```
wlc(config)# ip firewall sessions tcp-estabilished-timeout 3600
```

На интерфейсе был отключен firewall (ip firewall disable). После внесения этого интерфейса в security zone, удаления из конфигурации ip firewall disable и применения изменений – доступ для активных сессий с данного порта не закрылся согласно правилам security zone-pair

Изменения в конфигурации Firewall будут действовать только для новых сессий, сброса активных сессий в Firewall не происходит. Очистить активные сессии в firewall можно командой:

```
wlc# clear ip firewall session
```

Как полностью очистить конфигурация WLC и как сбросить на заводскую конфигурацию?

Очистка конфигурации происходит путем копирования пустой конфигурации в candidate-config и применения его в running-config.

```
wlc# copy system:default-config system:candidate-config
```

Процесс сброса на заводскую конфигурацию аналогичен.

```
wlc# copy system:factory-config system:candidate-config
```

Как привязать subinterface к созданным VLAN?

При создании саб-интерфейса VLAN создается и привязывается автоматически (прямая зависимость индекс sub – VID).

```
wlc(config)# interface gigabitethernet 1/0/1.100
```

После применения можно наблюдать информационные сообщения:

```
2016-07-14T012:46:24+00:00 %VLAN: creating VLAN 100
```

Есть ли функционал в контроллерах WLC для анализа трафика?

В контроллерах WLC реализована возможность анализировать трафик на интерфейсах из CLI. Сниффер запускается командой monitor:

```
wlc# monitor gigabitethernet 1/0/1
```

Как настроить ip prefix-list 0.0.0.0/0?

Ниже приведен пример конфигурации префикс-листа, разрешающего прием маршрута по умолчанию:

```
wlc(config)# ip prefix-list eltex
wlc(config-pl)# permit default-route
```

Проблема прохождения асинхронного трафика

В случае организации сети с асинхронной маршрутизацией, Firewall будет запрещать "неправильный (ошибочный)" входящий трафик (не открывающий новое соединение и не принадлежащий никакому установленному соединению) из соображений безопасности.

Разрешающее правило в Firewall не решит поставленную задачу для подобных схем. Решить задачу можно, отключив Firewall на входном интерфейсе:

```
wlc(config-if-gi)# ip firewall disable
```

Как можно сохранить локальную копию конфигурации контроллера?

Если необходимо скопировать текущую running или candidate – конфигурацию на самом контроллере – можно воспользоваться командой copy с указанием в качестве источника копирования "system:running-config" или "system:candidate-config", а в качестве назначения – файл в разделе "flash:data/".

```
wlc# copy system:candidate-config flash:data/temp.txt
```

Также существует возможность копирования ранее сохраненных конфигурационных файлов (автоматически из раздела flash:backup/ или вручную из раздела flash:data/) в candidate-конфигурацию:

```
wlc# copy flash:data/temp.txt system:candidate-config
wlc# copy flash:backup/config_20190918_164455 system:candidate-config
```

24 Приложение A. Packet Flow

24.1 Порядок обработки входящего/исходящего трафика сетевыми службами контроллерами WLC

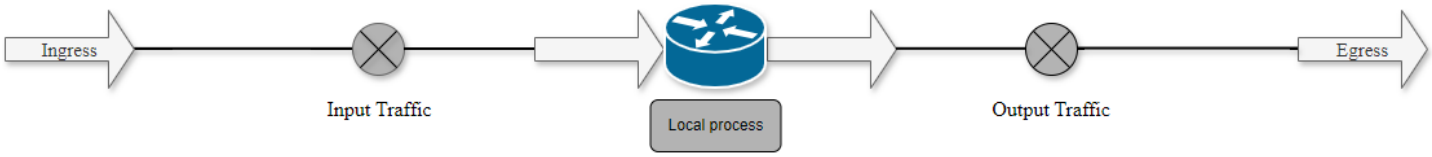


Таблица 25 – Порядок обработки входящего трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (Ограничение полосы пропускания, классификация и т. д.)
3	Инспектирование пакета сервисом IDS/IPS в режиме service-ips monitor[1]
4	Выполнение правил между специальными зонами (например, any/self, trusted/any)
5	Выполнение функций DOS defense[1]. На данном этапе выполняются функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets
6	Выполнение дефрагментации пакета
7	Выполнение начальных функций BRAS (Инициализация соединений, сессий)[1]
8	Выполнение HTTP/HTTPs прокси[1]
9	Функции Destination NAT[1]
10	Routing Decision (FIB)
11	Выполнение функций DOS defense[1]. На этапе данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan
12	Выполнение правил внутри зон (например, trusted/self)
13	Передача пакета в DPI[1]
14	Передача пакета в Netflow/Sflow (Ingress)[1]
15	Передача пакета в Antispam[1]
16	IPsec (decode)[1]. После выполнения этого шага происходит переход к п.3

Таблица 26 – Порядок обработки исходящего трафика

Шаг	Описание
1	Route Decision
2	Выполнение правил между зонами
3	tcp adjust-mss[1]
4	BRAS (Установка интерфейса для отправки пакета)[1]
5	Выполнение функций Source NAT[1]
6	IPsec (encode)[1]
Если необходимо шифрование, то после этого процесса выполняются следующие операции:	
6.1	Выполнение правил между зонами
6.2	tcp adjust-mss[1]
6.3	Netflow/sFlow (Egress)[1]
6.4	Выполнение функций Source NAT[1]
7	Выполнение фрагментации пакетов
8	Выполнение функций QoS (Ограничение полосы пропускания, классификация и т. д.)

[1]Данный функционал выполняется только при наличии необходимых настроек.

24.2 Порядок обработки транзитного трафика сетевыми службами контроллерами WLC

Таблица 27 – Порядок обработки транзитного трафика

Шаг	Описание
1	Выполнение функций ACL на входящем трафике
2	Выполнение функций QoS (Ограничение полосы пропускания, классификация и т. д.)
3	Выполнение правил, между специальными зонами (например, any/self, trusted/any)
4	Выполнение функций DOS defense[1]. На данном этапе выполняются функции защиты от DDOS из раздела firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets
5	Выполнение дефрагментации пакета
6	Выполнение начальных функций BRAS (Инициализация соединений, сессий)[1]
7	Выполнение HTTP/HTTPs прокси[1]
8	Функции Destination NAT[1]
9	Routing Decision (FIB)
Если пакет перед передачей необходимо обработать протоколом более высокого уровня, выполняются следующие действия:	
9.1	Выполнение функций DOS defense[1]. На данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan
9.2	Выполнение правил внутри зон (например, trusted/self)
9.3	Передача пакета в DPI[1]
9.4	Передача пакета в Netflow/Sflow (Ingress)[1]
9.5	Передача пакета в Antispam[1]
9.6	IPsec (decode)[1]. После выполнения этого шага происходит переход к п.3
10	Инспектирование пакета сервисом IDS/IPS в режиме service-ips inline[1]
11	tcp adjust-mss[1]

Шаг	Описание
12	Выполнение функций DOS defense[1]. На данном этапе выполняются специфичные функции защиты от DDOS из разделов firewall screen dos-defense, firewall screen spy-blocking, firewall screen suspicious-packets: ip firewall screen suspicious-packets large-icmp ip firewall screen dos-defense winnuke ip firewall screen spy-blocking port-scan
13	Выполнение правил между зонами (например, trusted/untrusted, untrusted/trusted, trusted/trusted)
14	Передача пакета в DPI[1]
15	Netflow/Sflow (Egress)[1]
16	BRAS (Установка интерфейса для отправки пакета)[1]
17	Выполнение функций Source NAT[1]
18	IPsec (encode)[1]
Если необходимо шифрование, то после этого процесса, выполняются следующие операции:	
18.1	Выполнение правил между зонами
18.2	tcp adjust-mss[1]
18.3	Netflow/sFflow (Egress)[1]
18.4	Выполнение функций Source NAT[1]
19	Выполнение фрагментации пакетов
20	Выполнение функций QoS (Ограничение полосы пропускания, классификация и т. д.)

[1]Данный функционал выполняется только при наличии необходимых настроек.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

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

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

На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к базе знаний или оставить интерактивную заявку:

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

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

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