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

Руководство по эксплуатации
Версия ПО 1.30.4

Содержание

1 Введение ... 5
1.1 Аннотация ... 5
1.2 Использование контроллера ... 5
1.3 Целевая аудитория ... 5
1.4 Условные обозначения ... 5
1.5 Подсказки, примечания и предупреждения ... 6
2 Quickstart ... 7
3 Описание изделий ... 9
3.1 Назначение ... 9
3.2 Функции ... 10
3.3 Основные технические характеристики ... 15
3.4 Конструктивное исполнение ... 19
3.5 Комплект поставки ... 31
4 Установка и подключение ... 32
4.1 Крепление кронштейнов ... 32
4.2 Установка устройства в стойку ... 32
4.3 Установка модулей питания WLC-3200 ... 33
4.4 Подключение питающей сети ... 34
4.5 Установка и удаление SFP-трансиверов ... 35
5 Интерфейсы управления ... 36
5.1 Интерфейс командной строки (CLI) ... 36
5.2 Типы и порядок именования интерфейсов контроллера ... 37
5.3 Типы и порядок именования туннелей контроллера ... 40
6 Начальная настройка устройств ... 42
6.1 Заводская конфигурация устройств ... 42
6.2 Подключение и конфигурирование устройства ... 43
7 Обновление программного обеспечения ... 49
7.1 Обновление программного обеспечения средствами системы ... 49
7.2 Обновление программного обеспечения из начального загрузчика ... 51
7.3 Обновление вторичного загрузчика (U-Boot) ... 52
8 Рекомендации по безопасной настройке ... 54
8.1 Общие рекомендации ... 54
8.2 Настройка системы логирования событий ... 54
8.3 Настройка политики использования паролей ... 55

8.4 Настройка политики AAA ... 56
8.5 Настройка удалённого управления ... 58
8.6 Настройка механизмов защиты от сетевых атак ... 59
9 Управление интерфейсами ... 61
10 Управление контроллером WLC ... 61
10.1 Настройка WLC ... 61
10.2 Управление через WEB-интерфейс ... 92
11 Управление туннелированием ... 184
12 Управление функциями второго уровня (L2) ... 184
13 Управление QoS ... 185
14 Управление маршрутизацией ... 185
15 Управление технологией MPLS ... 185
16 Управление безопасностью ... 185
17 Управление резервированием ... 185
18 Управление кластеризацей ... 186
18.1 Настройка Cluster ... 186
18.2 Подключение сервисов ... 204
19 Управление удаленным доступом ... 300
20 Управление сервисами ... 300
21 Мониторинг ... 300
22 Управление BRAS (Broadband Remote Access Server) ... 301
22.1 Алгоритм настройки ... 301
22.2 Пример настройки с SoftWLC ... 306
22.3 Пример настройки без SoftWLC ... 312
23 Статьи ... 318
23.1 LDAP-авторизация ... 318
23.2 RADIUS-сервер ... 319
23.3 TLS-авторизация ... 339
23.4 WIDS/WIPS ... 368
23.5 Активация функционала по лицензии ... 377
23.6 Анализ отладочной информации протокола RADIUS ... 380
23.7 Настройка доступа беспроводных клиентов по MAC-адресам ... 432
23.8 Настройка ограничения скорости трафика ... 435
23.9 Изменение пути хранения журналов WLC ... 437
23.10 Обновление точек доступа ... 443
23.11 Портальная авторизация ... 448
23.12 Резервирование WLC ... 534

24 Часто задаваемые вопросы 558
24.1 Ошибка "error - certificate is not yet valid" при comit 558
24.2 Как снизить MTU на ТД 558
24.3 Не удалось получить маршруты по BGP и/или OSPF, сконфигурированных в VRF 559
24.4 Закрываются сессии SSH/Telnet, проходящие через контроллер WLC 559
24.5 Как полностью очистить конфигурация WLC и как сбросить на заводскую конфигурацию? 560
24.6 Как привязать subinterface к созданным VLAN? 560
24.7 Есть ли функционал в контроллерах WLC для анализа трафика? 560
24.8 Как настроить ip prefix-list 0.0.0.0/0? 560
24.9 Проблема прохождения асинхронного трафика 560
24.10 Как можно сохранить локальную копию конфигурации контроллера? 561
25 Приложение A. Packet Flow 562
25.1 Порядок обработки входящего/исходящего трафика сетевыми службами контроллерами WLC 562
25.2 Порядок обработки транзитного трафика сетевыми службами контроллерами WLC 564

1 Введение

- Аннотация
- Использование контроллера
- Целевая аудитория
- Условные обозначения
- Подсказки, примечания и предупреждения

⚠ 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 реализации 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.

Обозначение	Описание
{ }	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 Подсказки, 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.

Подсказки содержат советы по использованию и настройке 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. Убедитесь, что WLC и подключаемая к нему точка доступа сброшены до заводских настроек. Если есть сомнения в том, что конфигурация устройств заводская, сбросьте 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. Подключите точку доступа напрямую в порт gi1/0/2. Если для питания точки доступа используется PoE-инжектор, то подключите точку в порт gi1/0/2 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. Включите порт gi1/0/1 WLC 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.
4. Для подключения к WLC в заводской конфигурации по ssh подключите ПК к любому свободному порту, кроме gi1/0/1, получите от контроллера адрес по DHCP и выполните подключение по ssh к admin@192.168.1.1.
5. Для корректной регистрации точек доступа на контроллере время на всех устройствах должно быть актуальным. Настроите NTP-сервер, чтобы контроллер получил актуальное время от вышестоящего сервера и точки доступа могли синхронизировать время с контроллером. Настроить NTP-сервер можно следующими командами:

```
#Отключите режим broadcast-client, который включен в заводской конфигурации и предполагает синхронизацию времени по широковещательным пакетам от сервера:
wlc(config)# no ntp broadcast-client enable

#Задайте адрес вышестоящего сервера NTP, с которым будет осуществляться синхронизация времени:
wlc(config)# ntp server <IP-ADDRESS>
#где
#<IP-ADDRESS> – IP-адрес NTP-сервера, задаётся в виде AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
#Задайте IP-адрес NTP сервера, который будет доступен в сети для вашего контроллера.

#Задайте минимальный интервал времени между отправкой сообщений NTP-серверу:
wlc(config-ntp-server)# minpoll 1

#Задайте максимальный интервал времени между отправкой сообщений NTP-серверу:
wlc(config-ntp-server)# maxpoll 4
wlc(config-ntp-server)# exit

#Активируйте работу протокола NTP:
wlc(config)# ntp enable

#Примените и сохраните настройки:
wlc# commit
wlc# confirm
```

6. После подключения к WLC аплинка и точки доступа, точка доступа автоматически получит с WLC адрес по DHCP из сети 192.168.1.0/24, синхронизируется время, зарегистрируется на встроенном Wi-Fi контроллере, получит конфигурацию, включит SSID, построит GRE-туннель до WLC для передачи абонентского трафика и будет готова для подключения enterprise-клиентов.
7. Для успешной авторизации клиента создайте 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

#Создайте 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 NTP и 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

- Назначение
- Функции
  - Функции интерфейсов
  - Функции при работе с MAC-адресами
  - Функции второго уровня сетевой модели OSI
  - Функции третьего уровня сетевой модели OSI
  - Функции туннелирования трафика
  - Функции управления и конфигурирования
  - Функции сетевой защиты
- Основные технические характеристики
- Конструктивное исполнение
  - Конструктивное исполнение WLC-15
  - Конструктивное исполнение WLC-30
  - Конструктивное исполнение WLC-3200
- Комплект поставки

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 3000
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.

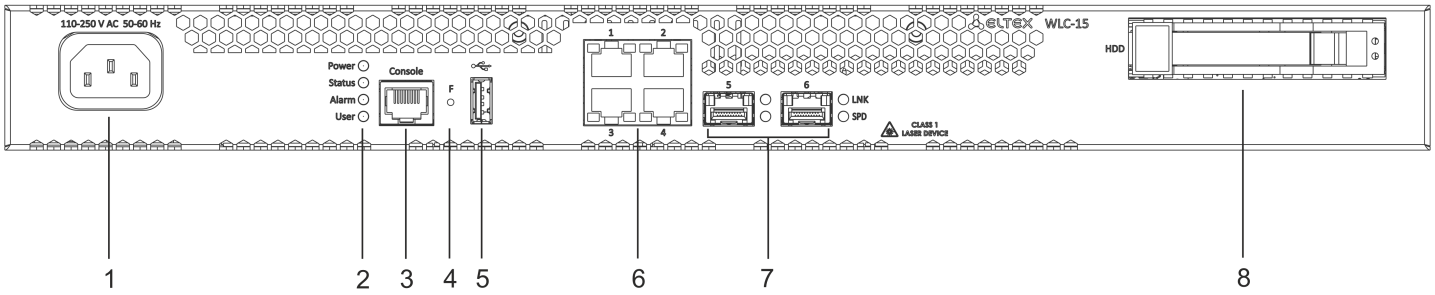


Рисунок 1 – Передняя панель WLC-15

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, использующийся 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.

№	Элемент передней панели	Описание
7	[5-6]	2 порта 1000BASE-X SFP.
8	HDD	Разъем для установки жесткого диска памяти. Зеленый индикатор: • диск не вставлен – не горит; • диск вставлен – горит; • есть активность на диске – мигает. Красный индикатор (будет поддержан в будущих версиях).

Задняя панель устройства WLC-15

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

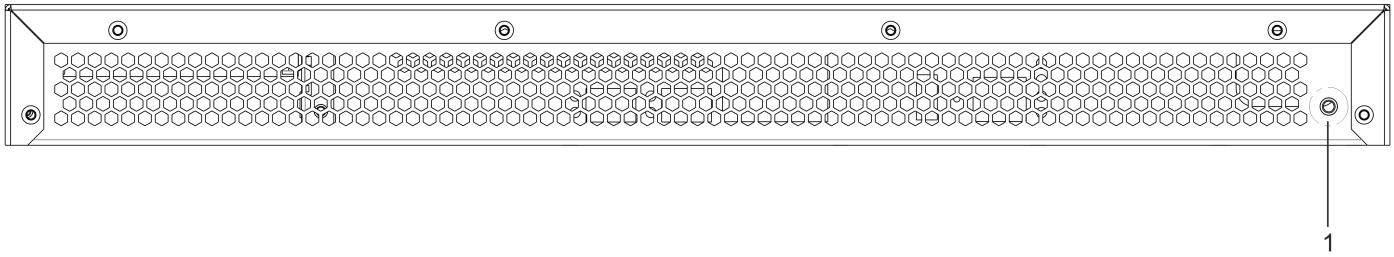


Рисунок 2 – Задняя панель WLC-15

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.

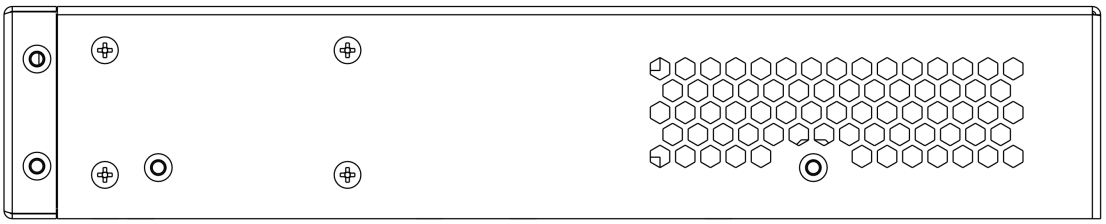


Рисунок 3 – Правая боковая панель WLC-15

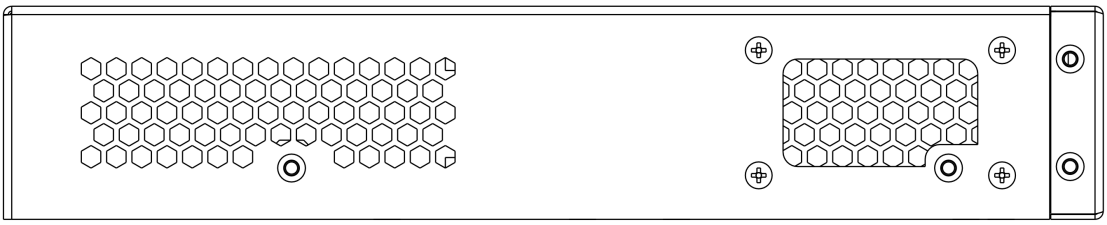


Рисунок 4 – Левая боковая панель WLC-15

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.

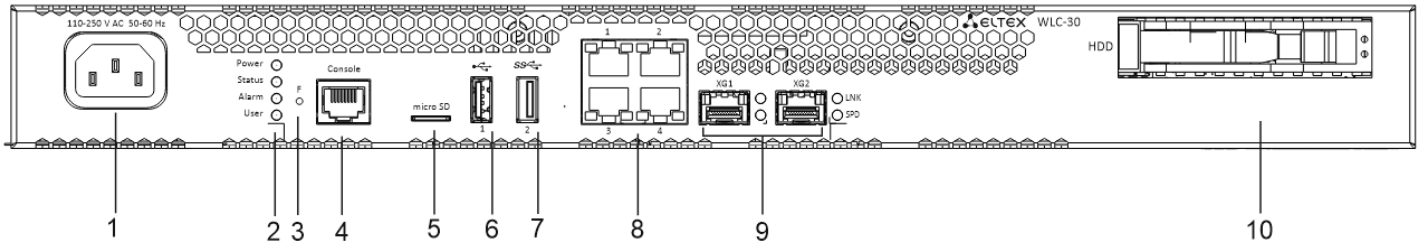


Рисунок 5 – Передняя панель WLC-30

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, использующийся 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.

№	Элемент передней панели	Описание
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.
9	XG1, XG2	2 порта 10GBASE-R (SFP+)1000BASE-X.
10	HDD	Разъем для установки жесткого диска памяти. Зеленый индикатор: • диск не вставлен – не горит; • диск вставлен – горит; • есть активность на диске – мигает. Красный индикатор (будет поддержан в будущих версиях).

Задняя панель устройства WLC-30

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

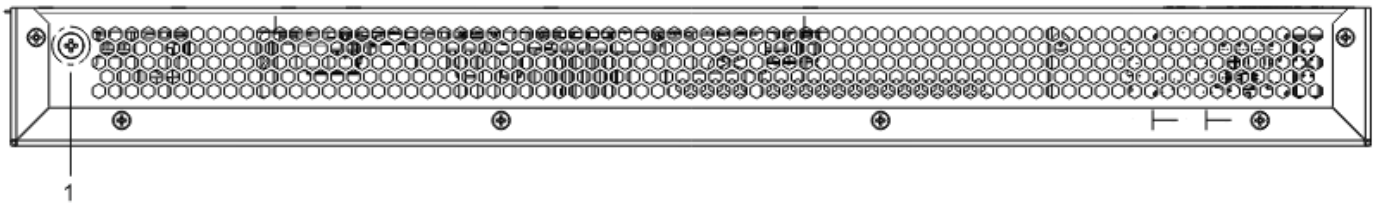


Рисунок 6 – Задняя панель WLC-30

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.

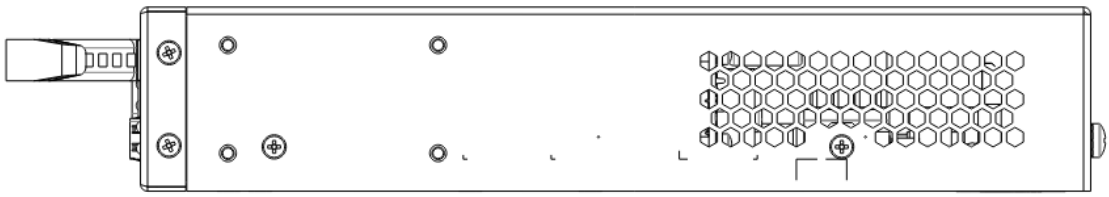


Рисунок 7 – Правая боковая панель WLC-30

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.

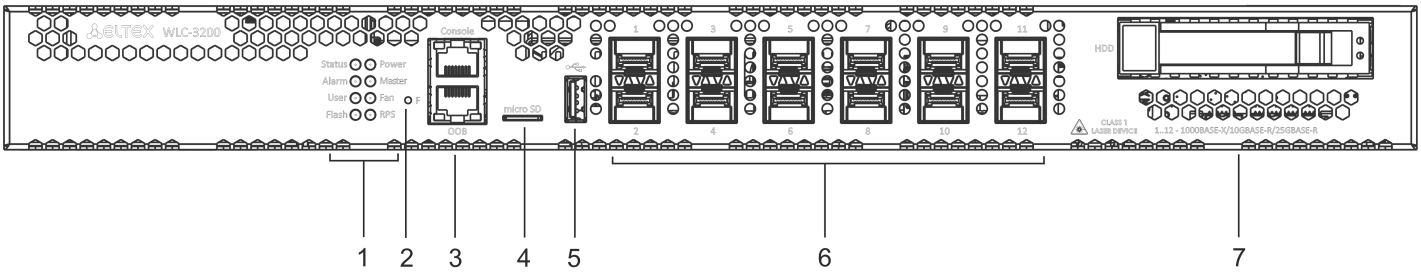


Рисунок 9 – Передняя панель WLC-3200

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, использующийся 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.

№	Элемент передней панели	Описание
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.
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. Зеленый индикатор: • диск не вставлен – не горит; • диск вставлен – горит; • есть активность на диске – мигает. Красный индикатор (будет поддержан в будущих версиях).

Задняя панель устройства WLC-3200

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

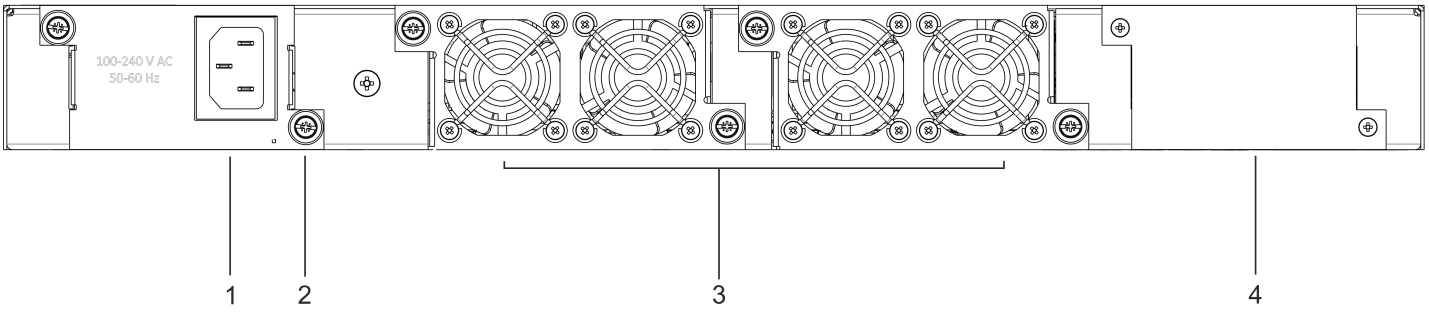


Рисунок 10 – Задняя панель WLC-3200

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.

№	Описание
4	Место для установки резервного источника питания.

Боковые панели устройства WLC-3200

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

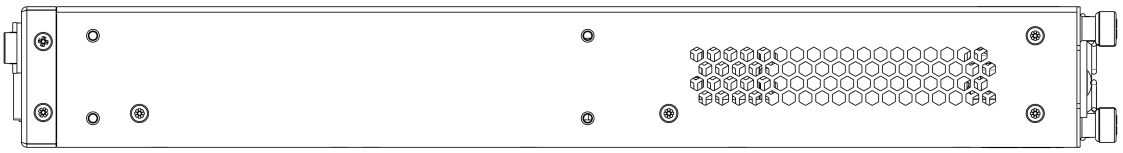


Рисунок 11 – Правая боковая панель WLC-3200

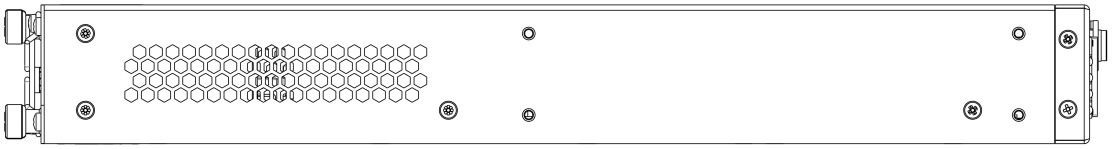


Рисунок 12 – Левая боковая панель WLC-3200

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.

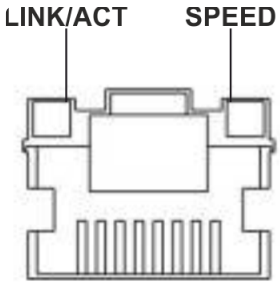


Рисунок 13 – Расположение индикаторов разъема RJ-45

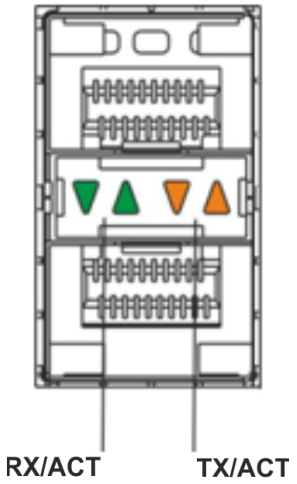


Рисунок 14 – Расположение индикаторов оптических интерфейсов

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.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
Alarm	Индикатор наличия и уровня аварии устройства.	-	-
VPN	Индикатор наличия активных VPN-сессий.	-	-
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.

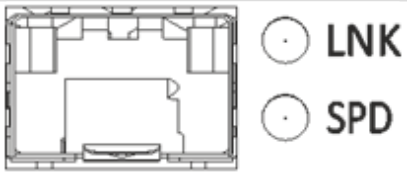


Рисунок 15 – Расположение индикаторов разъема SFP

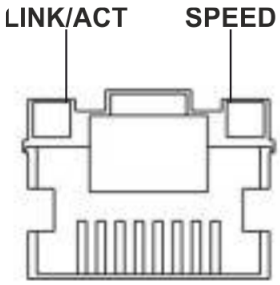


Рисунок 16 – Расположение индикаторов разъема RJ-45

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.
		Выключен	Отказ внутренних источников питания устройства.
Status	Индикатор текущего состояния устройства.	Зеленый	Устройство работает нормально.

Название индикатора	Функция индикатора	Состояние индикатора	Состояние устройства
		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.

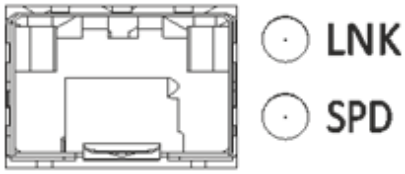


Рисунок 17 – Расположение индикаторов разъема SFP

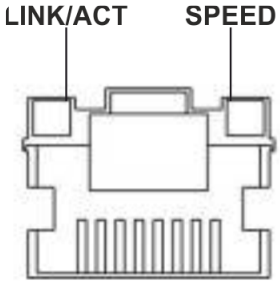


Рисунок 18 – Расположение индикаторов разъема RJ-45

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

- Крепление кронштейнов
- Установка устройства в стойку
- Установка модулей питания WLC-3200
- Подключение питающей сети
- Установка и удаление SFP-трансиверов
  - Установка трансивера
  - Удаление трансивера

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:

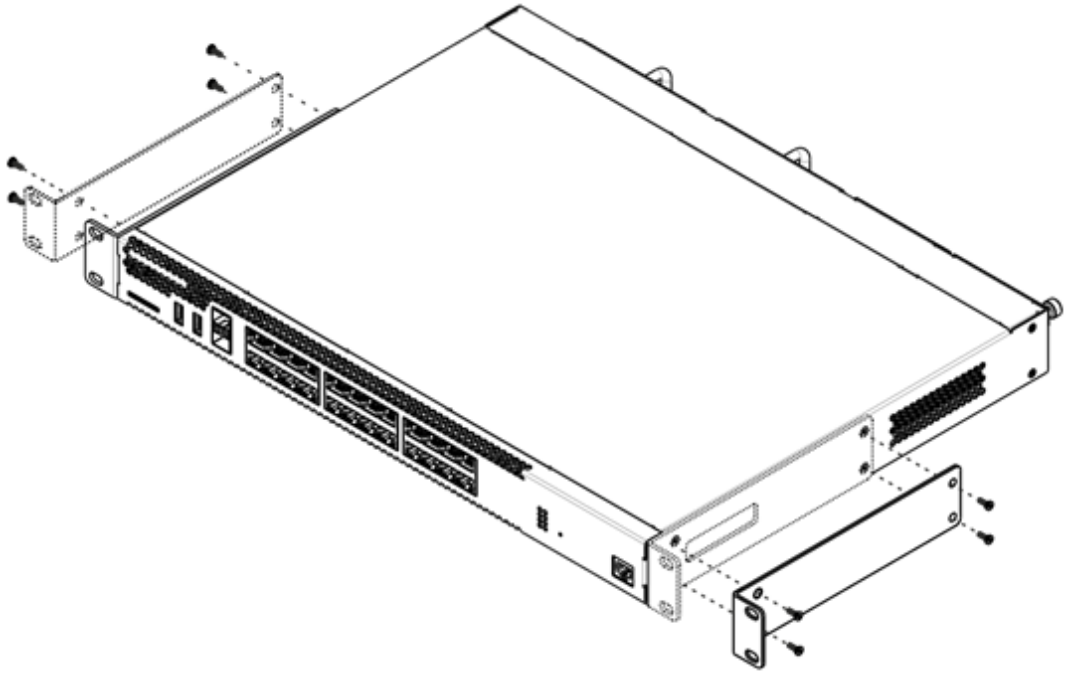


Рисунок 19 – Крепление кронштейнов

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.

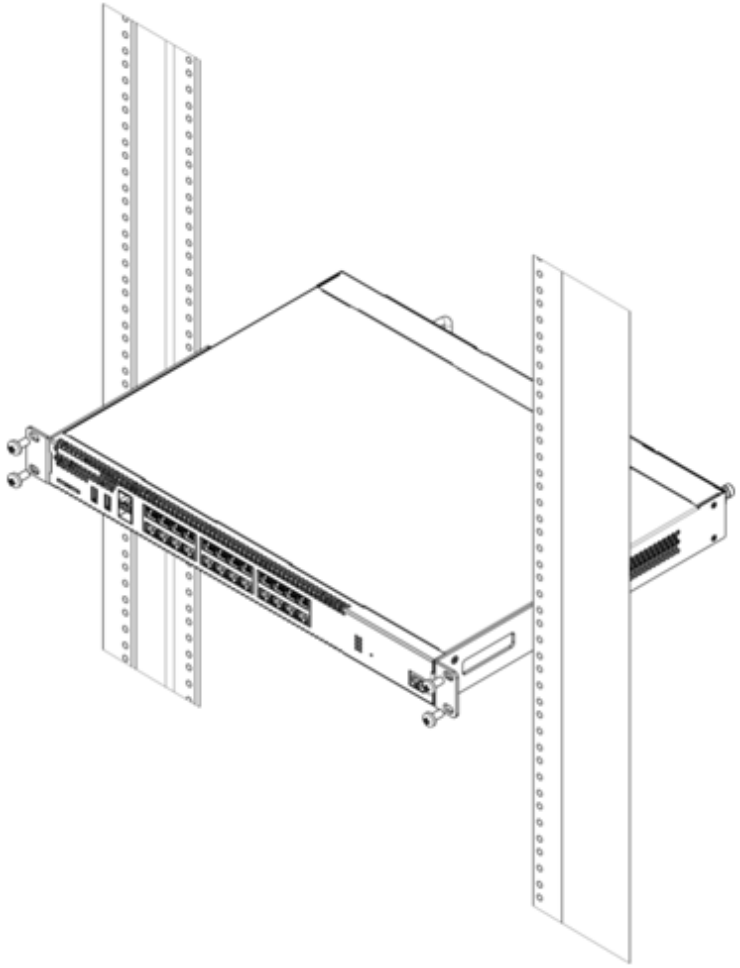


Рисунок 20 – Установка устройства в стойку

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.

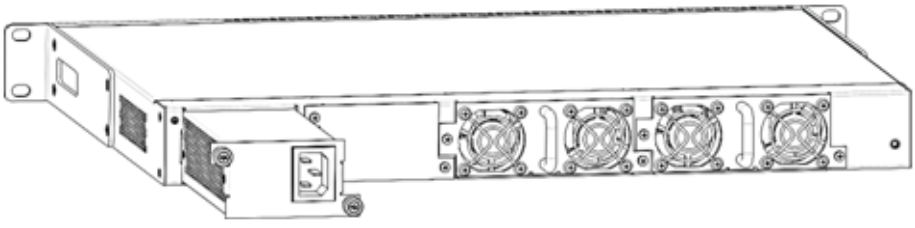


Рисунок 21 – Установка модулей питания

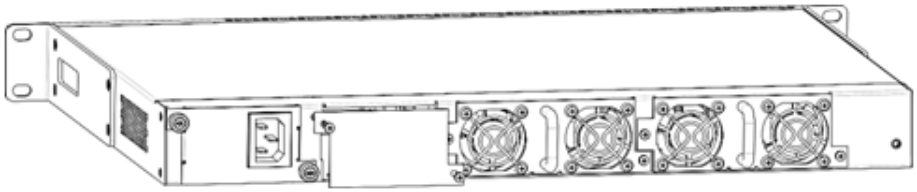


Рисунок 22 – Установка заглушки

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.

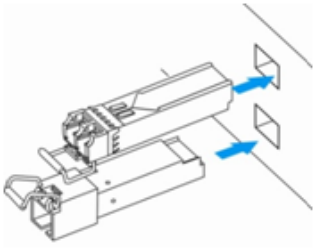


Рисунок 23– Установка SFP-трансиверов

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

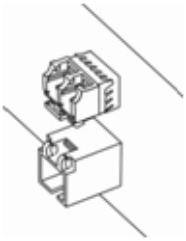


Рисунок 24 – Установленные SFP-трансиверы

4.5.2 Удаление трансивера

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

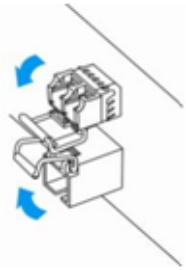


Рисунок 25 – Открытие защелки SFP-трансиверов

2. Извлеките модуль из слота.

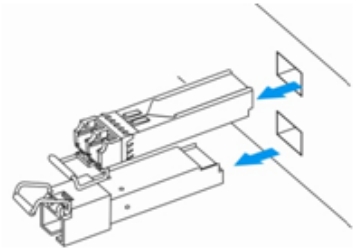


Рисунок 26 – Извлечение SFP-трансиверов

5 Интерфейсы управления

- Интерфейс командной строки (CLI)
- Типы и порядок именования интерфейсов контроллера
- Типы и порядок именования туннелей контроллера

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.
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.

Тип интерфейса	Обозначение
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**
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**

Тип интерфейса	Обозначение
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**
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**

Тип туннеля	Обозначение
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

- Заводская конфигурация устройств
  - Описание заводской конфигурации
- Подключение и конфигурирование устройства
  - Подключение к устройству
    - Подключение по локальной сети Ethernet
    - Подключение через консольный порт RS-232
  - Применение изменения конфигурации
  - Базовая настройка устройств
    - Изменение пароля пользователя «admin»
    - Создание новых пользователей
    - Назначение имени устройства
    - Настройка параметров публичной сети
    - Настройка удаленного доступа к устройству

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 Начальная настройка 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».

⚠ **У**четная 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 object-group <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 маршрутизатору 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 object-group ssh
wlc(config-zone-rule)# enable
wlc(config-zone-rule)# exit
wlc(config-zone-pair)# exit
```

7 Обновление программного обеспечения

- Обновление программного обеспечения средствами системы
- Обновление программного обеспечения из начального загрузчика
- Обновление вторичного загрузчика (U-Boot)

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.

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

- Общие рекомендации
- Настройка системы логирования событий
  - Рекомендации
  - Предупреждения
  - Пример настройки
- Настройка политики использования паролей
  - Рекомендации
  - Пример настройки
- Настройка политики AAA
  - Рекомендации
  - Предупреждения
  - Пример настройки
- Настройка удалённого управления
  - Рекомендации
  - Пример настройки
- Настройка механизмов защиты от сетевых атак
  - Рекомендации
  - Пример настройки

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

- Настройка WLC
- Управление через WEB-интерфейс

10.1 Настройка WLC

- Настройка контроллера WLC
  - Пример настройки
    - Задача
    - Решение
      - Настройка интерфейсов, сетевых параметров и firewall
      - Настройка NTP-сервера
      - Настройка DHCP-сервера
      - Настройка RADIUS-сервера
      - Настройка модуля управления точками доступа WLC
        - Настройка SSID
        - Настройка профилей конфигурации
        - Настройка локации
        - Определение подсетей обслуживаемых точек доступа
        - Авторегистрация точек доступа
        - Включение функционала WLC
      - Web-интерфейс
      - Обновление точек доступа
  - Алгоритм настройки
- Настройка AirTune
  - Алгоритм работы
  - Алгоритм настройки
  - Пример настройки

10.1.1 Настройка контроллера WLC

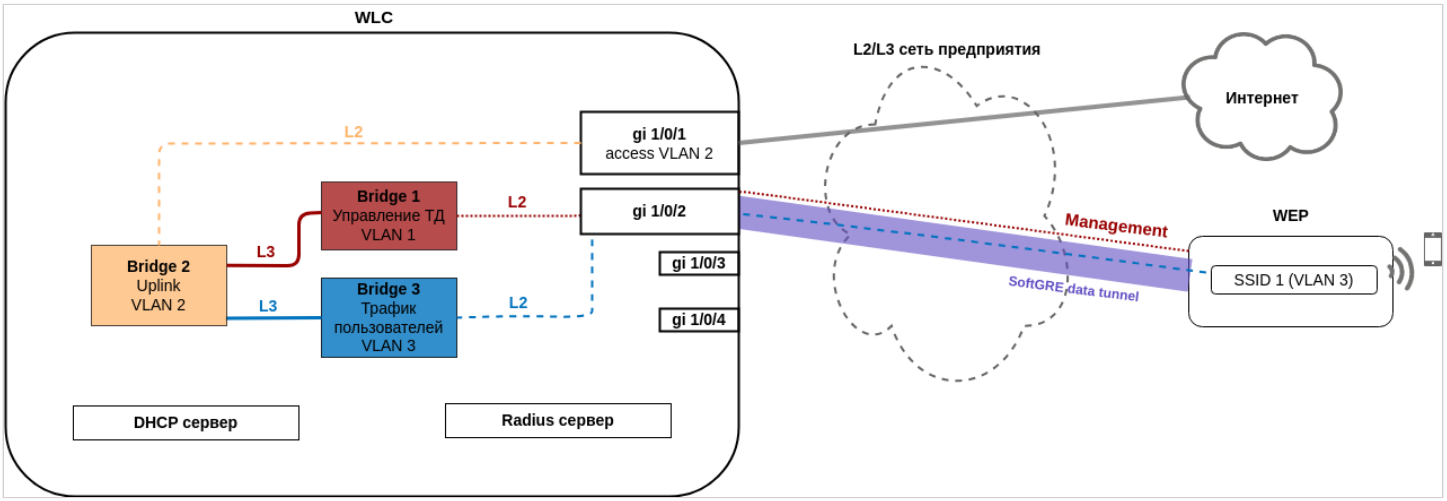
⚠ Функционал WLC можно активировать на сервисных маршрутизаторах ESR-15, ESR-15R, ESR-30 и ESR-3200 по инструкции.

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): выбранными профилями конфигурации 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.
    - 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

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

wlc(config)# object-group service web
wlc(config-object-group-service)# port-range 443
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 object-group 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 object-group dhcp_client
wlc(config-zone-pair-rule)# match destination-port object-group 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 object-group 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 object-group 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 object-group 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 object-group 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 object-group 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 object-group 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)# rule 110
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port object-group airtune
wlc(config-zone-pair-rule)# enable
wlc(config-zone-pair-rule)# exit
wlc(config-zone-pair)# rule 120
wlc(config-zone-pair-rule)# action permit
wlc(config-zone-pair-rule)# match protocol tcp
wlc(config-zone-pair-rule)# match destination-port object-group web
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 object-group dhcp_client
wlc(config-zone-pair-rule)# match destination-port object-group 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 object-group 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 object-group 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 object-group dhcp_server
wlc(config-zone-pair-rule)# match destination-port object-group 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, пользователями Wi-Fi и сетью 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)# no spanning-tree
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)# no spanning-tree
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)# no spanning-tree
wlc(config-bridge)# vlan 3
wlc(config-bridge)# mtu 1458
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 сервер SSH для доступа к контроллеру:

```
wlc(config)# ip ssh server
```

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 NTP-сервера

> ⚠ Необходимо обязательно синхронизировать время на контроллере и точках доступа, т. к. корректное время позволяет пройти проверку валидности сертификатов.

Для корректной регистрации точек доступа на контроллере требуется синхронизация времени. Настройте NTP-сервер, чтобы контроллер получил актуальное время от вышестоящего сервера. Затем укажите адрес контроллера в качестве NTP-сервера для точек доступа в 42 опции DHCP (пример настройки представлен в разделе Настройка DHCP-сервера), чтобы точки доступа также смогли получить актуальное время.

```
#Отключаем режим broadcast-client, который включен в заводской конфигурации и предполагает
синхронизацию времени по широковещательным пакетам от сервера:
wlc(config)# no ntp broadcast-client enable

#Задаем адрес вышестоящего сервера NTP, с которым будет осуществляться синхронизация времени:
wlc(config)# ntp server 46.146.231.187

#Задаем минимальный интервал времени между отправкой сообщений NTP-серверу:
wlc(config-ntp-server)# minpoll 1

#Задаем максимальный интервал времени между отправкой сообщений NTP-серверу:
wlc(config-ntp-server)# maxpoll 4
wlc(config-ntp-server)# exit

#Активируем работу протокола NTP:
wlc(config)# ntp enable
```

Настройка DHCP-сервера

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
```

Включите DHCP-сервер:

```
#Включаем DHCP-сервер:
wlc(config)# ip dhcp-server
```

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-сервер. 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

#Включаем RADIUS-сервер:
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 без проксирования, 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

#Включаем роуминг по стандартам 802.11k и 802.11v:
wlc(config-wlc-ssid-profile)# 802.11kv

#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

#По умолчанию доступ до точкам доступа закрыт. При необходимости, можно активировать доступ 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:
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:
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) 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

#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. Исключение составят точки
доступа, для которых создан индивидуальный профиль конфигурации по MAC-адресу. Правила в
индивидуальном профиле имеют приоритет.
```

```
#Указываем локацию, в которую будут попадать точки доступа данного пула адресов:
wlc(config-wlc-ip-pool)# ap-location default-location
wlc(config-wlc-ip-pool)# exit
```

По умолчанию параметр network имеет значение 0.0.0.0/0, то есть под правило попадает любой IP-адрес. Увидеть значение параметра по умолчанию можно с помощью команды *show running-config full wlc ip-pool*.
Если ip-pool ограничен конкретной подсетью и IP-адрес точки доступа не попадает в эту подсеть, а также для этой точки доступа не создан индивидуальный профиль по ее MAC-адресу, такая точка не будет 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 зарегистрированы 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 конфигурирования модуля управления точками доступа, а также мониторинга предусмотрен web-интерфейс, который доступен по протоколу HTTPS в заводской конфигурации. Доступ по HTTP можно включить командой (дополнительно потребуется настроить firewall для пропуска трафика по порту 80):

```
#Добавляем в группу сервиса WEB порт 80:
wlc(config)# object-group service web
wlc(config-object-group-service)# port-range 80,443
wlc(config-object-group-service)# exit

#Включаем HTTP-сервер
wlc(config)# ip http server
wlc(config)# end
wlc# commit
wlc# confirm
```

Web-интерфейс по умолчанию будет доступен по URL: https://<IP-address_wlc>, с учетной записью: 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 переподключении 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. Подробнее об обновлении точек доступа можно прочитать в статье Обновление точек доступа.

Алгоритм настройки

Раздел содержит алгоритм настройки модуля WLC, RADIUS-сервера и SoftGRE-контроллера.

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

Шаг	Описание	Команда	Ключи
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.
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 NAS	**wlc(config-softgre-controller)# nas-ip-address <ADDR>**	<ADDR> – IP-адрес источника в отправляемых RADIUS-пакетах, 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.

Шаг	Описание	Команда	Ключи
16	Указать профиль AAA.	**wlc(config-softgre-controller)# aaa radius-profile <NAME>**	<NAME> – имя профиля сервера, задается строкой до 31 символа.
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	Установить 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**	

Шаг	Описание	Команда	Ключи
25	Перейти в раздел конфигурирования контроллера.	**wlc(config)# wlc**	
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>minimal</th><th>low</th><th>middle</th><th>high</th><th>maximal</th></tr>
<tr><td>WEP-1L</td><td>3</td><td>6</td><td>10</td><td>13</td><td>16</td></tr>
<tr><td>WEP-2L</td><td>3</td><td>6</td><td>10</td><td>13</td><td>16</td></tr>
<tr><td>WEP-3L</td><td>11</td><td>12</td><td>14</td><td>15</td><td>16</td></tr>
<tr><td>WEP-200L</td><td>4</td><td>4</td><td>7</td><td>10</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>WEP-30L-Z</td><td>0</td><td>4</td><td>8</td><td>12</td><td>16</td></tr>
<tr><td>WEP-3ax</td><td>6</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
<tr><td>WOP-2L</td><td>3</td><td>6</td><td>10</td><td>13</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>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>WOP-30LI</td><td>0</td><td>4</td><td>8</td><td>12</td><td>16</td></tr>
<tr><td>WEP-2ac</td><td>5</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
<tr><td>WEP-2ac Smart</td><td>5</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
<tr><td>WOP-2ac</td><td>5</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
<tr><td>WOP-2ac:rev.B</td><td>5</td><td>8</td><td>11</td><td>14</td><td>16</td></tr>
<tr><td>WOP-2ac:rev.C</td><td>5</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>
</table>

Шаг	Описание	Команда	Ключи
35	Настроить работу режима автоматического уменьшения ширины канала при загруженном радиоэфире	**wlc(config-wlc-radio-5g-profile)# obss-coexistence {on | off}**	on – режим автоматического уменьшения ширины канала активирован; off – режим автоматического уменьшения ширины канала выключен.
36	Установить режим работы радиоинтерфейса.	**wlc(config-wlc-radio-5g-profile)# work-mode <WORK-MODE>**	<WORK-MODE> – режим работы, доступные значения: • anacax – для частотного диапазона 5 ГГц.
37	Задать список каналов для динамического выбора канала.	**wlc(config-wlc-radio-5g-profile)# limit-channels <CHANNEL>[,<CHANNEL>]**	<CHANNEL> – номер используемого канала, доступные значения: Для 5g каждый 4 канал из диапазонов: [36.. 64] [132.. 165]
38	Настроить ширину канала.	**wlc(config-wlc-radio-5g-profile)# bandwidth <BANDWIDTH>**	<BANDWIDTH> – ширина канала, доступные значения: • 20; • 40L; • 40U; • 80.

<table>
<tr><th>Шаг</th><th>Описание</th><th>Команда</th><th>Ключи</th></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>minimal</th><th>low</th><th>middle</th><th>high</th><th>maximal</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>WEP-3L</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>WEP-30L-Z</td><td>0</td><td>5</td><td>10</td><td>15</td><td>19</td></tr>
<tr><td>WEP-3ax</td><td>10</td><td>12</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>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>WOP-30LI</td><td>0</td><td>5</td><td>10</td><td>15</td><td>19</td></tr>
<tr><td>WEP-2ac</td><td>1</td><td>6</td><td>10</td><td>15</td><td>19</td></tr>
<tr><td>WEP-2ac Smart</td><td>11</td><td>13</td><td>15</td><td>17</td><td>19</td></tr>
<tr><td>WOP-2ac</td><td>1</td><td>6</td><td>10</td><td>15</td><td>19</td></tr>
<tr><td>WOP-2ac:rev.B</td><td>1</td><td>6</td><td>10</td><td>15</td><td>19</td></tr>
<tr><td>WOP-2ac:rev.C</td><td>1</td><td>6</td><td>10</td><td>15</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>
</table>

Шаг	Описание	Команда	Ключи
41	Создать профиль конфигурирования RADIUS-сервера.	**wlc(config-wlc)# radius-profile <RADIUS-ID>** **wlc(config-wlc-radius-profile)#**	<RADIUS-ID> – идентификатор RADIUS-сервера, задается строкой до 235 символов.
42	Указать IP-адрес RADIUS-сервера, который отвечает за аутентификацию.	**wlc(config-wlc-radius-profile)# auth-address <ADDR>**	<ADDR> – IP-адрес RADIUS-сервера, задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения [0..255].
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].

Шаг	Описание	Команда	Ключи
49	Установить режим безопасности подключения к SSID.	**wlc(config-wlc-ssid-profile)# security-mode <MODE>**	<MODE> – режим безопасности, доступные значения: • OWE • 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, WEP-30L-Z, WOP-30L, WOP-30LS, WEP-3L, WOP-30LI. 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).
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 локации.	**wlc(config-wlc-ap-location)# description <DESCRIPTION>**	<DESCRIPTION> – произвольное описание, задается строкой до 255 символов.
55	Указать существующие профили настроек радиоинтерфейсов точек доступа.	**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.

Шаг	Описание	Команда	Ключи
56	Указать существующий профиль общих настроек.	**wlc(config-wlc-ap-location)# ap-profile <NAME>**	<NAME> – название профиля, задается строкой до 235 символов.
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	Включить режим туннелирования для точек доступа локации	**wlc(config-wlc-ap-location)# mode tunnel**	
59	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.
60	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]. Под сеть 0.0.0.0/0 попадают все адреса.
61	Указать название локации, в которую попадут точки доступа с адресами из заданной подсети.	**wlc(config-wlc-ip-pool)# ap-location <NAME>**	<NAME> – название локации, задается строкой до 235 символов.
62	Перейти в настройки сервис-активатора.	**wlc(config-wlc)# service-activator** **wlc(config-wlc-service-activator)#**	
63	Настроить автоматическую регистрацию точек доступа на контроллере.	**wlc(config-wlc-service-activator)# aps join auto**	
64	Указать IP-адрес контроллера в сети точек 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].
65	Активировать работу контроллера.	**wlc(config-wlc)# enable**	

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 802.11r/k/v.

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.

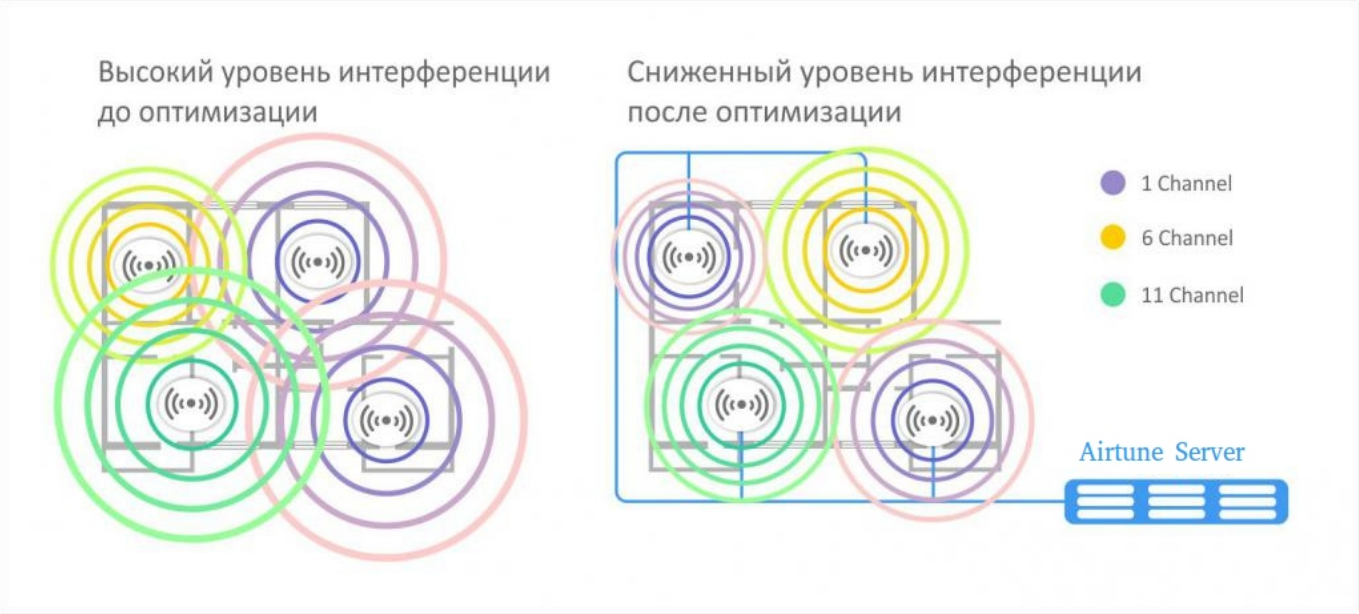
При работе функционала TPC/DCA точки доступа по команде от сервиса с помощью специальных пакетов (Action Frame) собирают информацию о радиосреде в текущий момент времени. Затем передают информацию на сервис, который выполняет анализ «качества радиоэфира» и проводит оптимизацию параметров для каждой точки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

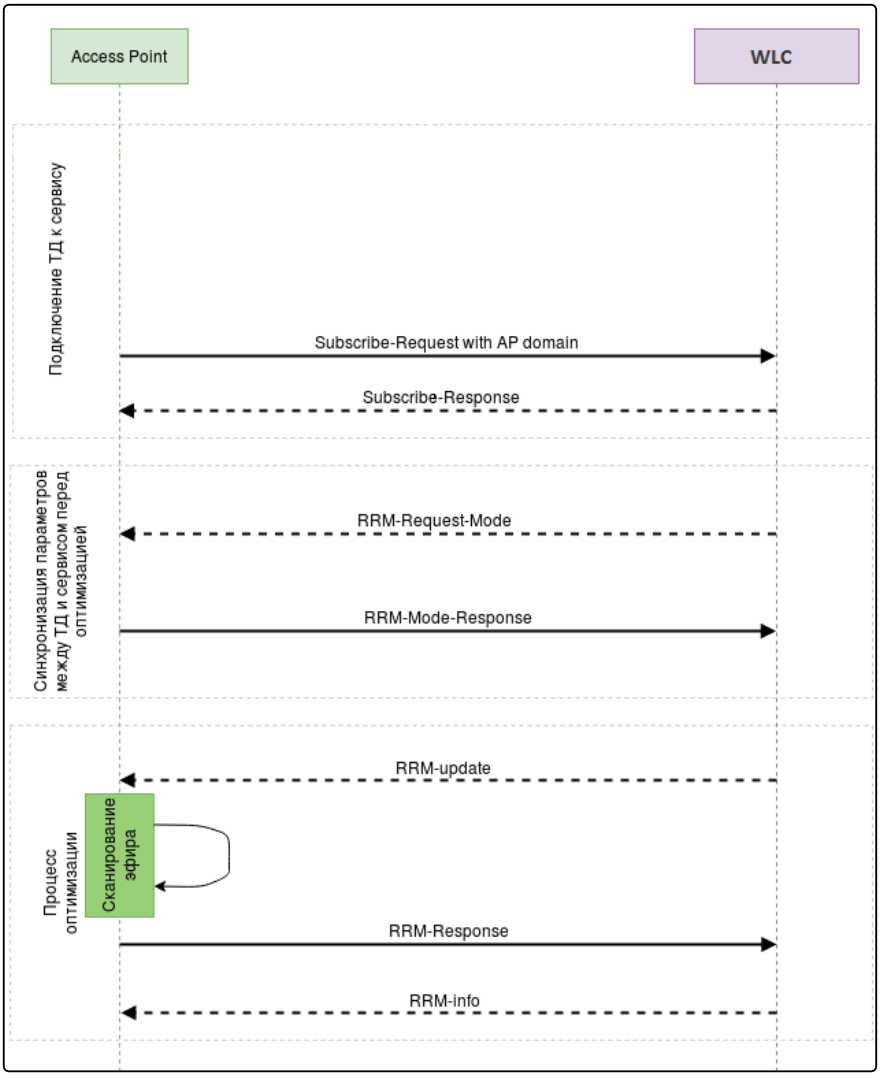
ТД при подключении к серверу (соединение между ТД и сервером осуществляется по протоколу WebSocket) отправляет сообщение "subscribe-request", где передает свои параметры, такие как:

- 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 локации 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. Сервер отправляет на ТД запрос «rrm-request-mode», чтобы актуализировать текущую информацию о них, т. к. оптимизация может начаться не только после подключения точки, а также планово либо по команде администратора спустя долгое время после первичного подключения.
4. ТД 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 локации, сервер в зависимости от настроек определяет для каждой точки оптимальную мощность, оптимальный канал, список соседей и отправляет сообщение «rrm-info».
8. ТД применяют рекомендованные настройки, и оптимизация считается завершенной.

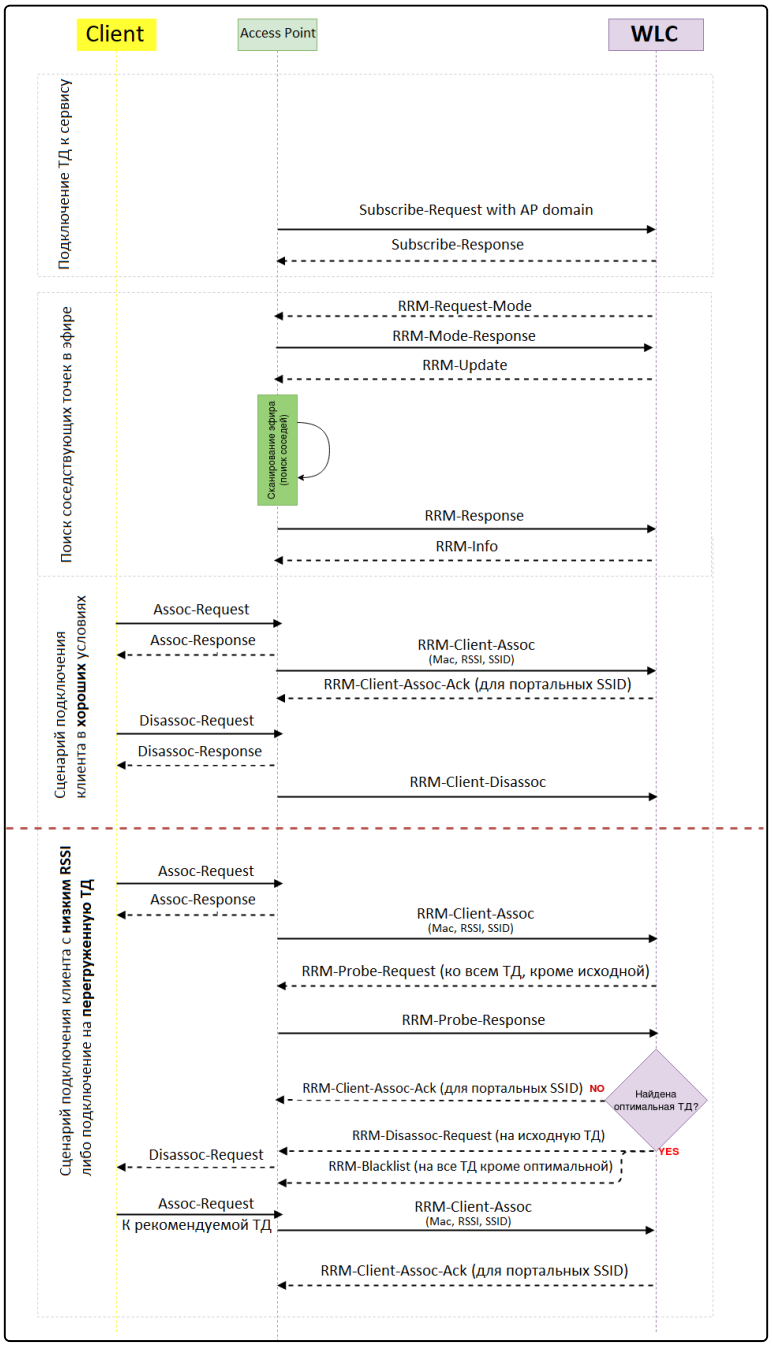
Оптимизация происходит в следующих случаях:

- новая точка добавилась в локацию;
- одна из ТД была отключена;
- на одной из точек были изменены радио параметры;
- по таймеру (optimization time);
- по команде администратора.

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 включена опция «optimization candidate neighbors», то первым этапом происходит поиск соседствующих точек в эфире.

   > В случае, если включена опция «optimization candidate all» в профиле AirTune, то пункт «Поиск соседствующих точек в эфире» будет пропущен, рассылка будет осуществляться всем ТД, находящимся в одной локации.

2. 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 этого 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 выполнены, 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

- Начало работы
  - Начало работы на устройствах WLC
  - Начало работы на устройствах ESR с лицензией WLC
- Основные элементы web-интерфейса
- Мониторинг
  - Меню «Беспроводная сеть»
    - Подменю «Локации»
      - Точки доступа
      - Клиенты
      - Отчёты RRM
      - Сессии Airtune
      - Данные RRM
      - Данные по роумингу
      - Виртуальные точки доступа
    - Подменю «Точки доступа»
      - Точки доступа
      - Новые точки доступа
    - Подменю «Проблемы конфигурации»
    - Подменю «Журнал событий»
      - Точки доступа
      - Клиенты
    - Подменю «Клиенты»
    - Подменю «Виртуальные точки доступа»
  - Меню «Система»
    - Подменю «Информация об устройстве»
    - Подменю «График загрузки CPU»
- Конфигурирование
  - Режим редактирования
  - Сохранение изменений
  - Общие принципы создания объектов
  - Меню «Беспроводная сеть»
    - Подменю «Локации»
      - Настройки локации
      - Настройки ТД
      - SSID профили
      - Настройки беспроводной части
    - Подменю «Общие настройки»
    - Подменю «Профили»
      - SSID
      - Настройки ТД
      - Радиопрофили
      - RADIUS
      - Airtune
      - Портал
      - Ограничение скорости ТД
    - Подменю «Индивидуальные настройки ТД»
      - Настройки радиоинтерфейса 2.4 ГГц
      - Настройки радиоинтерфейса 5 ГГц
    - Подменю «Планировщик обновления ПО ТД»
- Администрирование
  - Меню «ПО устройства»
  - Меню «Лицензии»
  - Меню «ПО точек доступа»

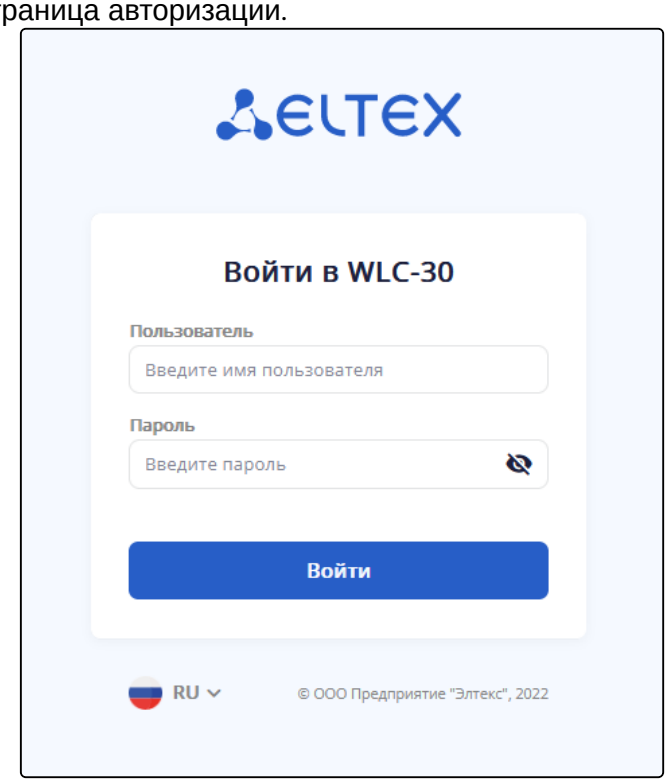
- Меню «Работа с файлами конфигурации»
  - Подменю «Актуальные файлы»
    - Загрузить файл конфигурации
    - Скачать файл конфигурации
    - Заводская конфигурация
  - Подменю «Сравнение конфигураций»

10.2.1 Начало работы

Начало работы на устройствах WLC

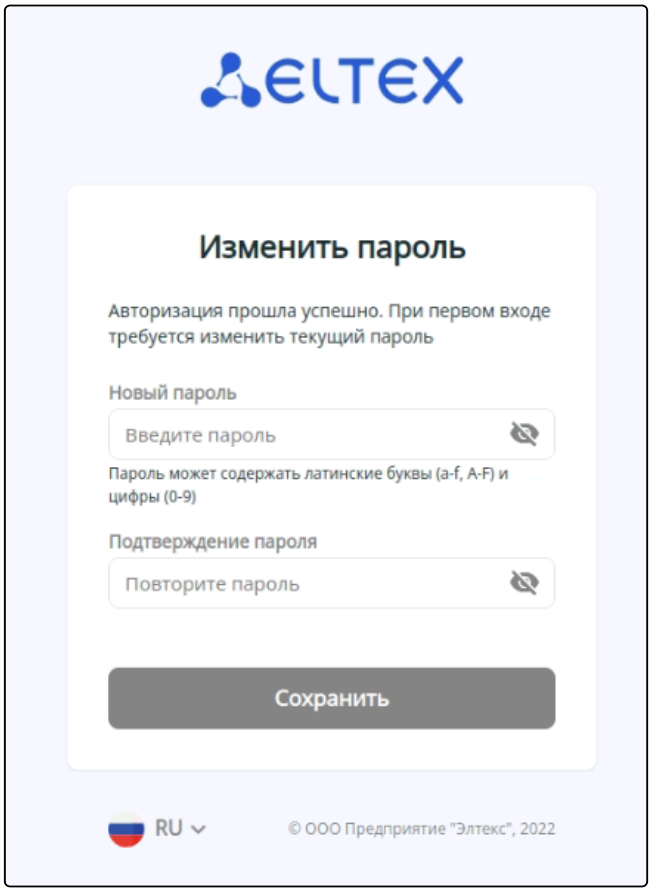
Web-интерфейс включен в заводской конфигурации на устройствах WLC и доступен по проколу HTTPS.

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.

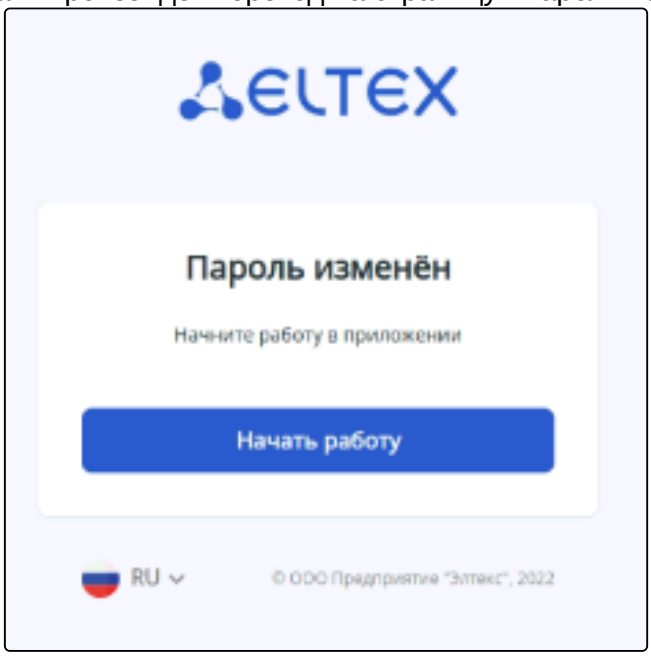


3. Введите имя пользователя и пароль в соответствующие поля.

> 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 группу web с портом 443.

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

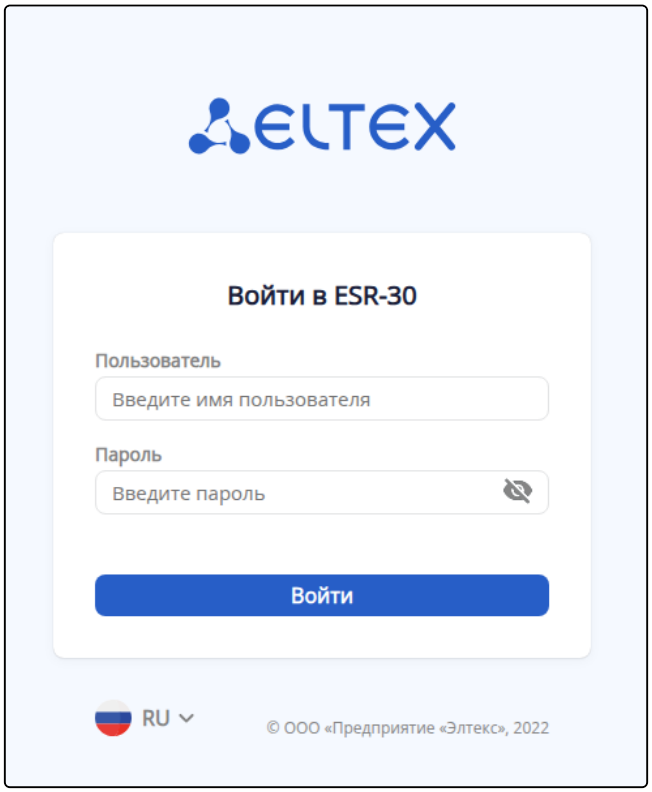
   Добавьте правило в зону trusted self.

```
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_esr> или https://<ip-address_esr>. При успешном обнаружении контроллера в окне браузера отобразится страница авторизации.



5. Введите имя пользователя и пароль в соответствующие поля.

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

6. 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 выхода – для завершения сеанса работы в web-интерфейсе под данным пользователем.
5. Поле основной информации – для просмотра данных подменю.
6. Кнопка выбора языка интерфейса (доступна русская и английская версии web-интерфейса) и 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
	Обновить ПО
	Деаутентификация клиента
	Скачать отчеты RRM
	Запуск оптимизации RRM

Элемент	Действие
	Очистить
	Фильтры
	Сравнить
	Копировать в Candidate
	Подсказка
	Внесены изменения в конфигурацию

10.2.3 Мониторинг

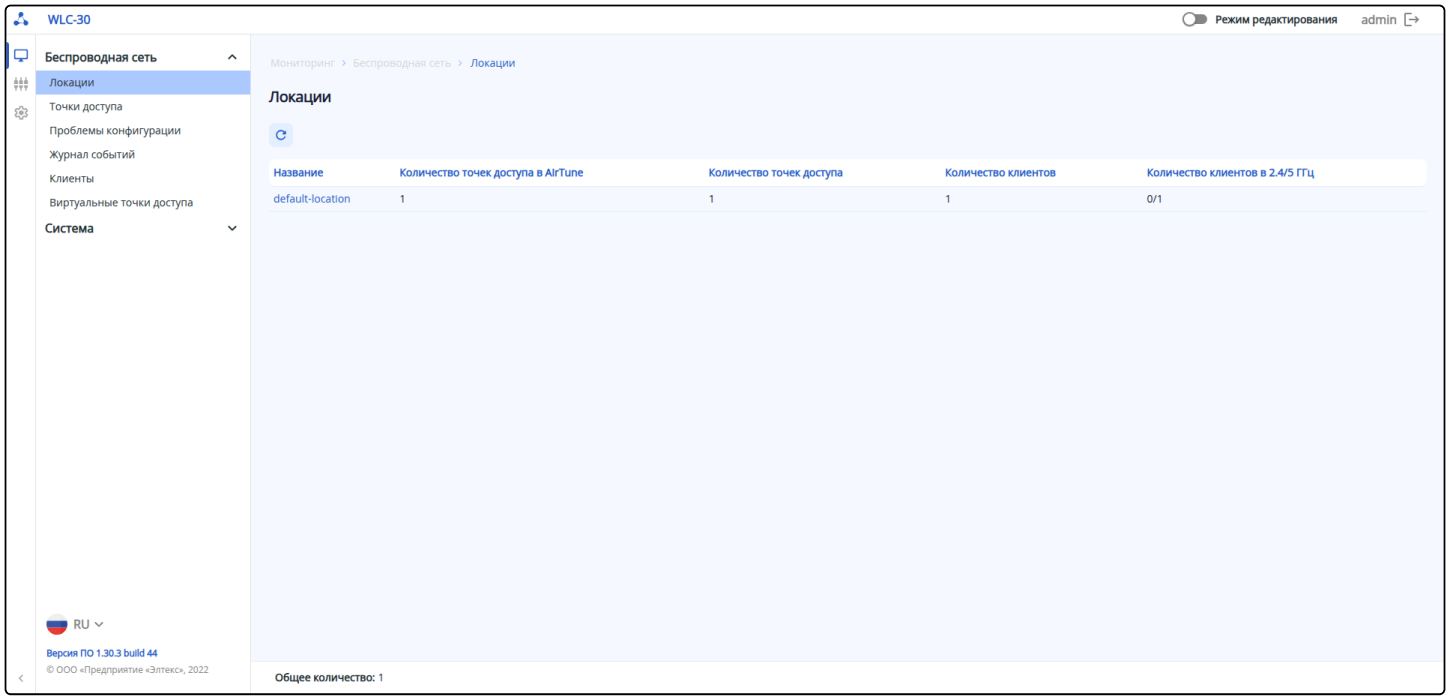
Меню «Беспроводная сеть»

Подменю «Локации»

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

Обновление страницы происходит при нажатии на кнопку «Обновить».

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



При переходе в локацию будут доступны списки точек доступа и клиентов, отчеты RRM, сессии точек доступа с сервисом Airtune, данные RRM, данные по роумингу и активные виртуальные точки доступа.

Точки доступа

На странице отображены точки доступа, которые зарегистрированы и находятся в выбранной локации. Параметр «Общее количество» показывает число зарегистрированных точек доступа в выбранной локации.

При большом количестве точек доступа в локации, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами.

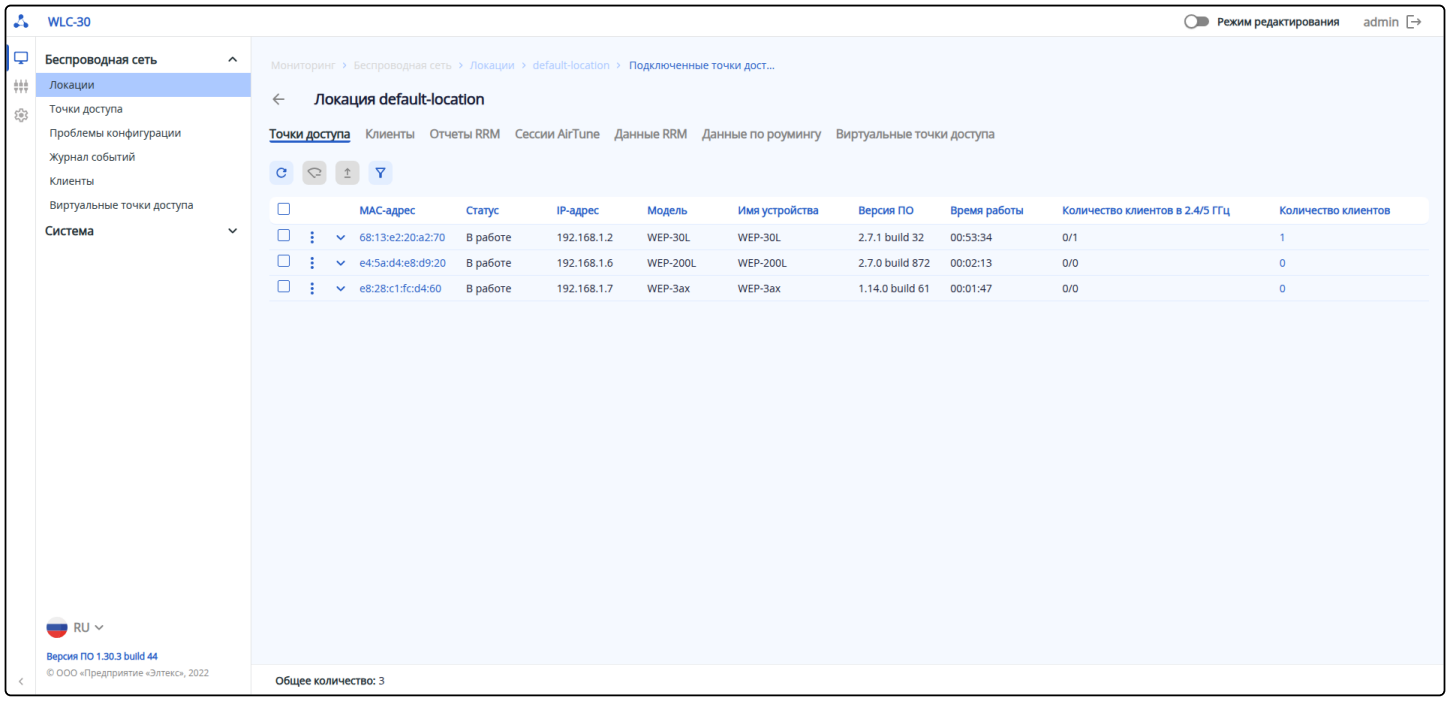
Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одну, несколько или все точки доступа на странице, чтобы применить к ним общие действия с помощью кнопок «Разрегистрировать» или «Обновить ПО».

При нажатии на кнопку «Разрегистрировать» и подтверждении действия, все выбранные точки доступа будут выведены из обслуживания. Если на момент разрегистрации точка доступа находится в работе (включена), она получит по DHCP 15 подопцию 43 опции и продолжит совершать новые попытки подключения к контроллеру.

При этом, если включена авторегистрация, то точка снова появится в локации в течение 5 минут. Если авторегистрация выключена, разрегистрированные точки доступа появятся в разделе «Точки доступа» → «Новые точки доступа».

При нажатии кнопки «Обновить ПО» запустится обновление всех выбранных с помощью чекбоксов точек доступа при условии наличия на контроллере ПО для необходимой модели ТД. Статус процесса обновления можно увидеть при обновлении страницы. Загрузка ПО точек доступа на контроллер осуществляется в меню «Администрирование» → «ПО точек доступа».

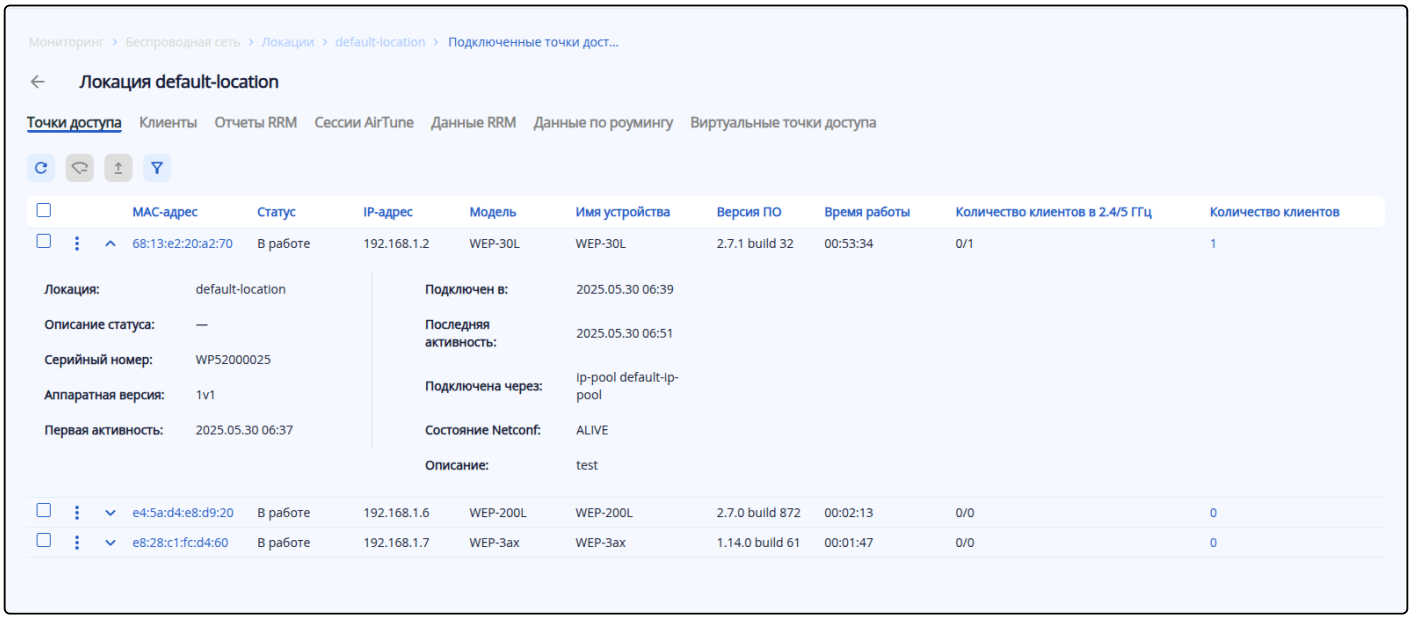


Для каждой ТД доступно контекстное меню со следующими действиями:

- *Разрегистрировать* − вывод из обслуживания точки доступа;
- *Обновить ПО* − запуск обновления программного обеспечения, если для данной модели ТД на контроллер загружен файл ПО;
- *Настроить* − создание индивидуального профиля настроек точки доступа, в котором присутствует возможность задать имя ТД, переопределить локацию или профиль общих настроек ТД, переопределить параметры радиопрофилей, такие как режим работы радиоинтерфейса, канал, ширина канала, мощность, а также отключить использование AirTune. Действие доступно при включенном режиме редактирования.

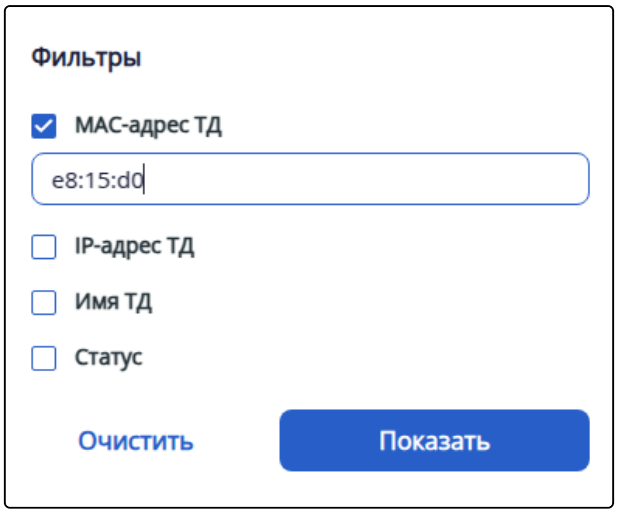
Таблица содержит данные:

- *MAC-адрес* − MAC-адрес точки доступа. При нажатии осуществляется переход на страницу «Точка доступа», которая содержит более подробную информацию о всех клиентах точки доступа и ее интерфейсах;
- *Статус* − состояние работы точки доступа;
- *IP-адрес* − IP-адрес точки доступа;
- *Модель* − модель точки доступа;
- *Имя устройства* − имя точки доступа;
- *Версия ПО* − версия программного обеспечения точки доступа;
- *Время работы* − время работы с момента последнего включения или перезагрузки устройства;
- *Количество клиентов в 2.4/5 ГГц* − число клиентов, подключенных к точке доступа в частотных диапазонах 2.4/5 ГГц соответственно;
- *Количество клиентов* − общее число клиентов, подключенных к точке доступа. При нажатии осуществляется переход на страницу "Клиенты", содержащую более подробную информацию по клиентам данной точки доступа.



При нажатии на кнопку будет раскрыта дополнительная информация:

- *Локация* − название 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;
- *Аппаратная 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 профиля подключения.



Для удобства предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *IP-адрес ТД* − IP-адрес точки доступа. Для поиска необходимо ввести IP-адрес полностью;
- *Имя ТД* − имя точки доступа, задается строкой. Поиск работает по частичному совпадению;
- *Статус ТД* − состояние работы точки доступа, осуществляется выбор из списка значений.

При использовании фильтров параметр «Общее количество» отображает общее количество отфильтрованных записей.

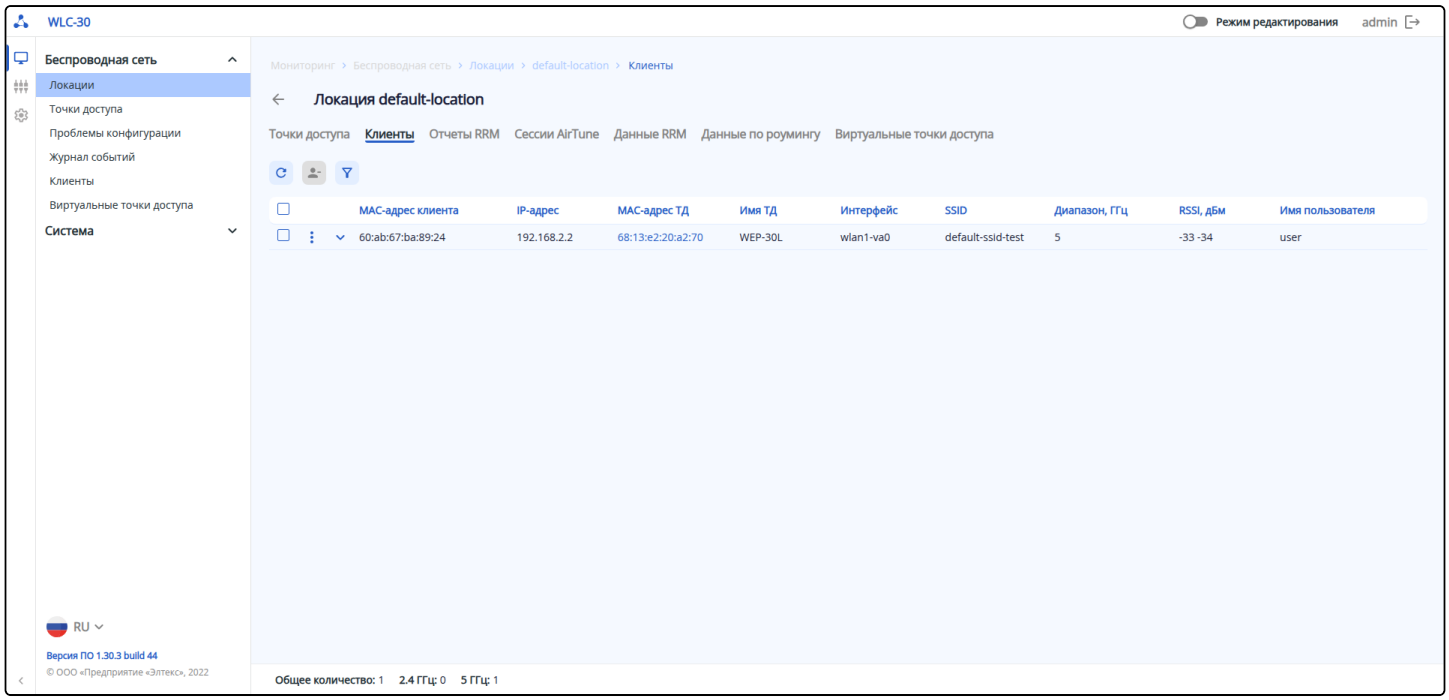
Клиенты

Страница содержит информацию о клиентах, подключенных к точкам доступа данной локации. В параметре «Общее количество» отображается общее число клиентов в локации и их распределение по частотным диапазонам.

При подключении большого количества клиентов, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами. Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одного, несколько или всех клиентов на странице, чтобы применить к ним общее действие с помощью кнопки «Деаутентификация клиента». При нажатии на кнопку выбранные клиенты будут деаутентифицированы.

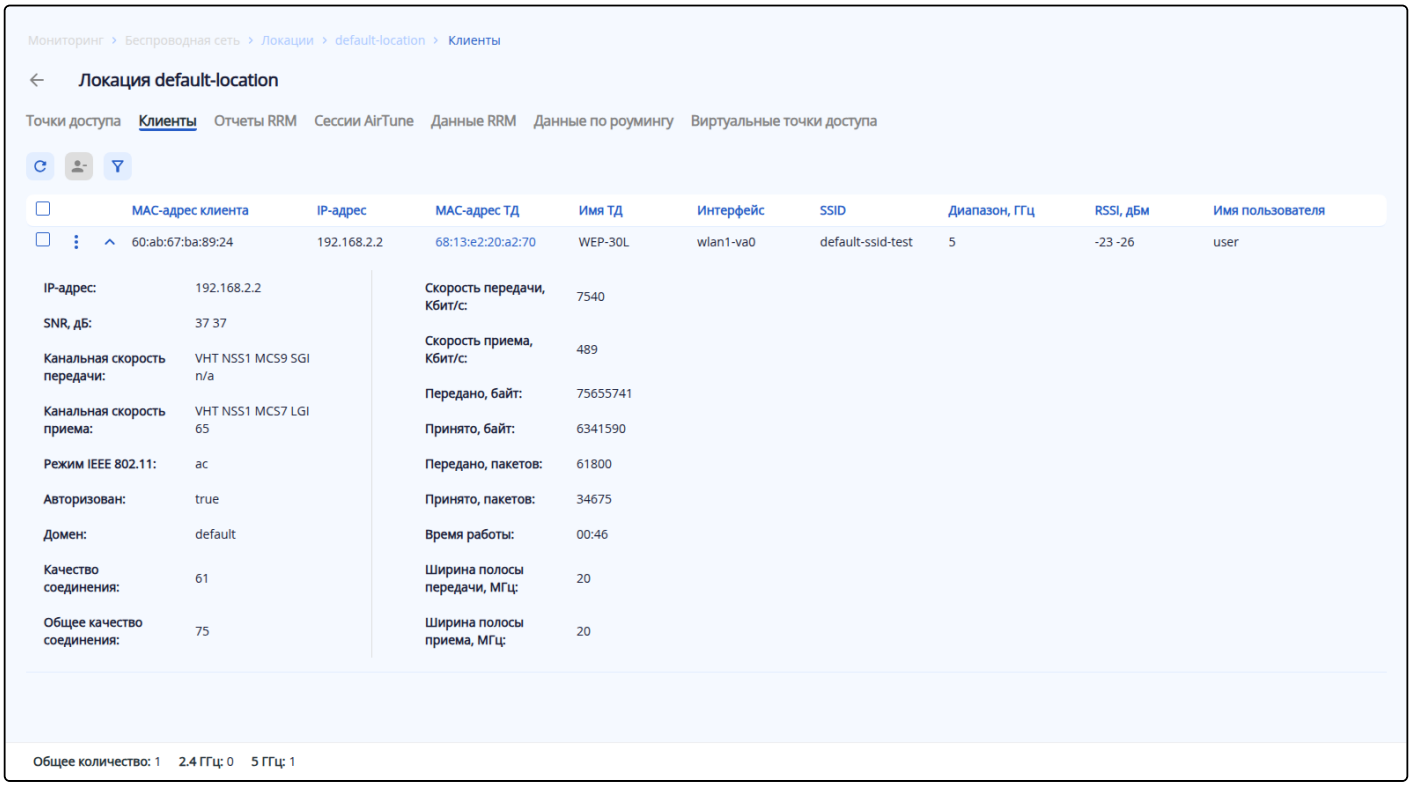
Для каждого клиента также доступно контекстное меню с действием «Деаутентификация клиента».



Основная информация включает в себя следующие параметры:

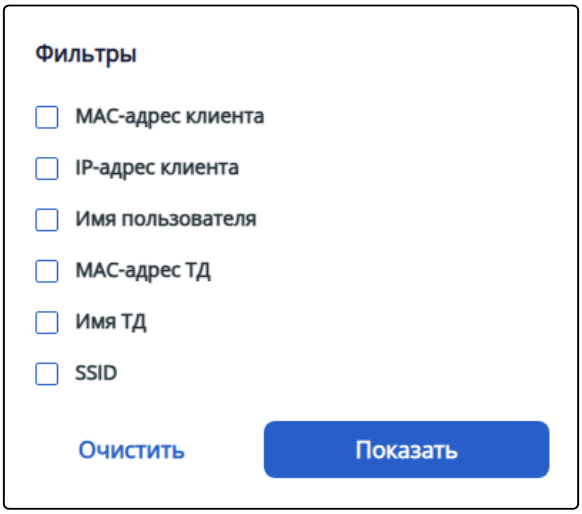
- *MAC-адрес клиента* – MAC-адрес подключенного устройства;
- *IP-адрес* – IP-адрес подключенного устройства;
- *MAC-адрес ТД* – MAC-адрес точки доступа, к которой подключено устройство;
- *Имя ТД* – имя точки доступа;
- *Интерфейс* – интерфейс взаимодействия точки доступа с подключенным устройством;
- *SSID* – название сети, к которой подключено устройство;
- *Диапазон, ГГц* – диапазон частот, в котором подключено устройство к точке доступа;
- *RSSI, дБм* – уровень принимаемого сигнала;
- *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;
- *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.



Для удобства предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *MAC-адрес клиента* − MAC-адрес клиента. Для поиска достаточно ввести один или несколько целых октетов;
- *IP-адрес клиента* − IP-адрес клиента. Для поиска необходимо ввести IP-адрес полностью;
- *Имя пользователя* − имя пользователя, указанное при регистрации в сети Wi-Fi, задается строкой. Поиск работает по частичному совпадению;
- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *Имя ТД* − имя точки доступа, задается строкой. Поиск работает по частичному совпадению;
- *SSID* − название SSID, к которому подключен клиент. Осуществляется выбор из списка значений с возможностью поиска по списку.

При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.

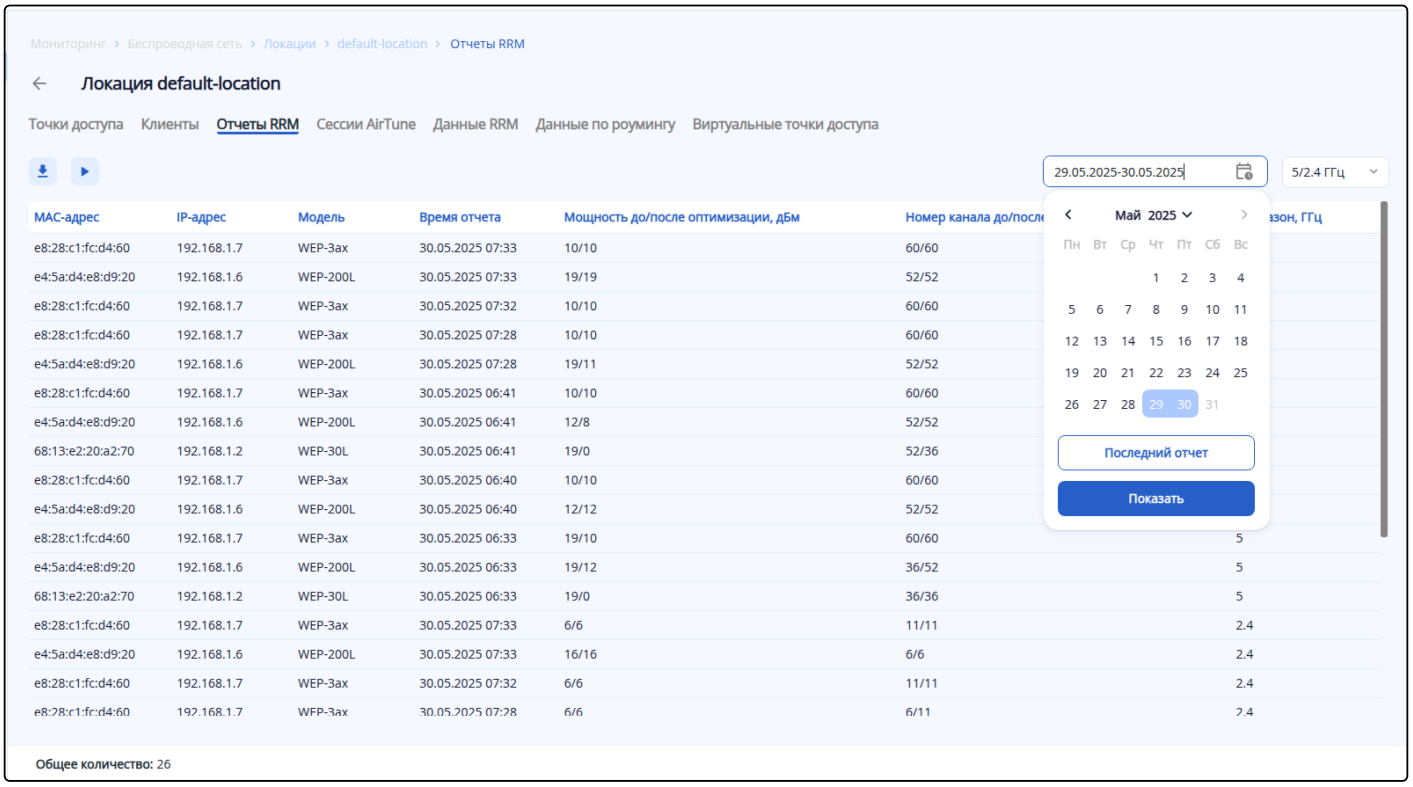
Отчёты RRM

На странице отображаются отчеты оптимизации. По умолчанию выводится последний отчет. В параметре «Общее количество» отображается количество радиоинтерфейсов, для которых была произведена оптимизация.

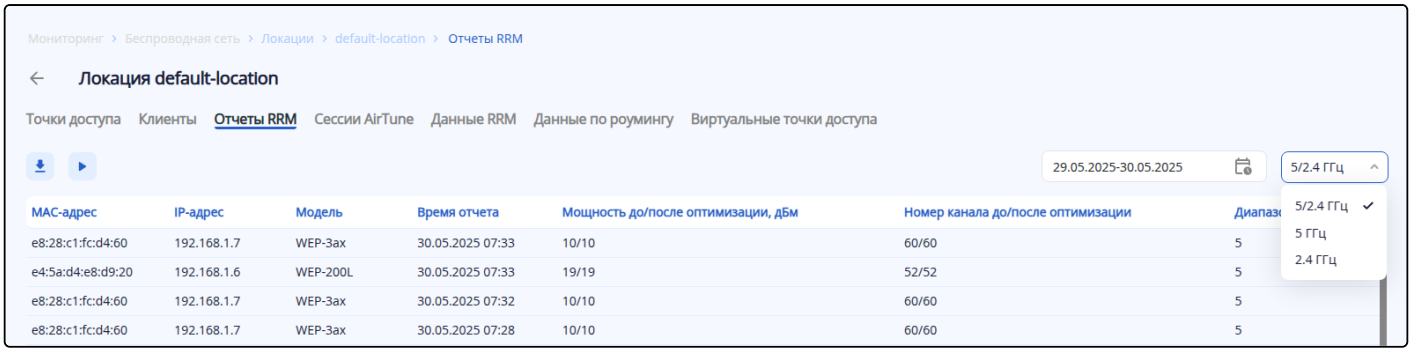
На странице можно запустить оптимизацию, нажав на кнопку «Запустить оптимизацию» . Данный процесс займет несколько минут.

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

Необходимую дату отчета можно выбрать с помощью календаря.



Отчеты RRM можно отфильтровать по частотному диапазону.



В таблице представлены данные:

- *MAC-адрес* − MAC-адрес точки доступа, которая управляется Airtune;
- *IP-адрес* − IP-адрес точки доступа, которая управляется Airtune;
- *Модель* − модель 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

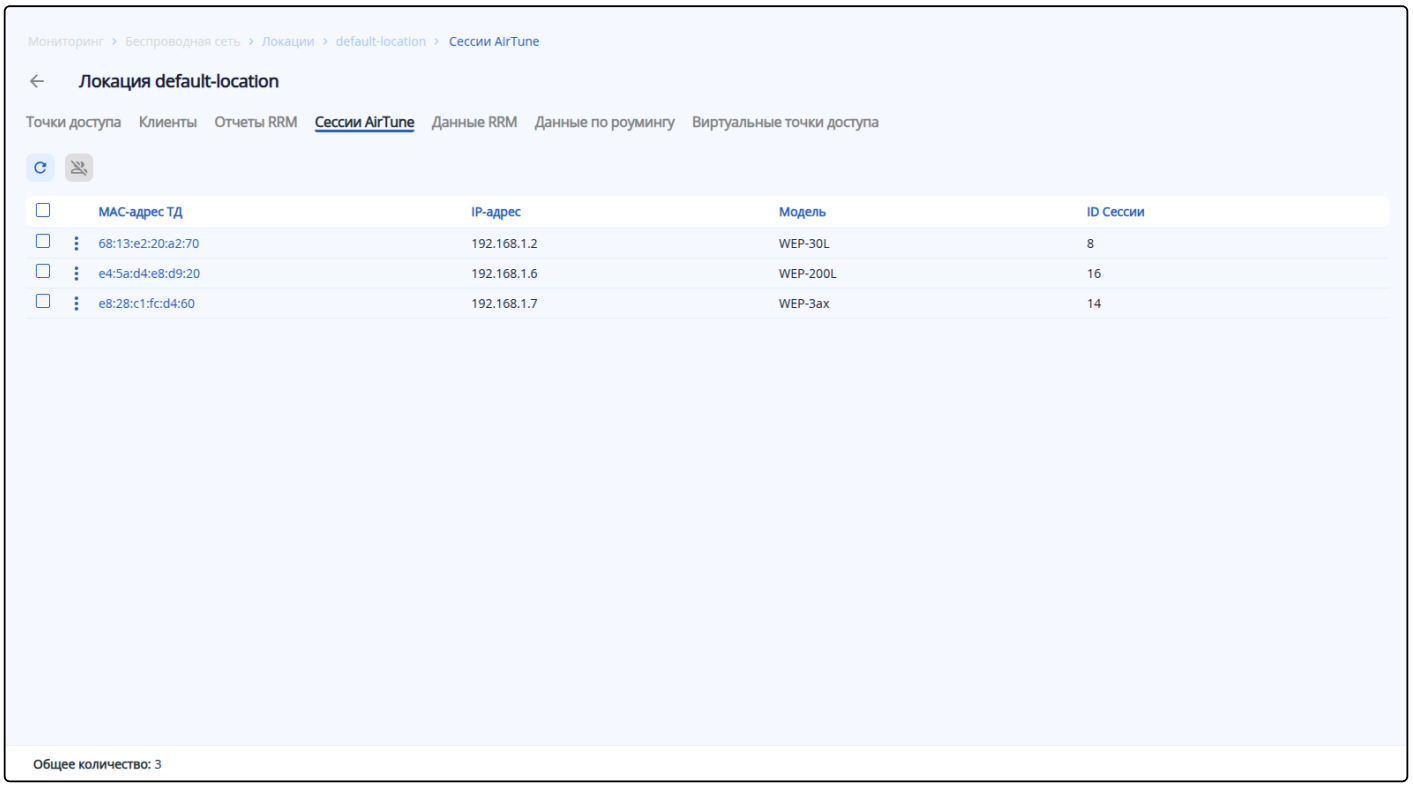
На странице представлены данные о точках доступа, которые на данный момент находятся под управлением сервиса Airtune. В параметре «Общее количество» отображается число сессий.

Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одну, несколько или все точки доступа, чтобы применить к ним общее действие с помощью кнопки «Разорвать сессии». От сервиса будут отключены выбранные

точки доступа, но они будут сразу переподключены, если для них не будет выключена работа сервиса в конфигурации.

Для каждой ТД также доступно контекстное меню с действием «Разорвать сессию».



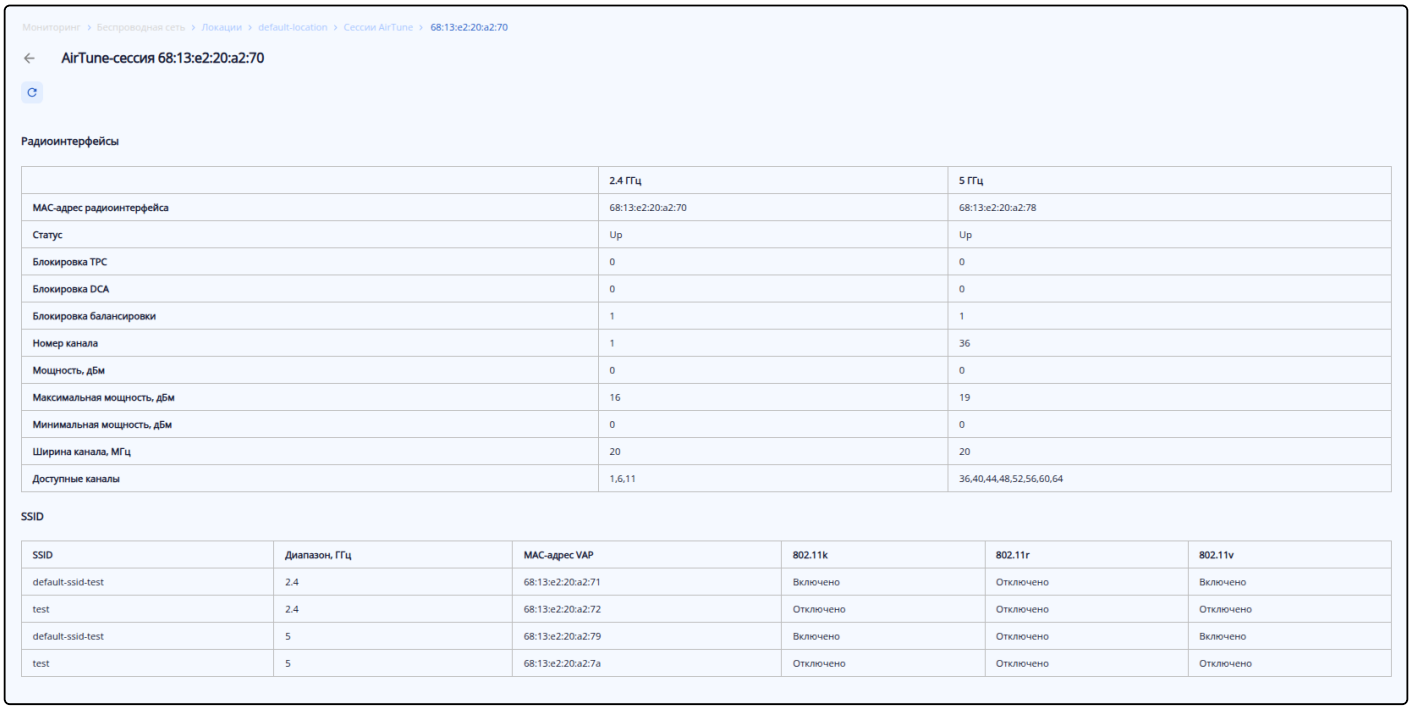
В таблице представлены данные:

- *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;
- *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

Для того чтобы попасть в «*Airtune-сессию*» нажмите на MAC-адрес устройства, для которого требуется информация.

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



Мониторинг › Беспроводная сеть › Локации › default-location › Сессии AirTune › 68:13:e2:20:a2:70

AirTune-сессия 68:13:e2:20:a2:70

Радиоинтерфейсы

	2.4 ГГц	5 ГГц
MAC-адрес радиоинтерфейса	68:13:e2:20:a2:70	68:13:e2:20:a2:78
Статус	Up	Up
Блокировка TPC	0	0
Блокировка DCA	0	0
Блокировка балансировки	1	1
Номер канала	1	36
Мощность, дБм	0	0
Максимальная мощность, дБм	16	19
Минимальная мощность, дБм	0	0
Ширина канала, МГц	20	20
Доступные каналы	1,6,11	36,40,44,48,52,56,60,64

SSID

SSID	Диапазон, ГГц	MAC-адрес VAP	802.11k	802.11r	802.11v
default-ssid-test	2.4	68:13:e2:20:a2:71	Включено	Отключено	Включено
test	2.4	68:13:e2:20:a2:72	Отключено	Отключено	Отключено
default-ssid-test	5	68:13:e2:20:a2:79	Включено	Отключено	Включено
test	5	68:13:e2:20:a2:7a	Отключено	Отключено	Отключено

Таблица «Радиоинтерфейсы» 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;
- *Блокировка балансировки* – статус блокировки балансировки клиентов на интерфейсе: *0* – блокировка отключена, *1* – блокировка активирована, т.к. на точке доступа функционал отключен или не поддерживается;
- *Номер канала* – номер беспроводного канала, на котором работает радиоинтерфейс;
- *Мощность, дБм* – мощность сигнала радиоинтерфейса;
- *Максимальная мощность, дБм* – максимальная мощность сигнала, которая доступна для радиоинтерфейса;
- *Минимальная мощность, дБм* – минимальная мощность сигнала, которая доступна для радиоинтерфейса;
- *Ширина канала, МГц* – ширина полосы частот канала, на которой работает радиоинтерфейс;
- *Доступные каналы* – список каналов, из которых выбирается один, который после оптимизации назначается на радиоинтерфейс.

Таблица «SSID» содержит:

- *SSID* – название 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;

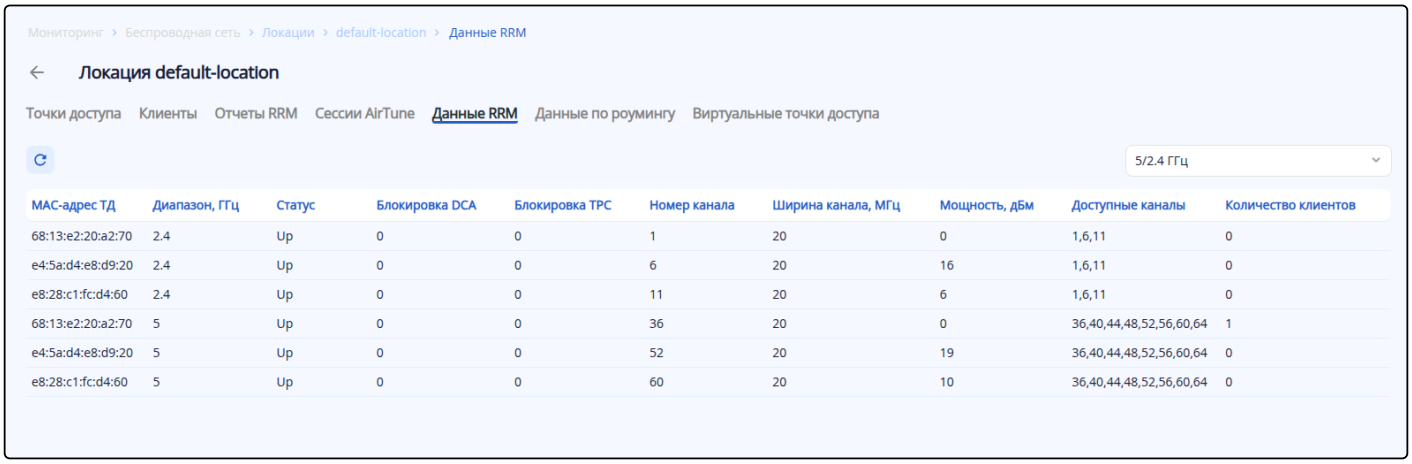
- *802.11v* – статус активности функционала роуминга стандарта 802.11v, который позволяет осуществлять балансировку клиентов между точками доступа, рекомендуя клиентам переключаться на менее нагруженные ТД.

Данные RRM

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

Обновление страницы происходит при нажатии на кнопку «Обновить».

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



MAC-адрес ТД	Диапазон, ГГц	Статус	Блокировка DCA	Блокировка TPC	Номер канала	Ширина канала, МГц	Мощность, дБм	Доступные каналы	Количество клиентов
68:13:e2:20:a2:70	2.4	Up	0	0	1	20	0	1,6,11	0
e4:5a:d4:e8:d9:20	2.4	Up	0	0	6	20	16	1,6,11	0
e8:28:c1:fc:d4:60	2.4	Up	0	0	11	20	6	1,6,11	0
68:13:e2:20:a2:70	5	Up	0	0	36	20	0	36,40,44,48,52,56,60,64	1
e4:5a:d4:e8:d9:20	5	Up	0	0	52	20	19	36,40,44,48,52,56,60,64	0
e8:28:c1:fc:d4:60	5	Up	0	0	60	20	10	36,40,44,48,52,56,60,64	0

В таблице отображены:

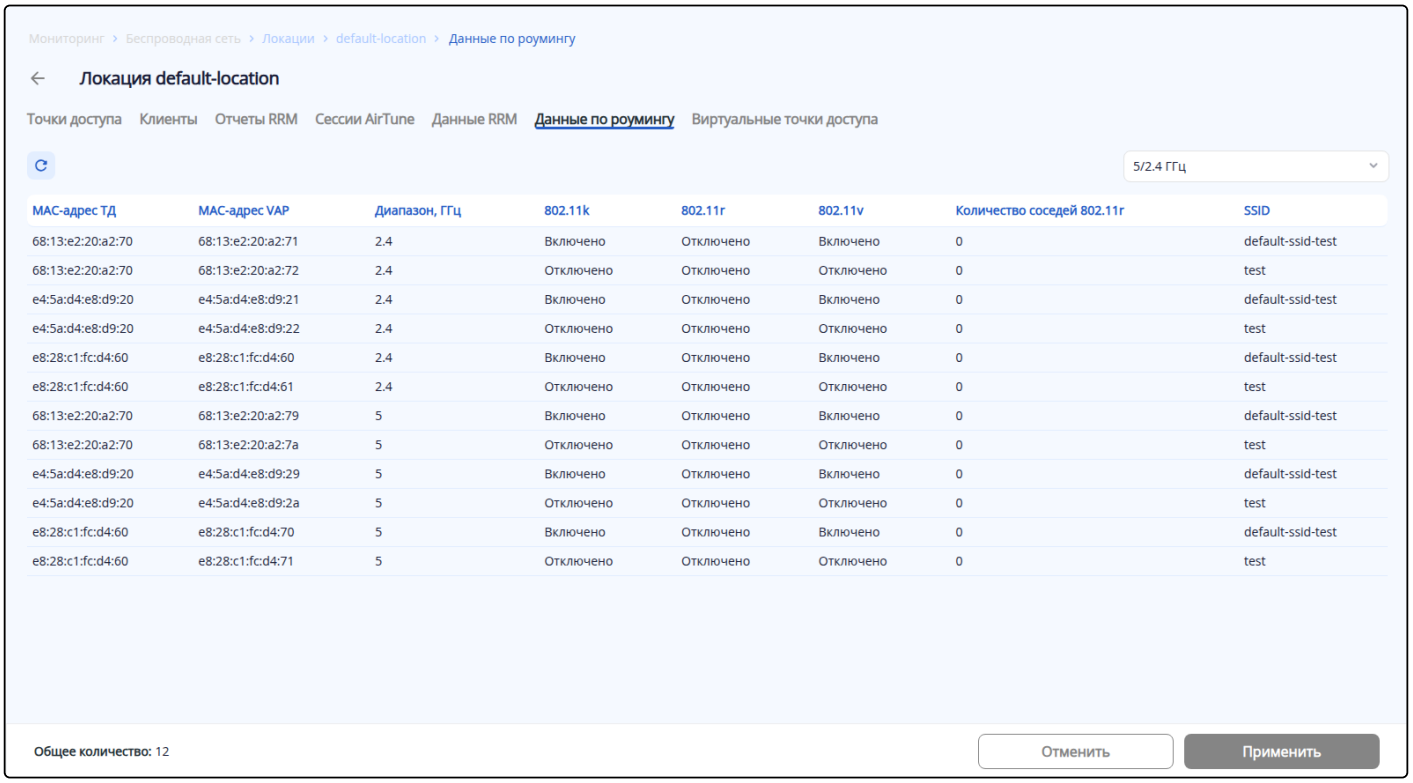
- *MAC-адрес ТД* – MAC-адрес точки доступа, которая управляется Airtune;
- *Диапазон, ГГц* – частотный диапазон радиоинтерфейса;
- *Статус* – состояние радиоинтерфейса: *Up* – радиоинтерфейс работает, *Down* – радиоинтерфейс отключен;
- *Блокировка DCA* – статус блокировки динамического распределения 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 котором 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 (VAP), которые обрабатываются сервисом Airtune. Страница предназначена для отображения текущего состояния конфигурации роуминга 802.11 k/r/v на всех точках доступа локации, а также количества соседей, между которыми сервис настроил роуминг.

Обновление страницы происходит при нажатии на кнопку «Обновить».

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



MAC-адрес ТД	MAC-адрес VAP	Диапазон, ГГц	802.11k	802.11r	802.11v	Количество соседей 802.11r	SSID
68:13:e2:20:a2:70	68:13:e2:20:a2:71	2.4	Включено	Отключено	Включено	0	default-ssid-test
68:13:e2:20:a2:70	68:13:e2:20:a2:72	2.4	Отключено	Отключено	Отключено	0	test
e4:5a:d4:e8:d9:20	e4:5a:d4:e8:d9:21	2.4	Включено	Отключено	Включено	0	default-ssid-test
e4:5a:d4:e8:d9:20	e4:5a:d4:e8:d9:22	2.4	Отключено	Отключено	Отключено	0	test
e8:28:c1:fc:d4:60	e8:28:c1:fc:d4:60	2.4	Включено	Отключено	Включено	0	default-ssid-test
e8:28:c1:fc:d4:60	e8:28:c1:fc:d4:61	2.4	Отключено	Отключено	Отключено	0	test
68:13:e2:20:a2:70	68:13:e2:20:a2:79	5	Включено	Отключено	Включено	0	default-ssid-test
68:13:e2:20:a2:70	68:13:e2:20:a2:7a	5	Отключено	Отключено	Отключено	0	test
e4:5a:d4:e8:d9:20	e4:5a:d4:e8:d9:29	5	Включено	Отключено	Включено	0	default-ssid-test
e4:5a:d4:e8:d9:20	e4:5a:d4:e8:d9:2a	5	Отключено	Отключено	Отключено	0	test
e8:28:c1:fc:d4:60	e8:28:c1:fc:d4:70	5	Включено	Отключено	Включено	0	default-ssid-test
e8:28:c1:fc:d4:60	e8:28:c1:fc:d4:71	5	Отключено	Отключено	Отключено	0	test

В таблице отображены следующие параметры:

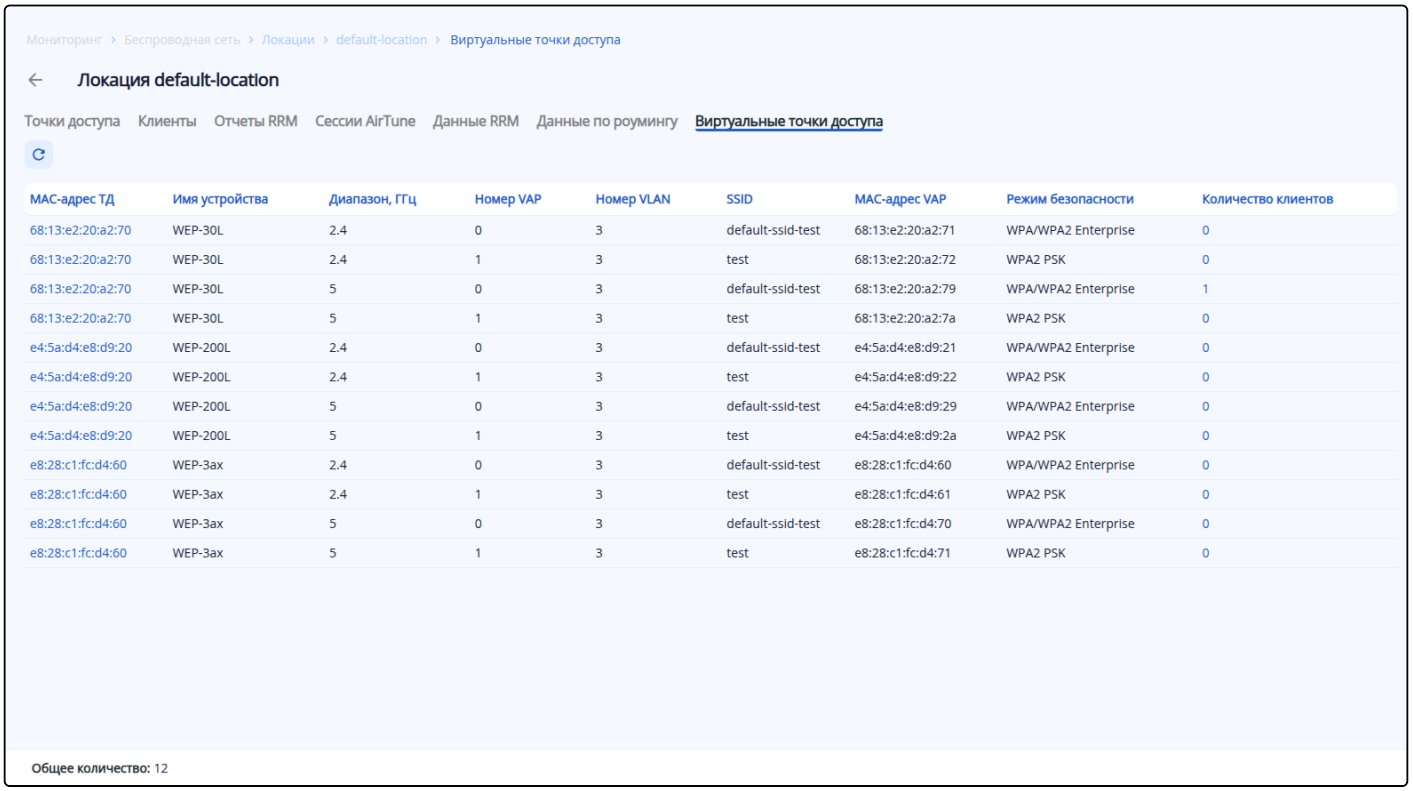
- *MAC-адрес ТД* – MAC-адрес точки доступа;
- *MAC-адрес VAP* – MAC-адрес виртуальной точки доступа;
- *Диапазон, ГГц* – частотный диапазон радиоинтерфейса;
- *802.11k* – статус активности синхронизации списков соседних точек доступа стандарта 802.11k, который позволяет клиенту, при ослабевании сигнала 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;
- *802.11v* – статус активности функционала роуминга стандарта 802.11v, который позволяет осуществлять балансировку клиентов между точками доступа, рекомендуя клиентам переключаться на менее нагруженные ТД;
- *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* – название сети, которое вещается пользователям.

Виртуальные точки доступа

На странице представлена информация о всех включенных виртуальных точках доступа (VAP) на точках доступа выбранной локации.

Обновление страницы происходит при нажатии на кнопку «Обновить».

Параметр «Общее количество» показывает число включенных виртуальных точек доступа, которые предоставляют услугу в выбранной локации.



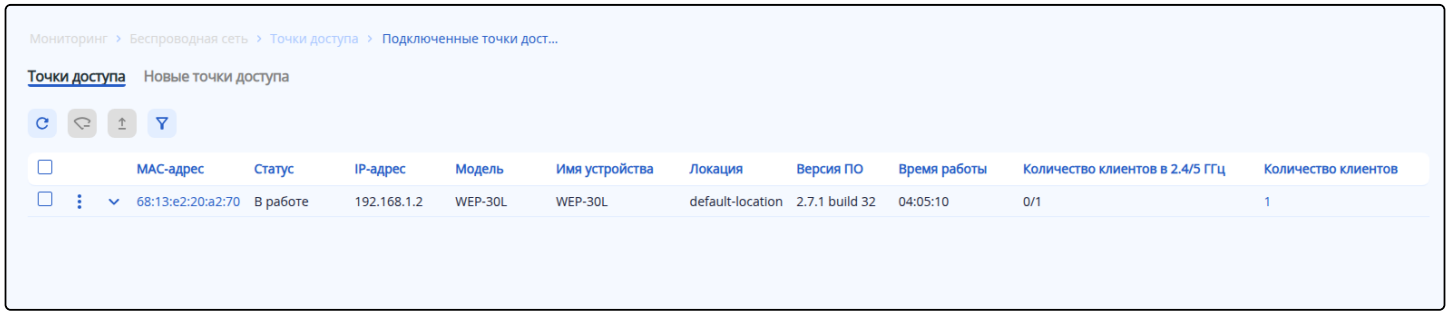
MAC-адрес ТД	Имя устройства	Диапазон, ГГц	Номер VAP	Номер VLAN	SSID	MAC-адрес VAP	Режим безопасности	Количество клиентов
68:13:e2:20:a2:70	WEP-30L	2.4	0	3	default-ssid-test	68:13:e2:20:a2:71	WPA/WPA2 Enterprise	0
68:13:e2:20:a2:70	WEP-30L	2.4	1	3	test	68:13:e2:20:a2:72	WPA2 PSK	0
68:13:e2:20:a2:70	WEP-30L	5	0	3	default-ssid-test	68:13:e2:20:a2:79	WPA/WPA2 Enterprise	1
68:13:e2:20:a2:70	WEP-30L	5	1	3	test	68:13:e2:20:a2:7a	WPA2 PSK	0
e4:5a:d4:e8:d9:20	WEP-200L	2.4	0	3	default-ssid-test	e4:5a:d4:e8:d9:21	WPA/WPA2 Enterprise	0
e4:5a:d4:e8:d9:20	WEP-200L	2.4	1	3	test	e4:5a:d4:e8:d9:22	WPA2 PSK	0
e4:5a:d4:e8:d9:20	WEP-200L	5	0	3	default-ssid-test	e4:5a:d4:e8:d9:29	WPA/WPA2 Enterprise	0
e4:5a:d4:e8:d9:20	WEP-200L	5	1	3	test	e4:5a:d4:e8:d9:2a	WPA2 PSK	0
e8:28:c1:fc:d4:60	WEP-3ax	2.4	0	3	default-ssid-test	e8:28:c1:fc:d4:60	WPA/WPA2 Enterprise	0
e8:28:c1:fc:d4:60	WEP-3ax	2.4	1	3	test	e8:28:c1:fc:d4:61	WPA2 PSK	0
e8:28:c1:fc:d4:60	WEP-3ax	5	0	3	default-ssid-test	e8:28:c1:fc:d4:70	WPA/WPA2 Enterprise	0
e8:28:c1:fc:d4:60	WEP-3ax	5	1	3	test	e8:28:c1:fc:d4:71	WPA2 PSK	0

Таблица содержит следующую информацию:

- *MAC-адрес ТД* – MAC-адрес точки доступа, на которой включена VAP. При нажатии осуществляется переход на страницу «Точка доступа», которая содержит более подробную информацию о всех клиентах точки доступа и ее интерфейсах;
- *Имя устройства* – имя точки доступа;
- *Диапазон, ГГц* – частотный диапазон радиоинтерфейса, на котором VAP предоставляет услугу;
- *Номер VAP* – порядковый номер виртуальной точки доступа. На каждой точке доступа нумерация VAP ведется с 0 для каждого радиоинтерфейса;
- *Номер VLAN* – идентификатор VLAN, в котором передается трафик Wi-Fi клиентов;
- *SSID* – название беспроводной сети;
- *MAC-адрес VAP* – MAC-адрес виртуальной точки доступа;
- *Режим безопасности* – тип шифрования данных, используемый на виртуальной точке доступа;
- *Количество клиентов* – число клиентов, подключенных к виртуальной точке доступа. При нажатии осуществляется переход на страницу «Клиенты», содержащую более подробную информацию по клиентам данной точки доступа.

Подменю «Точки доступа»

Данный раздел содержит список зарегистрированных точек доступа, а также список точек доступа, которые получили 15 подопцию 43 опции DHCP, пришли на контроллер и ожидают регистрации.



Точки доступа

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

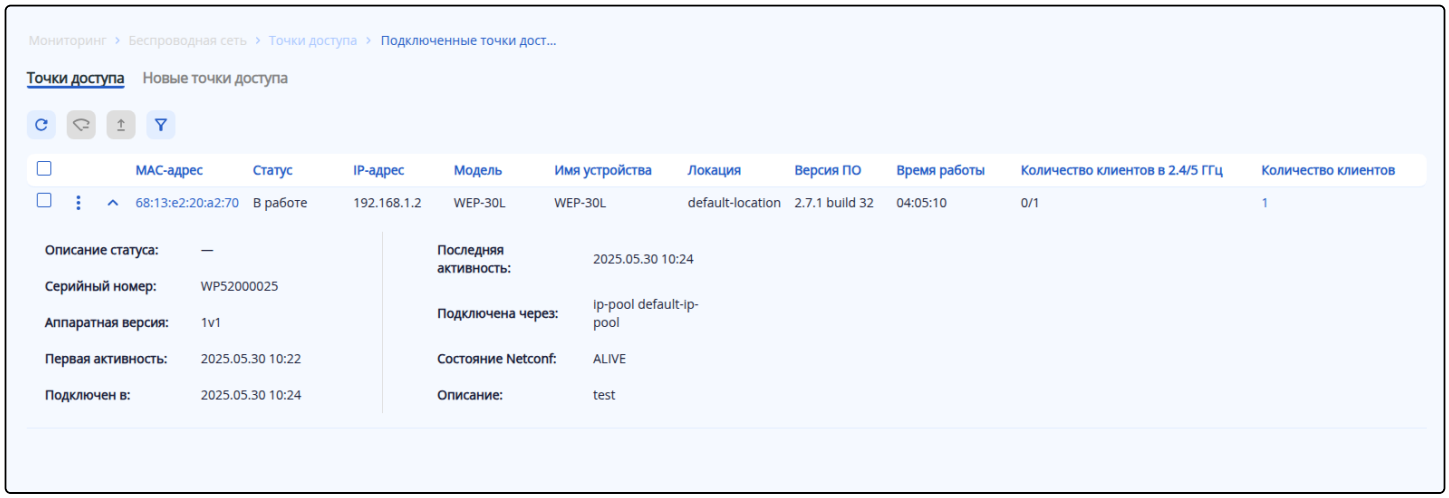
При появлении большого количества зарегистрированных точек доступа, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами. Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одну, несколько или все точки доступа на странице, чтобы применить к ним общие действия с помощью кнопок «Разрегистрировать» или «Обновить ПО».

При нажатии на кнопку «Разрегистрировать» и подтверждении действия, все выбранные точки доступа будут выведены из обслуживания. Если на момент разрегистрации точка доступа находится в работе (включена), она получит по DHCP 15 подопцию 43 опции и продолжит совершать новые попытки подключения к контроллеру.

При этом, если включена авторегистрация, то точка снова появится в локации в течение 5 минут. Если авторегистрация выключена, разрегистрированные точки доступа появятся в разделе «Точки доступа» → «Новые точки доступа».

При нажатии кнопки «Обновить ПО» запустится обновление всех выбранных с помощью чекбоксов точек доступа при условии наличия на контроллере ПО для необходимой модели ТД. Статус процесса обновления можно увидеть при обновлении страницы. Загрузка ПО точек доступа на контроллер осуществляется в меню «Администрирование» → «ПО точек доступа».



Для каждой ТД доступно контекстное меню со следующими действиями:

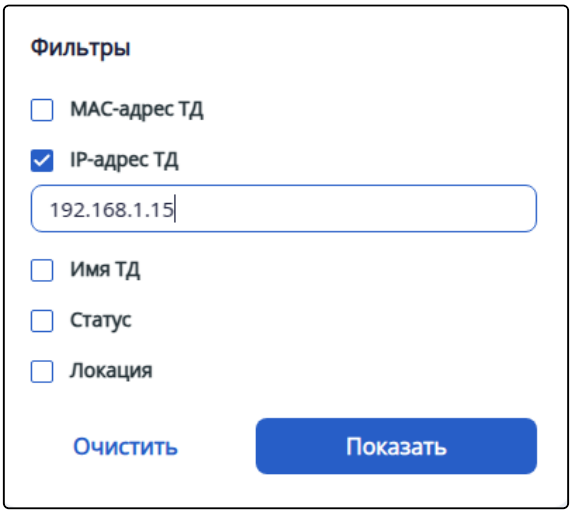
- *Разрегистрировать* − вывод из обслуживания точки доступа;
- *Обновить ПО* − запуск обновления программного обеспечения, если для данной модели ТД на контроллер загружен файл ПО;
- *Настроить* − создание индивидуального профиля настроек точки доступа, в котором присутствует возможность задать имя ТД, переопределить локацию или профиль общих настроек ТД, переопределить параметры радиопрофилей, такие как режим работы радиоинтерфейса, канал, ширина канала, мощность, а также отключить использование AirTune. Действие доступно при включенном режиме редактирования.

Таблица содержит данные:

- *MAC-адрес* − MAC-адрес точки доступа. При нажатии осуществляется переход на страницу «Точка доступа», которая содержит более подробную информацию о всех клиентах точки доступа и ее интерфейсах;
- *Статус* − состояние работы точки доступа;
- *IP-адрес* − IP-адрес точки доступа;
- *Модель* − модель точки доступа;
- *Имя устройства* − имя точки доступа;
- *Локация* − название локации, к которой относится точка доступа;
- *Версия ПО* − версия программного обеспечения точки доступа;
- *Время работы* − время работы с момента последнего включения или перезагрузки устройства;
- *Количество клиентов в 2.4/5 ГГц* − число клиентов, подключенных к точке доступа в частотных диапазонах 2.4/5 ГГц соответственно;
- *Количество клиентов* − общее число клиентов, подключенных к точке доступа. При нажатии осуществляется переход на страницу "Клиенты", содержащую более подробную информацию по клиентам данной точки 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;
- *Аппаратная версия* − HW-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.



Для удобства пользования таблицей предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *IP-адрес ТД* − IP-адрес точки доступа. Для поиска необходимо ввести IP-адрес полностью;
- *Имя ТД* − имя точки доступа, задается строкой. Поиск работает по частичному совпадению;
- *Статус ТД* − состояние работы точки доступа, осуществляется выбор из списка значений;
- *Локация* − название локации, к которой относится точка доступа. Осуществляется выбор из списка значений с возможностью поиска по списку.

При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.

Страница точки доступа

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

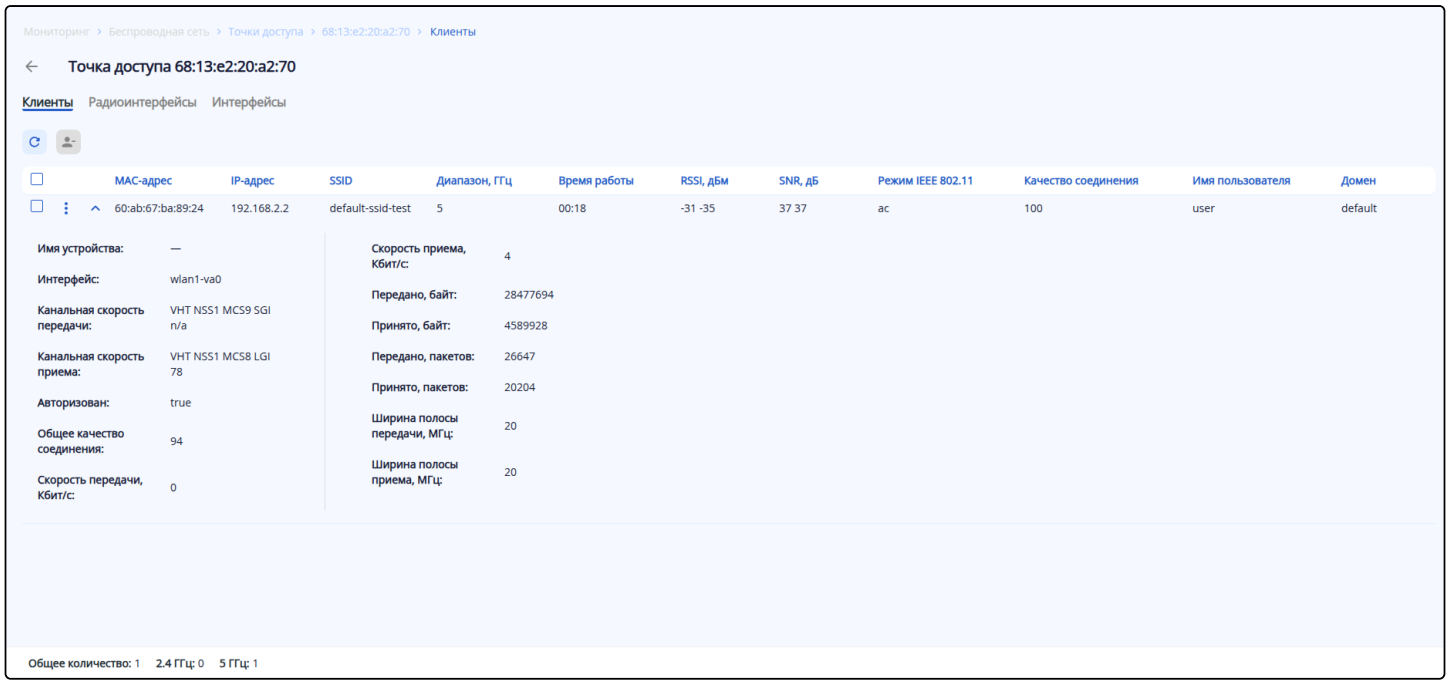
Клиенты

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.

Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одного, несколько или всех клиентов на странице, чтобы применить к ним общее действие с помощью кнопки «Деаутентификация клиента». При нажатии на кнопку выбранные клиенты будут деаутентифицированы.

Для каждого клиента также доступно контекстное меню с действием «Деаутентификация клиента».



В таблице представлены данные:

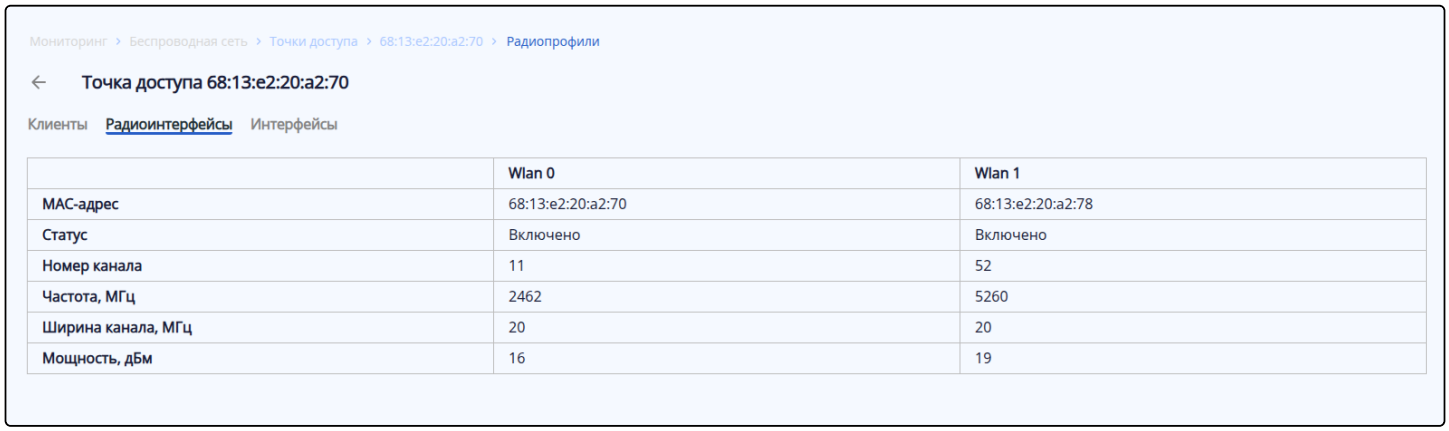
- *MAC-адрес* – MAC-адрес клиентского устройства;
- *IP-адрес* – IP-адрес клиентского устройства;
- *SSID* – имя сети, к которой подключено устройство;
- *Диапазон, ГГц* – диапазон частот, в котором подключено устройство к точке доступа;
- *Время работы* – время работы с момента подключения клиентского 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 устройства* − 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.

Радиоинтерфейсы



	Wlan 0	Wlan 1
MAC-адрес	68:13:e2:20:a2:70	68:13:e2:20:a2:78
Статус	Включено	Включено
Номер канала	11	52
Частота, МГц	2462	5260
Ширина канала, МГц	20	20
Мощность, дБм	16	19

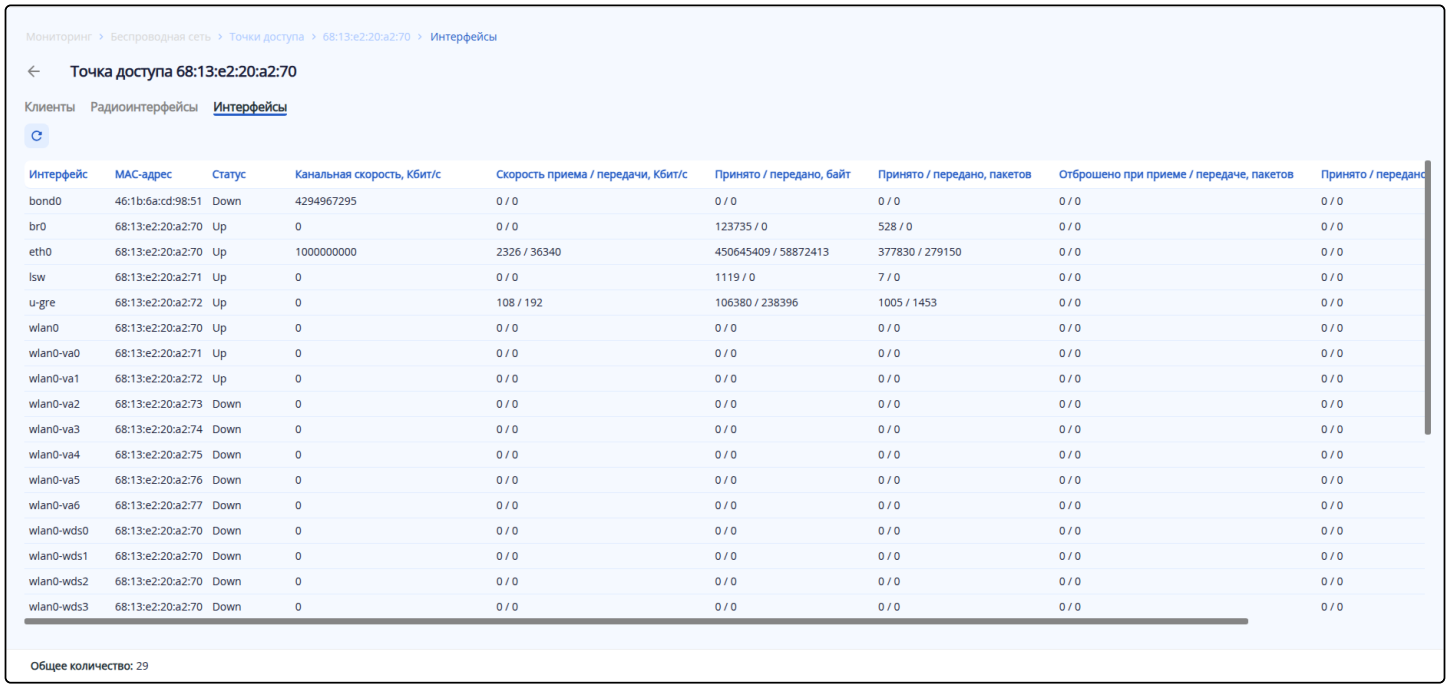
На странице представлена таблица с основными параметрами радиоинтерфейсов точки доступа:

- *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.

Обновление страницы происходит при нажатии на кнопку «Обновить».



Интерфейс	MAC-адрес	Статус	Канальная скорость, Кбит/с	Скорость приема / передачи, Кбит/с	Принято / передано, байт	Принято / передано, пакетов	Отброшено при приеме / передаче, пакетов	Принято / передано
bond0	46:1b:6a:cd:98:51	Down	4294967295	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
br0	68:13:e2:20:a2:70	Up	0	0 / 0	123735 / 0	528 / 0	0 / 0	0 / 0
eth0	68:13:e2:20:a2:70	Up	1000000000	2326 / 36340	450645409 / 58872413	377830 / 279150	0 / 0	0 / 0
lsw	68:13:e2:20:a2:71	Up	0	0 / 0	1119 / 0	7 / 0	0 / 0	0 / 0
u-gre	68:13:e2:20:a2:72	Up	0	108 / 192	106380 / 238396	1005 / 1453	0 / 0	0 / 0
wlan0	68:13:e2:20:a2:70	Up	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va0	68:13:e2:20:a2:71	Up	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va1	68:13:e2:20:a2:72	Up	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va2	68:13:e2:20:a2:73	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va3	68:13:e2:20:a2:74	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va4	68:13:e2:20:a2:75	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va5	68:13:e2:20:a2:76	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-va6	68:13:e2:20:a2:77	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-wds0	68:13:e2:20:a2:70	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-wds1	68:13:e2:20:a2:70	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-wds2	68:13:e2:20:a2:70	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0
wlan0-wds3	68:13:e2:20:a2:70	Down	0	0 / 0	0 / 0	0 / 0	0 / 0	0 / 0

Таблица содержит данные:

- *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 находятся в процессе регистрации или ожидают ее. Параметр «Общее количество» показывает общее число незарегистрированных точек доступа. При появлении большого количества новых точек доступа, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами. Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одну, несколько или все точки доступа на странице, чтобы применить к ним общее действие с помощью кнопки «Зарегистрировать». При нажатии на кнопку «Зарегистрировать» и подтверждении действия будет произведена попытка регистрации всех выбранных точек доступа, при успешном выполнении которой, точки доступа появятся на странице «Точки доступа».

Для каждой ТД также доступно контекстное меню с действием «Зарегистрировать».

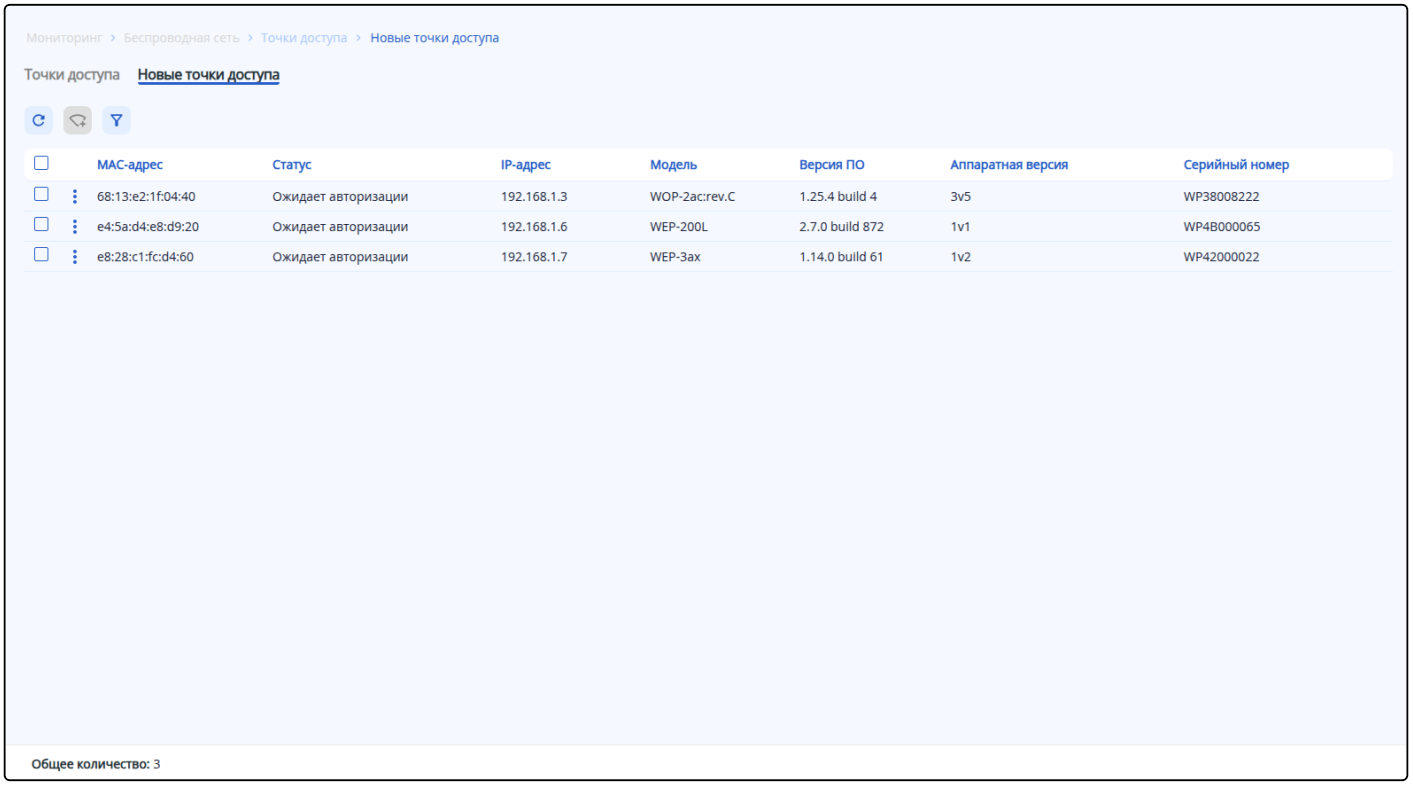
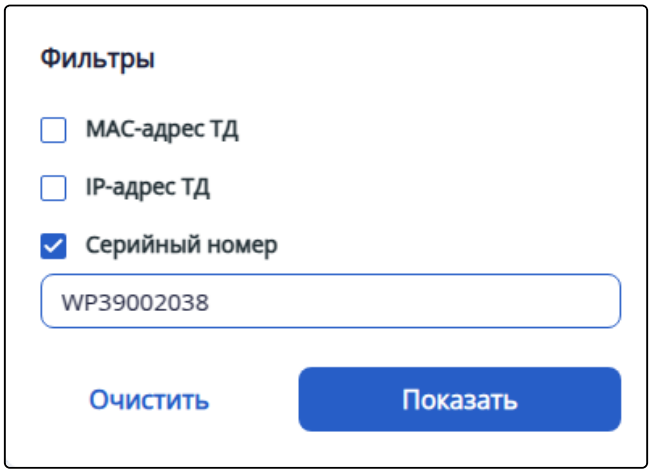


Таблица содержит данные:

- *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;
- *Аппаратная версия* − HW-версия аппаратного обеспечения устройства;
- *Серийный номер* − серийный номер устройства, установленный заводом-изготовителем.



Для удобства пользования таблицей предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *IP-адрес ТД* − IP-адрес точки доступа. Для поиска необходимо ввести IP-адрес полностью;
- *Серийный номер* − серийный номер точки доступа, установленный заводом-изготовителем. Задается строкой, поиск работает по частичному совпадению.

При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.

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.

Обновление страницы происходит при нажатии на кнопку «Обновить».

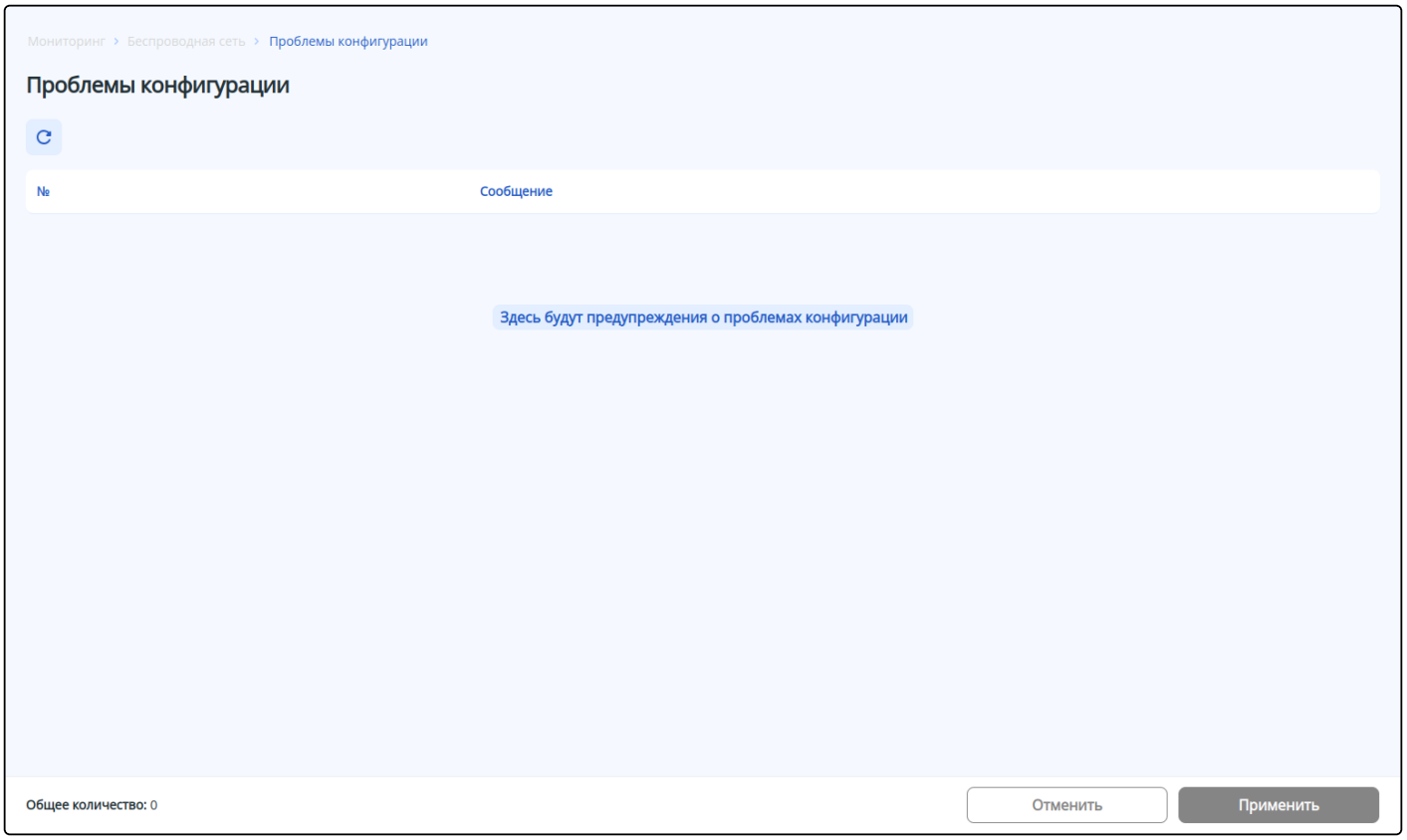


Таблица содержит данные:

- *№* − номер сообщения;
- *Сообщение* − сообщение о проблеме конфигурации.

Подменю «Журнал событий»

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

Точки доступа

На странице представлен журнал событий точек доступа с временными метками. В параметре «Общее количество» отображается общее количество записей в журнале. При появлении большого количества записей, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами.

Обновление страницы происходит при нажатии на кнопку «Обновить». Кнопка «Очистить» удаляет журнал событий.

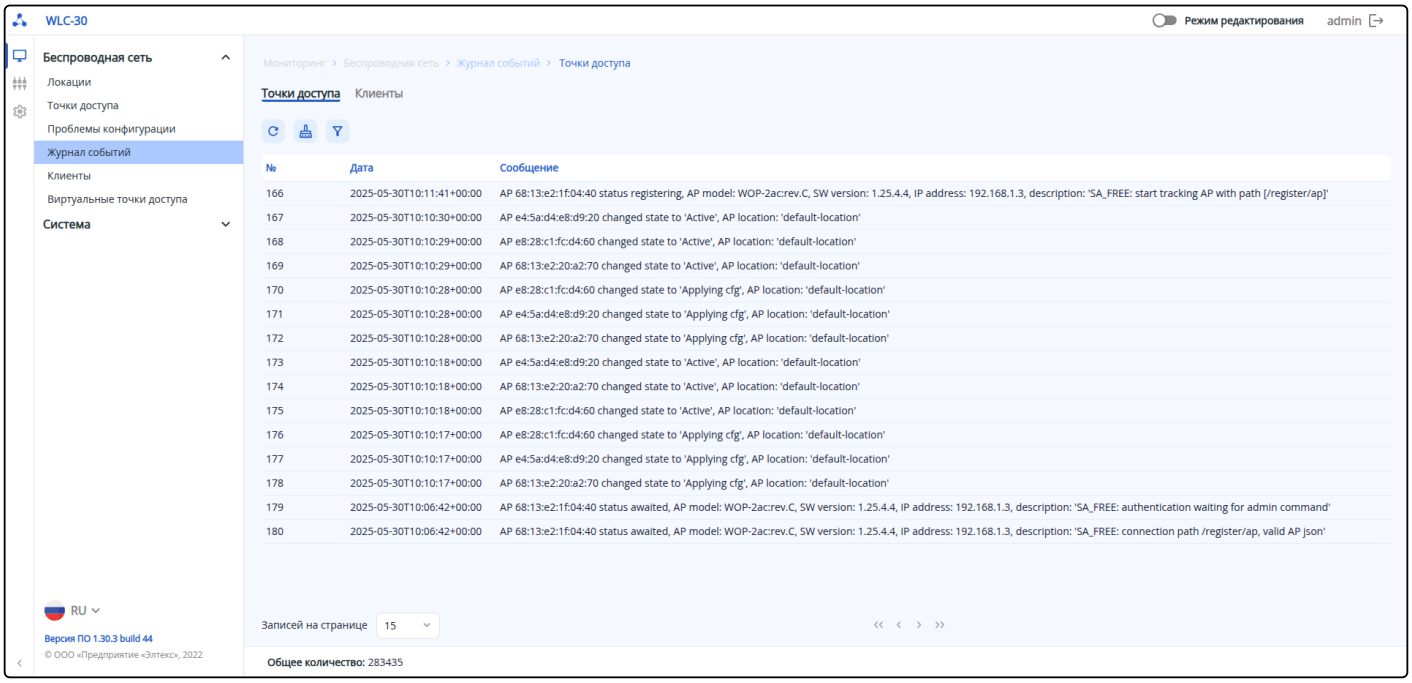
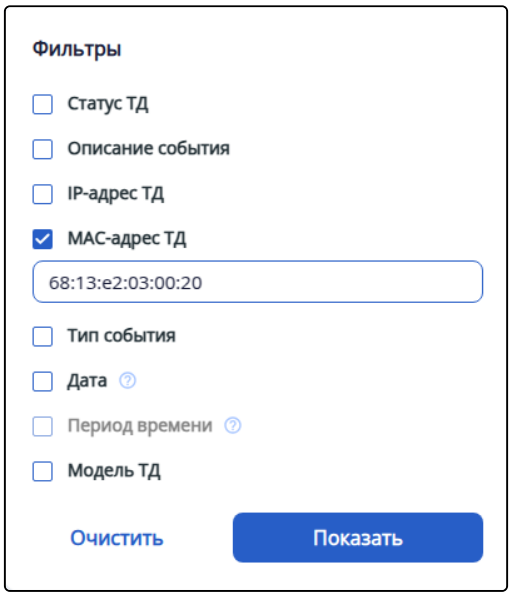


Таблица содержит данные:

- *№* − номер сообщения;
- *Дата* − дата события;
- Сообщение − событие, произошедшее с точкой доступа (изменение статуса, применение конфигурации, отключение, обновление ПО и т. п.).

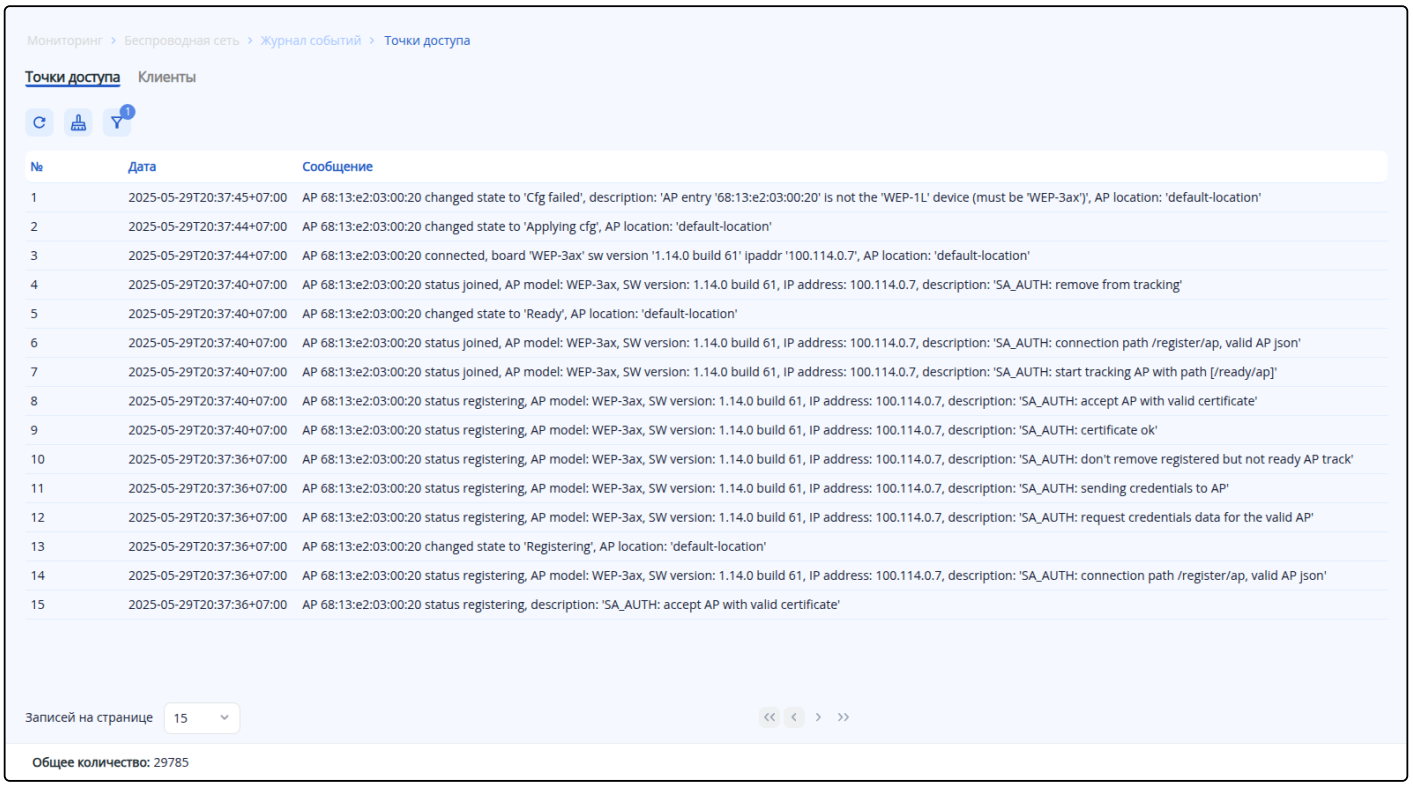


Для удобства использования журнала предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *Статус ТД* − состояние работы точки доступа, осуществляется выбор из списка значений;
- *Описание события* − описание события, задается строкой;
- *IP-адрес ТД* − IP-адрес точки доступа. Для поиска необходимо ввести IP-адрес полностью;
- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *Тип события* − тип события, осуществляется выбор из списка значений;
- *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;
- *Период времени* − период времени фиксации события в журнале. Доступно для ввода после выбора даты;

- *Модель ТД* – модель точки доступа, осуществляется выбор из списка значений.

При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.



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 общее количество записей в журнале. При появлении большого количества записей, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами.

Обновление страницы происходит при нажатии на кнопку «Обновить». Кнопка «Очистить» удаляет журнал событий.

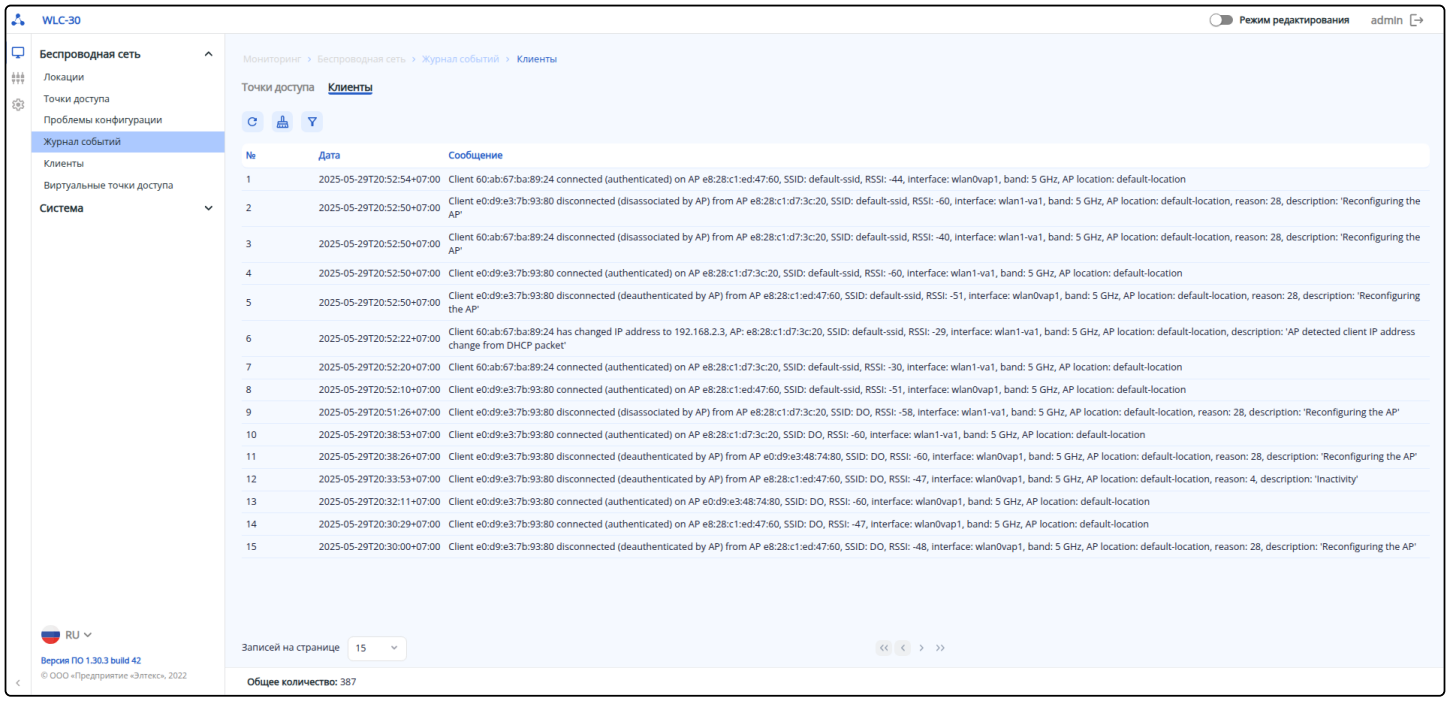
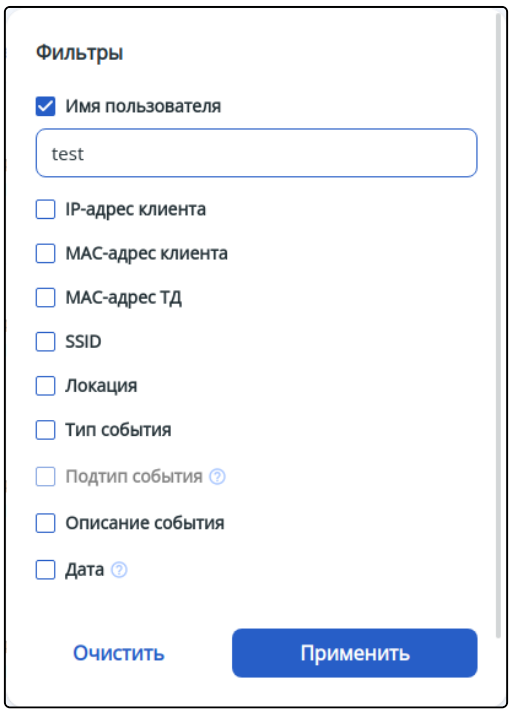


Таблица содержит данные:

- *№* − номер сообщения;
- *Дата* − дата события;
- *Сообщение* − событие, произошедшее с клиентом Wi-Fi (подключение, отключение, ошибка регистрации, роуминг и т. п.).



Для удобства использования журнала предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

- *Имя пользователя* − имя пользователя, указанное при регистрации в сети Wi-Fi, задается строкой. Поиск работает по частичному совпадению;
- *IP-адрес клиента* − IP-адрес клиента. Для поиска необходимо ввести IP-адрес полностью;
- *MAC-адрес клиента* − MAC-адрес 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;
- *SSID* – название сети, к которой подключен клиент. Допускается ввод вручную или выбор из списка значений. Поиск работает по частичному совпадению;
- *Локация* – название локации точки доступа. Допускается ввод вручную или выбор из списка значений. Поиск работает по частичному совпадению;
- *Тип события* – тип события, осуществляется выбор из списка значений;
- *Подтип события* – подтип события, осуществляется выбор из списка значений;
- *Описание события* – описание события, задается строкой. 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.

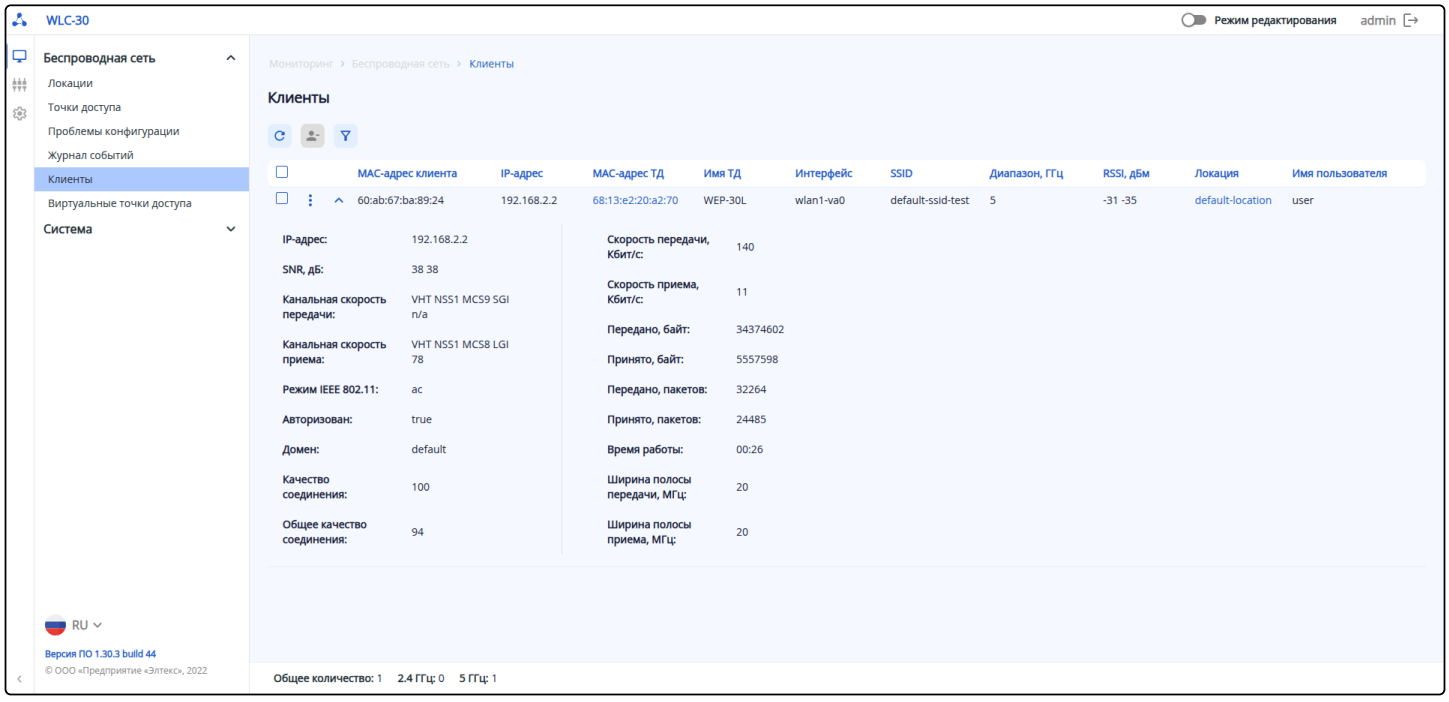
При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.

Подменю «Клиенты»

Страница содержит информацию о клиентах, подключенных ко всем точкам доступа контроллера. Параметр «Общее количество» показывает общее число клиентов и их распределение по частотным диапазонам. При подключении большого количества клиентов, на странице появляется параметр "Записей на странице" с возможными значениями: 15, 50, 100, 150 и 200, а также появляется возможность переключения между страницами. Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать одного, несколько или всех клиентов на странице, чтобы применить к ним общее действие с помощью кнопки «Деаутентификация клиента». При нажатии на кнопку выбранные клиенты будут деаутентифицированы.

Для каждого клиента также доступно контекстное меню с действием «Деаутентификация клиента».



В таблице представлена основная информация по клиенту:

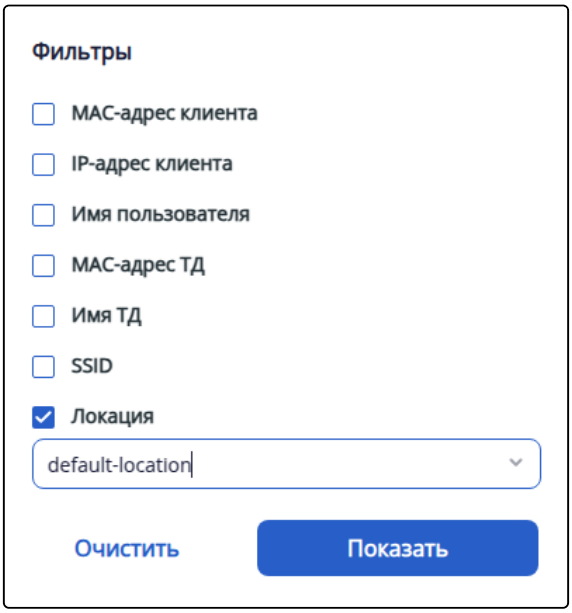
- *MAC-адрес клиента* – MAC-адрес подключенного устройства;
- *IP-адрес клиента* – IP-адрес подключенного устройства;
- *MAC-адрес ТД* – MAC-адрес точки доступа, к которой подключено устройство;
- *Имя ТД* – имя точки доступа;

- *Интерфейс* – интерфейс взаимодействия точки доступа с подключенным устройством;
- *SSID* – название сети, к которой подключено устройство;
- *Диапазон, ГГц* – диапазон частот, в котором подключено устройство к точке доступа;
- *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;
- *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.



Для удобства пользования таблицей предусмотрены фильтры. Используйте кнопку , чтобы настроить фильтры. Поиск доступен по следующим ключевым параметрам:

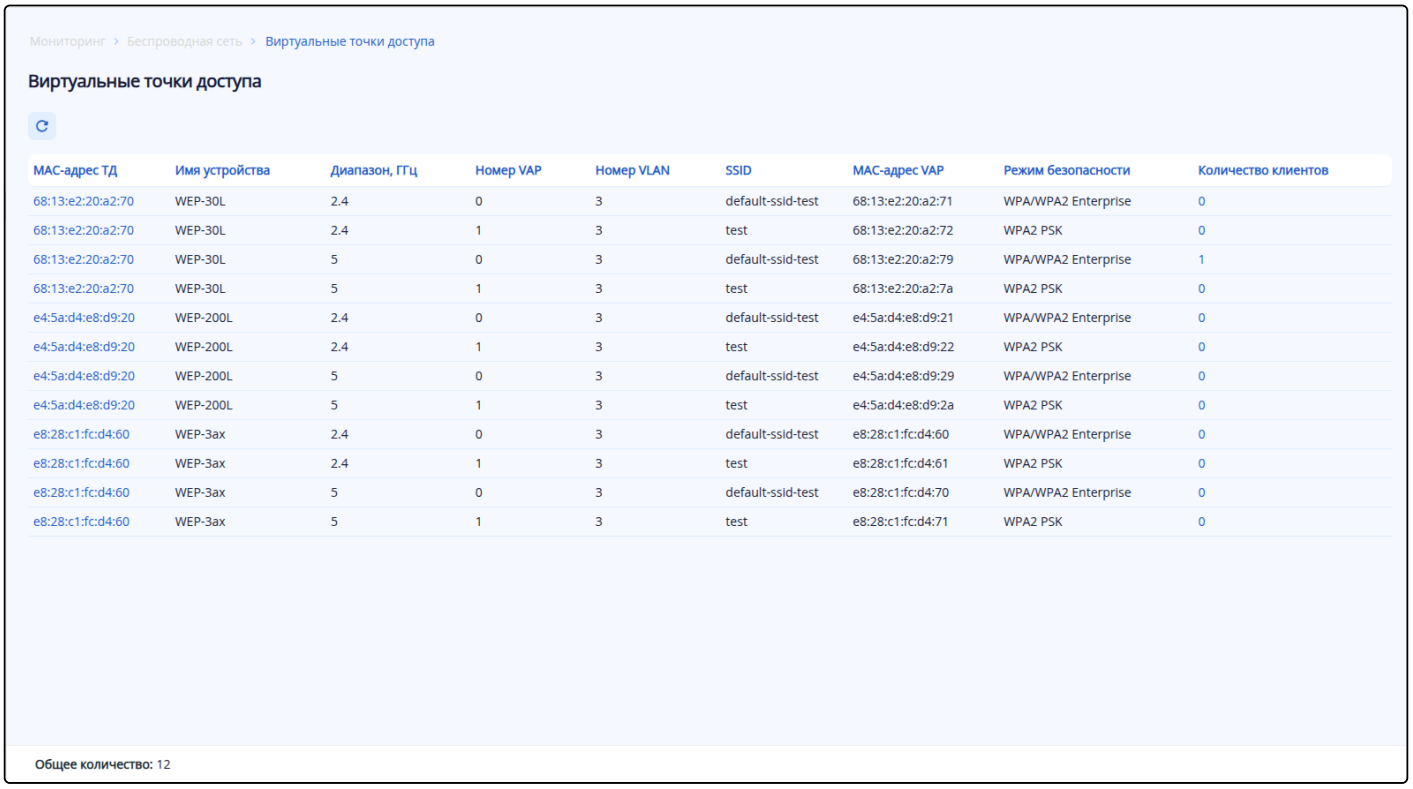
- *MAC-адрес клиента* − MAC-адрес клиента. Для поиска достаточно ввести один или несколько целых октетов;
- *IP-адрес клиента* − IP-адрес клиента. Для поиска необходимо ввести IP-адрес полностью;
- *Имя пользователя* − имя пользователя, указанное при регистрации в сети Wi-Fi, задается строкой. Поиск работает по частичному совпадению;
- *MAC-адрес ТД* − MAC-адрес точки доступа. Для поиска достаточно ввести один или несколько целых октетов;
- *Имя ТД* − имя точки доступа, задается строкой. Поиск работает по частичному совпадению;
- *SSID* − название SSID, к которому подключен клиент. Осуществляется выбор из списка значений с возможностью поиска по списку;
- *Локация* − название локации точки доступа, к которой подключен клиент. Осуществляется выбор из списка значений с возможностью поиска по списку.

При использовании фильтров, параметр «Общее количество» отображает общее количество отфильтрованных записей.

Подменю «Виртуальные точки доступа»

На странице представлена информация о всех включенных виртуальных точках доступа (VAP) во всех локациях контроллера.

Параметр «Общее количество» показывает число включенных виртуальных точек доступа, которые предоставляют услугу во всех локациях. Обновление страницы происходит при нажатии на кнопку «Обновить».



MAC-адрес ТД	Имя устройства	Диапазон, ГГц	Номер VAP	Номер VLAN	SSID	MAC-адрес VAP	Режим безопасности	Количество клиентов
68:13:e2:20:a2:70	WEP-30L	2.4	0	3	default-ssid-test	68:13:e2:20:a2:71	WPA/WPA2 Enterprise	0
68:13:e2:20:a2:70	WEP-30L	2.4	1	3	test	68:13:e2:20:a2:72	WPA2 PSK	0
68:13:e2:20:a2:70	WEP-30L	5	0	3	default-ssid-test	68:13:e2:20:a2:79	WPA/WPA2 Enterprise	1
68:13:e2:20:a2:70	WEP-30L	5	1	3	test	68:13:e2:20:a2:7a	WPA2 PSK	0
e4:5a:d4:e8:d9:20	WEP-200L	2.4	0	3	default-ssid-test	e4:5a:d4:e8:d9:21	WPA/WPA2 Enterprise	0
e4:5a:d4:e8:d9:20	WEP-200L	2.4	1	3	test	e4:5a:d4:e8:d9:22	WPA2 PSK	0
e4:5a:d4:e8:d9:20	WEP-200L	5	0	3	default-ssid-test	e4:5a:d4:e8:d9:29	WPA/WPA2 Enterprise	0
e4:5a:d4:e8:d9:20	WEP-200L	5	1	3	test	e4:5a:d4:e8:d9:2a	WPA2 PSK	0
e8:28:c1:fc:d4:60	WEP-3ax	2.4	0	3	default-ssid-test	e8:28:c1:fc:d4:60	WPA/WPA2 Enterprise	0
e8:28:c1:fc:d4:60	WEP-3ax	2.4	1	3	test	e8:28:c1:fc:d4:61	WPA2 PSK	0
e8:28:c1:fc:d4:60	WEP-3ax	5	0	3	default-ssid-test	e8:28:c1:fc:d4:70	WPA/WPA2 Enterprise	0
e8:28:c1:fc:d4:60	WEP-3ax	5	1	3	test	e8:28:c1:fc:d4:71	WPA2 PSK	0

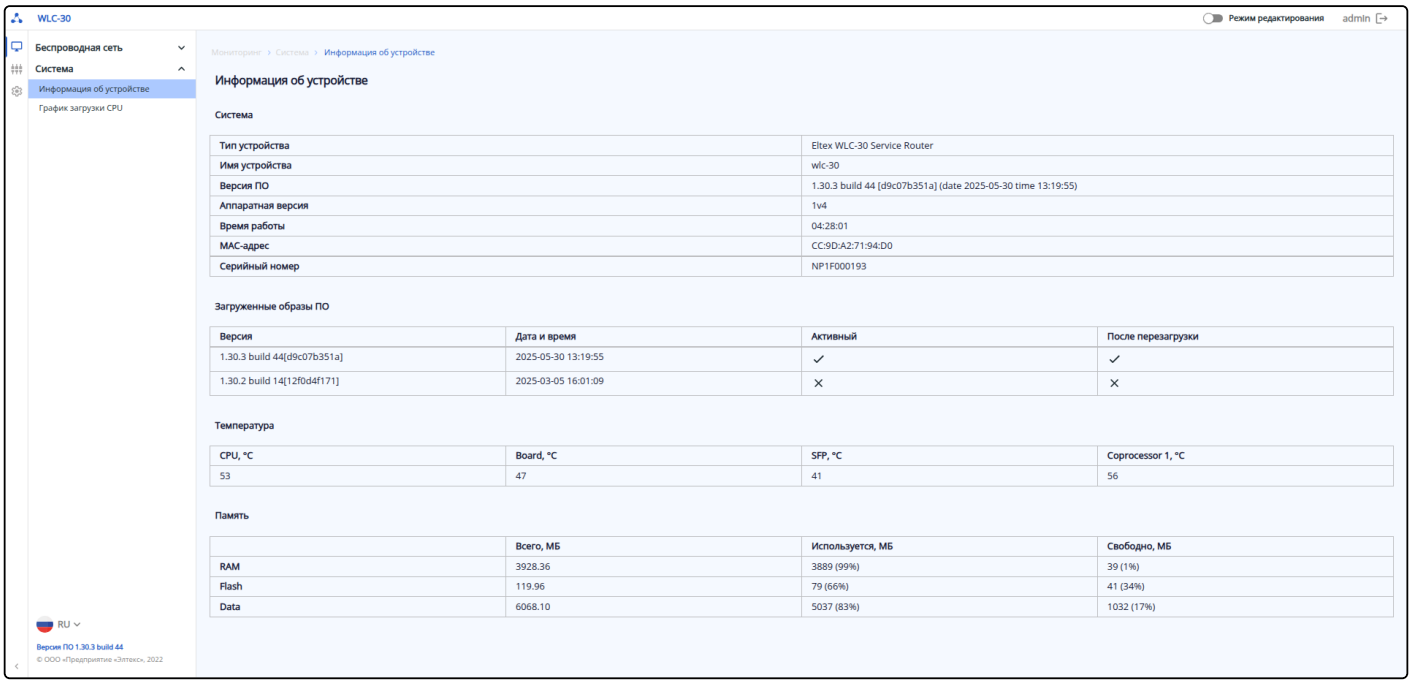
Таблица содержит следующую информацию:

- *MAC-адрес ТД* − MAC-адрес точки доступа, на которой включена VAP. При нажатии осуществляется переход на страницу «Точка доступа», которая содержит более подробную информацию о всех клиентах точки доступа и ее интерфейсах;
- *Имя устройства* − имя точки доступа;
- *Диапазон, ГГц* − частотный диапазон радиоинтерфейса, на котором VAP предоставляет услугу;
- *Номер VAP* − порядковый номер виртуальной точки доступа. На каждой точке доступа нумерация VAP ведется с 0 для каждого радиоинтерфейса;
- *Номер VLAN* − идентификатор VLAN, в котором передается трафик Wi-Fi клиентов;
- *SSID* − название беспроводной сети;
- *MAC-адрес VAP* − MAC-адрес виртуальной точки доступа;
- *Режим безопасности* − тип шифрования данных, используемый на виртуальной точке доступа;
- *Количество клиентов* − число клиентов, подключенных к виртуальной точке доступа. При нажатии осуществляется переход на страницу "Клиенты", содержащую более подробную информацию по клиентам данной точки доступа.

Меню «Система»

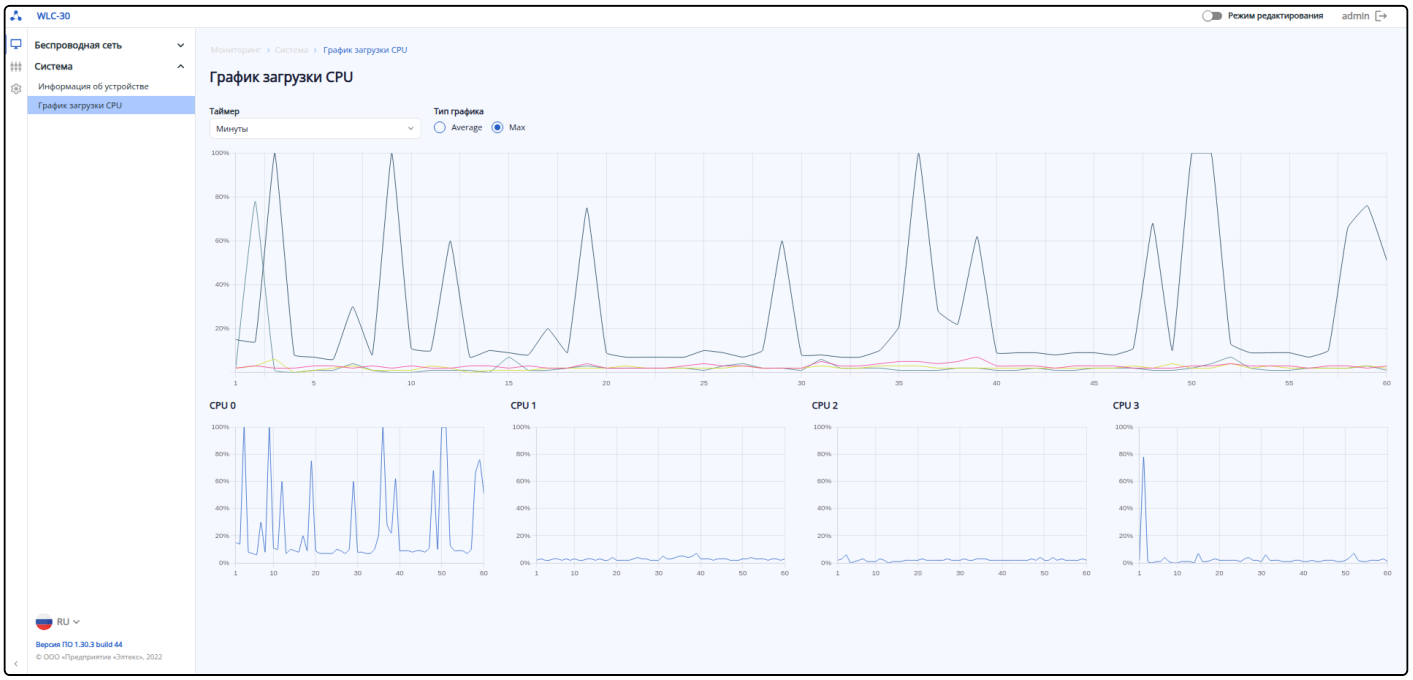
Подменю «Информация об устройстве»

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



Подменю «График загрузки CPU»

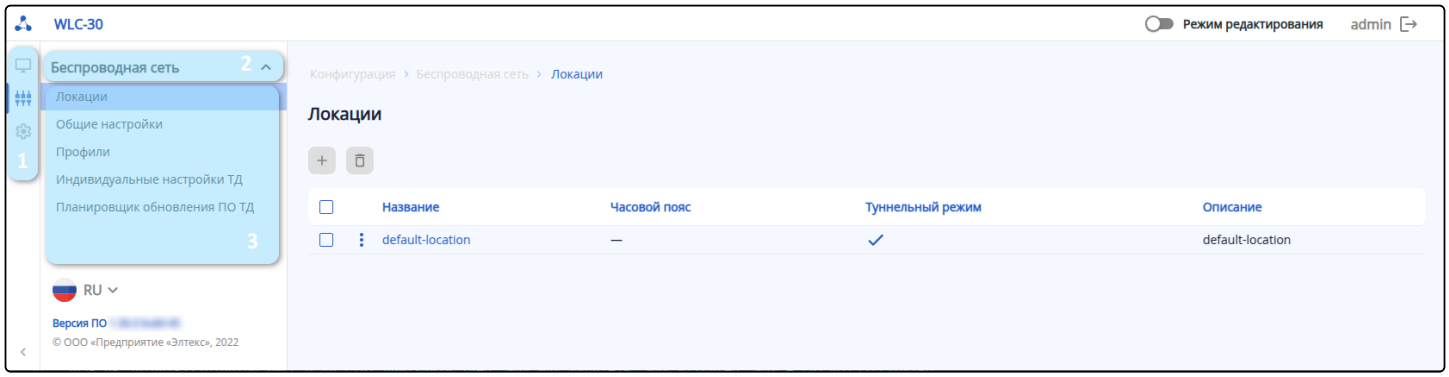
На странице представлен общий график загрузки всех CPU устройства, а также индивидуальные графики для каждого CPU.



В параметре "Таймер" осуществляется выбор единиц измерения периода времени, за который отображается график: секунды, минуты, часы. Параметр "Тип графика" определяет, какие значения будут отображаться на графике - средние за период или максимальные.

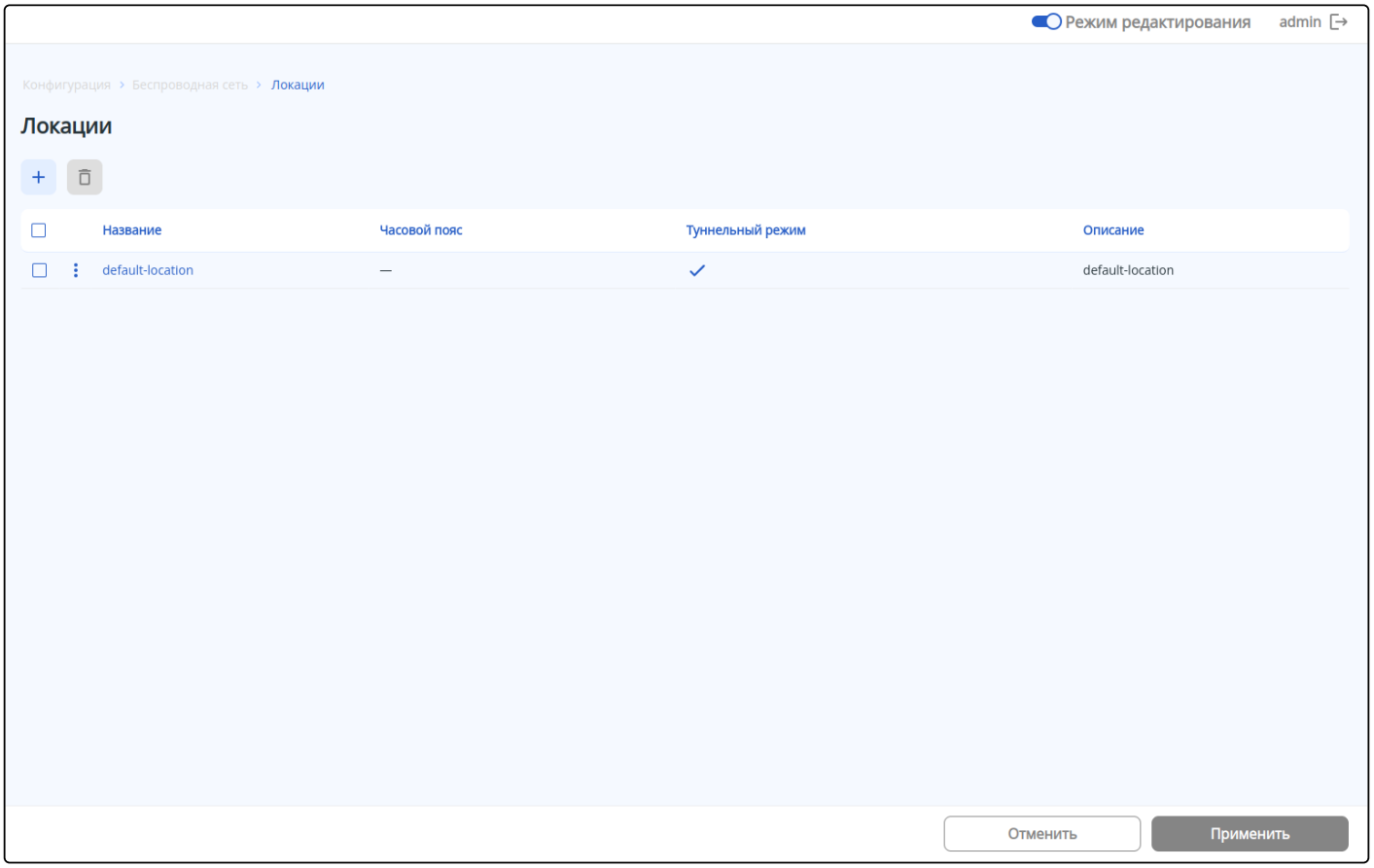
10.2.4 Конфигурирование

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



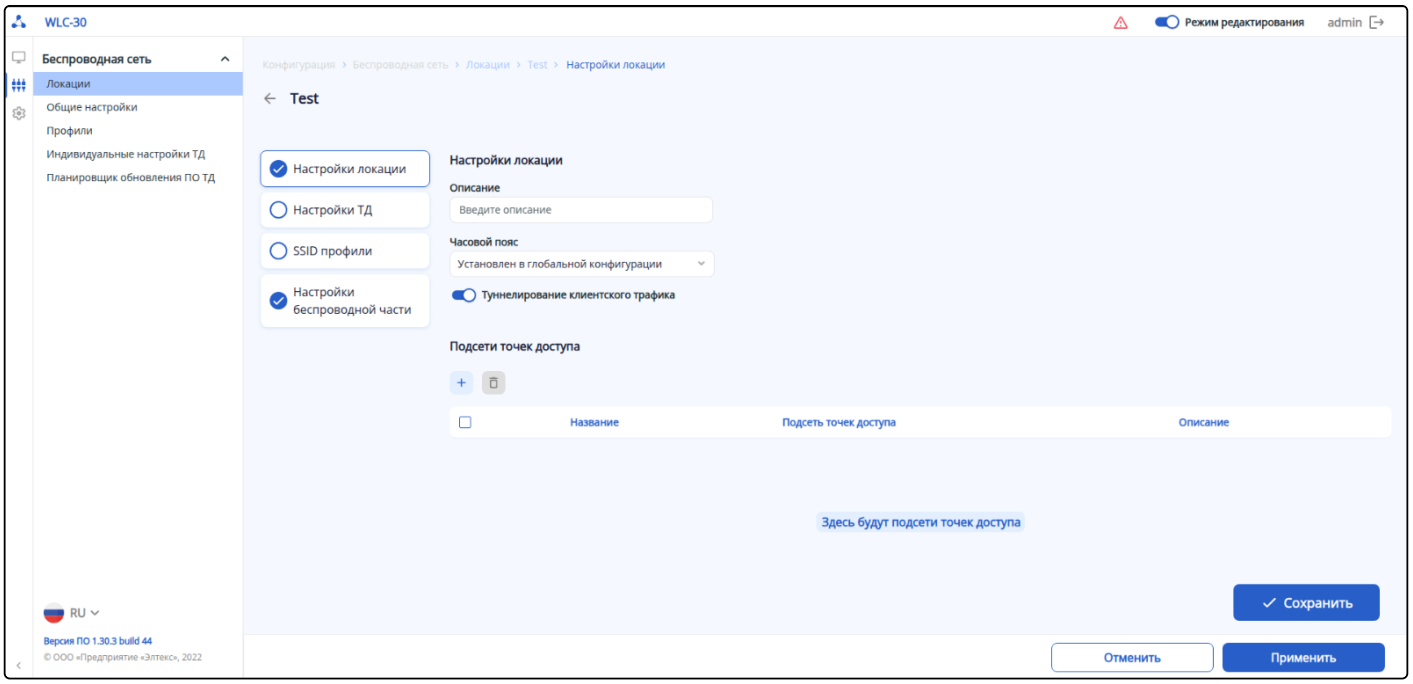
Режим редактирования

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.

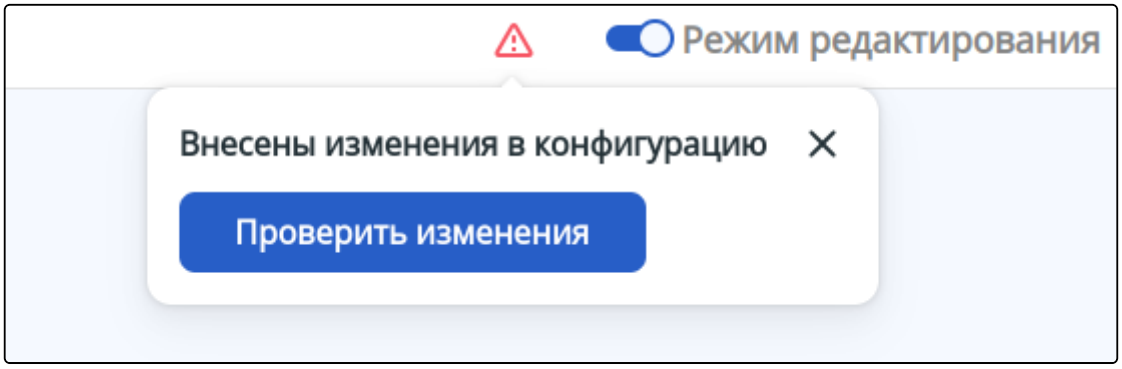


Сохранение изменений

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

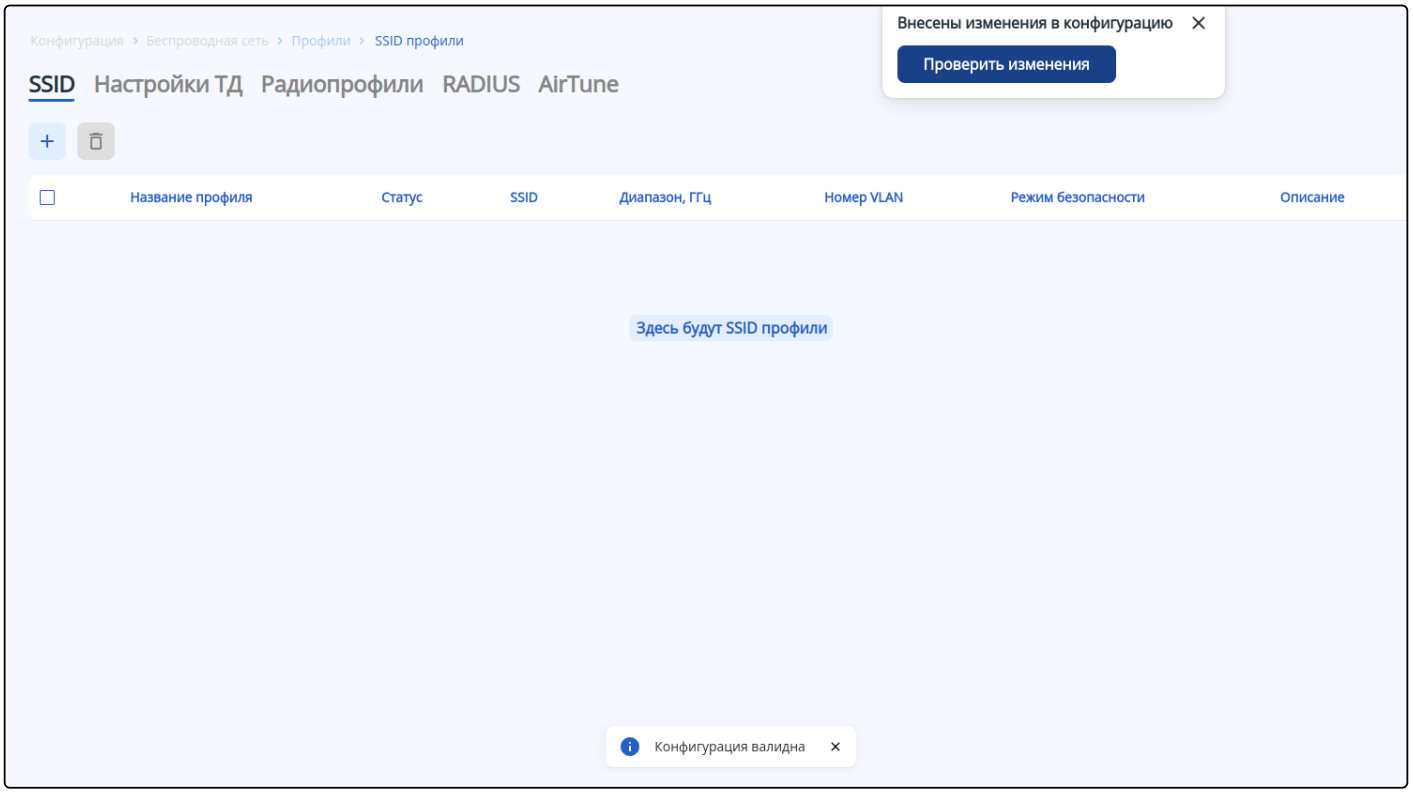


Наличие любых изменений в текущей конфигурации отражается на верхней панели страницы с помощью иконки .

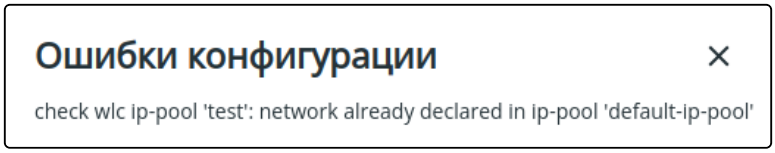


Проверить корректность настроенной конфигурации до применения настроек можно с помощью кнопки «Проверить изменения».

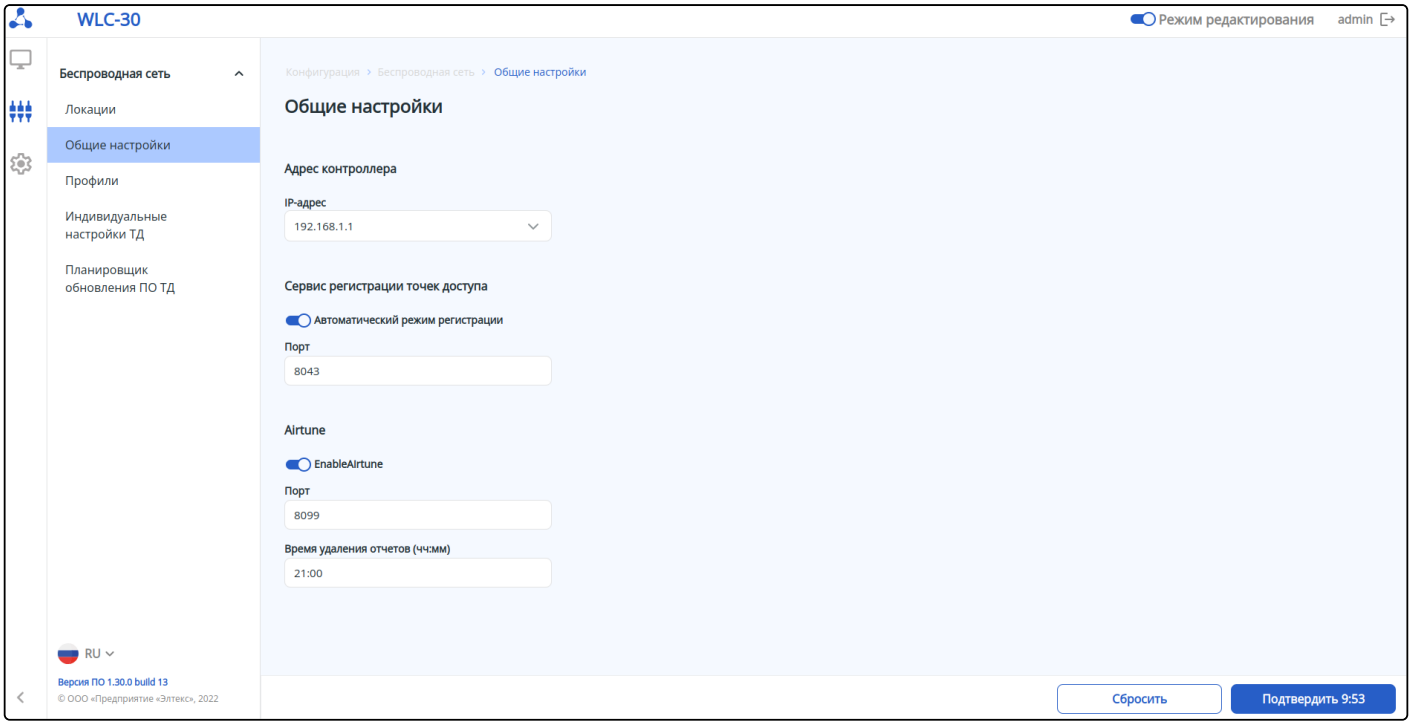
Если конфигурация корректна, то после нажатия на кнопку «Проверить изменения» отобразится сообщение «Конфигурация валидна».



Если конфигурация не валидна, то проверка покажет, какие ошибки присутствуют в конфигурации.



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



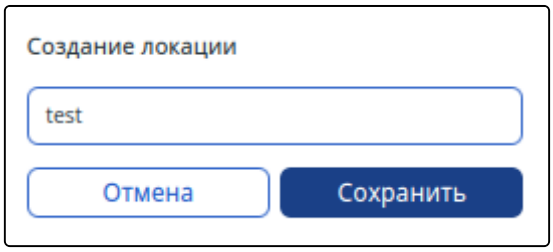
После нажатия кнопки «Применить» запускается таймер, в течение которого действуют внесенные изменения. Чтобы полностью сохранить изменения необходимо нажать кнопку «Подтвердить».

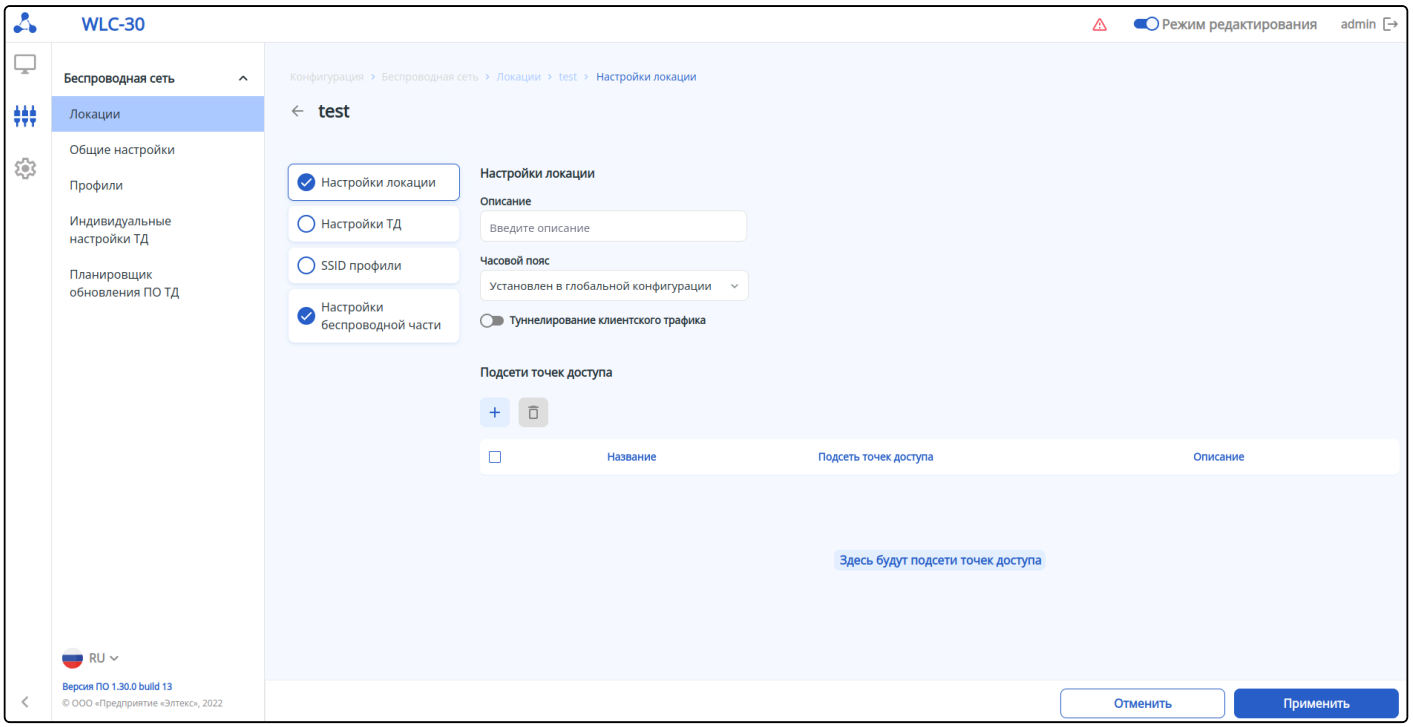
Кнопка «Сбросить» используется для отмены действия внесенных изменений. После окончания таймера внесённые изменения также будут отменены автоматически. Следует учитывать, что изменения при этом остаются в CANDIDATE конфигурации и могут быть снова применены с помощью кнопки «Применить» или могут быть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



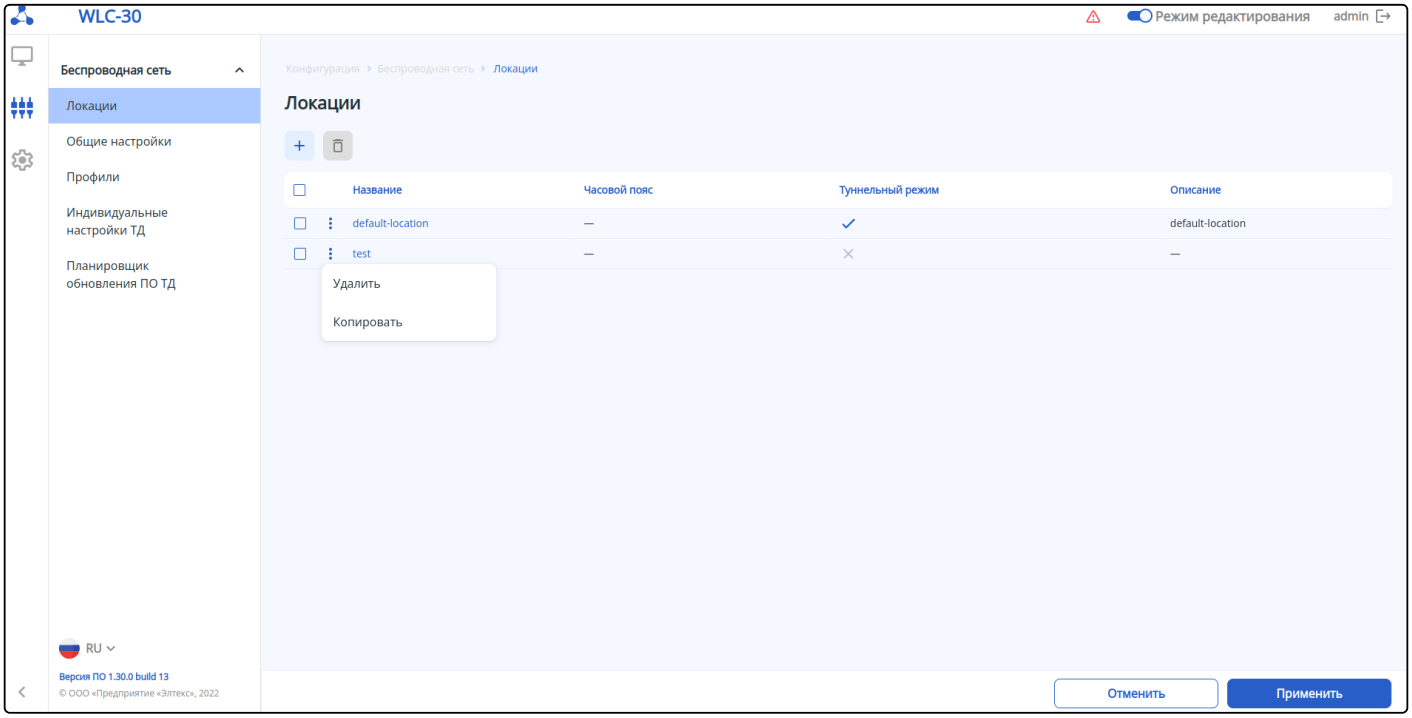


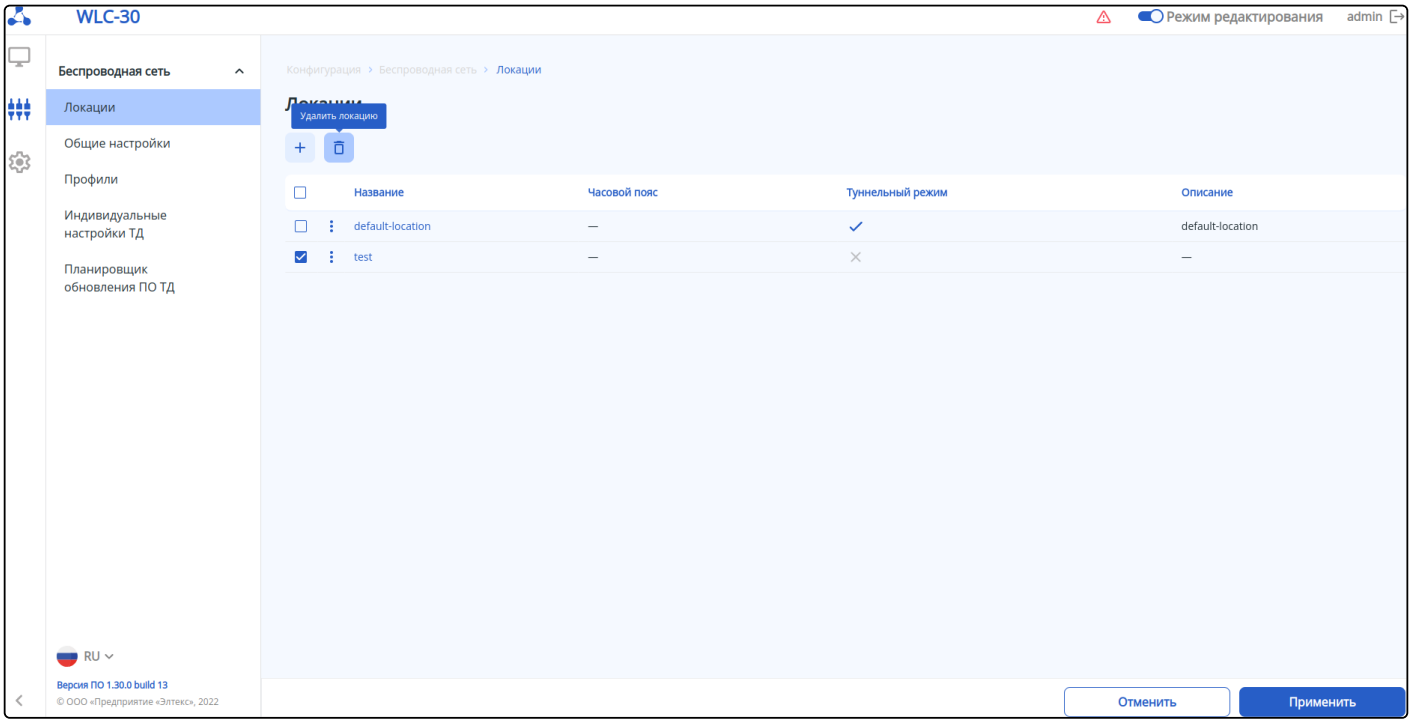
После создания объекта автоматически осуществляется переход на страницу его настройки.

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, чтобы удалить их одновременно.

Примеры представлены на рисунках ниже:





Меню «Беспроводная сеть»

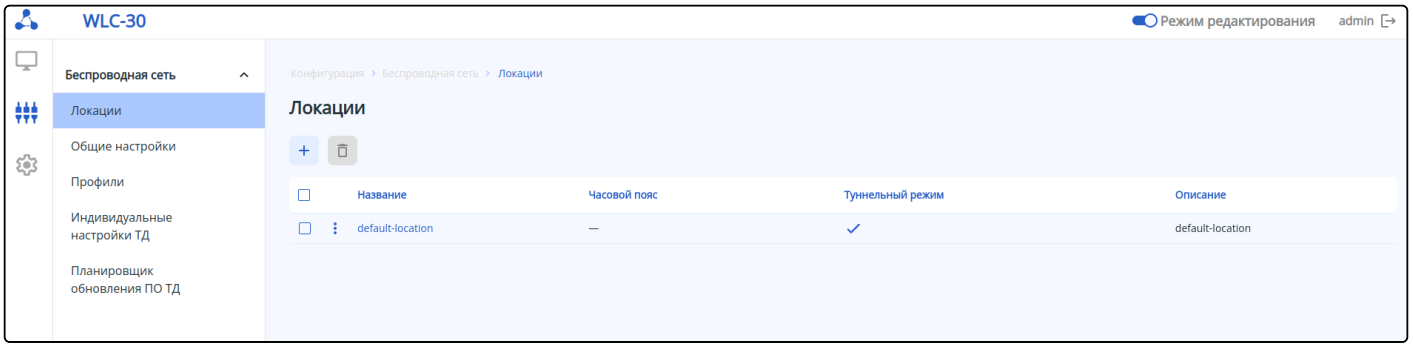
Подменю «Локации»

На странице «Локации» представлены локации, имеющиеся в конфигурации.

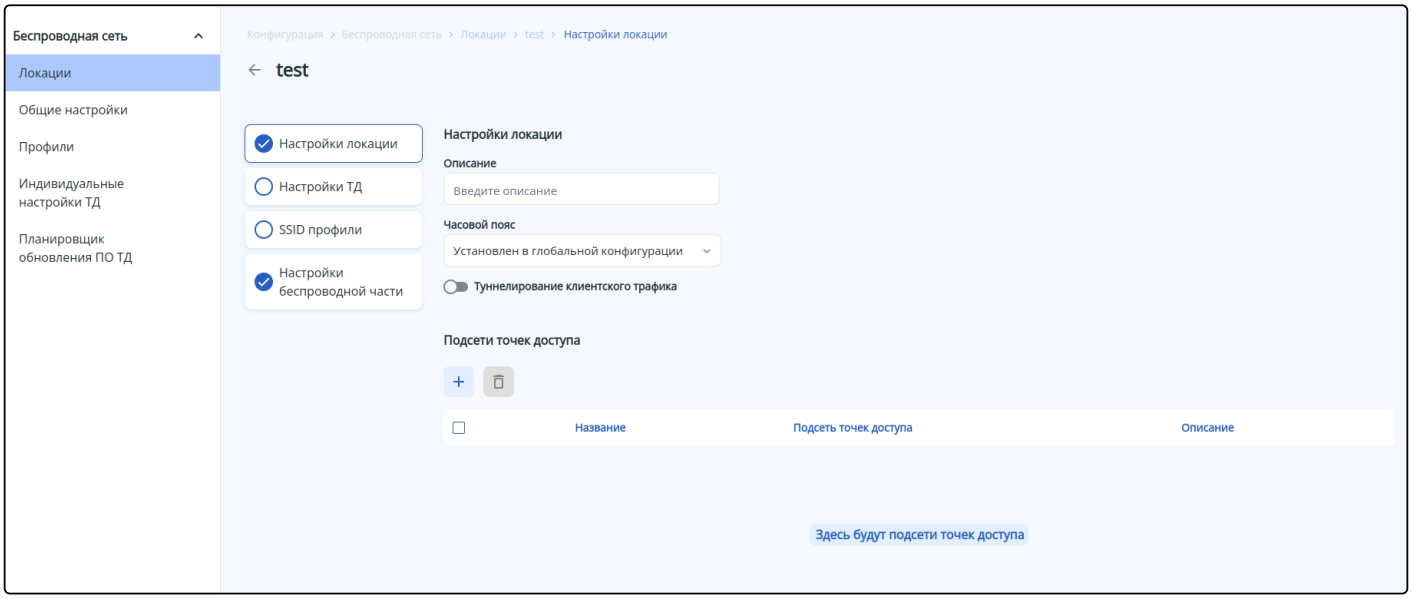
> Для создания, удаления и редактирования локации должен быть включен режим редактирования.

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

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



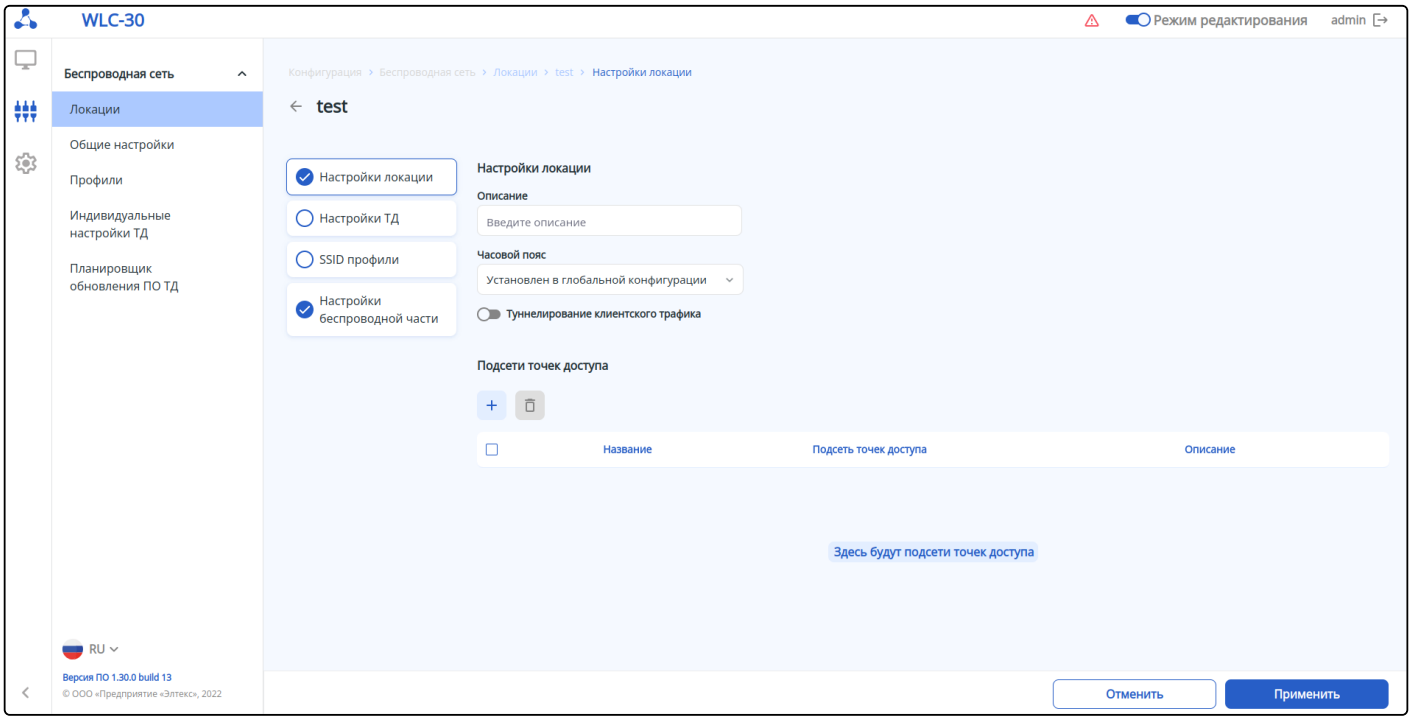
Для редактирования существующей локации нажмите на ее название в списке. Настройка локации разделена на несколько шагов, выполнять шаги можно в произвольном порядке.



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

- Описание: default-location;
- Туннелирование клиентского трафика: включено;
- Подсети точек доступа: ТД любой подсети будут конфигурироваться по настройкам этой локации;
- 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.

Настройки локации

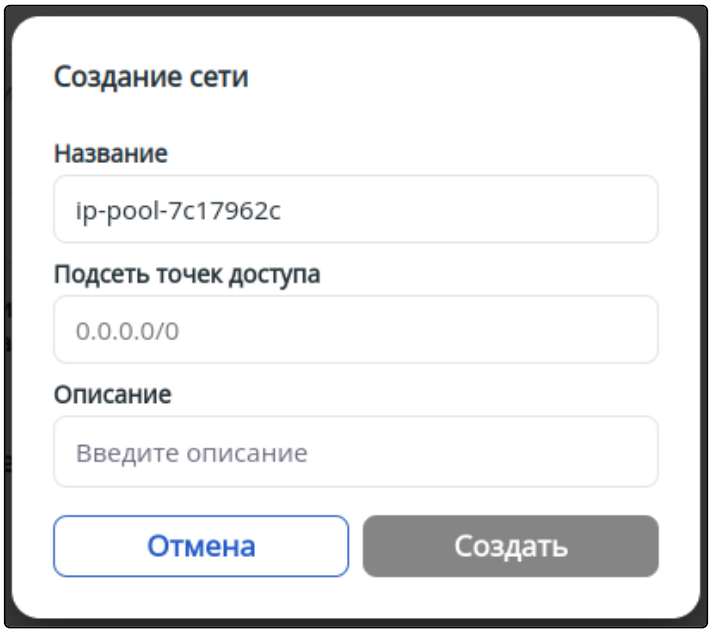


Данный шаг содержит общие настройки для локации:

- *Описание* – описание для локации. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Часовой пояс* – часовой пояс для точек доступа данной 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 глобальной конфигурации контроллера.
- *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, кроме тех, для которых локация определена через индивидуальные настройки;
- *Описание* − описание для подсети.

Настройки ТД

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

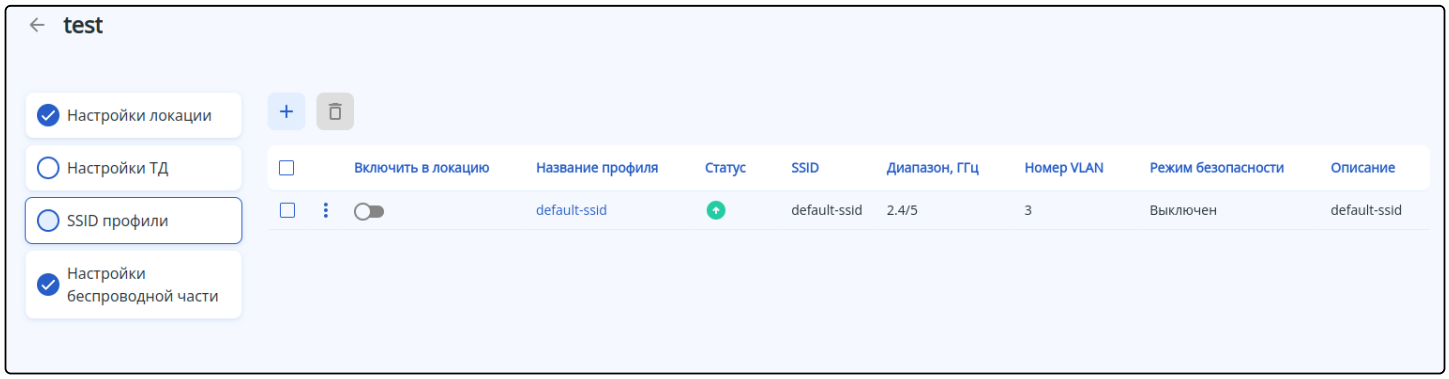
Для добавления существующего профиля в локацию используется переключатель «Включить в локацию».

На странице в таблице представлены основные настройки каждого профиля:

- 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.

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



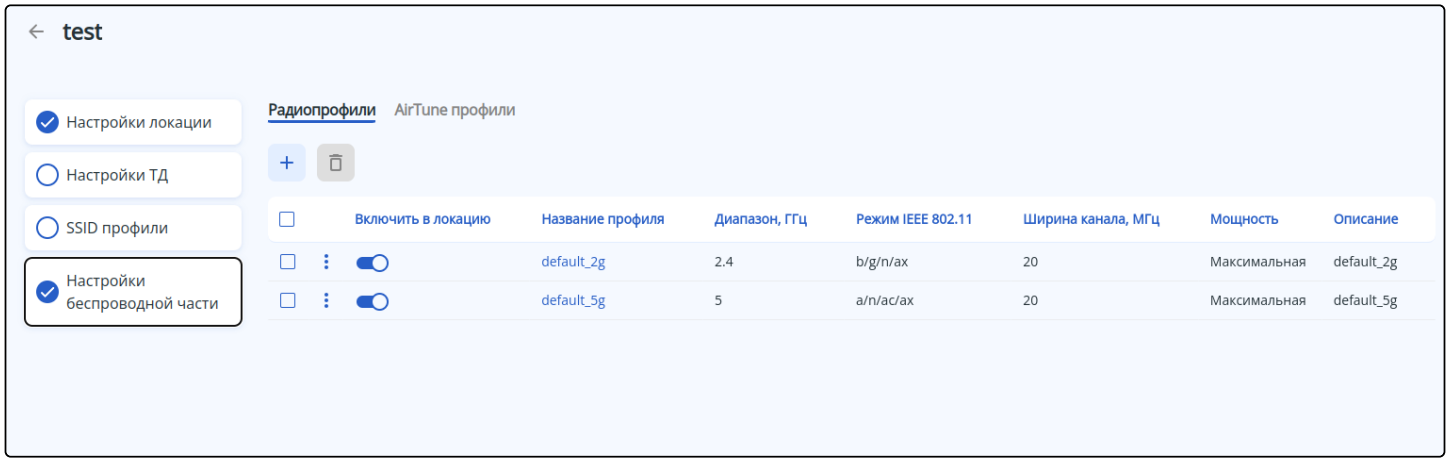
В локацию может быть добавлен один или несколько SSID-профилей. Для этого используется переключатель «Включить в локацию».

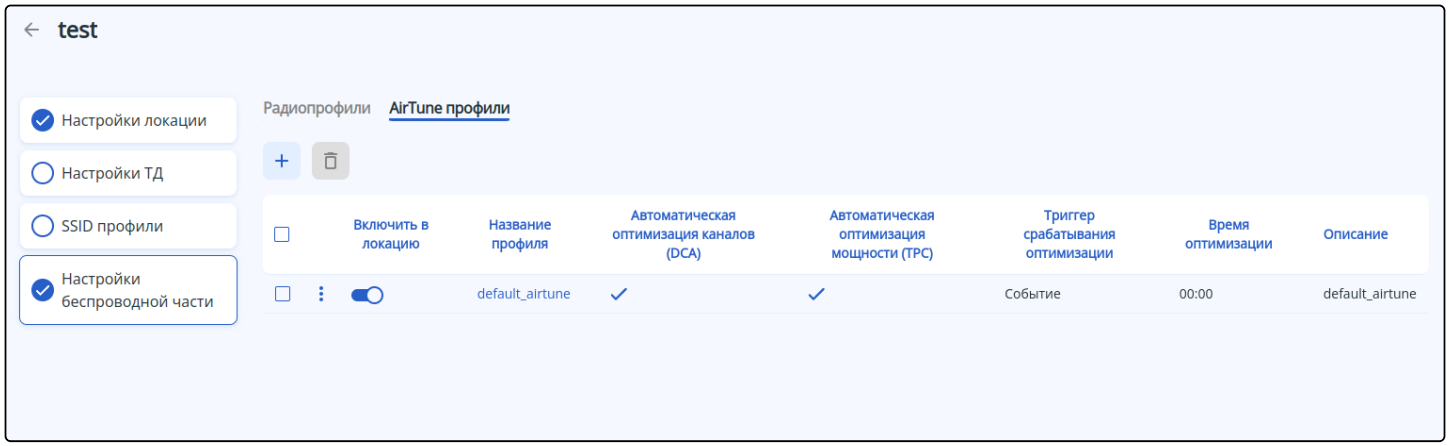
Основные настройки профиля SSID представлены в таблице:

- Название профиля SSID;
- Статус работы SSID;
- Название сети (SSID);
- Диапазон вещания;
- Номер VLAN;
- Режим безопасности;
- Описание.

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





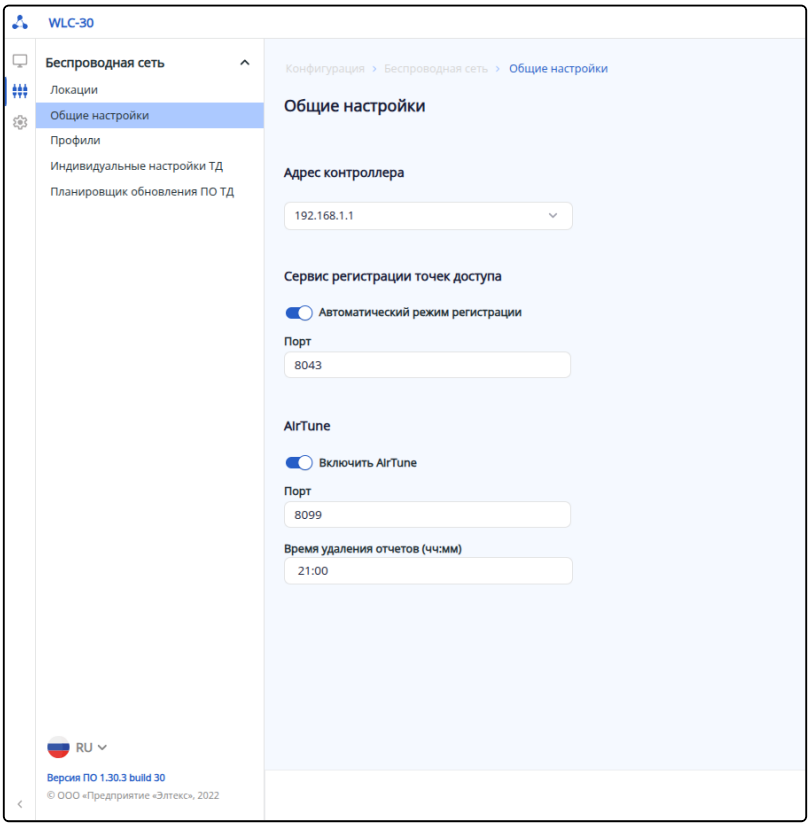
Для добавления в локацию радиопрофилей и airtune-профилей используются переключатели «Включить в локацию».

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 «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 представлены следующие параметры:

Адрес контроллера:

- *IP-адрес* – IP-адрес контроллера, по которому точки доступа будут взаимодействовать с WLC. Значение по умолчанию: отсутствует. Возможен ввод значения, в этом случае параметр задаётся в виде: AAA.BBB.CCC.DDD, где каждая часть принимает значения от 0 до 255. А также возможен выбор значения из списка существующих адресов интерфейсов контроллера.

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» 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».

Подменю «Профили»

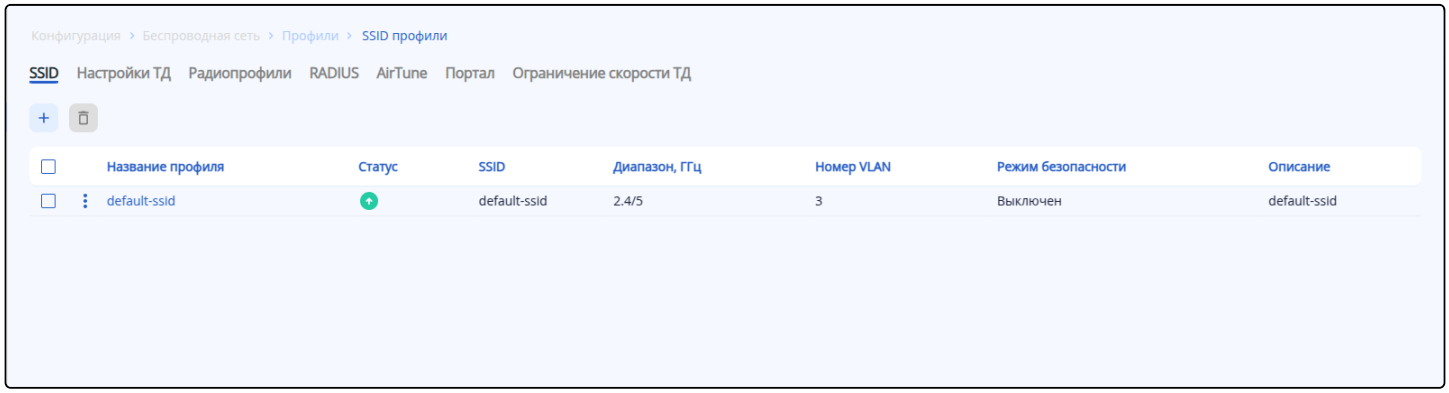
SSID

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:

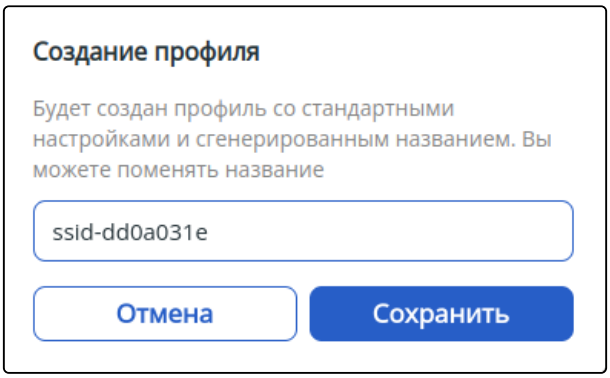
Общие настройки:

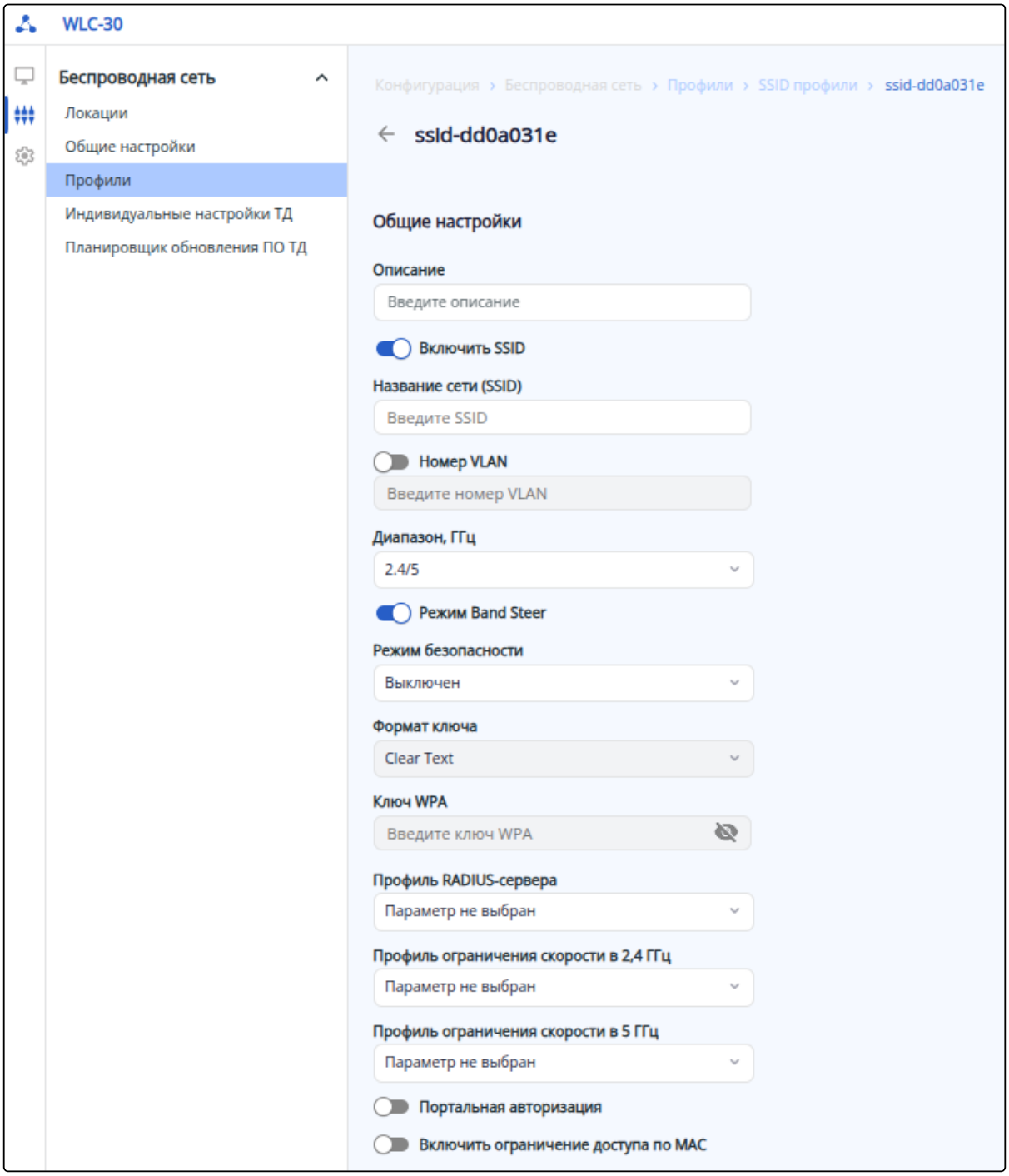
- Описание: default-ssid
- Статус: включен
- Название сети (SSID): default-ssid
- Номер VLAN: 3
- Диапазон, ГГц: 2.4/5
- Режим Band Steer: отключено
- Режим безопасности: WPA2 Enterprise
- Профиль RADIUS-сервера: default-radius
- Профиль ограничения скорости в 2,4 ГГц: не задан
- Профиль ограничения скорости в 5 ГГц: не задан
- Портальная авторизация: отключено
- Включить ограничение доступа по MAC: отключено

Расширенные настройки:

- Транслировать SSID: включено
- Максимальное количество клиентов: ограничение 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. Возможные значения: включено/отключено. Значение по умолчанию: включено;
  Если SSID включен, то в таблице профилей в столбце «Статус» отображается его наглядное цветовое обозначение:
  - − SSID включен;
  - − SSID выключен.

- *Название сети (SSID)* – название беспроводной сети, которая будет вещаться пользователям. Возможные значения: строка до 32 символов. Значение по умолчанию: отсутствует;

  ⚠ Данный параметр является обязательным при создании SSID-профиля.

- *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.
- *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: 2.4/5 ГГц.
- *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: включено.

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

- *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-3L, WEP-30L, WEP-30L-Z, WOP-30L, WOP-30LS, WOP-30LI.
  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 ограничения скорости в 2.4 ГГц* – параметр позволяет выбрать созданный ранее профиль ограничения скорости в диапазоне 2.4 ГГц, а также позволяет создать и настроить новый профиль. Возможные значения для названия профиля: строка до 235 символов. Значение по умолчанию: отсутствует.
- *Профиль ограничения скорости в 5 ГГц* – параметр позволяет выбрать созданный ранее профиль ограничения скорости в диапазоне 5 ГГц, а также позволяет создать и настроить новый профиль. Возможные значения для названия профиля: строка до 235 символов. Значение по умолчанию: отсутствует.
- *Портальная авторизация* – переключатель активирует портальную авторизацию на SSID. Значение по умолчанию: отключено;
- *Профиль портала* – параметр позволяет выбрать созданный ранее профиль портала, а также позволяет создать и настроить новый профиль. Настройка доступна только при включенной портальной авторизации. Возможные значения для названия профиля: строка до 235 символов. Значение по умолчанию: отсутствует.
- *Включить ограничение доступа по MAC* – переключатель активирует функцию ограничения доступа клиентов к SSID по их MAC-адресам. Возможные значения: включено/отключено. Значение по умолчанию: отключено;
- *Режим доступа* – выбор способа ограничения доступа по MAC-адресам. Настройка доступна при включенной функции ограничения доступа по MAC. Возможные значения:
  - MAC аутентификация на RADIUS – аутентификация будет проходить по MAC-адресам, заданным на RADIUS-сервере. Данный режим доступа не может использоваться при включенном режиме безопасности Enterprise. В текущей версии создать учетные записи на RADIUS-сервере возможно только через CLI. Учетная запись для MAC аутентификации должна содержать в параметре "user": MAC-адрес клиента в формате AA-BB-CC-DD-EE-FF (верхний регистр важен), а в параметре "password": "NOPASSWORD". Подробное описание представлено в разделе "Настройка доступа беспроводных клиентов по MAC-адресам".

    > При режиме доступа "MAC аутентификация на RADIUS", в случае, если учетные записи с MAC-адресами клиентов не созданы на RADIUS-сервере, то:
    > - при политике "Разрешить" – доступ будет запрещен всем устройствам;
    > - при политике "Запретить" – доступ будет разрешен всем устройствам.

  - Доступ по спискам MAC-адресов на ТД – доступ к SSID будет осуществляться по локальным спискам MAC-адресов на точке доступа. Список определяется параметром "Группа MAC-адресов".

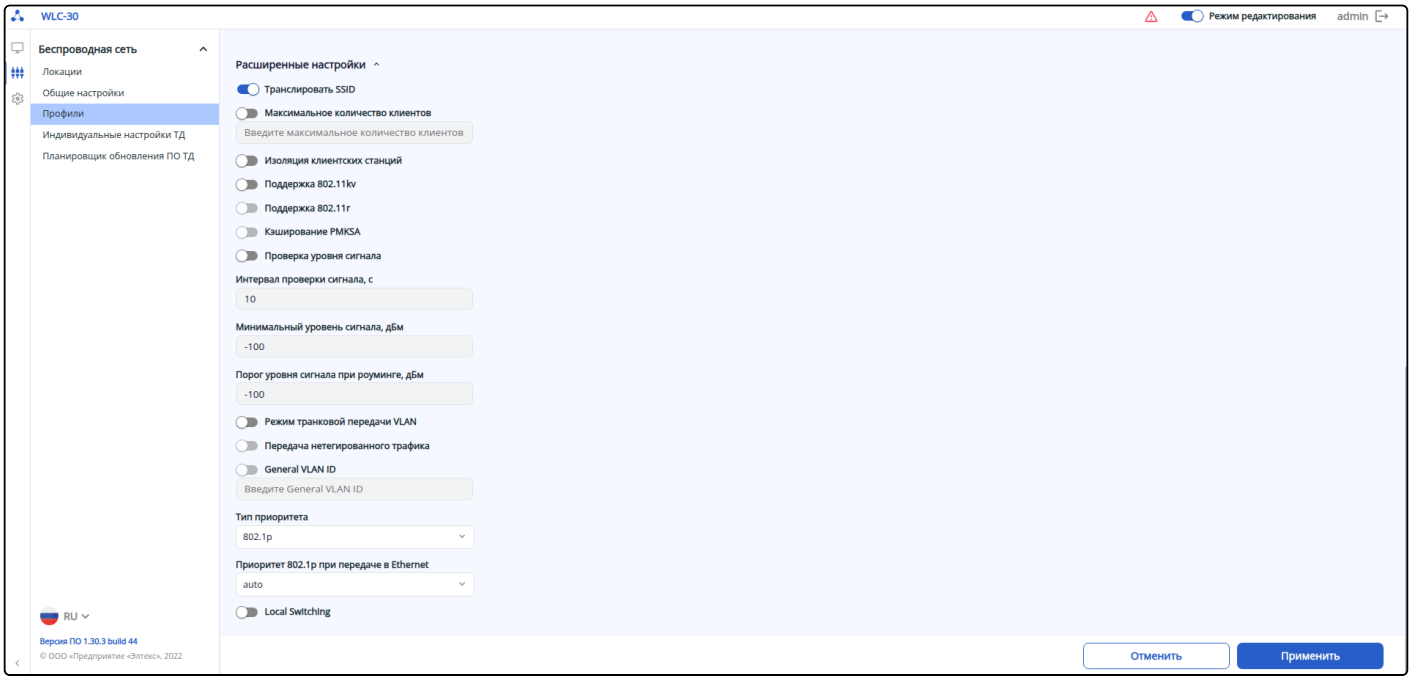
    > При режиме доступа по спискам MAC-адресов, в случае, если группа адресов не задана, то:
    > - при политике "Разрешить" – доступ будет разрешен всем устройствам;
    > - при политике "Запретить" – доступ будет запрещен всем устройствам.

- *Политика доступа* – выбор политики доступа к SSID. Настройка доступна только при включенной функции ограничения доступа по MAC. Возможные значения:

  - Разрешить – к данному SSID будет разрешено подключаться только тем клиентам, чьи MAC-адреса содержатся в списке на точке доступа или на RADIUS-сервере. Всем остальным доступ будет запрещен;
  - Запретить – к данному SSID будет запрещено подключаться только тем клиентам, чьи MAC-адреса содержатся в списке на точке доступа или на RADIUS-сервере. Всем остальным доступ будет разрешен.
- *Группа MAC-адресов* – выбор группы, содержащей список MAC-адресов клиентов, которым, в зависимости от политики доступа, разрешен или запрещен доступ к данному SSID. Настройка доступна только при включенной функции ограничения доступа по MAC и выбранном режиме доступа по спискам MAC-адресов на точке доступа. Создать список MAC-адресов в текущей версии контроллера возможно только через CLI, используя команду object-group mac.

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 General 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 1 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, выгрузку логов с ТД на TFTP-сервер и задавать настройки для портальной авторизации.

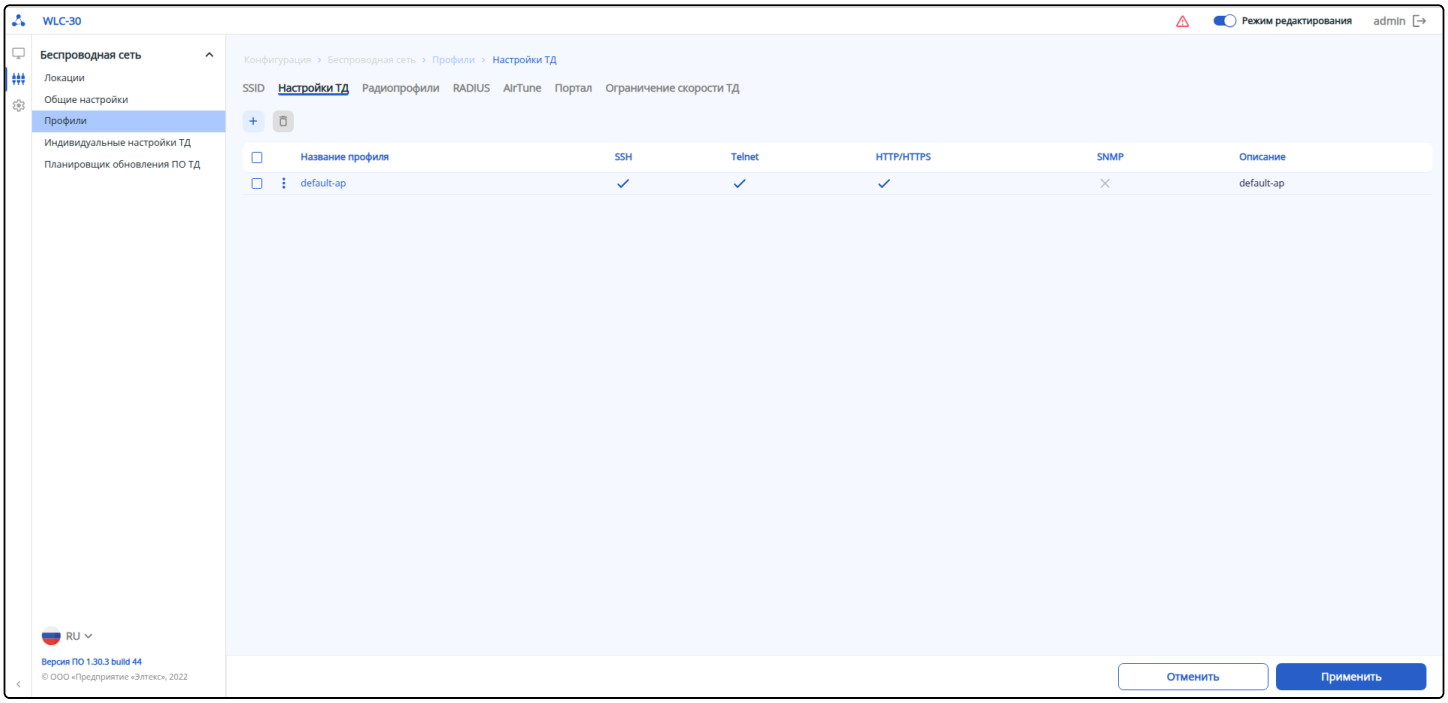
> Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

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.



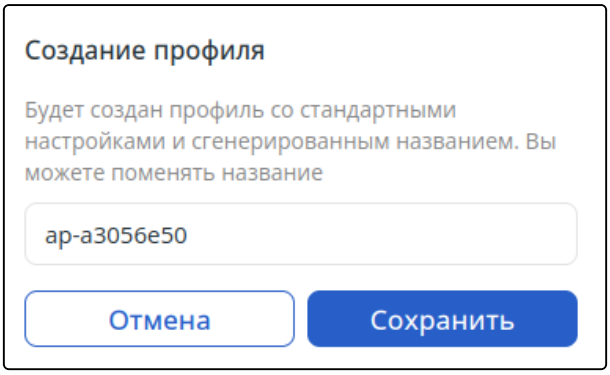
В заводской конфигурации уже создан профиль с названием «default-ap» со следующими параметрами:

- Описание: default_ap;
- Формат пароля: Encrypted;
- Пароль: 8CB5107EA7005AFF (password);
- Код страны: RU;
- 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: включен
  - 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.
- Портальная авторизация
  - IP-алиас ТД: отсутствует;
  - Переопределение названий параметров в URL перенаправления: отключено;
  - Сертификат: отсутствует;
  - Пароль приватного ключа: отсутствует;
  - Использовать HTTPS: отключено.
- Настройки логирования сервисов ТД: отключено у всех сервисов.

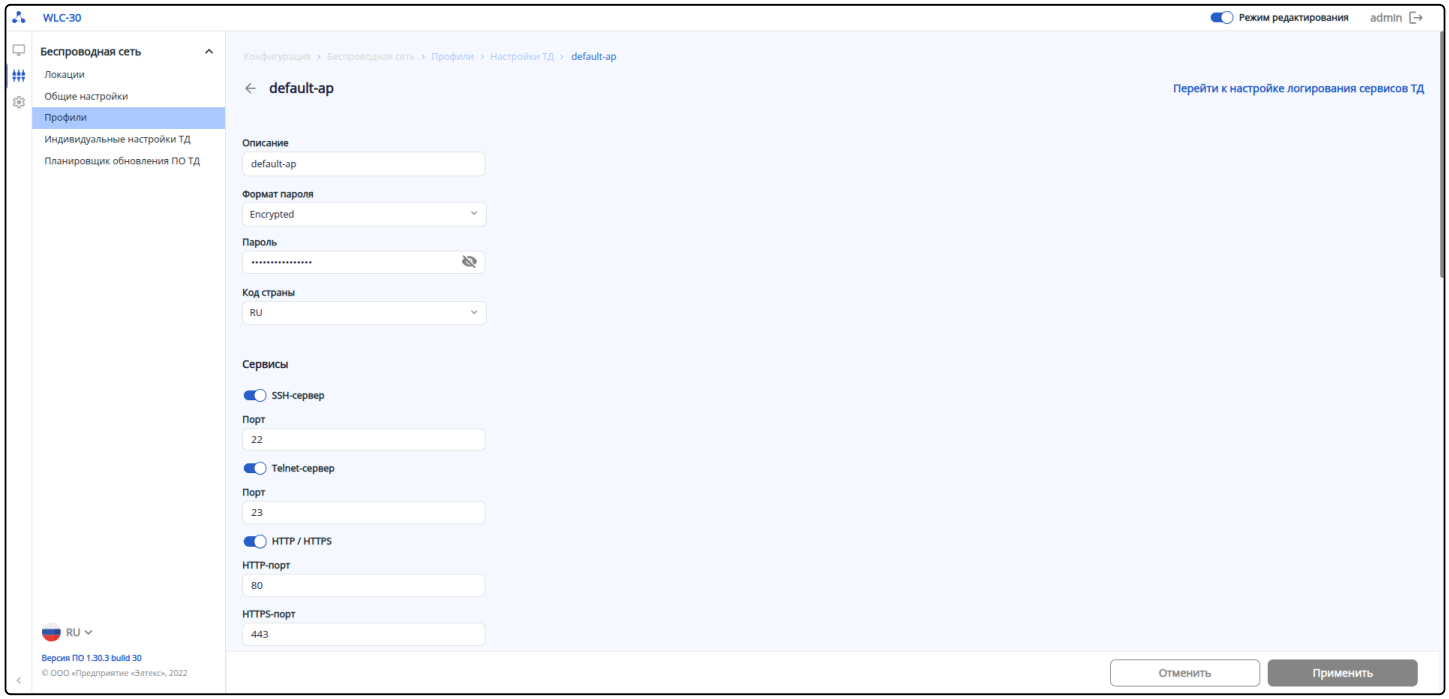
⚠ В заводской конфигурации в профиле default-ap все сервисы **SSH/Telnet/HTTP/HTTPS/SNMP выключены.**

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».



ℹ 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 разделе «Профиль настроек ТД», а также в разделе «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.
- *Код страны* – код названия страны, в которой работает точка доступа. В зависимости от выбранного значения будут применены ограничения к полосе частот и мощности передатчика, которые действуют в данной стране. Значение по умолчанию: RU (Россия). Возможные значения: RU.
- *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.

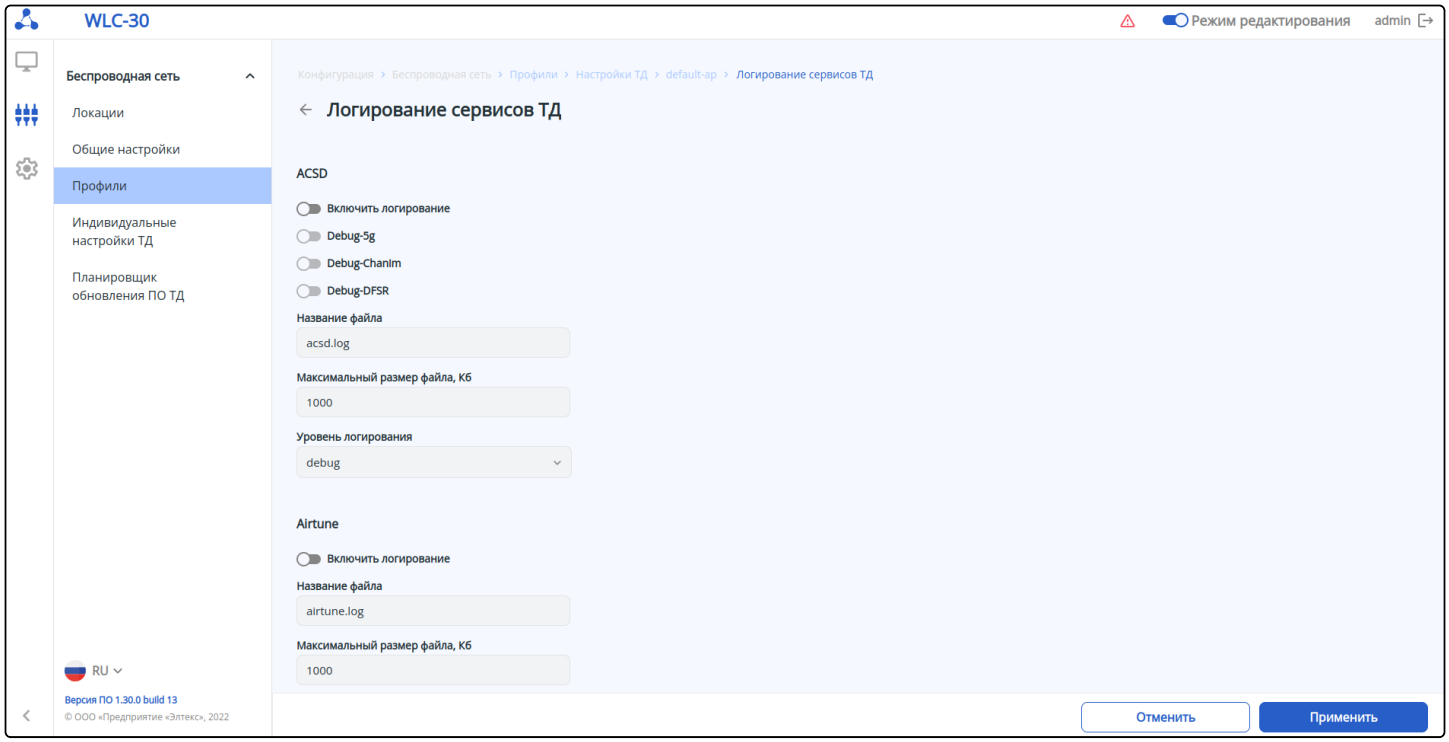
- *HTTP/HTTPS* – переключатель управляет возможностью подключения к web-конфигуратору ТД через HTTP и HTTPS. Значение по умолчанию: отключено. Возможные значения: включено/отключено:
  - *HTTP порт* – порт для подключения к web-конфигуратору ТД по HTTP. Значение по умолчанию: 80. Возможные значения: 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* – настройка параметров сервиса syslog:
  - Включить – 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* – настройка параметров автовыгрузки логов на с точки доступа на сервер TFTP:
  - *Включить* – 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.

- *Портальная авторизация* – настройка параметров портальной авторизации:
  - I*P-алиас ТД* – доменное имя, на которое будет совершаться перенаправление клиентов. Возможные значения: формат доменного имени до 63 символов. Если параметр не задан, будет использоваться значение "redirect.loc", заданное на точке доступа по умолчанию;
  - *Переопределение названий параметров в URL перенаправления* – после саморегистрации на внешнем портале (при авторизации через RADIUS) клиенту возвращается URL редиректа на точку доступа, который содержит параметры: username, password, redirect_url, error_url. Если портал будет использовать другие названия для параметров, необходимо задать в данном разделе новые названия, чтобы точка доступа могла их корректно обработать для проведения авторизации через RADIUS:
    - H*овое название параметра "error-url"* – новое название для параметра, содержащего URL, куда будет переадресован клиент в случае ошибки авторизации. Значение по умолчанию: отсутствует. Возможные значения: строка до 255 символов.
    - *Новое название параметра "redirect-url"* – новое название параметра, содержащего исходный URL, запрошенный клиентом. Клиент будет переадресован на данный URL в случае успешной авторизации. Значение по умолчанию: отсутствует. Возможные значения: строка до 255 символов;
    - *Новое название параметра "password"* – новое название параметра, содержащего пароль для клиента. Значение по умолчанию: отсутствует. Возможные значения: строка до 255 символов;
    - *Новое название параметра "username"* – новое название параметра, содержащего имя пользователя. Значение по умолчанию: отсутствует. Возможные значения: строка до 255 символов;
  - *Сертификат* – выбор или загрузка сертификата для шифрования трафика при перенаправлении клиента на точку доступа при портальной авторизации. Сертификат должен быть для домена, указанного в параметре IP-алиас ТД;
  - *Формат пароля* – параметр, определяющий в каком формате далее будет задан пароль приватного ключа сертификата. Значение по умолчанию: Clear-Text.
    Возможные значения:
    - Clear-Text;
    - Encrypted.
  - *Пароль приватного ключа* – пароль приватного ключа сертификата для портальной авторизации. 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 – задается хеш пароля по алгоритму sha512 строкой от 16 до 128 символов в формате HEX;
  - *Использовать HTTPS* – переключатель активирует использование протокола HTTPS для перенаправления клиентов на точку доступа при портальной авторизации.

Логирование сервисов ТД

Страница настроек трассировки сервисов точек доступа открывается по ссылке «Перейти к режиму настройки логирования сервисов ТД» 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 для сервисов **ACSD, Airtune, Captive Portal APBD, MonitorD, NetworkD**:
  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.

Возможные значения для сервисов **Band Steer, Captive Portal**:
error – лог будет записываться с уровнем error;
warn – лог будет записываться с уровнем warning;
debug – лог будет записываться с уровнем debug.

Возможные значения для сервиса **Hostapd**:
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;
excessive – лог будет записываться с уровнем excessive;
msgdump – лог будет записываться с уровнем msgdump.

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».

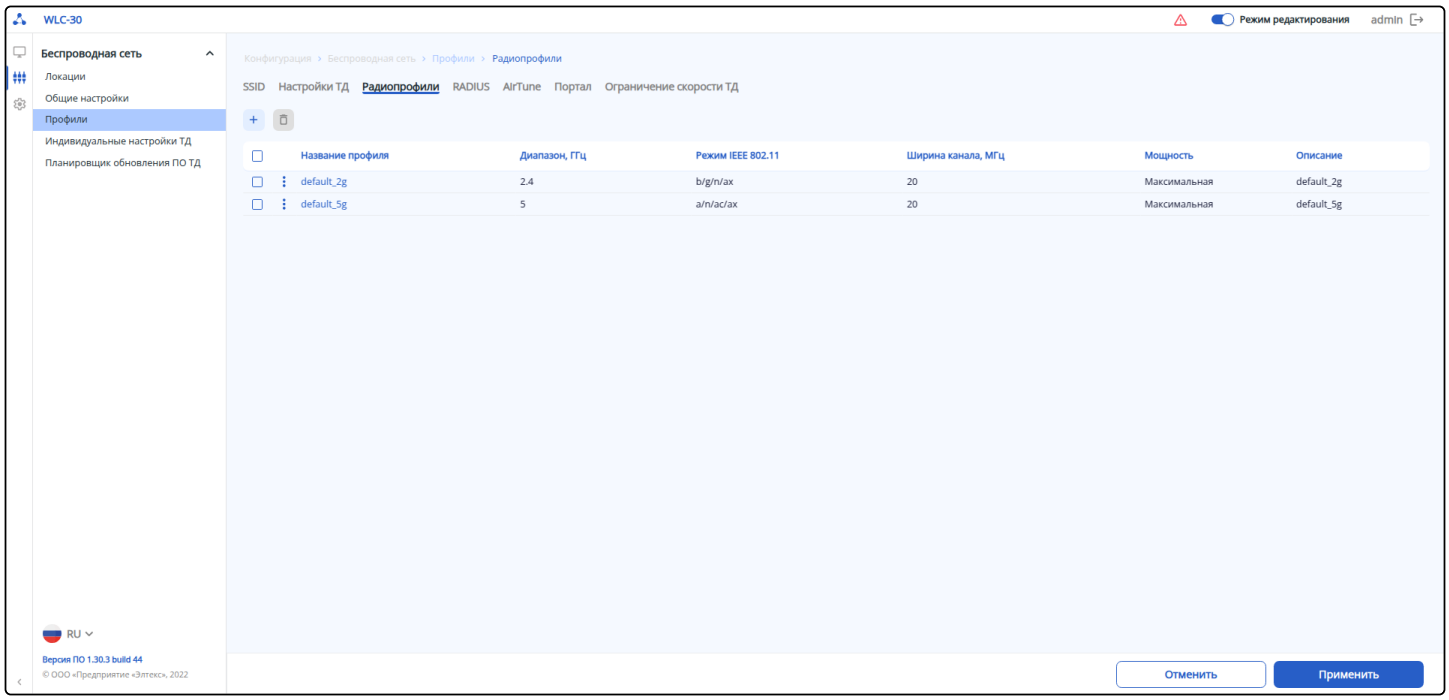
Радиопрофили

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;
- OBSS Coexistence: отключено;
- Мощность: максимальная;
- Список каналов: 1,6,11;
- Режим работы DHCP Snooping: оставить опцию 82 без изменений.

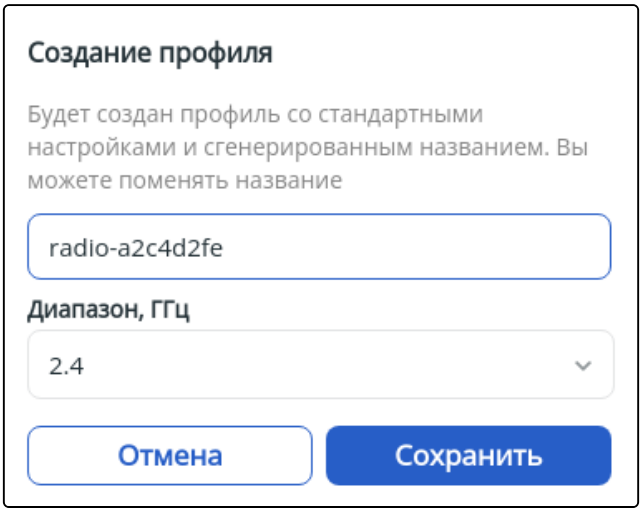
Профиль default_5g

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

- Режим работы DHCP Snooping: оставить опцию 82 без изменений.

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
WEP-3L	11	12	13	15	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
WEP-30L-Z	0	4	8	12	16
WOP-30L	0	4	8	12	16
WOP-30LI	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
WEP-3L	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
WEP-30L-Z	0	5	10	15	19
WOP-30L	0	5	10	15	19
WOP-30LI	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

- *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; DFS-каналы доступны для выбора;
  - disabled – механизм выключен. DFS-каналы не доступны для выбора;
  - forced – механизм выключен. DFS-каналы доступны для выбора;
- *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.
- *Режим работы DHCP Snooping* – действие, применяемое к 82 опции DHCP. Значение по умолчанию: оставить опцию 82 без изменений. Возможные значения:
  - Оставить опцию 82 без изменений – опция 82 не обрабатывается точкой доступа, будет использовано значение опции, указанное в запросах от клиента, если таковое имеется;
  - Удалить опцию 82 – значение опции 82 будет удалено точкой доступа;
  - Заменить опцию 82 – значение опции 82 будет изменено/добавлено точкой доступа.
    При выборе данного значения для настройки открываются параметры:
    - Формат Circuit ID опции 82 DHCP – замена значения параметра Circuit ID. Значение по умолчанию: MAC-адрес ТД + SSID. Возможные значения:
      - MAC-адрес ТД + SSID – замена значения параметра Circuit ID на MAC-адрес точки доступа и название SSID в формате <MAC-адрес ТД>-<SSID>;
      - SSID – замена значения параметра Circuit ID на название SSID;
      - Другой – замена значения параметра Circuit ID на значение, указанное в параметре "Circuit ID";
        - Circuit ID – произвольное значение, которое будет передаваться в Circuit ID. Значение по умолчанию: отсутствует. Возможные значения: строка до 52 символов.
    - Формат Remote ID опции 82 DHCP – замена значения параметра Remote ID. Значение по умолчанию: MAC-адрес клиента. Возможные значения:

- MAC-адрес ТД – замена значения параметра Remote ID на MAC-адрес ТД;
- MAC-адрес клиента – замена значения параметра Remote ID на MAC-адрес клиента;
- Локация – замена значения параметра Remote ID на название локации;
- Другой – замена значения параметра Remote ID на значение, указанное в параметре "Remote ID";
    - Remote ID – произвольное значение, которое будет передаваться в Remote ID. Значение по умолчанию: отсутствует. Возможные значения: строка до 63 символов.
- Формат MAC-адреса для опции 82 DHCP – определяет разделитель октетов MAC-адреса, который передается в Circuit ID и/или Remote ID. Значение по умолчанию: XX:XX:XX:XX:XX:XX. Возможные значения:
    - XX:XX:XX:XX:XX:XX – в качестве разделителя выступает знак двоеточия;
    - XX-XX-XX-XX-XX-XX – в качестве разделителя выступает знак тире;

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».

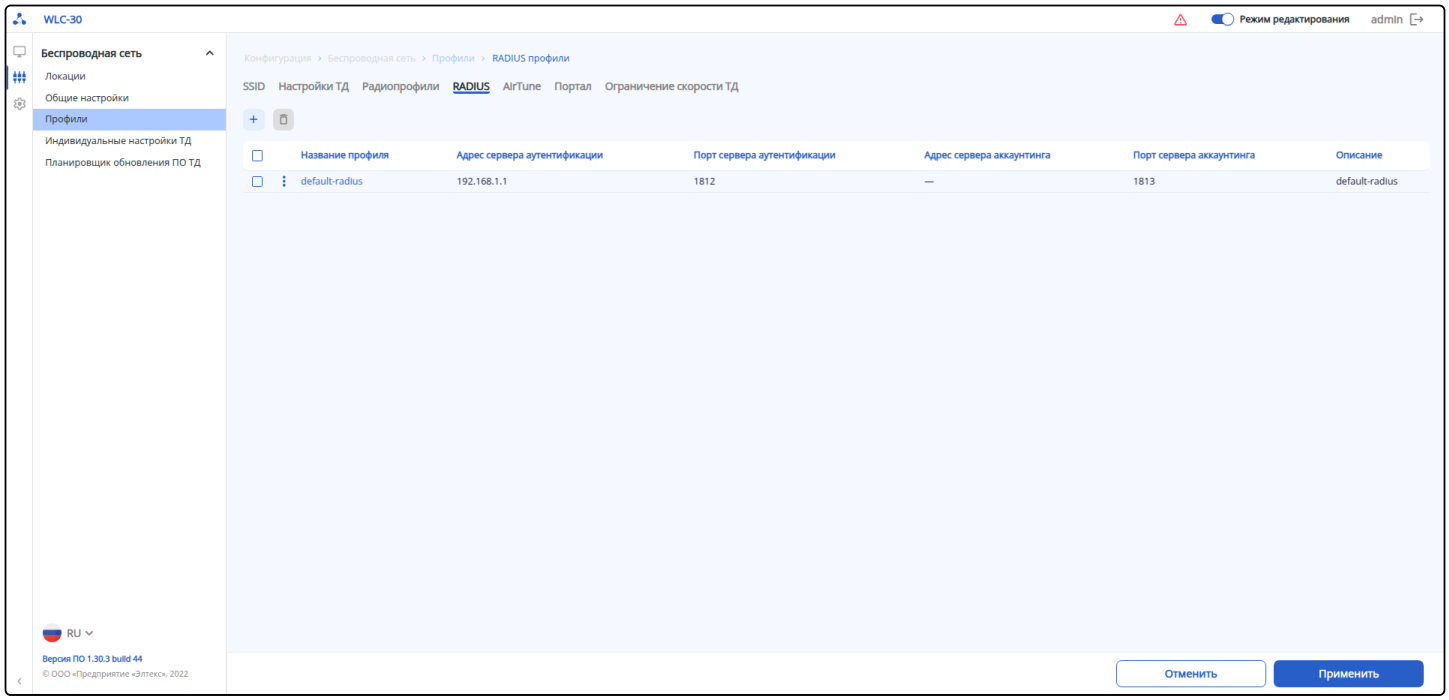
RADIUS

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

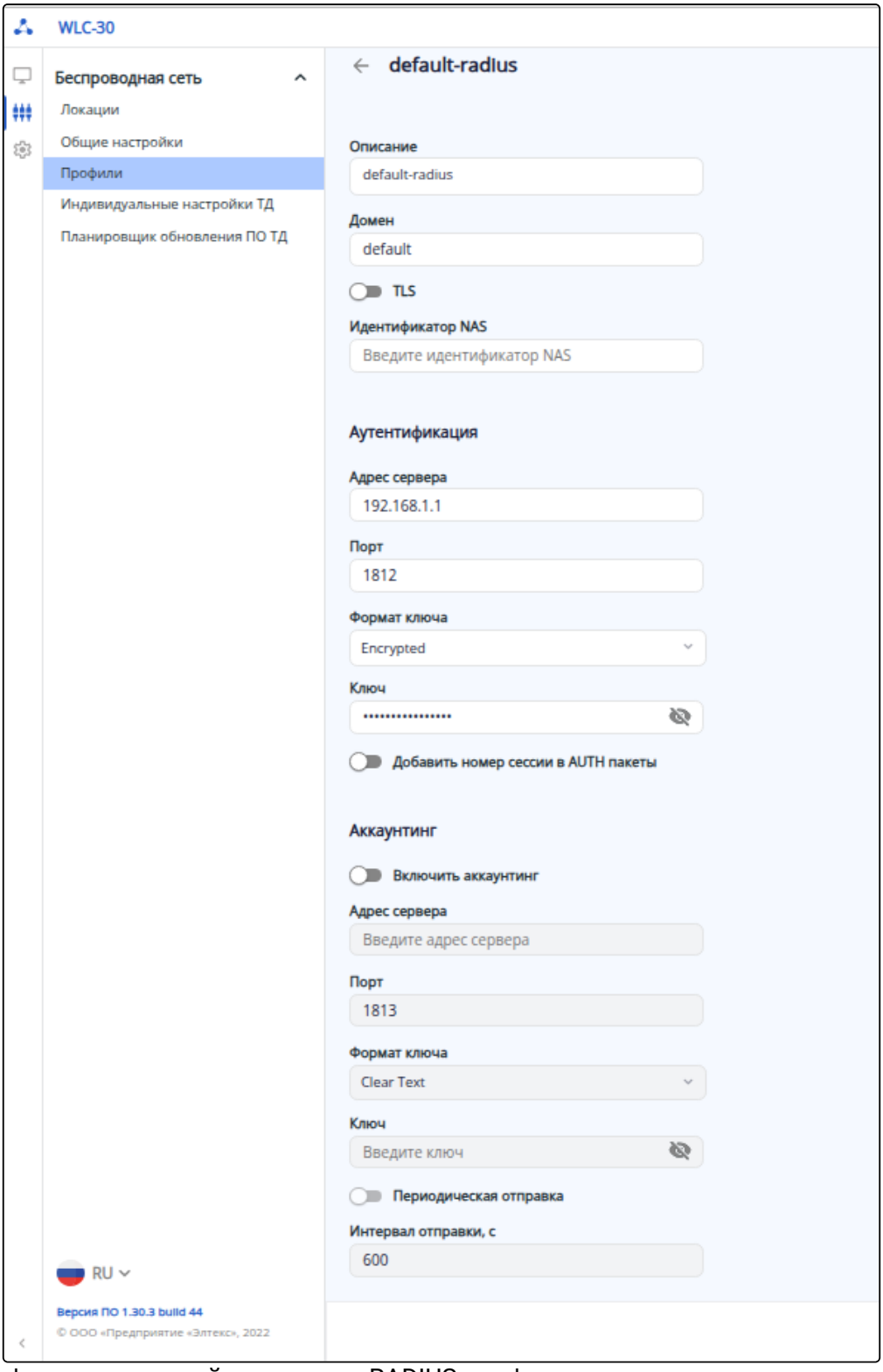
> Для создания, удаления и редактирования профиля должен быть включен режим редактирования.

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;
- Идентификатор NAS: отсутствует.

Аутентификация:

- Адрес сервера: 192.168.1.1;

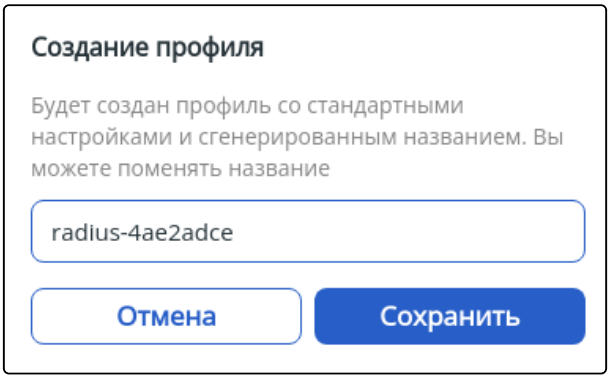
- Порт: 1812;
- Формат ключа: Encrypted;
- Ключ (хеш): 8CB5107EA7005AFF
- Добавить номер сессии в AUTH-пакеты: отключено.

Аккаунтинг:

- Включить аккаунтинг: отключено;
- Адрес сервера: отсутствует;
- Порт: 1813;
- Формат ключа: Clear Text;
- 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;
- *Идентификатор NAS* – идентификатор NAS. Если параметр не определен, то в качестве идентификатора NAS в RADIUS и HTTP(S) пакетах будет использоваться MAC-адрес точки доступа. Возможные значения: строка до 235 символов, кроме символа ' " '.

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 64 символов;
  - если выбран формат ключа Encrypted – задается хеш ключа по алгоритму sha512 строкой от 16 до 128 символов.

⚠ Ключ является обязательным параметром при создании RADIUS-профиля.

- *Добавить номер сессии в AUTH пакеты* – переключатель активирует передачу идентификатора сессии аккаунтинга в запросах аутентификации Access-Request на RADIUS. 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 64 символов;
  - если выбран формат ключа Encrypted – задается хеш ключа по алгоритму sha512 строкой от 16 до 128 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

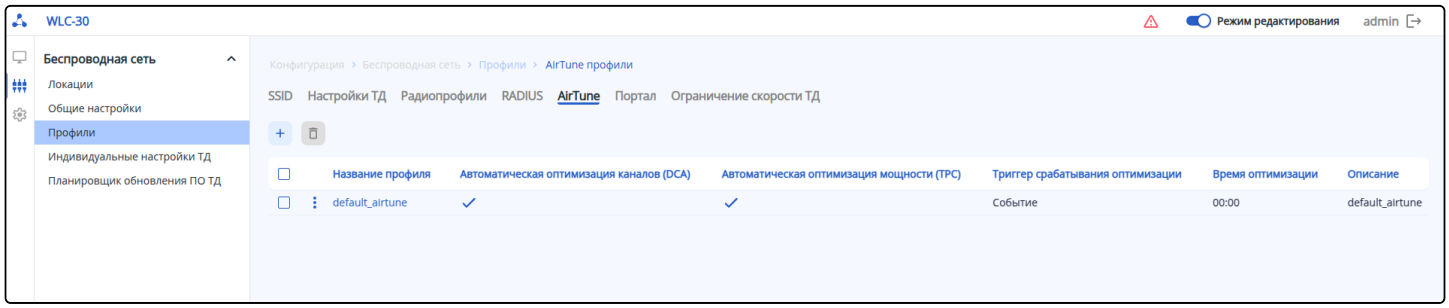
На странице представлены в виде таблицы профили Airtune, имеющиеся в конфигурации. Профили работы данного сервиса позволяют автоматически настраивать такие параметры радиоинтерфейсов точек доступа, как мощность и каналы, а также позволяют управлять балансировкой клиентов и настройками роуминга.

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

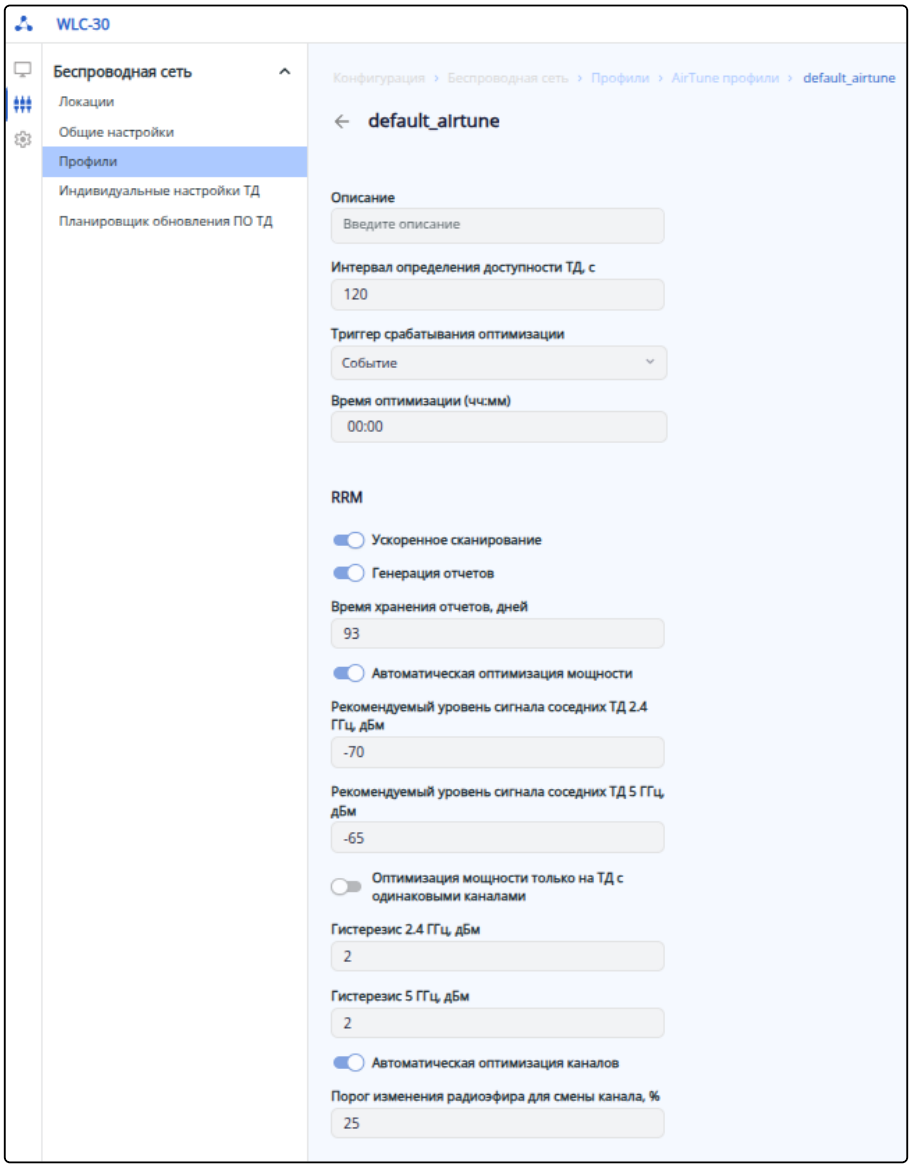
Если Airtune-профиль добавлен в локацию, некоторые параметры радиоинтерфейсов точек доступа в данной локации будут находиться под управлением airtune (если Airtune так же включен глобально на странице «Общие настройки»). Соответственно, когда Airtune включен в локации, менять параметры, связанные с мощностью 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.

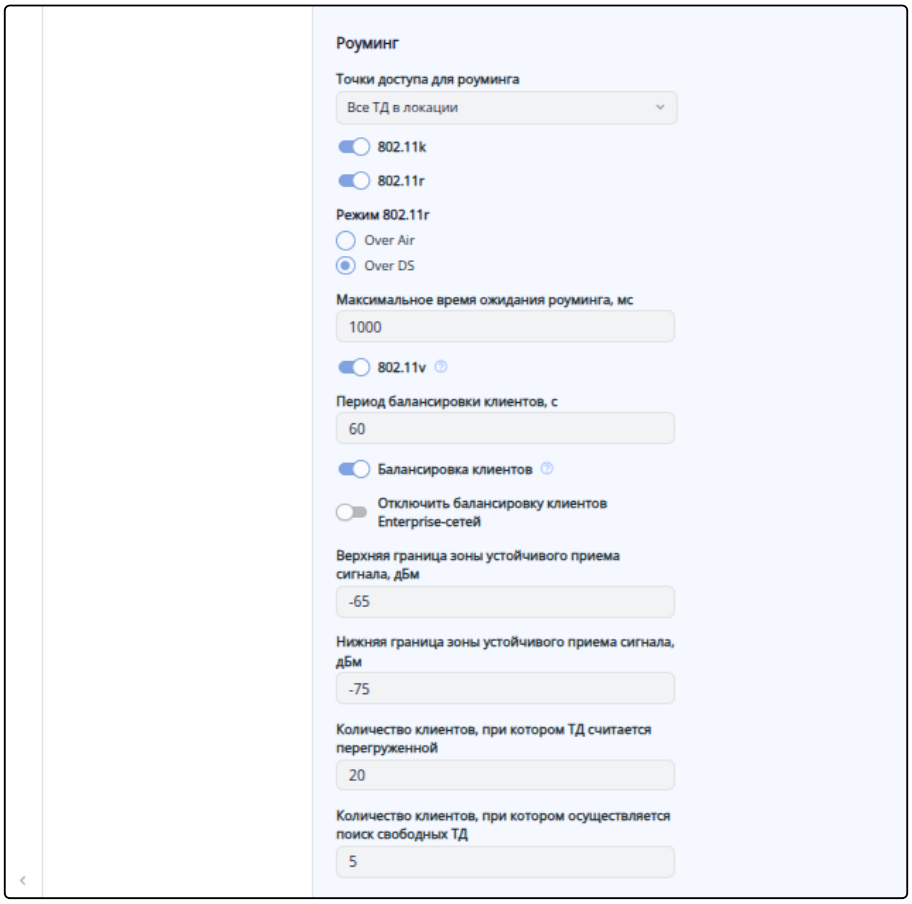
В таблице содержатся основные параметры для каждого профиля, такие как:

- 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.


WLC-30
Беспроводная сеть
Локации
Общие настройки
Профили
Индивидуальные настройки ТД
Планировщик обновления ПО ТД
Конфигурация › Беспроводная сеть › Профили › AirTune профили › default_airtune
default_airtune
Описание
Введите описание
Интервал определения доступности ТД, с
120
Триггер срабатывания оптимизации
Событие
Время оптимизации (чч:мм)
00:00
RRM
Ускоренное сканирование
Генерация отчетов
Время хранения отчетов, дней
93
Автоматическая оптимизация мощности
Рекомендуемый уровень сигнала соседних ТД 2.4 ГГц, дБм
-70
Рекомендуемый уровень сигнала соседних ТД 5 ГГц, дБм
-65
Оптимизация мощности только на ТД с одинаковыми каналами
Гистерезис 2.4 ГГц, дБм
2
Гистерезис 5 ГГц, дБм
2
Автоматическая оптимизация каналов
Порог изменения радиоэфира для смены канала, %
25



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

Общие:

- Описание: default-airtune;
- Интервал определения доступности ТД: 120 с;
- Триггер срабатывания оптимизации: событие;
- Время оптимизации: 00:00.

RRM:

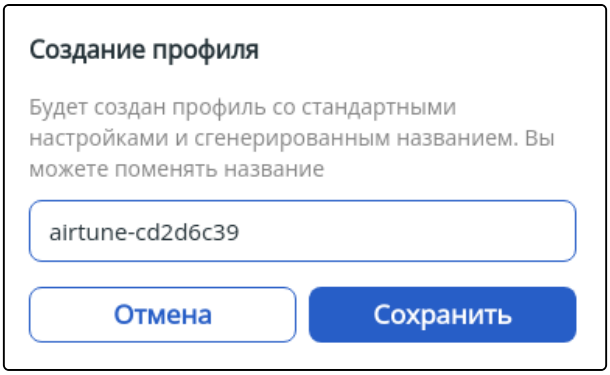
- Ускоренное сканирование: включено;
- Генерация отчетов: включено;
- Время хранения отчетов: 93 дня;
- Автоматическая оптимизация мощности: включено;
- Рекомендуемый уровень сигнала соседних ТД 2.4 ГГц: -70 дБм;
- Рекомендуемый уровень сигнала соседних ТД 5 ГГц: -65 дБм;
- Оптимизация мощности только 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;
- 802.11v: включено;
- Период балансировки клиентов: 60 с;

- 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.

⚠ Параметры "802.11v" и "Период балансировки клиентов" актуальны только для точек доступа WEP-1L, WEP-2L, WOP-2L, WOP-20L, WEP-200L, WEP-3L, WEP-30L, WEP-30L-Z, WOP-30L, WOP-30LS, WOP-30LI, WEP-3ax.

- *802.11v* – переключатель активирует функционал роуминга стандарта 802.11v и балансировку клиентов по всем ТД в локации. Функционал работает совместно со стандартом 802.11k, роуминг осуществляется по общим спискам. Для его работы в SSID-профиле должна быть включена опция 802.11kv. Помимо помощи роумингу клиента в соответствии со стандартом 802.11v, активируется работа балансировки клиентов. Переключение клиентов на другие ТД работает в зависимости от пороговых значений, установленных в параметрах *"Количество клиентов, при котором ТД считается перегруженной"* и *"Количество клиентов, при котором осуществляется поиск свободных ТД"*. Если количество клиентов на ТД превысило значение, указанное в параметре *"Количество клиентов, при котором осуществляется поиск свободных ТД"*, то AirTune понизит приоритет данной ТД в списках 802.11k/v для подключения новых пользователей, и разошлет информацию об этом всем её соседям. Если количество клиентов на ТД превысило значение, указанное в параметре *"Количество клиентов, при котором ТД считается перегруженной"*, то AirTune понизит приоритет данной ТД до нуля и исключит ее из рассылки возможных ТД для роуминга. А также начнет рекомендовать "нагруженной" ТД переключить нескольких клиентов на соседние ТД по стандарту 802.11v. Последует клиентское устройство совету точки доступа или нет, гарантировать невозможно, так как в конечном счете решение о переключении на другую точку доступа принимает клиентская сторона. Данный вид роуминга доступен только для тех клиентских устройств, которые поддерживают 802.11v. Значение по умолчанию: включено.
  Возможные значения: включено/отключено.
- *Период балансировки клиентов* – период балансировки клиентов между точками доступа в рамках стандарта 802.11v. Значение по умолчанию: 60 с. Возможные значения: от 0 до 86400 секунд.

⚠ Параметры "Балансировка клиентов", "Отключить балансировку клиентов Enterprise-сетей", "Верхняя граница зоны устойчивого приема сигнала" и "Нижняя граница зоны устойчивого приема сигнала" актуальны только для точек доступа WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:revB и WOP-2ac:rev.C.

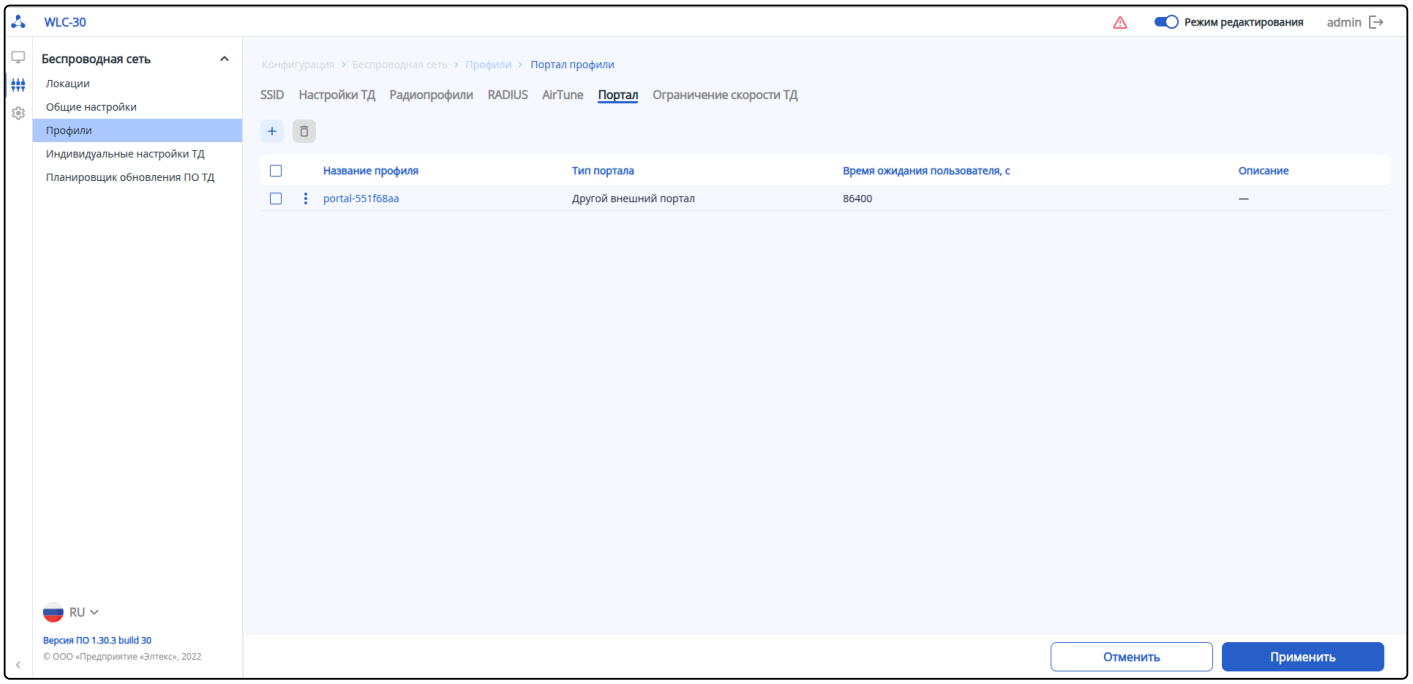
- *Балансировка клиентов* – переключатель активирует балансировку клиентов по всем ТД в домене, независимо от их фактического расположения. Функционал нужен для равномерного распределения клиентов между ТД, чтобы избежать перегрузки одной из ТД, если в зоне видимости клиента есть более свободная ТД. 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».

Портал

На данной странице в виде таблицы представлены профили настроек портальной авторизации, имеющиеся в конфигурации.

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

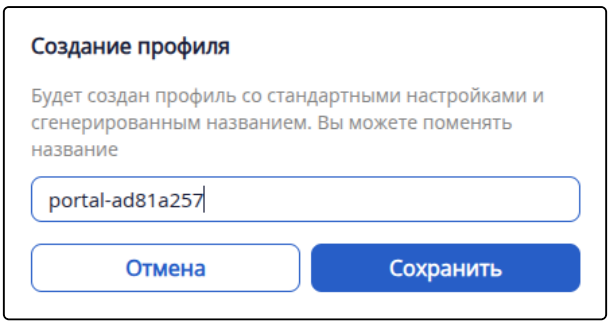


В таблице содержатся основные параметры для каждого профиля, такие как:

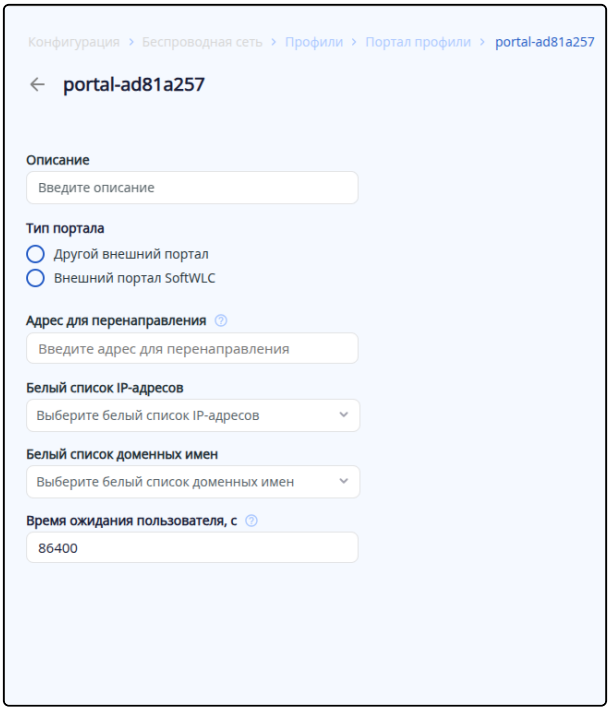
- Название профиля;
- Тип портала;
- Время ожидания пользователя;
- Описание профиля.

В заводской конфигурации профили портала отсутствуют.

Для создания профиля портала 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».



Профиль настроек портала



Страница содержит следующие параметры:

- *Описание* – описание для профиля настроек портала. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Тип портала* – параметр, определяющий, какой портал будет использоваться для авторизации пользователей. Значение по умолчанию: отсутствует.
  Возможные значения:
  - *Другой внешний портал* – режим интеграции со сторонним внешним порталом при авторизации через RADIUS.
  - *Внешний портал SoftWLC* – режим интеграции с внешним порталом Eltex, входящим в состав SoftWLC.
- *Адрес для перенаправления* – адрес внешнего виртуального портала, на который будет перенаправлен пользователь при подключении к беспроводной сети. Значение по умолчанию: отсутствует. Примеры задания URL:
  - для внешнего портала SoftWLC: https://192.168.0.1:8080/eltex_portal/. URL содержит адрес портала, порт и путь.
  - для другого внешнего портала:
    - URL без параметров: https://eltex-co.ru.
      Когда URL указывается без параметров, к нему автоматически добавляются параметры таким образом, что результирующий URL для указанного примера будет иметь вид:
      https://eltex-co.ru/?switch_url=<SWITCH_URL>&ap_mac=<AP_MAC>&client_mac=<CLIENT_MAC>&wlan=<SSID>&redirect=<ORIGINAL_URL>
      Добавленные параметры URL имеют следующие значения:
      switch_url – URL для перенаправления клиента после авторизации на портале;
      ap_mac – MAC-адрес точки доступа, к которой подключен клиент;
      client_mac – MAC-адрес клиента;
      wlan – название SSID, к которому подключен клиент;
      redirect – URL, который клиент запрашивал первоначально.
    - URL с параметрами: https://eltex-co.ru/?action_url=<SWITCH_URL>&ap_addr=<AP_MAC>&client_addr=<CLIENT_MAC>&ssid_name=<SSID>&red_url=<ORIGINAL_URL>&nas_id=<NAS_ID>&nas_ip=<NAS_IP>
      Используется, если необходимо изменить названия для параметров, которые подставляются автоматически, или дополнить URL другими параметрами. В этом случае URL задается полностью со всеми параметрами, используя необходимые

названия. Он может содержать один или несколько плейсхолдеров определенного формата: <SWITCH_URL>, <AP_MAC>, <CLIENT_MAC>, <SSID>, <ORIGINAL_URL>, <NAS_ID>, <NAS_IP>.

- *Название виртуального портала* − название портала, сконфигурированного на SoftWLC, на который будет перенаправлен пользователь при подключении к беспроводной сети. Задается только если тип портала установлен "Внешний портал SoftWLC". Возможные значения: строка до 235 символов. Значение по умолчанию: отсутствует;
- *Белый список IP-адресов* − выбор группы, содержащей IP-адреса, к которым пользователю разрешен доступ до авторизации. Параметр необязательный. Адрес портала добавляется в белый список автоматически, поэтому задавать его не требуется. Значение по умолчанию: отсутствует;
- *Белый список доменных имен* − выбор группы, содержащей доменные имена (или регулярные выражения), к которым пользователю разрешен доступ до авторизации. Параметр необязательный. Адрес портала добавляется в белый список автоматически, поэтому задавать его не требуется. Значение по умолчанию: отсутствует;

В WEB-интерфейсе возможен только выбор уже существующей группы белых списков. Задать группу адресов можно через интерфейс CLI в разделах object-group network и object-group url.

- *Время ожидания пользователя* — временной интервал, в течение которого точка доступа хранит информацию об отключенном беспроводном клиенте и не проводит MAB-авторизацию при повторном его подключении. Возможные значения: от 0 до 604800. При установке значения "0" точка доступа будет хранить информацию о клиенте до тех пор, пока не будет перезагружена. Значение по умолчанию: 86400;

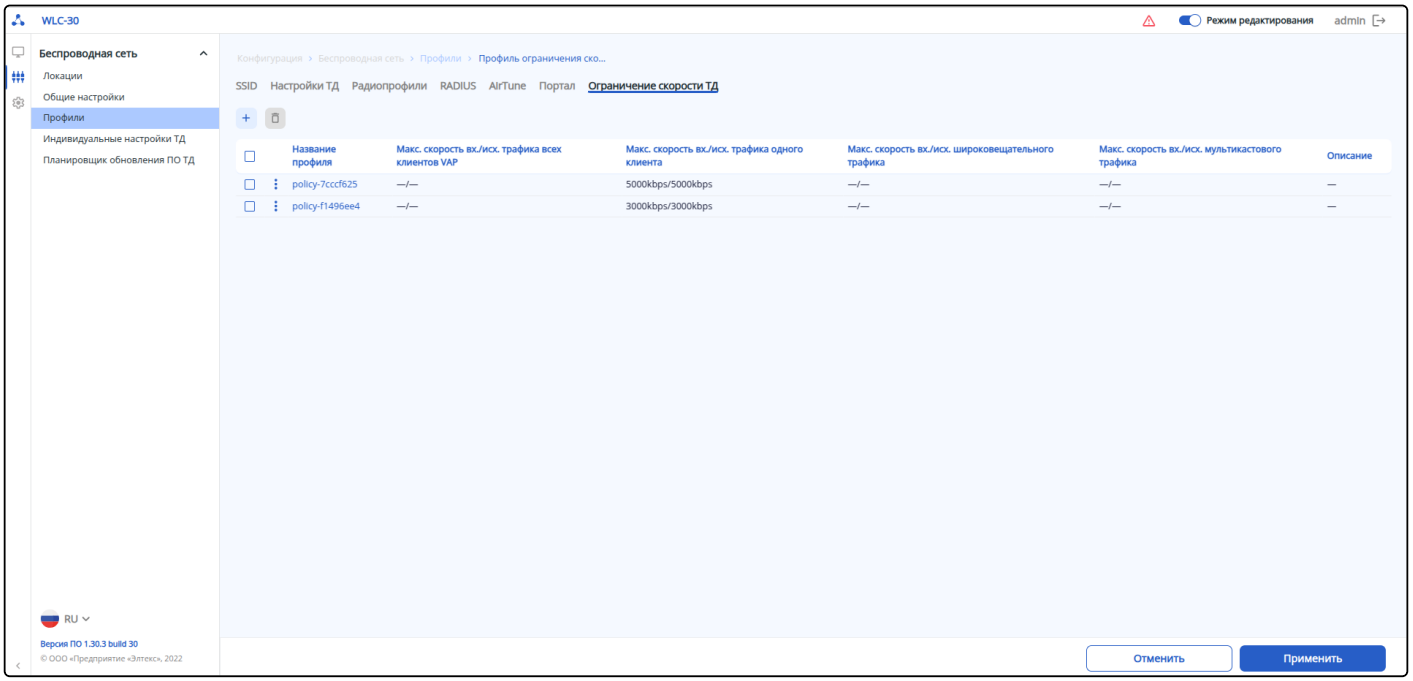
После настройки параметров сохраните, а затем примените конфигурацию с помощью соответствующих кнопок. При необходимости отмените изменения и удалите их с помощью кнопок «Сбросить» и «Отменить».

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

Ограничение скорости ТД

На данной странице в виде таблицы представлены имеющиеся в конфигурации профили настроек ограничения скорости, которое выполняется точкой доступа. Данные профили позволяют управлять максимальной скоростью входящего и исходящего трафика для одного клиента, для всех клиентов, подключенных к VAP, а также ограничивать скорость широковещательного и мультикастового трафика.

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

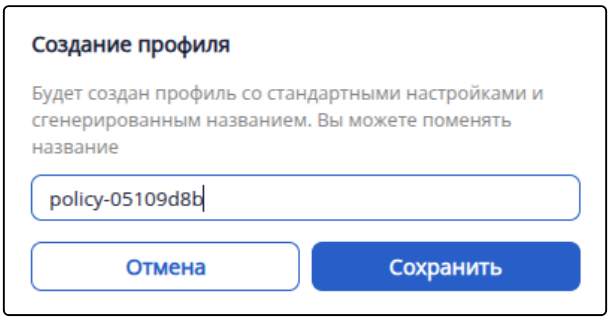


В таблице содержатся основные параметры для каждого профиля, такие как:

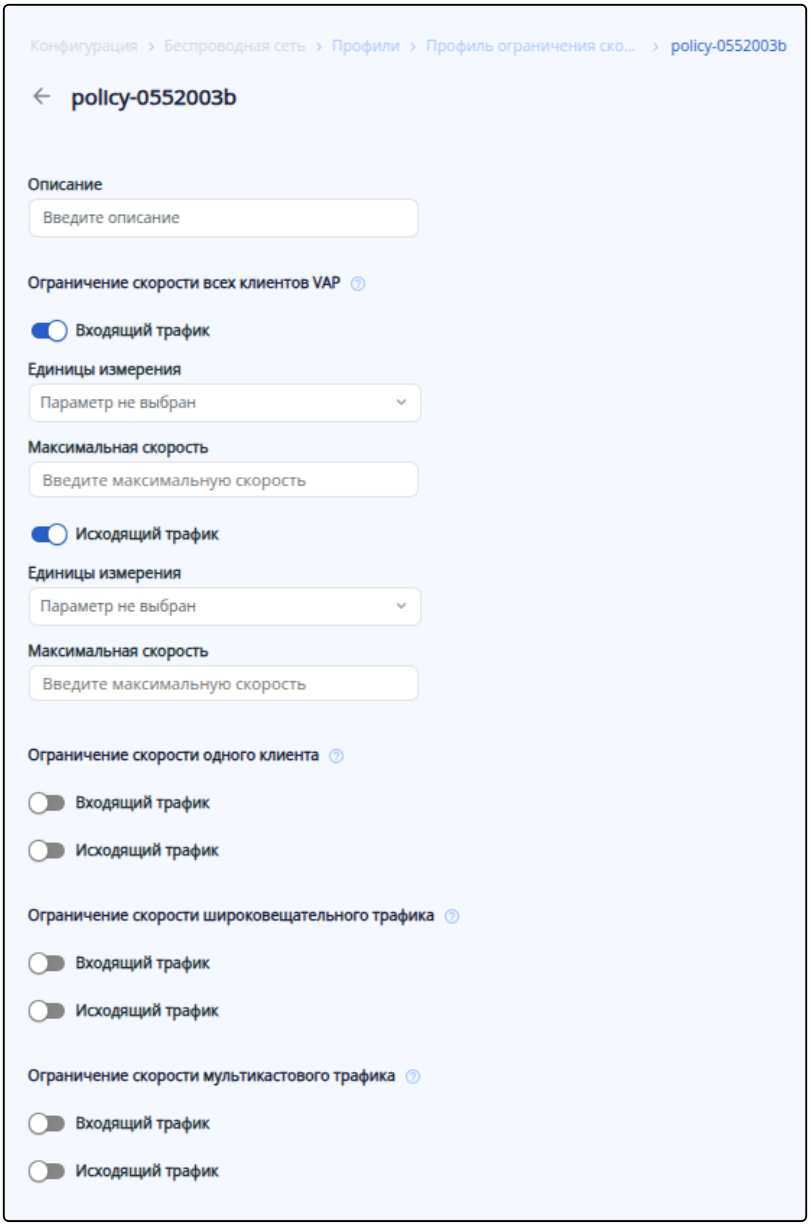
- Название профиля;
- Максимальная скорость входящего и исходящего трафика всех (в сумме) беспроводных клиентов виртуальной точки доступа (VAP);
- Максимальная скорость входящего и исходящего трафика для каждого беспроводного клиента;
- Максимальная скорость входящего и исходящего широковещательного трафика;
- Максимальная скорость входящего и исходящего мультикастового трафика;
- Описание профиля.

В заводской конфигурации профили ограничения скорости отсутствуют.

Для создания профиля ограничения скорости 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».



Профиль ограничения скорости



Страница содержит:

- *Описание* − описание для профиля ограничения скорости. Возможные значения: строка до 255 символов. Значение по умолчанию: отсутствует;
- *Описание разделов:*
- "Ограничение скорости всех клиентов VAP" − позволяет задать ограничение скорости для всех беспроводных клиентов (в сумме) одной виртуальной точки доступа (VAP), на которой установлен SSID с данным профилем. Настройка не поддерживается на точках доступа WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C;
- "Ограничение скорости одного клиента" − позволяет задать ограничение скорости для каждого беспроводного клиента виртуальной точки доступа (VAP), на которой установлен SSID с данным профилем. Настройка не поддерживается на точках доступа WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C;
- "Ограничение скорости широковещательного трафика" − позволяет задать ограничение скорости для широковещательного трафика. Настройка не поддерживается на точках доступа WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C и WEP-3ax;
- "Ограничение скорости мультикастового трафика" − позволяет задать ограничение скорости для многоадресного трафика. Настройка не поддерживается на точках доступа WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac:rev.B, WOP-2ac:rev.C и WEP-3ax.

В каждом разделе задаются параметры ограничения скорости для входящего и/или исходящего трафика:

- Входящий трафик − переключатель активирует ограничение скорости для трафика, идущего к беспроводному клиенту. Значение по умолчанию: отключено;
- Исходящий трафик − переключатель активирует ограничение скорости для трафика, идущего от беспроводного клиента. Значение по умолчанию: отключено;
- Единицы измерения − выбор единиц измерения для значения максимальной скорости, задаваемой ниже. Значение по умолчанию: отсутствует. Возможные значения: kbps (Кбит/с); pps (пакет в секунду);
- Максимальная скорость − ограничение скорости. Значение по умолчанию: отсутствует. Возможные значения: от 0 до 2000000000;

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.

Подменю «Индивидуальные настройки ТД»

На данной странице в виде таблицы представлены основные настройки индивидуальных профилей ТД. Профили создаются персонально для каждой точки доступа при необходимости переопределения на ней общих параметров радиоинтерфейсов, локации, профиля настроек ТД, работы Airtune или для задания имени устройства. В качестве названия профиля используется MAC-адрес точки доступа.

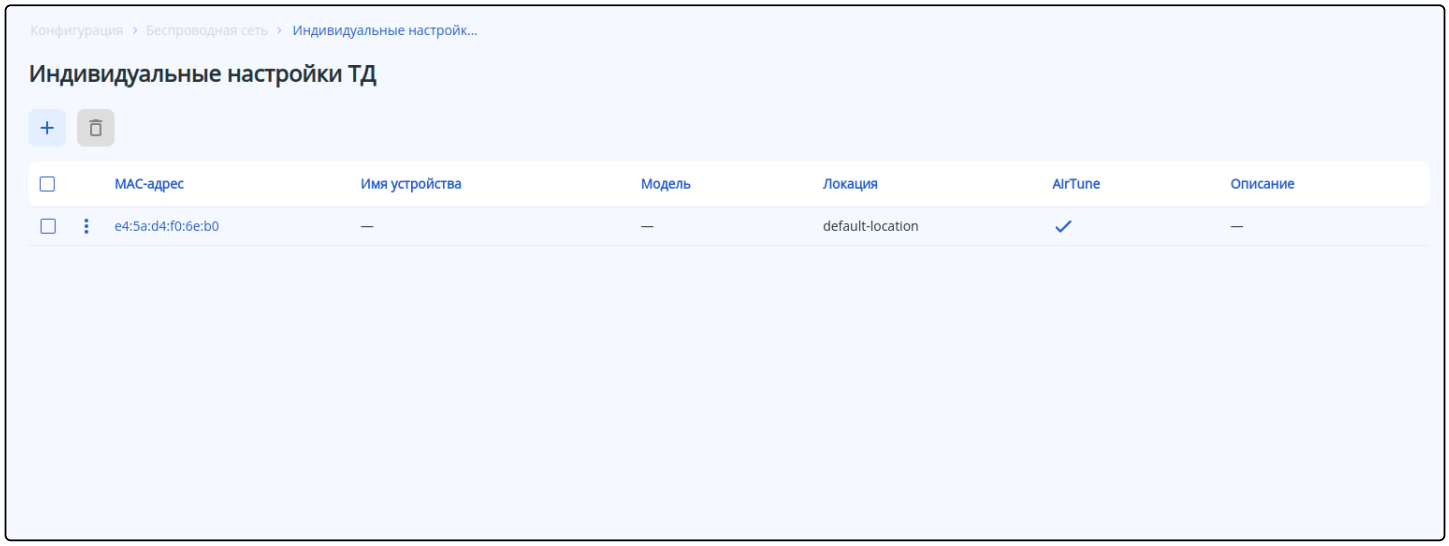


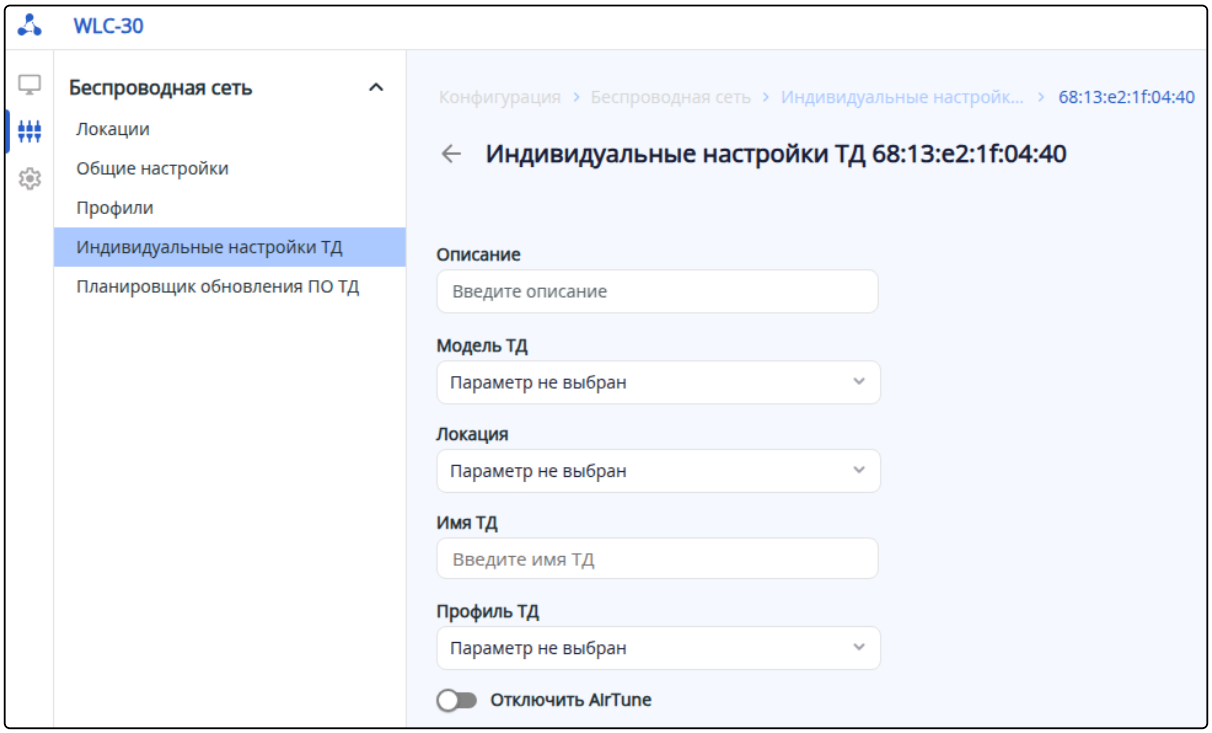
Таблица содержит данные:

- *MAC-адрес ТД* − MAC-адрес точки доступа;
- *Имя устройства* − имя точки доступа;
- *Модель* − модель точки доступа;
- *Локация* − название локации, к которой относится точка доступа;
- *AirTune* − статус AirTune (по умолчанию включен);
- *Описание* − описание профиля индивидуальных настроек точки доступа.

Для создания нового профиля настроек используйте кнопку «Создать индивидуальные настройки ТД». Откроется окно, где в качестве названия необходимо указать MAC-адрес ТД. После нажатия кнопки «Сохранить» откроется страница, содержащая параметры для настройки. При необходимости отмены создания нового профиля, используйте кнопку «Отмена».

Для редактирования существующих настроек нажмите на MAC-адрес в списке.

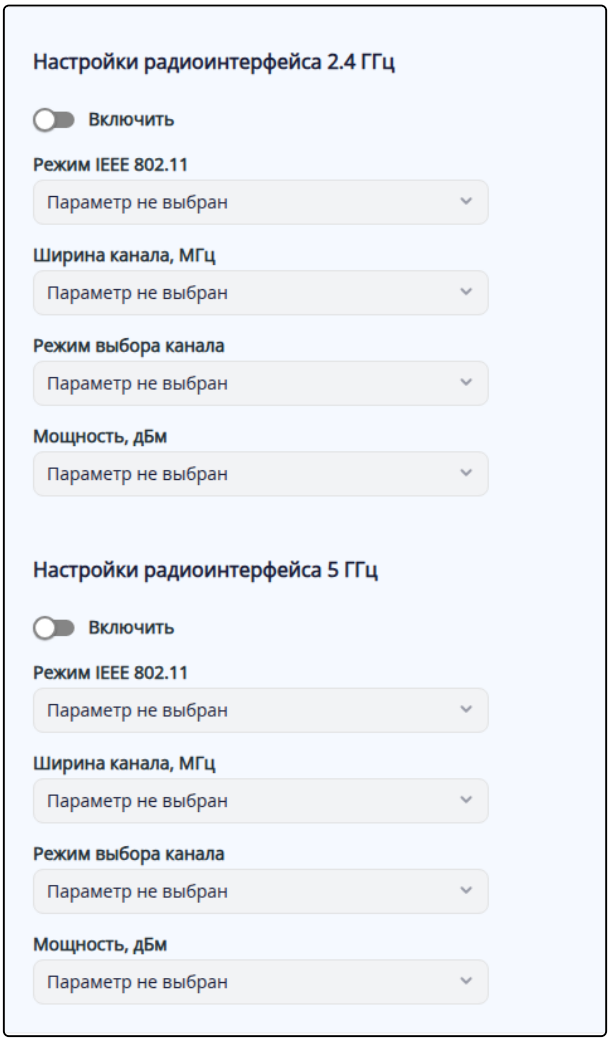
Для создания, удаления и редактирования настроек должен быть включен режим редактирования.



Страница настроек содержит следующие параметры:

- *Описание* − описание профиля настроек;
- *Модель ТД* − модель точки доступа;
- *Локация* − локация точки доступа. Дает возможность переопределить локацию для точки доступа, независимо от настройки подсетей локации. Параметр позволяет выбрать существующую локацию, а также создать и настроить новую;
- *Имя ТД* − имя точки доступа;
- *Профиль ТД* − общий профиль настроек ТД. Дает возможность переопределить профиль общих настроек ТД, указанный в локации. Параметр позволяет выбрать существующий профиль, а также создать и настроить новый;
- *Отключить AirTune* − отключение работы сервиса AirTune индивидуально для точки доступа, если он включен в локацию, которой принадлежит точка.

Для настройки радиоинтерфейсов необходимо обязательно выбрать модель ТД и локацию.



Настройки радиоинтерфейса 2.4 ГГц

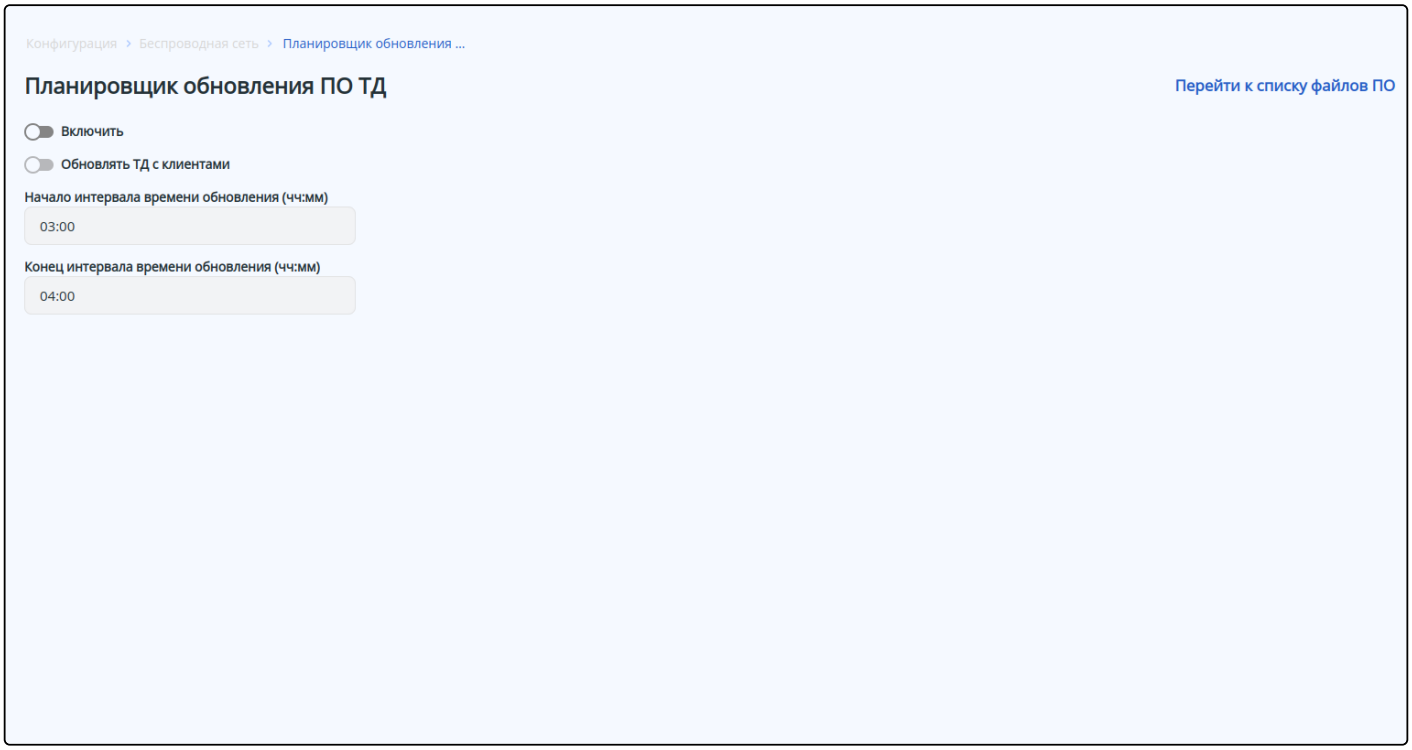
- *Включить* − переключатель активирует раздел настроек радиоинтерфейса в 2.4 ГГц для переопределения его параметров индивидуально для точки доступа.
- *Режим IEEE 802.11* − режим работы радиоинтерфейса. Возможные значения (доступные режимы различаются на точках доступа разных моделей):
  - n;
  - b/g;
  - b/g/n;
  - n/ax;
  - b/g/n/ax;
  - ax.
- *Ширина канала, МГц* − ширина полосы частот канала, на котором работает радиоинтерфейс точки доступа. Возможные значения:
  - 20;
  - 40L;
  - 40U.
- *Режим выбора канала* − режим выбора канала. Возможные значения:
  - Статический − позволяет выставить на радиоинтерфейсе определенный канал;
  - Автоматический − выбор канала будет осуществляться автоматически в зависимости от радиоэфира. Список каналов для автовыбора задается ниже.
- *Каналы* − выбор радиоканала. При статическом режиме доступен выбор только одного канала. При автоматическом режиме выбирается список каналов.
- *Мощность, дБм* − мощность сигнала радиоинтерфейса.

Настройки радиоинтерфейса 5 ГГц

- *Включить* − переключатель активирует раздел настроек радиоинтерфейса в 5 ГГц для переопределения его параметров индивидуально для точки доступа.
- *Режим IEEE 802.11* − режим работы радиоинтерфейса. Возможные значения (доступные режимы различаются на точках доступа разных моделей):
  - a;
  - a/n;
  - a/n/ac;
  - ax;
  - a/n/ac/ax/.
- *Ширина канала, МГц* − ширина полосы частот канала, на котором работает радиоинтерфейс точки доступа. Возможные значения:
  - 20;
  - 40L;
  - 40U;
  - 80.
- *Режим выбора канала* − режим выбора канала. Возможные значения:
  - Статический − позволяет выставить на радиоинтерфейсе определенный канал;
  - Автоматический − выбор канала будет осуществляться автоматически в зависимости от радиоэфира. Список каналов для автовыбора задается ниже.
- *Каналы* − выбор радиоканала. При статическом режиме доступен выбор только одного канала. При автоматическом режиме выбирается список каналов.
- *Мощность, дБм* − мощность сигнала радиоинтерфейса.

Подменю «Планировщик обновления ПО ТД»

Данная страница подменю используется для настройки обновления программного обеспечения точек доступа по расписанию.



Для настройки доступны следующие параметры:

- *Включить* − переключатель, который позволяет включить и выключить обновление ПО ТД по расписанию. Значение по умолчанию: отключено.

- *Обновлять ТД с клиентами* − переключатель, который позволяет включить и выключить возможность обновления ПО ТД, если в момент обновления к ней подключены клиенты. Значение по умолчанию: отключено.
- *Начало интервала времени обновления (чч:мм)* − определяет начало промежутка времени обновления. Значение по умолчанию: 03:00.
- *Конец интервала времени обновления (чч:мм)* − определяет конец промежутка времени обновления. Значение по умолчанию: 04:00.

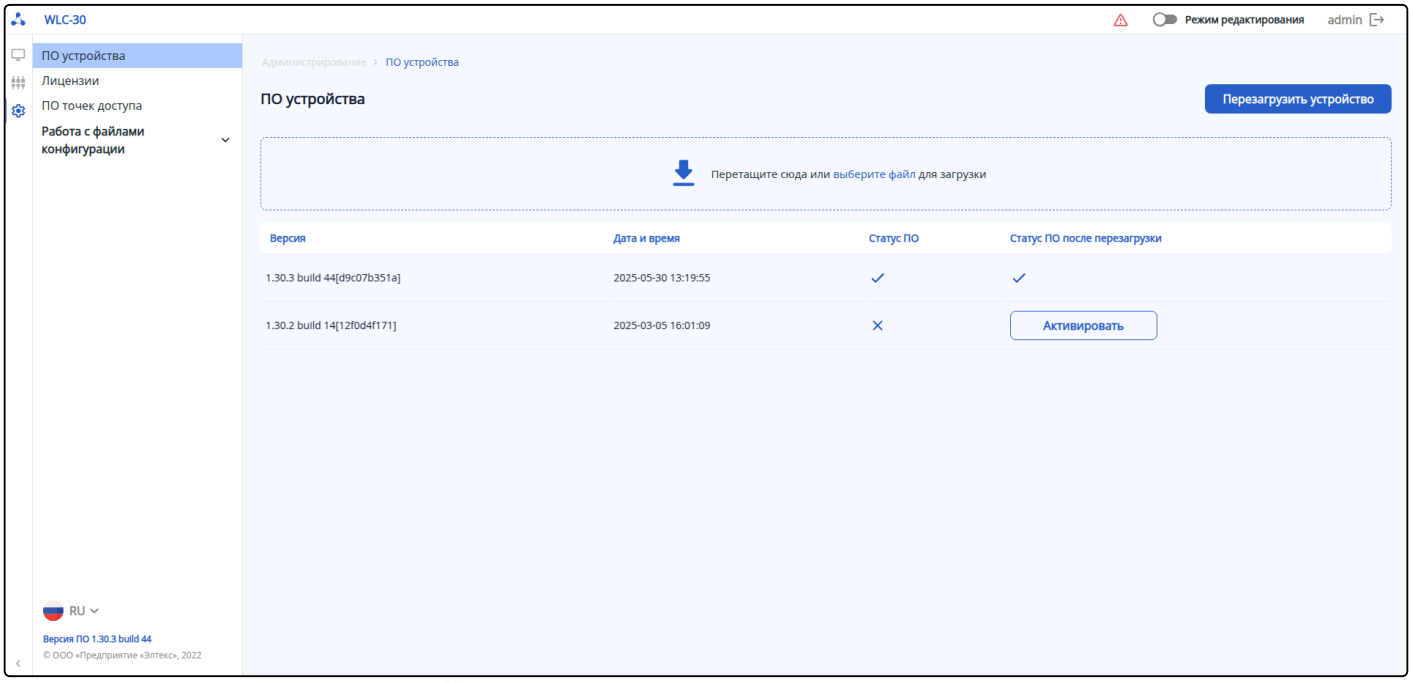
При включении планировщика обновление будет выполняться в заданный промежуток времени в соответствии с часовым поясом локации для тех моделей точек доступа, для которых на контроллер загружены файлы ПО. Просмотр загруженных файлов, а также загрузка новых файлов ПО точек доступа на контроллер доступна на странице «ПО точек доступа». Для перехода используйте кнопку «Перейти к списку файлов ПО».

10.2.5 Администрирование

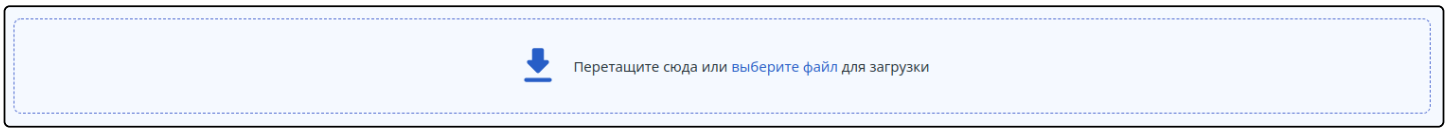
Для перехода к администрированию необходимо в главном меню выбрать элемент «Администрирование».

Меню «ПО устройства»

На странице находится информация об установленном программном обеспечении на устройстве, а также есть возможность загрузить и установить новое ПО и перезагрузить контроллер.

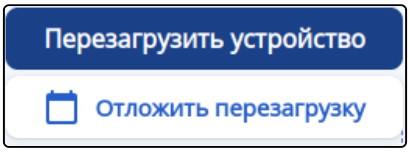


Для загрузки нового ПО используйте специальное поле, обозначенное следующим образом:

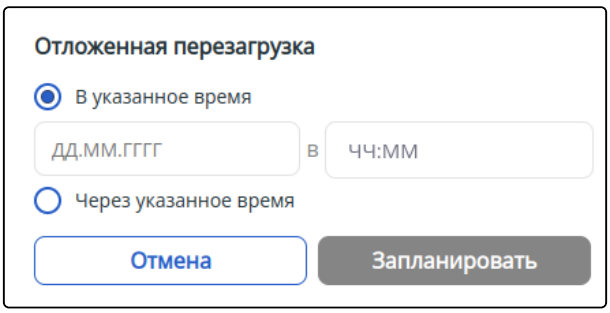


Файл можно перетащить в границы указанного поля или найти и выбрать на ПК, нажав кнопку «Выберите файл». После успешной загрузки файла, он появится в таблице ниже. Для установки ПО необходимо нажать кнопку «Активировать» в графе «Статус ПО после перезагрузки». После того, как файл будет отмечен в той же графе, необходимо перезагрузить устройство для завершения установки ПО. Используйте для этого кнопку «Перезагрузить устройство», при нажатии на которую начнется перезагрузка.

Есть возможность отложить перезагрузку, чтобы избежать прерывания сервиса в рабочее время. Опция «Отложить перезагрузку» становится доступна при наведении курсора на кнопку «Перезагрузить устройство».



При выборе этой опции можно указать конкретную дату и время перезагрузки в формате: день, месяц, год и часы, минуты. А также можно запланировать перезагрузку через указанное время.



После указания даты и времени нажмите кнопку «Запланировать». Рядом с кнопкой "Перезагрузить устройство" появится иконка, при нажатии на которую, будет доступна информация о дате перезагрузки. Для отмены запланированной перезагрузки, нажмите кнопку "Отменить" в появившемся окне.

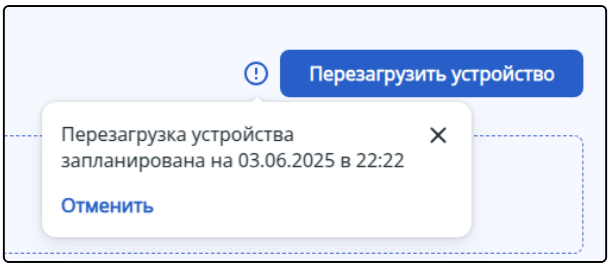
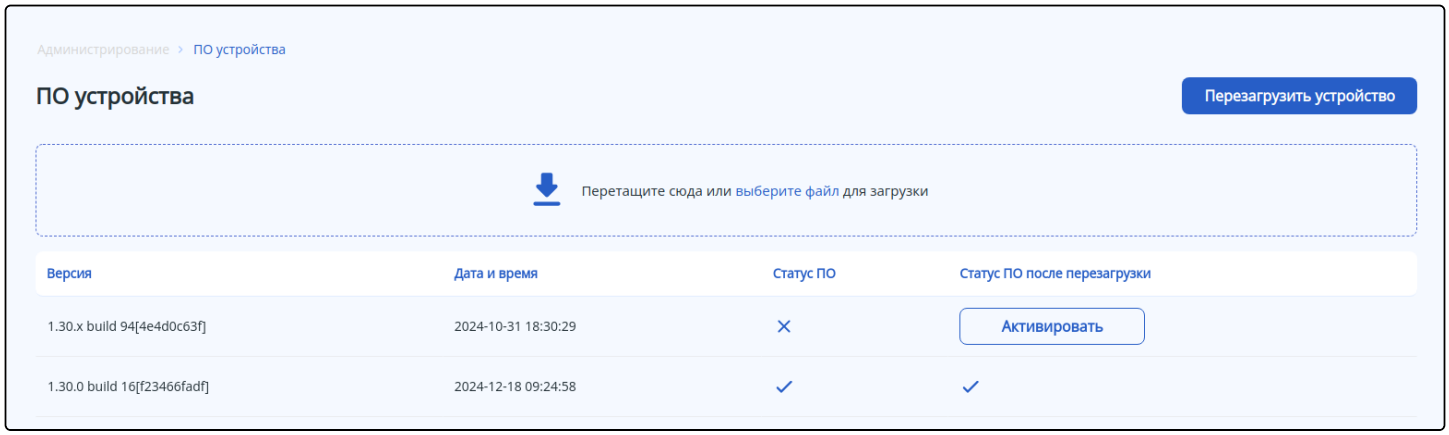


Таблица содержит данные по двум файлам ПО, загруженным на устройство, один из которых является активным в данный момент, а второй – резервным с возможностью переключаться между ними.

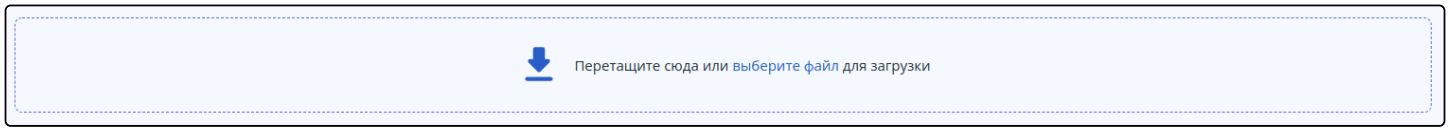
- *Версия* – версия загруженного программного обеспечения;
- *Дата и время* – дата и время выпуска файла ПО;
- *Статус ПО* – показывает текущее состояние для каждой версии ПО:
  - статус, обозначенный ✓, показывает, что ПО используется в данный момент;
  - статус, обозначенный ✗, показывает, что ПО в данный момент не активно, но загружено на устройство и может быть активировано с помощью кнопки «Активировать» в следующей графе.
- *Статус ПО после перезагрузки* – показывает, какое ПО будет использоваться после перезагрузки контроллера:
  - статус ✓ показывает, что данное ПО будет активным после перезагрузки;
  - кнопка Активировать позволяет сделать данный образ ПО активным после перезагрузки.



Меню «Лицензии»

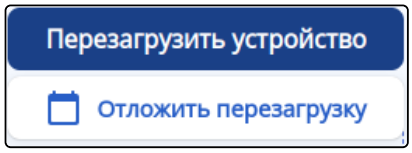
На странице находится информация об установленных лицензиях на устройстве, а также присутствует возможность загрузить новую лицензию и перезагрузить контроллер.

Для загрузки новой лицензии используйте специальное поле, обозначенное следующим образом:

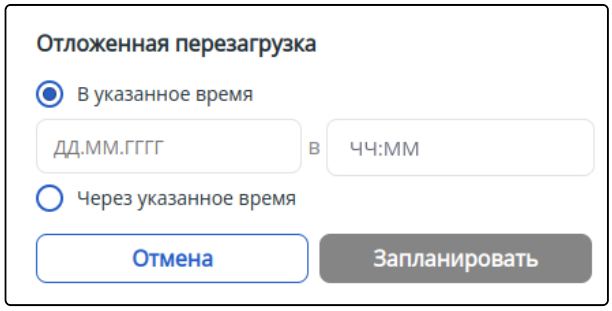


Файл можно перетащить в границы указанного поля или найти и выбрать на ПК, нажав кнопку «Выберите файл». После успешной загрузки файла, в таблице ниже появится информация о доступном функционале загруженной лицензии, который будет иметь статус «Candidate». Чтобы активировать данный функционал необходимо перезагрузить контроллер. Для этого используйте кнопку «Перезагрузить устройство», при нажатии на которую начнется перезагрузка.

Есть возможность отложить перезагрузку, чтобы избежать прерывания сервиса в рабочее время. Опция «Отложить перезагрузку» становится доступна при наведении курсора на кнопку «Перезагрузить устройство».



При выборе этой опции есть возможность указать конкретную дату и время перезагрузки в формате день, месяц, год и часы, минуты. А также есть возможность запланировать перезагрузку через указанное время.



После указания времени нажмите кнопку «Запланировать». Рядом с кнопкой "Перезагрузить устройство" появится иконка, при нажатии на которую, будет доступна информация о дате перезагрузки. Для отмены запланированной перезагрузки, нажмите кнопку "Отменить" в появившемся окне.

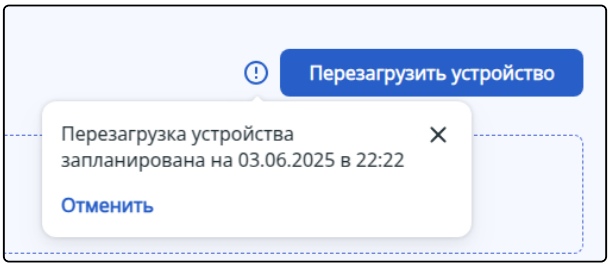
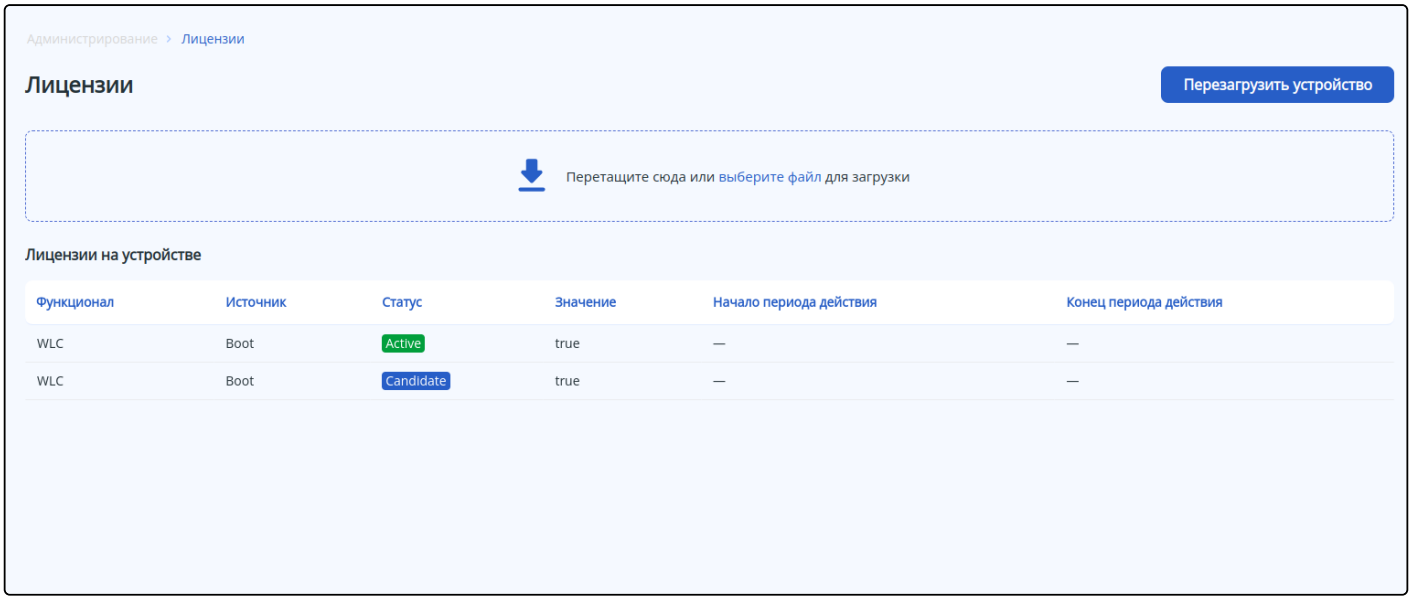


Таблица лицензий содержит следующие данные:

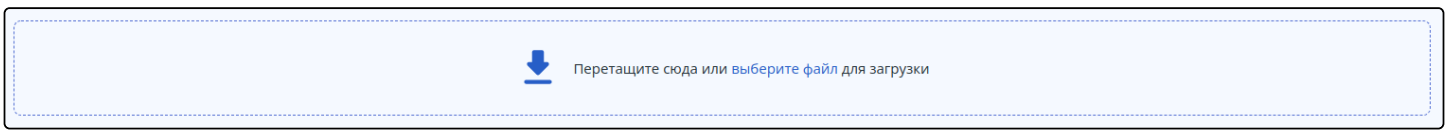
- *Функционал* – название функционала, доступного по лицензии.
- *Источник* – источник установки лицензии. Возможные варианты:
  - boot – лицензия поставляется с устройством в заводской комплектации;
  - file – лицензия загружена отдельным файлом на контроллер;
  - ELM – лицензия предоставляется сервисом ELM.
- *Статус* – текущее состояние лицензии. Возможные варианты:
  - Active – лицензия активна в данный момент;
  - Candidate – лицензия будет активна после перезагрузки контроллера.
- *Значение* – указывает ограничение по лицензии. Возможные значения:
  - true – лицензия работает без конкретных ограничений;
  - <N> – лицензия работает с указанным ограничением. Например, если для лицензии «WLC-AP» значение равно 200, то к контроллеру WLC-30 можно подключить 200 точек доступа, вместо базовых 150.
- *Начало периода действия* – дата начала действия лицензии.
- *Конец периода действия* – дата окончания действия лицензии.



Меню «ПО точек доступа»

На странице находится информация о загруженных на контроллер файлах ПО точек доступа, а также есть возможность загрузить новые файлы ПО и удалить неактуальные файлы.

Для загрузки новых файлов ПО используйте специальное поле, обозначенное следующим образом:



Файл можно перетащить в границы указанного поля или найти и выбрать файл на ПК, нажав кнопку «Выберите файл». После успешной загрузки файла он появится в таблице ниже.

Обновить ПО на точках доступа можно одним из двух способов:

- В заданное время для всех точек доступа. Для этого используйте кнопку «Перейти в планировщик обновлений», включите и настройте обновление по расписанию. Обновление запустится в указанное время в соответствии с часовым поясом локации для тех моделей точек доступа, для которых на контроллер загружены файлы ПО.
- Вручную на выбранных точках доступа. Для этого перейдите в меню «Мониторинг"/"Беспроводная сеть"/"Точки доступа». С помощью чекбоксов выберите точки доступа, которые необходимо обновить и нажмите кнопку «Обновить ПО». После этого запустится обновление на всех выбранных точках доступа при условии наличия на контроллере файлов ПО для выбранных моделей ТД.

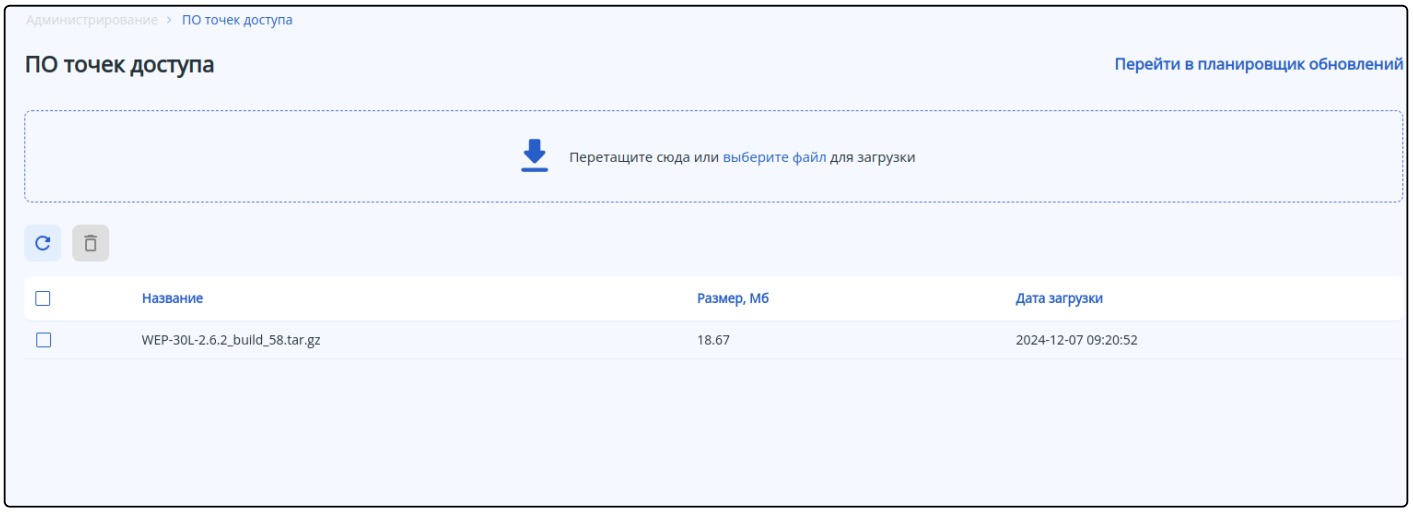


Таблица с файлами ПО содержит следующие данные:

- *Название* − название файла программного обеспечения точки доступа;
- *Размер, Мб* − размер файла в мегабайтах;
- *Дата загрузки* − дата загрузки файла на контроллер.

Чтобы удалить неактуальные файлы ПО с контроллера, выберите их в таблице с помощью чекбоксов и нажмите кнопку «Удалить». Все выбранные файлы будут удалены.

Меню «Работа с файлами конфигурации»

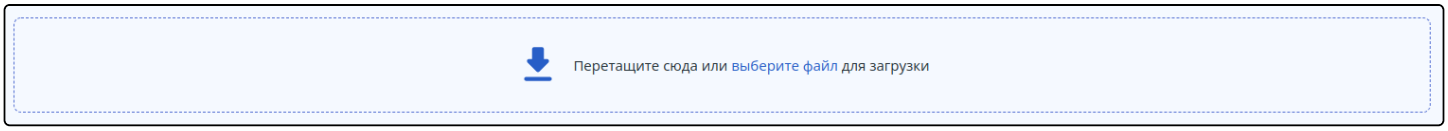
Подменю «Актуальные файлы»

На странице представлена возможность сохранить действующую Running-конфигурацию, сохранить текущую Candidate-конфигурацию, сбросить конфигурацию устройства к заводским настройкам, а также возможность загрузить резервную копию файла конфигурации на устройство.

Загрузить файл конфигурации

Для загрузки файла конфигурации должен быть включен режим редактирования.

Для загрузки файла конфигурации используйте специальное поле, обозначенное следующим образом:



Скачать файл конфигурации

На странице доступно скачивание двух файлов конфигурации с помощью кнопок:

- *Running* – скачивание файла действующей Running-конфигурации контроллера (конфигурация, которая используется на данный момент);
- *Candidate* – скачивание файла текущей Candidate-конфигурации контроллера (конфигурация, в которую были внесены, но еще не применены, изменения относительно действующей конфигурации).

Заводская конфигурация

Для сброса конфигурации к заводским настройкам должен быть включен режим редактирования.

Чтобы сбросить устройство к заводским установкам необходимо сначала скопировать заводскую конфигурацию в Candidate-конфигурацию, а затем применить ее и подтвердить изменения. Используйте для этого кнопки «Копировать в Candidate», а затем «Применить» и «Подтвердить».

После применения заводской конфигурации возможна потеря доступа.
В заводской конфигурации доступ к web-интерфейсу контроллера осуществляется по протоколу HTTPS с учетными данными: пользователь — *admin*, пароль — *password*.

Подменю «Архивные файлы»

Страница содержит информацию о резервных копиях файлов конфигурации.

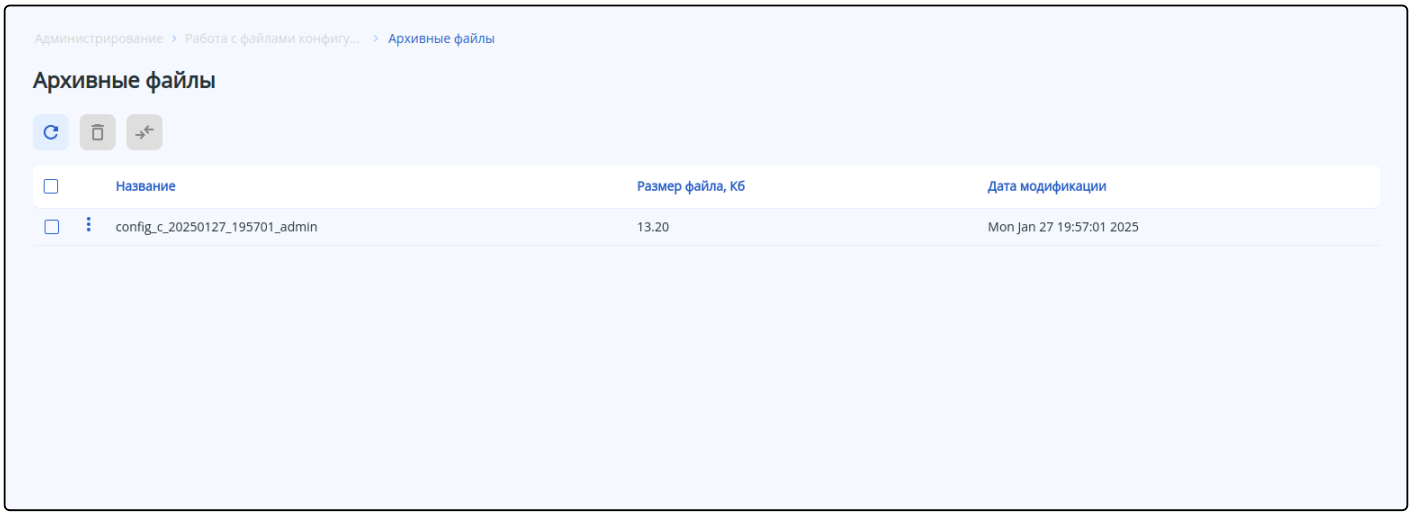
Обновление страницы происходит при нажатии на кнопку «Обновить».

С помощью чекбоксов можно выбрать один, несколько или все файлы, чтобы применить к ним общее действие с помощью кнопки «Удалить файлы». При нажатии на кнопку «Удалить файлы» и подтверждении действия, все выбранные файлы будут удалены.

При выборе одного или двух файлов становится доступна кнопка «Сравнить», при нажатии на которую осуществляется переход на страницу «Сравнение конфигураций» для последующего сравнения файлов.

Для каждого файла также доступно контекстное меню с действиями:

- *Копировать в Candidate* – происходит копирование конфигурации из выбранного файла в Candidate-конфигурацию. Опция доступна только при включенном режиме редактирования;
- *Удалить* – архивный файл конфигурации будет удален;
- *Сравнить* – осуществляется переход на страницу «Сравнение конфигураций» для последующего сравнения файлов.



Список файлов представлен в таблице. Таблица содержит данные:

- *Название* − название файла резервной копии конфигурации;
- *Размер, Кб* − размер файла указанный в килобайтах;
- *Дата модификации* − дата и время последней модификации файла.

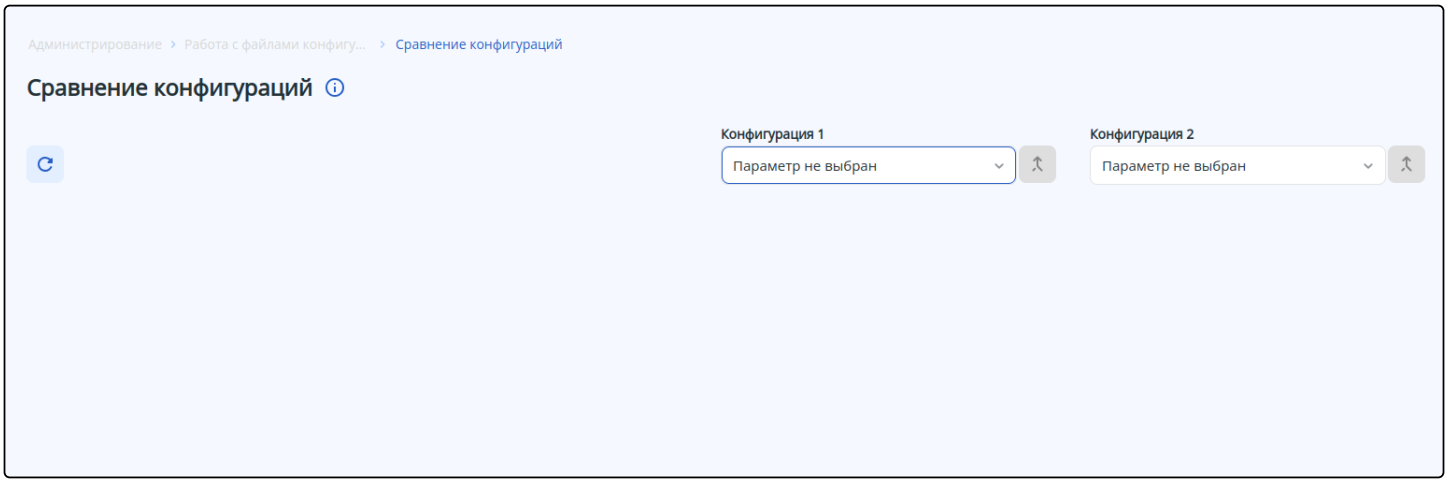
Настройки создания архивных файлов описана в документации «Управление программным обеспечением и конфигурацией».

Подменю «Сравнение конфигураций»

На странице осуществляется построчное сравнение выбранных файлов конфигурации.

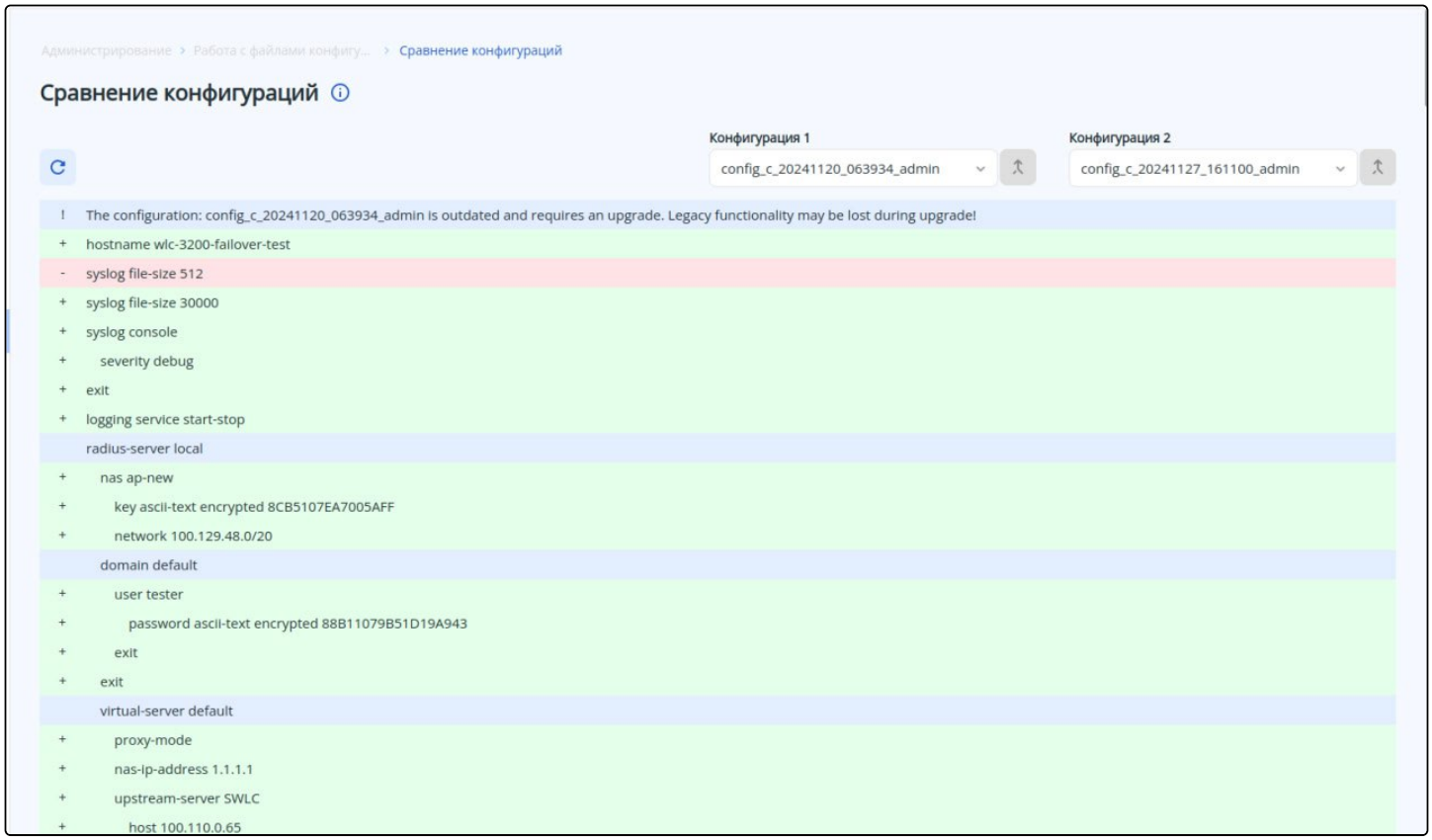
Обновление страницы происходит при нажатии на кнопку «Обновить».

Для того, чтобы сравнить два файла, необходимо выбрать их в соответствующих полях: «Конфигурация 1» и «Конфигурация 2». Кнопка «Копировать в Candidate» − копирует выбранную конфигурацию в конфигурацию «Candidate». Для применения используйте кнопку «Применить». Опция доступна только при включенном режиме редактирования.



Для сравнения могут быть выбраны следующие файлы:

- Архивные файлы конфигурации;
- Текущая Running-конфигурация;
- Текущая Candidate-конфигурация;
- Factory-config − заводская конфигурация;
- Default-config − дефолтная конфигурация.



При сравнении конфигураций используются следующие обозначения:

- *Зеленый цвет и знак "+"* – настройка присутствует в конфигурации 2, но отсутствует в конфигурации 1;
- *Красный цвет и знак "-"* – настройка отсутствует в конфигурации 2, но присутствует в конфигурации 1;
- *Синий цвет* – изменения в строке отсутствуют, используется для обозначения разделов конфигурации, которые содержат отличия.

Если файл содержит устаревшую версию конфигурации, это будет указано в первой строке вывода.

Для того чтобы сравнить архивную конфигурацию, которая была сделана на версиях ПО 1.26.1 и ниже, при выполнении сравнения система автоматически выполняет апгрейд версии конфигурации на актуальную в рамках текущей версии ПО контроллера.

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

Резервирование WLC описано в статье резервирование WLC.

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

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

18 Управление кластеризацей

18.1 Настройка Cluster

Cluster используется для резервирования работы устройств в сети. Резервирование обеспечивается за счет синхронизации работы различных сервисов между устройствами, а также за счет организации единой точки управления устройствами.

> ⚠ Нумерация портов зависима от номера юнита.
> У юнита 1 нумерация интерфейса будет 1/0/x. У юнита 2 нумерация интерфейсов будет 2/0/x. Чтобы не потерять доступ до устройства после смены номера юнита необходимо настроить интерфейсы с нумерацией 2/0/x заранее.

18.1.1 Алгоритм настройки

Шаг	Описание	Команда	Ключи
1	Перейти в режим конфигурирования сетевого моста, который будет использован в качестве кластерного интерфейса.	**wlc(config)# bridge <BR-NUM>**	<BR-NUM> – номер сетевого моста.
2	Указать IPv4-адрес и маску подсети для кластерного интерфейса. Необходимо установить адрес для всех юнитов кластера. (Для работы кластерного интерфейса поддерживается только IPv4-адресация.)	**wlc(config-bridge)# ip address <ADDR/LEN> [unit <ID>]**	<ADDR/LEN> – IP-адрес и длина маски подсети, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. <ID> – номер юнита, принимает значения [1..2]. Дополнительные функции IPv4-адресации см. в разделе Настройка IP-адресации.
3	Установить идентификатор VRRP-маршрутизатора.	**wlc(config-bridge)# vrrp id <VRID>**	<VRID> – идентификатора VRRP-маршрутизатора, принимает значения [1..255].

Шаг	Описание	Команда	Ключи
4	Установить виртуальный IP-адрес VRRP-маршрутизатора (адрес должен быть из той же подсети, что и ip address).	**wlc(config-bridge)# vrrp ip <ADDR/LEN> [secondary]**	<ADDR/LEN> – виртуальный IP-адрес и длина маски, задаётся в виде AAA.BBB.CCC.DDD/EE, где каждая часть AAA – DDD принимает значения [0..255] и EE принимает значения [1..32]. Можно указать несколько IP-адресов перечислением через запятую. Может быть назначено до 8 IP-адресов на интерфейс. secondary – ключ для установки дополнительного IP-адреса.
5	Установить принадлежность VRRP-маршрутизатора к группе. Группа предоставляет возможность синхронизировать несколько VRRP-процессов, так если в одном из процессов произойдет смена мастера, то в другом процессе также произойдёт смена ролей.	**wlc(config-bridge)# vrrp group <GRID>**	<GRID> – идентификатор группы VRRP-маршрутизатора, принимает значения [1..32].
6	Включить VRRP-процесс на IP-интерфейсе.	**wlc(config-bridge)# vrrp**	
7	Активировать сетевой мост.	**wlc(config-bridge)# enable**	
8	Перейти в режим конфигурирования кластера.	**wlc(config)# cluster**	
9	Установить интерфейс, через который будет происходить обмен служебными сообщениями между юнитами в кластере.	**wlc(config-cluster)# cluster-interface bridge [<BRIDGE-ID>]**	<BRIDGE-ID> – идентификационный номер моста, задается в виде, описанном в разделе Типы и порядок именования интерфейсов маршрутизатора.
10	Отключить синхронизацию конфигураций в кластере между юнитами (не обязательно).	**wlc(config-cluster)# sync config disable**	
11	Перейти в режим конфигурирования юнита в кластере.	**wlc(config-cluster)# unit <ID>**	<ID> – номер юнита, принимает значения [1..2].

Шаг	Описание	Команда	Ключи
12	Настроить MAC-адрес для определенного юнита.	**wlc(config-cluster-unit)# mac-address <ADDR>**	<ADDR> – MAC-адрес сетевого моста, задаётся в виде XX:XX:XX:XX:XX:XX, где каждая часть принимает значения [00..FF].
13	Включить работу кластера.	**wlc(config-cluster)# enable**	
14	Сменить юнит у устройства (смена юнита устройства вступает в силу после перезагрузки.)	**wlc# set unit id <ID>**	<ID> – номер юнита, принимает значения [1..2].

⚠ Данные между юнитами кластера через канал синхронизации передаются в открытом виде. Также все вводимые команды конфигурирования, содержащие чувствительную информацию не в encrypted-виде, будут переданы в том же виде, в котором введены, после чего будут преобразованы в encrypted-вид.

18.1.2 Пример настройки кластера

В настоящем руководстве приведено описание настройки кластера для администратора сервисного маршрутизатора wlc (далее — маршрутизатор).

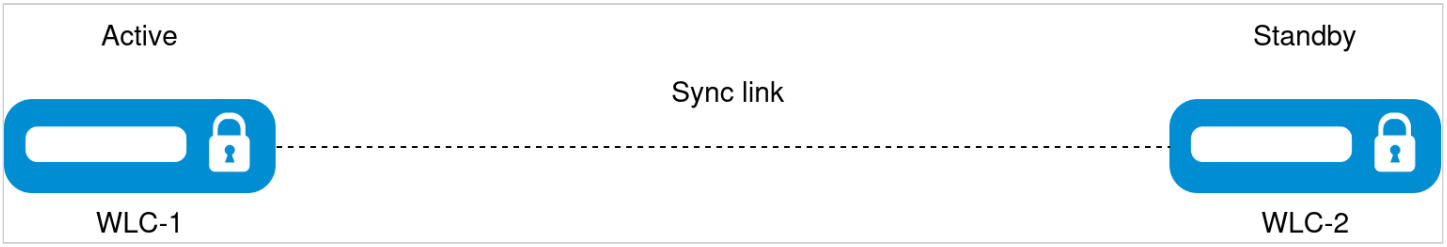


Схема реализации HA Cluster

Первичная настройка кластера

Для более удобного и ясного восприятия рекомендуется переименовать устройства. В кластерной версии прошивки предусмотрена возможность указать имя устройства с привязкой к юниту. Устройство будет использовать только тот hostname, юнитом которого он является:

WLC-1

```
wlc# configure
wlc(config)# hostname wlc-1 unit 1
wlc(config)# hostname wlc-2 unit 2
```

⚠ Более приоритетным является **hostname**, указанный с привязкой к **unit**.

Необходимо удалить заводские настройки Bridge, чтобы далее сконфигурировать его с нуля:

WLC-1

```
wlc-1(config)# no bridge 1
```

Создайте VLAN 2449, который будет выступать как vlan управления для ТД:

WLC-1

```
wlc-1(config)# vlan 2449
```

Укажите параметр, который отвечает за постоянное состояние UP:

WLC-1

```
wlc-1(config-vlan)# force-up
wlc-1(config-vlan)# exit
```

Для того чтобы задать адресацию на Bridge, предварительно необходимо удалить заводские настройки интерфейса:

WLC-1

```
wlc-1(config)# no interface gigabitethernet 1/0/2
```

Создайте Bridge для управления ТД:

WLC-1

```
wlc-1(config)# bridge 5
```

Укажите VLAN:

WLC-1

```
wlc-1(config-bridge)# vlan 2449
```

Задайте зону безопасности:

WLC-1

```
wlc-1(config-bridge)# security-zone trusted
```

Необходимо задать адресацию для первого и второго юнита кластера:

WLC-1

```
wlc-1(config-bridge)# ip address 192.168.1.3/24 unit 1
wlc-1(config-bridge)# ip address 192.168.1.2/24 unit 2
```

Настройте VRRP:

WLC-1

```
wlc-1(config-bridge)# vrrp id 2
wlc-1(config-bridge)# vrrp ip 192.168.1.1/32
wlc-1(config-bridge)# vrrp group 1
wlc-1(config-bridge)# vrrp
```

Отключите работу spanning-tree и включите работу Bridge:

WLC-1

```
wlc-1(config-bridge)# no spanning-tree
wlc-1(config-bridge)# enable
wlc-1(config-bridge)# exit
```

Перейдите к конфигурированию интерфейса Первого юнита:

WLC-1

```
wlc-1(config)# interface gigabitethernet 1/0/2
```

Для удобства укажите описание интерфейса:

WLC-1

```
wlc-1(config-if-gi)# description "Local"
```

Переведите режим работы интерфейса в L2:

WLC-1

```
wlc-1(config-if-gi)# mode switchport
```

Укажите режим работы интерфейса trunk:

WLC-1

```
wlc-1(config-if-gi)# switchport mode trunk
```

Добавьте VLAN 3 и 2449, которые будут обрабатываться интерфейсом:

WLC-1

```
wlc-1(config-if-gi)# switchport trunk allowed vlan add 3,2449
wlc-1(config-if-gi)# exit
```

Сконфигурируйте интерфейс Второго юнита. Настройки идентичны с интерфейсом, сконфигурированным выше:

WLC-1

```
wlc-1(config)# interface gigabitethernet 2/0/2
wlc-1(config-if-gi)# description "Local"
wlc-1(config-if-gi)# mode switchport
wlc-1(config-if-gi)# switchport mode trunk
wlc-1(config-if-gi)# switchport trunk allowed vlan add 3,2449
wlc-1(config-if-gi)# exit
```

Настройка кластерного интерфейса

Для полноценной работы кластера требуется сконфигурировать кластерный интерфейс, который будет использоваться для передачи control plane трафика. В качестве кластерного интерфейса назначен bridge. В качестве механизма, отвечающего за определение ролей устройств, участвующих в резервировании, назначен протокол VRRP. Настройки cluster-интерфейса должны быть идентичны для всех участников кластера.

Так как кластер выполняет синхронизацию состояний между устройствами, необходимо создать зону безопасности SYNC (synchronization) и разрешить прохождение трафика протокола VRRP:

WLC-1

```
wlc-1(config)# security zone SYNC
wlc-1(config-security-zone)# exit
wlc-1(config)# security zone-pair SYNC self
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol icmp
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# rule 2
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol vrrp
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Перейдите к настройкам кластерного интерфейса:

WLC-1

```
wlc-1(config)# bridge 1
```

⚠ В версии ПО 1.30.4 в качестве cluster-интерфейса поддержан только bridge.

Укажите, к какому VLAN относится bridge, и зону безопасности:

WLC-1

```
wlc-1(config-bridge)# vlan 1
wlc-1(config-bridge)# security-zone SYNC
```

Далее укажите IP-адреса:

WLC-1

```
wlc-1(config-bridge)# ip address 198.51.100.254/24 unit 1
wlc-1(config-bridge)# ip address 198.51.100.253/24 unit 2
```

⚠ Для работы кластерного интерфейса поддерживается только IPv4-адресация.
На cluster-интерфейсе необходима настройка адресов с привязкой к unit.

Настройте идентификатор VRRP, принадлежность VRRP-маршрутизатора к группе, IP-адрес VRRP:

WLC-1

```
wlc-1(config-bridge)# vrrp id 1
wlc-1(config-bridge)# vrrp group 1
wlc-1(config-bridge)# vrrp ip 198.51.100.1/24
```

⚠ Для настройки кластера адрес VRRP должен быть исключительно из той же подсети, что и адреса на интерфейсе.

Включите протокол VRRP и bridge:

WLC-1

```
wlc-1(config-bridge)# vrrp
wlc-1(config-bridge)# enable
wlc-1(config-bridge)# exit
```

Настройте физические порты для выделенного линка синхронизации маршрутизаторов wlc-1 и wlc-2:

WLC-1

```
wlc-1(config)# interface gigabitethernet 1/0/3
wlc-1(config-if-gi)# description "Network: SYNC"
wlc-1(config-if-gi)# mode switchport
wlc-1(config-if-gi)# exit
wlc-1(config)# interface gigabitethernet 2/0/3
wlc-1(config-if-gi)# description "Network: SYNC"
wlc-1(config-if-gi)# mode switchport
wlc-1(config-if-gi)# exit
```

Для проверки работы протокола VRRP выполните следующую команду:

WLC-1

```
wlc-1# show vrrp
Virtual router   Virtual IP                          Priority   Preemption   State
--------------   ---------------------------------   --------   ----------   ------
1                198.51.100.1/24                     100        Enabled      Backup
2                192.168.1.1/32                      100        Enabled      Backup
```

Можно увидеть, что устройство приняло состояние Backup. Через 10 секунд устройство примет состояние Master.

Настройка кластера

Для запуска кластера необходимо указать заранее настроенный кластерный интерфейс и юниты, которые будут выполнять роли Active и Standby.

Перейдите в режим настройки кластера:

WLC-1

```
wlc-1(config)# cluster
```

Настройте юниты:

WLC-1

```
wlc-1(config-cluster)# unit 1
wlc-1(config-cluster-unit)# mac-address E4:5A:D4:A0:BE:35
wlc-1(config-cluster-unit)# exit
wlc-1(config-cluster)# unit 2
wlc-1(config-cluster-unit)# mac-address A8:F9:4B:AF:35:84
wlc-1(config-cluster-unit)# exit
```

⚠ В качестве mac-address указывается системный MAC-адрес устройства, его можно узнать с помощью команды **show system | include MAC**.
Данный блок настройки кластера должен присутствовать на обоих юнитах.

Укажите кластерный интерфейс, созданный ранее, и активируйте кластер:

WLC-1

```
wlc-1(config-cluster)# cluster-interface bridge 1
wlc-1(config-cluster)# enable
wlc-1(config-cluster)# exit
```

Перейдите к настройке NTP:

WLC-1

```
wlc-1(config)# ntp server 100.110.0.65
```

⚠ Для работы синхронизации сервисов WLC, а также кластера необходима синхронизация времени между юнитами.
В примере указан демонстрационный IP-адрес NTP-сервера.

Укажите минимальное время опроса и максимальное время опроса:

WLC-1

```
wlc-1(config-ntp-server)# minpoll 1
wlc-1(config-ntp-server)# maxpoll 4
wlc-1(config-ntp-server)# exit
```

Отключите ntp broadcast-client:

WLC-1

```
wlc-1(config)# no ntp broadcast-client enable
```

Укажите часовой пояс:

WLC-1

```
wlc-1(config)# clock timezone gmt +7
wlc-1(config)# exit
```

После настроек кластера конфигурация на wlc-1 и wlc-2 должны выглядеть идентично, следующим образом:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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

syslog max-files 3
syslog file-size 512
syslog file tmpsys:syslog/default
  severity info
exit

radius-server local
  nas ap
    key ascii-text password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
```

```
exit
interface gigabitethernet 1/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 1/0/2
  description "Local"
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 1/0/3
  mode switchport
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  description "Local"
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  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
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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
```

```
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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

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
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit
```

Первое устройство полностью настроено и готово к работе.
Аналогичные настройки необходимо произвести на втором устройстве. Также возможна настройка второго устройства средствами ZTP.

⚠ Для активации процесса ZTP необходимо на втором устройстве запустить dhcp-client на bridge-интерфейсе, физический интерфейс которого будет включен в кластерный интерфейс первого устройства.
В качестве примера такой конфигурации подойдет factory-конфигурация. (В factory-конфигурации для vwlc нет настроенного dhcp-client).
В процессе ZTP устройство автоматически выставит себе:
1) Конфигурацию;
2) Юнит;
3) Версию ПО, на котором работает Active wlc;
4) Лицензию, если она предварительно загружена на Active wlc.

Чтобы изменить юнит второго устройства, выполните следующие команды:

WLC-2

```
wlc-2# set unit id 2
Unit ID will be 2 after reboot
wlc-2# reload system
Do you really want to reload system now? (y/N): y
```

⚠ На заводской конфигурации unit принимает значение по умолчанию (unit = 1).
Смена юнита устройства вступает в силу после перезагрузки.

⚠ При изменении номера юнита контролера не происходит автоматической конвертации конфигурации.
В случае если до контролера настроен удаленный доступ и у него меняется номер юнита, необходимо до перезагрузки настроить ip-интерфейсы для нового юнита аналогично текущим.

⚠ В заводской конфигурации присутствуют настройки интерфейсов только для юнита по умолчанию (unit = 1).
При копировании и применении заводской конфигурации настройка номера юнита не изменяется на значение по умолчанию.
Установить номер юнита по умолчанию возможно следующими способами:
1. Используя консольное подключение;
2. Зажав функциональную кнопку "F" на 15 секунд.

Убедитесь, что настройка юнита применилась успешно:

WLC-2

```
wlc-2# show unit id
Unit ID is 2
Unit ID will be 2 after reboot
```

⚠ Объединение устройств в кластер невозможно, если они относятся к одному и тому же юниту. Исключение — процесс ZTP, так как в процессе ZTP нужный unit у устройства выставится автоматически.

После выполнения этих шагов кластер будет успешно запущен. Текущее состояние кластера можно узнать, выполнив команду:

WLC-1

```
wlc-1# show cluster status
Unit   Hostname              Role         MAC address         State           IP address
----   --------------------  -----------  ------------------  --------------  ---------------
1*     wlc-1                 Active       e4:5a:d4:a0:be:35   Joined          198.51.100.254
2      wlc-2                 Standby      a8:f9:4b:af:35:84   Joined          198.51.100.253
```

⚠ После включения кластера и установления юнитов в состояние **Joined**, настройка устройств осуществляется настройкой **Active** устройства.

Синхронизируются команды конфигурации, а также команды: **commit**, **confirm**, **rollback**, **restore**, **save, copy <source> system:candidate-config.**
В случае, если конфигурирование осуществляется на **Standby**, то **синхронизации не будет**.
Есть возможность отключения синхронизации командой **sync config disable**.
Если между юнитами кластера не будет синхронизирована версия ПО, то команды **commit**, **confirm** не будут синхронизироваться на **Standby** устройство.

После выполнения этих шагов кластер будет успешно запущен. Текущее состояние синхронизации подсистем кластера можно узнать, выполнив команду:

WLC-1

```
wlc-1# show cluster sync status
System part              Synced
-----------------------  ------
candidate-config         Yes
running-config           Yes
SW version               Yes
licence                  Yes
licence (After reboot)   Yes
date                     Yes
```

⚠ В версии 1.30.4 не поддержана синхронизация шифрованных паролей.

⚠ Через минуту после включения кластера синхронизируется время, на Standby установится время Active-юнита.
Синхронизация времени проверяется раз в минуту, в случае расхождения время синхронизируется.

Синхронизация файлов лицензий

Для синхронизации файлов лицензий в кластере необходимо загрузить их все на Active-устройство командой **copy** в директорию **system:cluster-unit-licences**.

Все загруженные лицензии в данной директории передаются остальным участникам кластера.

Пример

```
wlc-1# copy tftp://<IP_address>:/licence system:cluster-unit-licences
|************************| 100% (680B) Licence loaded successfully.
```

⚠ На каждый wlc нужна отдельная лицензия (Wi-Fi, BRAS и т. д.).
Для активации функций кластера отдельная лицензия не нужна.

Установка файлов лицензий

Установить лицензию в кластере можно одним из способов:

1. Загрузить индивидуально лицензию на каждое устройство, как в случае с обычным wlc вне кластера.
2. Загрузить лицензию для Active-юнита в **system:licence** (данная лицензия также автоматически загрузится и в **system:cluster-unit-licences**), лицензии для Standby загрузить в **system:cluster-unit-licences** на Active-юните, после чего либо выполнить команду **sync cluster system force** либо подключить Standby по ZTP.

Пример

```
wlc-1# copy tftp://<IP_address>:/licence system:cluster-unit-licences
|************************| 100% (680B) Licence loaded successfully.
wlc-1#
wlc-1#
wlc-1#
wlc-1# show cluster-unit-licences
Serial number     Features
---------------   ------------------------------------------------------------
NP0B003634        BRAS,IPS,WIFI
NP0B009033        BRAS,IPS,WIFI
wlc-1# sync cluster system force
```

Команда **sync cluster system force** выполняет синхронизацию подсистем, включая в себя синхронизацию конфигурации **running-config**, **candidate-config**, **версии ПО**, **лицензии**. По окончанию синхронизации **Stanby** устройство кластера перезагрузится для применения новой версии прошивки, а также лицензии.
При использовании команды **sync cluster system force**, даже если все подсистемы кластеры синхронизированы (команда **show cluster sync status**), **Stanby** устройство начнет синхронизацию подсистем и по окончанию перезагрузится.

18.2 Подключение сервисов

После успешной настройки кластера можно приступать к конфигурации сервисов.

18.2.1 Настройка WLC

Настройка резервирования функционала WLC включает в себя резервирования ТД, SoftGRE-туннелей и сертификатов между юнитами. Данная настройка реализует отказоустойчивую работу сети для клиентов, подключенных к ТД во время выхода из строя одного из юнита. В момент переключения мастерства VRRP ТД переподключаются ко второй ноде, для клиента это происходит бесшовно.

Для настройки синхронизации требуется сконфигурировать несколько обязательных сервисов, таких как:

- WLC;
- SoftGRE-Controller;
- DHCP-server;
- Crypto-sync;
- WEB.

Настройка резервирования остальных сервисов выходит за рамки настройки WLC. Ознакомится с настройкой других сервисов можно в других главах данной статьи.

На клиентских интерфейсах, где включен vrrp, необходимо включить:

```
vrrp timers garp refresh 60
```

Данная команда определяет интервал, по истечении которого будет происходить периодическая отправка Gratuituous ARP-сообщений, пока маршрутизатор находится в состоянии Master. Настройку нужно включать, если клиентский трафик туннелируется.

Пример настройки

Настройка будет выполнена на базе заводской конфигурации с преднастроенным функционалом кластера. Интерфейсы Gi 1/0/3 + Gi 2/0/3 связывают два юнита между собой для реализации функционала кластера, интерфейсы Gi 1/0/2 + Gi 2/0/2 смотрят в сторону точки доступа.

Задача:

- 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 WEB profiles

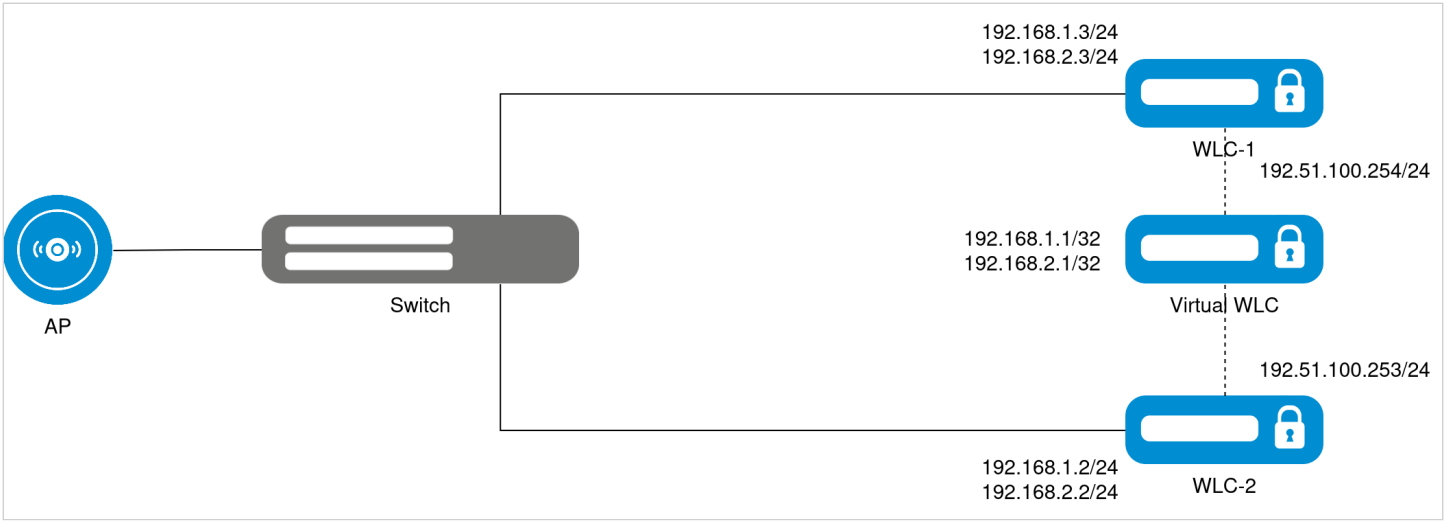


Схема реализации WLC

Исходная конфигурация кластера:

WLC-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 2
```

```
vlan 2449
 force-up
exit

security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit

interface gigabitethernet 1/0/2
  description "Local"
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 1/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/2
  description "Local"
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit

security zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
```

```
    enable
  exit
  rule 3
    action permit
    match protocol ah
    enable
  exit
exit
```

Решение:

Перейдите в режим конфигурации:

WLC-1

```
wlc-1# config
```

Создайте object-group для открытия портов в настройках Firewall, через которые синхронизируются сертификаты:

WLC-1

```
wlc-1(config)# object-group service sync
```

Укажите порт, который используется для синхронизации сертификатов:

WLC-1

```
wlc-1(config-object-group-service)# port-range 873
wlc-1(config-object-group-service)# exit
```

Создайте object-group для открытия портов в настройках Firewall, через которые синхронизируются туннели SoftGRE:

WLC-1

```
wlc-1(config)# object-group service softgre_controller
```

Укажите порт, который используется для синхронизации туннелей SoftGRE:

WLC-1

```
wlc-1(config-object-group-service)# port-range 1337
wlc-1(config-object-group-service)# exit
```

Сконфигурируйте object-group для настройки failover-сервисов SYNC_SRC:

WLC-1

```
wlc-1(config)# object-group network SYNC_SRC
```

Укажите IP-адреса для Первого и Второго юнитов кластера:

WLC-1

```
wlc-1(config-object-group-network)# ip address-range 198.51.100.254 unit 1
wlc-1(config-object-group-network)# ip address-range 198.51.100.253 unit 2
wlc-1(config-object-group-network)# exit
```

Сконфигурируйте object-group для настройки failover-сервисов SYNC_SRC:

WLC-1

```
wlc-1(config)# object-group network SYNC_DST
```

Укажите IP-адреса для Первого и Второго юнитов кластера:

WLC-1

```
wlc-1(config-object-group-network)# ip address-range 198.51.100.253 unit 1
wlc-1(config-object-group-network)# ip address-range 198.51.100.254 unit 2
wlc-1(config-object-group-network)# exit
```

Перейдите в Bridge 3.

WLC-1

```
wlc-1(config)# bridge 3
```

Удалите IP-адрес, который стоит по умолчанию в заводской конфигурации, затем укажите IP-address для первого и второго юнитов кластера:

WLC-1

```
wlc-1(config-bridge)# no ip address all
wlc-1(config-bridge)# ip address 192.168.2.3/24 unit 1
wlc-1(config-bridge)# ip address 192.168.2.2/24 unit 2
```

Укажите индентификатор VRRP:

WLC-1

```
wlc-1(config-bridge)# vrrp id 3
```

Укажите виртуальный VRRP-адрес:

WLC-1

```
wlc-1(config-bridge)# vrrp ip 192.168.2.1/24
```

Укажите группу VRRP:

WLC-1

```
wlc-1(config-bridge)# vrrp group 1
```

Включить периодическую отправку Gratuituous ARP-сообщений, когда контроллер находится в состоянии Master:

WLC-1

```
wlc-1(config-bridge)# vrrp timers garp refresh 60
```

Включите работу VRRP:

WLC-1

```
wlc-1(config-bridge)# vrrp
```

Отключите работу spanning-tree:

WLC-1

```
wlc-1(config-bridge)# no spanning-tree
```

Включите Bridge:

WLC-1

```
wlc-1(config-bridge)# enable
wlc-1(config-bridge)# exit
```

Перейдите в режим конфигурирования резервирования ip failover:

WLC-1

```
wlc-1(config)# ip failover
```

В качестве локального адреса укажите object-group SYNC_SRC:

WLC-1

```
wlc-1(config-failover)# local-address object-group SYNC_SRC
```

В качестве удаленного адреса укажите object-group SYNC_DST:

WLC-1

```
wlc-1(config-failover)# remote-address object-group SYNC_DST
```

Укажите группу VRRP:

WLC-1

```
wlc-1(config-failover)# vrrp-group 1
wlc-1(config-failover)# exit
```

Перейдите в блок конфигурации синхронизации сертификатов:

WLC-1

```
wlc-1(config)# crypto-sync
```

Укажите режим работы:

WLC-1

```
wlc-1(config-crypto-sync)# remote-delete
```

Включите работу синхронизации сертификатов:

WLC-1

```
wlc-1(config-crypto-sync)# enable
wlc-1(config-crypto-sync)# exit
```

Перейдите в блок настройки SoftGRE-туннелей:

WLC-1

```
wlc-1(config)# softgre-controller
```

Включите работу синхронизации:

WLC-1

```
wlc-1(config-softgre-controller)# failover
wlc-1(config-softgre-controller)# exit
```

Перейдите в блок конфигурации WLC:

WLC-1

```
wlc-1(config)# wlc
```

Включите работу синхронизации сервиса WLC:

WLC-1

```
wlc-1(config-wlc)# failover
wlc-1(config-wlc)# exit
```

Перейдите в конфигурацию security-zone, где добавьте разрешение на прохождение VRRP трафика:

WLC-1

```
wlc-1(config)# security zone-pair trusted self
```

Создайте правило:

WLC-1

```
wlc-1(config-security-zone-pair)# rule 11
```

Укажите действие правила – разрешение:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# action permit
```

Укажите совпадение по протоколу VRRP:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match protocol vrrp
```

Включите правило:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
```

Создайте правило:

WLC-1

```
wlc-1(config-security-zone-pair)# rule 12
```

Укажите действие правила – разрешение:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# action permit
```

Укажите совпадение по протоколу TCP:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match protocol tcp
```

Укажите совпадение по порту назначения, в качестве которого выступает object-group:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match destination-port object-group sync
```

Включите правило:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Перейдите в конфигурацию security-zone и откройте порты для синхронизации сертификатов и SoftGRE-туннелей:

WLC-1

```
wlc-1(config)# security zone-pair SYNC self
```

Создайте новое правило:

WLC-1

```
wlc-1(config-security-zone-pair)# rule 4
```

Укажите действие правила – разрешение:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# action permit
```

Укажите совпадение по протоколу TCP:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match protocol tcp
```

Укажите совпадение по порту назначения, в качестве которого выступает object-group:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match destination-port object-group softgre_controller
```

Включите правило:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Перейдите в конфигурацию security-zone, где добавьте разрешение на прохождение VRRP-трафика в клиентской зоне:

WLC-1

```
wlc-1(config)# security zone-pair users self
```

Создайте правило:

WLC-1

```
wlc-1(config-security-zone-pair)# rule 11
```

Укажите действие правила – разрешение:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# action permit
```

Укажите совпадение по протоколу VRRP:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match protocol vrrp
```

Включите правило:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Для настройки правил зон безопасности создайте профиль для порта Firewall-failover:

WLC-1

```
wlc-1(config)# object-group service FAILOVER
```

Укажите порт, который используется для синхронизации сессий Firewall:

WLC-1

```
wlc-1(config-object-group-service)# port-range 9999
wlc-1(config-object-group-service)# exit
```

Перейдите в конфигурацию security zone-pair для синхронизации сервисов кластера:

WLC-1

```
wlc-1(config)# security zone-pair SYNC self
```

Создайте новое правило:

WLC-1

```
wlc-1(config-security-zone-pair)# rule 5
```

Укажите действие правила:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# action permit
```

Укажите совпадение по протоколу UDP:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match protocol udp
```

Укажите совпадение по порту назначения, в качестве которого выступает object-group:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
```

Включите работу нового правила:

WLC-1

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Перейдите к настройке Firewall-failover:

WLC-1

```
wlc-1(config)# ip firewall failover
```

Укажите режим резервирования сессий unicast:

WLC-1

```
wlc-1(config-firewall-failover)# sync-type unicast
```

Укажите номер UDP-порта службы резервирования сессий Firewall:

WLC-1

```
wlc-1(config-firewall-failover)# port 9999
```

Включите резервирование сессий Firewall:

WLC-1

```
wlc-1(config-firewall-failover)# enable
wlc-1(config-firewall-failover)# exit
```

Нужно удалить пулы, заданные в заводской конфигурации и задать новые, в которых будут исключены VRRP-адреса:

Перейдите в конфигурирование пула DHCP-сервера для ТД:

WLC-1

```
wlc-1(config)# ip dhcp-server pool ap-pool
```

Удалите пул и создайте новый:

WLC-1

```
wlc-1(config-dhcp-server)# no address-range 192.168.1.2-192.168.1.254
wlc-1(config-dhcp-server)# address-range 192.168.1.4-192.168.1.254
wlc-1(config-dhcp-server)# exit
```

Перейдите в конфигурирование пула DHCP-сервера для клиентов:

WLC-1

```
wlc-1(config)# ip dhcp-server pool users-pool
```

Удалите пул и создайте новый:

WLC-1

```
wlc-1(config-dhcp-server)# no address-range 192.168.2.2-192.168.2.254
wlc-1(config-dhcp-server)# address-range 192.168.2.4-192.168.2.254
wlc-1(config-dhcp-server)# exit
```

Перейдите к настройке синхронизации DHCP-сервера между юнитами:

WLC-1

```
wlc-1(config)# ip dhcp-server failover
```

Укажите режим работы:

WLC-1

```
wlc-1(config-dhcp-server-failover)# mode active-standby
```

Включите работу синхронизации:

WLC-1

```
wlc-1(config-dhcp-server-failover)# enable
wlc-1(config-dhcp-server-failover)# exit
```

Включите синхронизацию WEB-интерфейса:

WLC-1

```
wlc-1(config)# ip http failover
```

Примените и подтвердите внесенные изменения:

WLC-1

```
wlc-1# commit
wlc-1# confirm
```

Полная конфигурация WLC-1

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group service FAILOVER
  port-range 9999
exit
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
```

```
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
```

```
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit
```

```
tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    enable
  exit
  rule 4
    action permit
    match protocol tcp
    match destination-port object-group softgre_controller
    enable
  exit
  rule 5
    action permit
    match protocol udp
    match destination-port object-group FAILOVER
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Статус синхронизации сервисов можно посмотреть командой:

WLC-1

```
wlc-1# show high-availability state
VRRP role:                          Master
AP Tunnels:
    State:                          Successful synchronization
    Last synchronization:           2025-02-05 16:38:12
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
VRF:                                --
    State:                          Successful synchronization
    Last synchronization:           2025-02-05 16:38:28
crypto-sync:
    State:                          Successful synchronization
    Last synchronization:           2025-02-05 16:38:29
Firewall:
Firewall sessions and NAT translations:
```

```
    Tracking VRRP Group            1
    Tracking VRRP Group state:     Master
    State:                         Successful synchronization
    Fault Reason:                  --
    Last synchronization:          2025-02-05 16:38:30
WLC:
    State:                         Successful synchronization
    Last synchronization:          2025-02-05 16:38:29
WEB profiles:
    State:                         Successful synchronization
    Last synchronization:          2025-02-05 16:38:36
```

Статус синхронизации VRRP можно посмотреть командой:

WLC-1

```
wlc-1# show vrrp
Virtual router   Virtual IP                          Priority   Preemption   State
Synchronization group ID
--------------   ---------------------------------   --------   ----------   ------
-------------------------
1                198.51.100.1/32                     100        Enabled      Master   1
2                192.168.1.1/32                      100        Enabled      Master   1
3                192.168.2.1/32                      100        Enabled      Master   1
```

18.2.2 Настройка MultiWAN

Технология MultiWAN позволяет организовать отказоустойчивое соединение с резервированием линков от нескольких провайдеров, а также решает проблему балансировки трафика между резервными линками.

С алгоритмом настройки MultiWAN можно ознакомиться по ссылке в разделе Алгоритм настройки MultiWAN.

Пример настройки

Задача:

Настроить MultiWAN в кластере маршрутизаторов wlc-1 и wlc-2 со следующими параметрами:

- обеспечить резервирование линков от нескольких провайдеров;
- обеспечить балансировку трафика в соотношении 70/30.

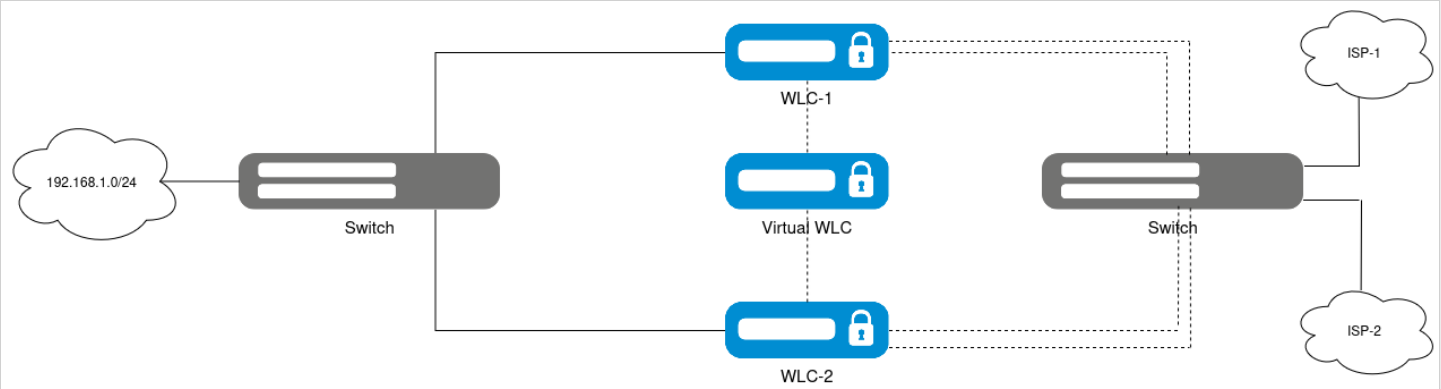


Схема реализации MultiWAN

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
```

```
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
vlan 20
exit

no spanning-tree

domain lookup enable

security zone trusted
exit
security zone untrusted
exit
security zone users
exit
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  enable
exit
bridge 2
  description "ISP1_ISP2"
  vlan 2
  security-zone untrusted
  ip address 192.0.3.4/24 unit 1
  ip address 192.0.3.3/24 unit 2
  vrrp id 4
  vrrp ip 192.0.3.2/24
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.3/24 unit 1
```

```
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit
 bridge 20
  description "ISP1_ISP2"
  vlan 20
  security-zone untrusted
  ip address 192.0.4.4/24 unit 1
  ip address 192.0.4.3/24 unit 2
  vrrp id 4
  vrrp ip 192.0.4.2/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit

interface gigabitethernet 1/0/1
  mode switchport
  switchport trunk allowed vlan add 2,20
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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport trunk allowed vlan add 2,20
```

```
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
```

```
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Создайте список IP-адресов для проверки целостности соединения:

WLC-1

```
wlc-1(config)# wan load-balance target-list WAN
wlc-1(config-wan-target-list)# target 1
wlc-1(config-wan-target)# ip address 8.8.8.8
wlc-1(config-wan-target)# enable
wlc-1(config-wan-target)# exit
wlc-1(config-wan-target-list)# exit
```

Настройте WAN на интерфейсе в сторону провайдера ISP1:

WLC-1

```
wlc-1(config)# bridge 2
wlc-1(config-bridge)# wan load-balance nexthop 192.0.3.1
wlc-1(config-bridge)# wan load-balance target-list WAN
wlc-1(config-bridge)# wan load-balance enable
wlc-1(config-bridge)# exit
```

Настройте WAN на интерфейсе в сторону провайдера ISP2:

WLC-1

```
wlc-1(config)# bridge 20
wlc-1(config-bridge)# wan load-balance nexthop 192.0.4.1
wlc-1(config-bridge)# wan load-balance target-list WAN
wlc-1(config-bridge)# wan load-balance enable
wlc-1(config-bridge)# exit
```

Укажите статический маршрут и создайте правило для балансировки трафика:

WLC-1

```
wlc-1(config)# ip route 0.0.0.0/0 wan load-balance rule 1 10
wlc-1(config)# wan load-balance rule 1
wlc-1(config-wan-rule)# outbound interface bridge 2 70
wlc-1(config-wan-rule)# outbound interface bridge 20 30
wlc-1(config-wan-rule)# enable
wlc-1(config-wan-rule)# exit
```

Проверить состояние работы MultiWAN можно с помощью команды:

WLC-1

```
wlc-1# show wan rules
Rule 1 detailed information:
    VRF:          default
    Failover:     Disabled
    Network: 0.0.0.0/0 Metric: 10
        br2 Weight: 70 Nexthop: 192.0.3.1 [Active]
```

```
        br20 Weight: 30 Nexthop: 192.0.4.1 [Active]
```

Также состояние работы MultiWAN можно проверить с помощью команды:

WLC-1

```
ESR-1# show wan interfaces status
Interface              Nexthop                  Status     Uptime/Downtime
                                                           (d,h:m:s)
--------------------   ----------------------   --------   --------------------
br2                    192.0.3.1                Active     00,00:00:44
br20                   192.0.4.1                Active     00,00:00:45
```

18.2.3 Настройка IPsec VPN

IPsec — это набор протоколов, обеспечивающих защиту данных, передаваемых по протоколу IP. Данный набор протоколов позволяет осуществлять подтверждение подлинности (аутентификацию), проверку целостности и шифрование IP-пакетов, а также включает в себя протоколы для защищённого обмена ключами в сети Интернет.
IPsec представляет собой совокупность протоколов, предназначенных для защиты данных, передаваемых по IP. Данный набор обеспечивает аутентификацию, проверку целостности и шифрование IP-пакетов, а также включает механизмы для безопасного обмена ключами в сети Интернет.

Пример настройки

Задача:

- обеспечить безопасность данных, передаваемых между LAN-сетями, посредством использования протокола IPsec, предоставляющего аутентификацию, проверку целостности и шифрование IP-пакетов;
- обеспечить, чтобы IPsec применялся для шифрования VTI-туннеля;
- создать зашифрованный IPsec-туннель, основанный на VIP IP-адресе.

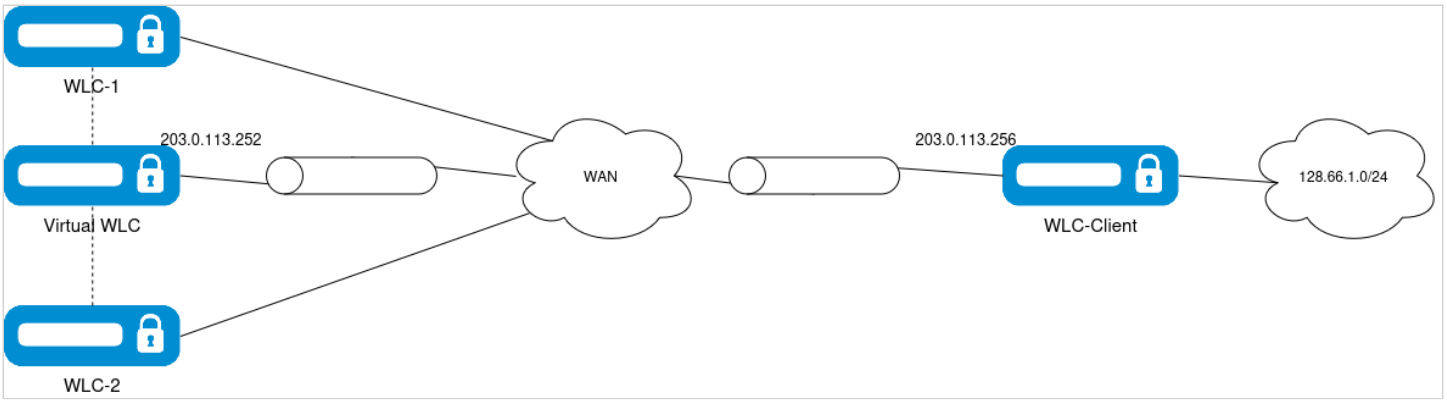


Схема реализации IPsec VPN

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
```

```
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  enable
exit
bridge 2
  vlan 2
  security-zone untrusted
  ip address 192.0.3.2/24 unit 1
  ip address 192.0.3.1/24 unit 2
  vrrp id 4
  vrrp ip 203.0.113.252/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.3/24 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Решение:

Создайте профиль ISAKMP-портов, необходимых для работы протокола IPsec, включающий разрешение UDP-пакетов на порту 500 (а также на порту 4500 для поддержки NAT-T при необходимости):

WLC-1

```
wlc-1(config)# object-group service ISAKMP
wlc-1(config-object-group-service)# port-range 500
wlc-1(config-object-group-service)# port-range 4500
wlc-1(config-object-group-service)# exit
```

Добавьте правила, разрешающие прохождение пакетов протоколов VRRP и ESP, а также UDP-пакетов с портами 500 и 4500, через IPsec-туннель:

WLC-1

```
wlc-1(config)# security zone-pair untrusted self
wlc-1(config-security-zone-pair)# rule 2
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol udp
wlc-1(config-security-zone-pair-rule)# match destination-port object-group ISAKMP
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# rule 3
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol esp
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Создайте зону безопасности IPsec и туннель VTI, через который будет перенаправляться трафик в IPsec-туннель. В качестве локального шлюза назначьте VIP IP-адрес, настроенный на интерфейсах в сторону зоны WAN, а в качестве удалённого шлюза − IP-адрес соответствующего интерфейса:

WLC-1

```
wlc-1(config)# security zone IPSEC
wlc-1(config-security-zone)# exit
wlc-1(config)# tunnel vti 1
wlc-1(config-vti)# security-zone IPSEC
wlc-1(config-vti)# local address 203.0.113.252
wlc-1(config-vti)# remote address 203.0.113.256
wlc-1(config-vti)# ip address 128.66.0.6/30
wlc-1(config-vti)# enable
wlc-1(config-vti)# exit
```

Добавьте правило, разрешающее прохождение трафика между зонами LAN и IPSEC:

WLC-1

```
wlc-1(config)# security zone-pair trusted IPSEC
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
```

```
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
wlc-1(config)# security zone-pair IPSEC trusted
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Создайте профиль протокола IKE, в котором задайте следующие параметры безопасности: группу Диффи-Хэллмана 2, алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5. Данные настройки обеспечивают надежную защиту IKE-соединения:

WLC-1

```
wlc-1(config)# security ike proposal ike_prop
wlc-1(config-ike-proposal)# dh-group 2
wlc-1(config-ike-proposal)# authentication algorithm md5
wlc-1(config-ike-proposal)# encryption algorithm aes128
wlc-1(config-ike-proposal)# exit
```

Создайте политику протокола IKE. В политике указывается список профилей протокола IKE, по которым могут согласовываться узлы и ключ аутентификации:

WLC-1

```
wlc-1(config)# security ike policy ike_pol
wlc-1(config-ike-policy)# pre-shared-key ascii-text password
wlc-1(config-ike-policy)# proposal ike_prop
wlc-1(config-ike-policy)# exit
```

Создайте шлюз протокола IKE с указанием VTI-туннеля, применимой политики, версии протокола и режима перенаправления трафика в туннель, а также отключите mobike:

WLC-1

```
wlc-1(config)# security ike gateway ike_gw
wlc-1(config-ike-gw)# version v2-only
wlc-1(config-ike-gw)# ike-policy ike_pol
wlc-1(config-ike-gw)# mode route-based
wlc-1(config-ike-gw)# mobike disable
wlc-1(config-ike-gw)# bind-interface vti 1
wlc-1(config-ike-gw)# exit
```

Создайте профиль параметров безопасности для IPsec-туннеля, в котором укажите алгоритм шифрования AES 128 bit и алгоритм аутентификации MD5, обеспечивая надежную защиту передаваемых данных:

WLC-1

```
wlc-1(config)# security ipsec proposal ipsec_prop
wlc-1(config-ipsec-proposal)# authentication algorithm md5
wlc-1(config-ipsec-proposal)# encryption algorithm aes128
```

```
wlc-1(config-ipsec-proposal)# exit
```

Создайте политику для IPsec-туннеля, в которой укажите перечень профилей IPsec-туннеля, используемых для согласования параметров безопасности между узлами:

WLC-1

```
wlc-1(config)# security ipsec policy ipsec_pol
wlc-1(config-ipsec-policy)# proposal ipsec_prop
wlc-1(config-ipsec-policy)# exit
```

Создайте IPsec VPN, в котором задаются следующие параметры: шлюз IKE-протокола, политика IPsec-туннеля, режим обмена ключами и способ установления соединения:

WLC-1

```
wlc-1(config)# security ipsec vpn ipsec
wlc-1(config-ipsec-vpn)# ike establish-tunnel route
wlc-1(config-ipsec-vpn)# ike gateway ike_gw
wlc-1(config-ipsec-vpn)# ike ipsec-policy ipsec_pol
wlc-1(config-ipsec-vpn)# enable
wlc-1(config-ipsec-vpn)# exit
```

Добавьте статический маршрут до встречной клиентской подсети через VTI туннель:

WLC-1

```
wlc-1(config)# ip route 128.66.1.0/24 128.66.0.5
```

⚠ Аналогичную настройку требуется выполнить на устройстве, находящемся на другой стороне туннеля.

Просмотр состояния туннеля осуществляется с помощью следующей команды:

WLC-1

```
wlc-1# show tunnels status
Tunnel              Admin    Link     MTU      Local IP           Remote IP          Last change
                    state    state                                                   (d,h:m:s)
-----------------   -----    -----    ------   ----------------   ----------------   -------------
vti 1               Up       Up       1500     203.0.113.252      203.0.113.256      00,03:34:00
```

Посмотреть состояние IPsec-туннеля можно с помощью команды:

WLC-1

```
wlc-1# show security ipsec vpn status
Name                              Local host        Remote host       Initiator spi
Responder spi        State
-------------------------------   ---------------   ---------------   ------------------
------------------   -----------
```

```
ipsec                              203.0.113.252     203.0.113.256     0x1c0c2099fb85d30b
0x3af77a1a17302fb9   Established
```

Посмотреть список и параметры подключившихся к IPsec-VPN-клиентов можно с помощью команды:

WLC-1

```
wlc-1# show security ipsec vpn authentication ipsec
Local host        Remote host       Local subnet          Remote subnet         Authentication
State
---------------   ---------------   -------------------   -------------------
-----------------------------------------   -----------
203.0.113.252     203.0.113.256     no child SA           no child SA           Pre-shared key
Established
```

Посмотреть конфигурацию IPsec-VPN можно с помощью следующей команды:

WLC-1

```
wlc-1# show security ipsec vpn configuration ipsec
VRF:                        --
Description:                --
State:                      Enabled
IKE:
    Establish tunnel:           route
    IPsec policy:               ipsec_pol
    IKE gateway:                ike_gw
    IKE DSCP:                   63
    IKE idle-time:              0s
    IKE rekeying:               Enabled
        Margin time:                540s
        Margin kilobytes:           0
        Margin packets:             0
        Randomization:              100%
```

18.2.4 Настройка Firewall failover

Firewall failover необходим для резервирования сессий Firewall.

С алгоритмом настройки Firewall failover можно ознакомиться по ссылке в разделе Алгоритм настройки Firewall failover.

Пример настройки

Задача:

Настроить Firewall failover в кластере маршрутизаторов wlc-1 и wlc-2 со следующими параметрами:

- режим резервирования сессий unicast;
- номер UDP-порта службы резервирования 9999;
- клиентская подсеть: 192.168.1.0/24.

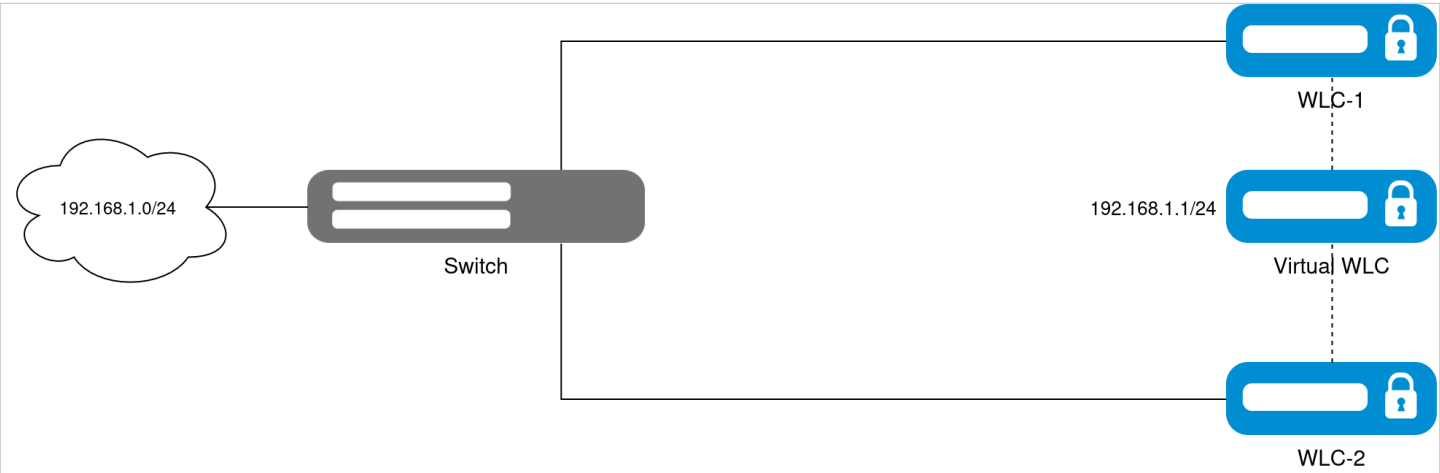


Схема реализации Firewall-failover

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7
```

```
ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Решение:

> ⚠ Для работы резервирования сессий Firewall необходимо иметь преднастройки ip failover и object-group network, указанные в конфигурации кластера выше.

Для настройки правил зон безопасности создайте профиль для порта Firewall failover:

WLC-1

```
wlc-1(config)# object-group service FAILOVER
wlc-1(config-object-group-service)# port-range 9999
wlc-1(config-object-group-service)# exit
```

Создайте разрешающее правило для зоны безопасности SYNC, разрешив прохождение трафика Firewall failover:

WLC-1

```
wlc-1(config)# security zone-pair SYNC self
wlc-1(config-security-zone-pair)# rule 4
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol udp
wlc-1(config-security-zone-pair-rule)# match destination-port object-group FAILOVER
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Выполните настройку Firewall failover. Настройте режим резервирования сессий unicast:

WLC-1

```
wlc-1(config)# ip firewall failover
wlc-1(config-firewall-failover)# sync-type unicast
```

Настройте номер UDP-порта службы резервирования сессий Firewall:

WLC-1

```
wlc-1(config-firewall-failover)# port 9999
```

Включите резервирование сессий Firewall:

WLC-1

```
wlc-1(config-firewall-failover)# enable
wlc-1(config-firewall-failover)# exit
```

После успешного запуска Firewall failover можно посмотреть состояние резервирования сессий Firewall с помощью следующей команды:

WLC-1

```
wlc-1# show ip firewall failover
Communication interface:                    bridge 1
Status:                                     Running
Bytes sent:                                 1200
Bytes received:                             1168
Packets sent:                               76
Packets received:                           77
Send errors:                                0
Receive errors:                             0
Resend queue:
    Active entries:                         1
    Errors:
        No space left:                      0
Hold queue:
    Active entries:                         0
    Errors:
        No space left:                      0
```

Также возможно узнать текущее состояние Firewall failover сервиса, выполнив команду:

WLC-1

```
wlc-1# show high-availability state
DHCP server:
    State:                          Disabled
    Last state change:              --
crypto-sync:
    State:                          Disabled
Firewall sessions and NAT translations:
VRF:                                --
    Tracking VRRP Group             1
    Tracking VRRP Group state:      Master
    State:                          Successful synchronization
    Fault Reason:                   --
    Last synchronization:           2025-01-09 13:36:13
```

18.2.5 Настройка DHCP failover

DHCP failover позволяет обеспечить высокую доступность службы DHCP.

С алгоритмом настройки DHCP failover можно ознакомиться по ссылке в разделе Алгоритм настройки DHCP failover.

Пример настройки

Задача:

Настроить DHCP-failover в кластере маршрутизаторов wlc-1 и wlc-2 со следующими параметрами:

- в качестве default-router используется IP-адрес VRRP;
- в качестве dns-server используется IP-адрес VRRP;
- установить в качестве необходимого режима работы резервирования active-standby;
- клиентская подсеть: 192.168.2.0/24.

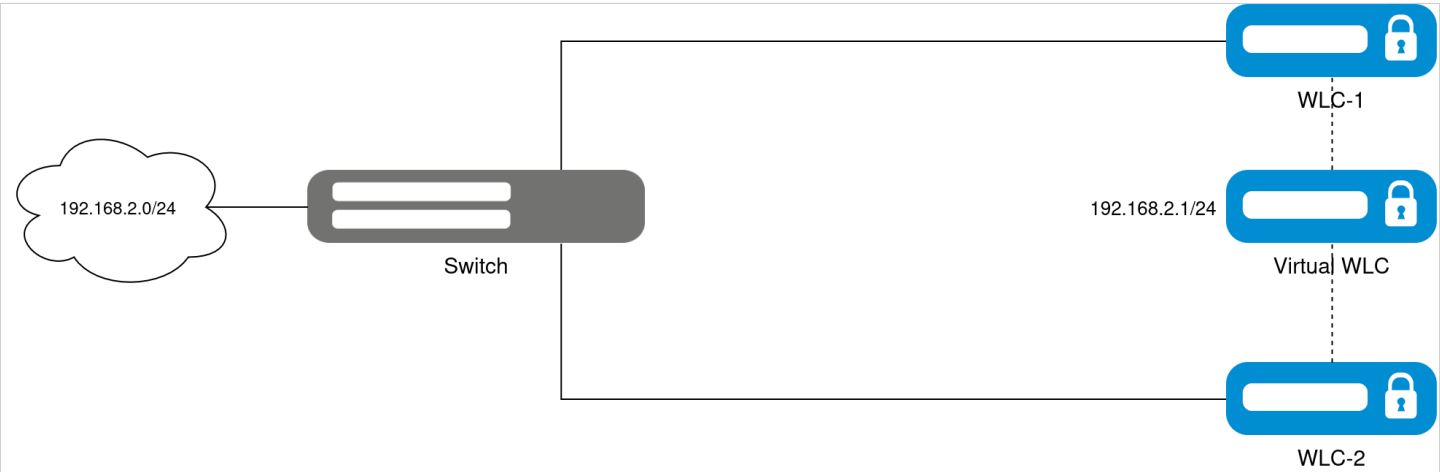


Схема реализации DHCP-failover

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
```

```
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit
```

```
ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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

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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
```

```
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Решение:

⚠ Для работы резервирования DHCP-сервера необходимо иметь преднастройки ip failover и object-group network, указанные в конфигурации кластера выше.

Перейдите к настройке резервирования DHCP-сервера:

WLC-1

```
wlc-1(config)# ip dhcp-server failover
```

Установите режим работы резервирования:

WLC-1

```
wlc-1(config-dhcp-server-failover)# mode active-standby
```

⚠ Для работы в кластере необходимо использовать режим active-standby.

Включите DHCP-failover:

WLC-1

```
wlc-1(config-dhcp-server-failover)# enable
wlc-1(config-dhcp-server-failover)# exit
```

Посмотреть состояние резервирования DHCP-сервера можно с помощью команды:

WLC-1

```
wlc-1# show ip dhcp server failover
VRF:                              --
    Mode:                         Active-Standby
    Role:                         Master
    State:                        Synchronized
    Last synchronization:         2025-01-09 12:00:57
```

Посмотреть состояние резервирования сессий DHCP можно с помощью команды:

WLC-1

```
wlc-1# show high-availability state
DHCP server:
VRF:                               --
    Mode:                          Active-Standby
    State:                         Successful synchronization
    Last synchronization:          2025-01-09 12:01:21
crypto-sync:
    State:                         Disabled
Firewall sessions and NAT translations:
    State:                         Disabled
```

Выданные адреса DHCP можно посмотреть с помощью команды:

WLC-1

```
wlc-1# show ip dhcp binding
IP address         MAC / Client ID                                                  Binding type
Lease expires at
----------------   ---------------------------------------------------------------  ------------
--------------------
192.168.2.10       02:00:00:69:91:12                                                active
2025-01-09 23:58:36
192.168.2.11       02:00:00:2a:a6:85                                                active
2025-01-09 23:58:39
```

18.2.6 Настройка SNMP

Протокол SNMP (Simple Network Management Protocol) реализует модель «менеджер–агент» для централизованного управления сетевыми устройствами: агенты, установленные на устройствах, собирают данные, структурированные в MIB, а менеджер запрашивает информацию, мониторинг состояние сети, контролирует производительность и вносит изменения в конфигурацию оборудования.

С алгоритмом настройки можно ознакомиться по ссылке в разделе Настройка SNMP-сервера и отправки SNMP TRAP.

Пример настройки

Задача:

- обеспечить возможность мониторинга сети через management-интерфейс каждого устройства в кластере:
- обеспечить возможность мониторинга состояния сети и внесения изменений в конфигурацию устройства, выполняющего роль VRRP Master;
- устройство управления (MGMT) доступно по IP-адресу 192.168.1.12.

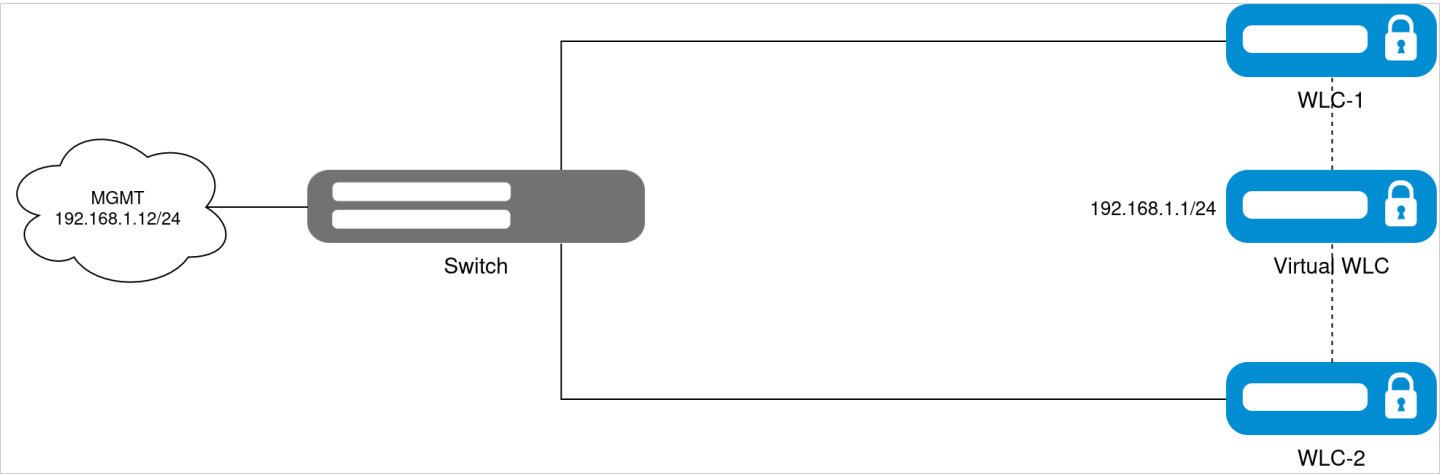


Схема реализации SNMP

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
```

```
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit
```

```
ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
```

```
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Решение:

Создайте профиль SNMP-портов, предоставляющий доступ в MGMT зону безопасности:

WLC-1

```
wlc-1(config)# object-group service SNMP
wlc-1(config-object-group-service)# port-range 161
wlc-1(config-object-group-service)# port-range 162
wlc-1(config-object-group-service)# exit
```

Добавьте правило, предусматривающее проверку, что порт назначения UDP-пакетов соответствует профилю SNMP-портов:

WLC-1

```
wlc-1(config)# security zone-pair trusted self
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol udp
wlc-1(config-security-zone-pair-rule)# match destination-port object-group SNMP
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Активируйте SNMP-сервер, настроив параметр snmp-community для обеспечения аутентификации и корректного доступа к данным мониторинга:

WLC-1

```
wlc-1(config)# snmp-server
wlc-1(config)# snmp-server community cluster rw
```

Благодаря данной настройке обеспечивается возможность централизованного мониторинга и управления как отдельными устройствами, так и устройством, выполняющим роль VRRP Master:

WLC-1

```
cluester@cluester-System:~$ snmpset -v2c -c cluster 192.168.1.3 .1.3.6.1.2.1.1.5.0 s 'wlc-1'
SNMPv2-MIB::sysName.0 = STRING: wlc-1
cluester@cluester-System:~$ snmpset -v2c -c cluster 192.168.1.2 .1.3.6.1.2.1.1.5.0 s 'wlc-2'
SNMPv2-MIB::sysName.0 = STRING: wlc-2
cluester@cluester-System:~$ snmpset -v2c -c cluster 192.168.1.1 .1.3.6.1.2.1.1.5.0 s 'VRRP-
Master'
SNMPv2-MIB::sysName.0 = STRING: VRRP-Master
```

18.2.7 Настройка Source NAT

Source NAT (SNAT) представляет собой механизм, осуществляющий замену исходного IP-адреса в заголовках IP-пакетов, проходящих через сетевой шлюз. При передаче трафика из внутренней (локальной) сети во внешнюю (публичную) сеть, исходный адрес заменяется на один из назначенных публичных IP-адресов шлюза. В ряде случаев осуществляется дополнительное преобразование исходного порта (NATP − Network Address and Port Translation), что обеспечивает корректное направление обратного трафика. При поступлении пакетов из публичной сети в локальную происходит обратная процедура − восстановление оригинальных значений IP-адреса и порта для обеспечения корректной маршрутизации внутри внутренней сети.

С алгоритмом настройки можно ознакомиться по ссылке в разделе Алгоритм настройки Source NAT.

Пример настройки

Задача:

- предоставить доступ в Интернет хостам, находящимся в локальной сети;
- клиентская подсеть: 192.168.2.0/24;
- публичный IP адрес − VIP-адрес на интерфейсе.

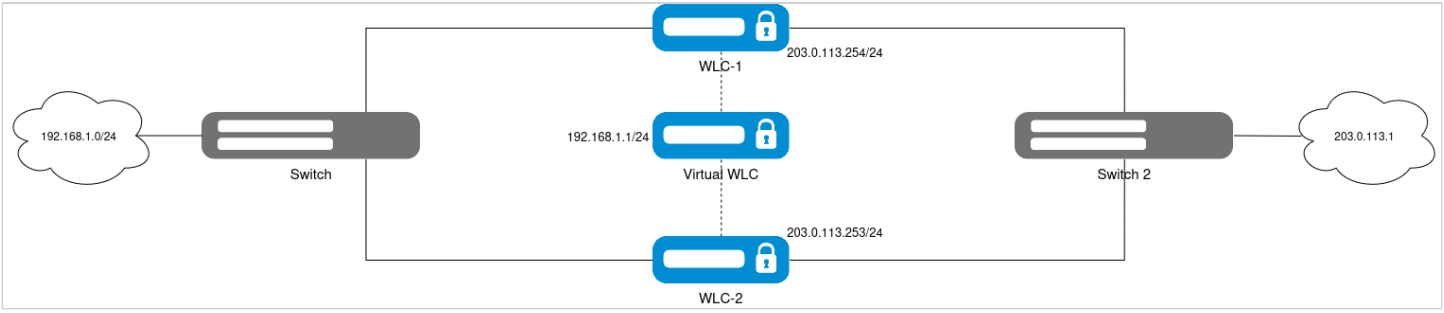


Схема реализации Source NAT

Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
```

```
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  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 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
```

```
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
exit
```

Решение:

Сконфигурируйте необходимые сетевые интерфейсы для подключения к провайдеру с указанием их принадлежности к зоне безопасности:

WLC-1

```
wlc-1(config)# br 2
wlc-1(config-bridge)# no ip address dhcp
wlc-1(config-bridge)# ip address 203.0.113.254/24 unit 1
wlc-1(config-bridge)# ip address 203.0.113.253/24 unit 2
wlc-1(config-bridge)# vrrp id 4
wlc-1(config-bridge)# vrrp ip 203.0.113.252/32
wlc-1(config-bridge)# vrrp group 1
wlc-1(config-bridge)# vrrp
wlc-1(config-bridge)# exit
```

Добавьте статический маршрут для выхода в интернет:

WLC-1

```
wlc-1(config)# ip route 0.0.0.0/0 203.0.113.1
```

Создайте список IP-адресов, которые будут иметь возможность выхода в Интернет:

WLC-1

```
wlc-1(config)# object-group network INTERNET_USERS
wlc-1(config-object-group-network)# ip address-range 192.168.2.4-192.168.2.254
wlc-1(config-object-group-network)# exit
```

Добавьте правило, предусматривающее проверку, принадлежит ли адрес источника диапазону INTERNET_USERS, что обеспечивает соблюдение установленных ограничений на выход в публичную сеть:

WLC-1

```
wlc-1(config)# security zone-pair users untrusted
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match source-address object-group INTERNET_USERS
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Создайте пул исходных NAT-адресов, в который включите виртуальный IP-адрес (VIP), назначенный WAN-интерфейсу:

WLC-1

```
wlc-1(config)# nat source
wlc-1(config-snat)# pool TRANSLATE_ADDRESS
wlc-1(config-snat-pool)# ip address-range 203.0.113.252
wlc-1(config-snat-pool)# exit
wlc-1(config-snat)# exit
```

Добавьте набор правил SNAT. В атрибутах набора укажите применение правил исключительно для пакетов, направляемых в зону WAN. При этом правила осуществляют проверку адреса источника на принадлежность к пулу INTERNET_USERS и выполняют трансляцию исходного адреса в VIP IP-адрес интерфейса:

WLC-1

```
wlc-1(config)# nat source
wlc-1(config-snat)# ruleset SNAT
wlc-1(config-snat-ruleset)# to zone untrusted
wlc-1(config-snat-ruleset)# rule 1
wlc-1(config-snat-rule)# match source-address object-group INTERNET_USERS
wlc-1(config-snat-rule)# action source-nat pool TRANSLATE_ADDRESS
wlc-1(config-snat-rule)# enable
wlc-1(config-snat-rule)# exit
wlc-1(config-snat-ruleset)# exit
wlc-1(config-snat)# exit
```

Просмотр таблицы NAT-трансляций осуществляется посредством следующей команды:

WLC-1

```
wlc-1# show ip nat translations
Prot    Inside source           Inside destination      Outside source          Outside
destination     Pkts         Bytes
----    ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------
icmp    192.0.2.12              203.0.113.1             203.0.113.252           203.0.113.1
--            --
```

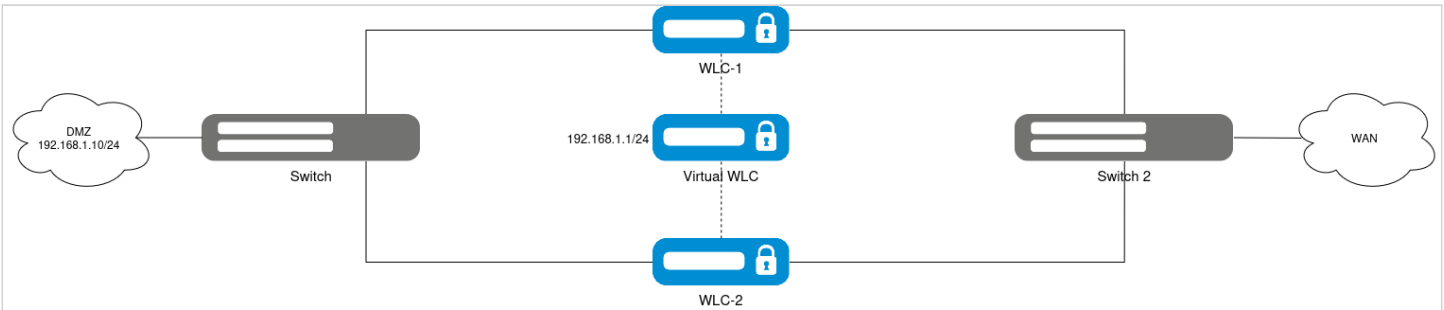
18.2.8 Настройка Destination NAT

Функция Destination NAT (DNAT) выполняет преобразование IP-адреса назначения в заголовках пакетов, проходящих через сетевой шлюз. DNAT применяется для перенаправления трафика, адресованного на IP-адрес в публичном сегменте сети, на «реальный» IP-адрес сервера, расположенного в локальной сети за шлюзом.

Пример настройки

Задача:

- организовать публичный доступа к серверу, находящемуся в частной сети и не имеющему публичного сетевого адреса;
- сервер доступен по адресу: 192.168.1.10/24.



Исходная конфигурация кластера:

```
cluster
  cluster-interface bridge 1
  unit 1
    mac-address e4:5a:d4:a0:be:35
  exit
  unit 2
    mac-address a8:f9:4b:af:35:84
  exit
  enable
exit

hostname wlc-1
hostname wlc-1 unit 1
hostname wlc-2 unit 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
object-group network SYNC_SRC
  ip address-range 198.51.100.254 unit 1
  ip address-range 198.51.100.253 unit 2
exit
object-group network SYNC_DST
  ip address-range 198.51.100.253 unit 1
  ip address-range 198.51.100.254 unit 2
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 password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  domain default
    user test
      password ascii-text password1
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
radius-server host 127.0.0.1
  key ascii-text password
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
security zone SYNC
exit

bridge 1
  vlan 1
  security-zone SYNC
```

```
  ip address 198.51.100.254/24 unit 1
  ip address 198.51.100.253/24 unit 2
  vrrp id 1
  vrrp ip 198.51.100.1/24
  vrrp group 1
  vrrp
  enable
exit
bridge 2
  vlan 2
  security-zone untrusted
  ip address 192.0.3.2/24 unit 1
  ip address 192.0.3.1/24 unit 2
  vrrp id 4
  vrrp ip 203.0.113.252/32
  vrrp group 1
  vrrp
  no spanning-tree
  enable
exit
bridge 3
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.3/24 unit 1
  ip address 192.168.2.2/24 unit 2
  vrrp id 3
  vrrp ip 192.168.2.1/32
  vrrp group 1
  vrrp timers garp refresh 60
  vrrp
  no spanning-tree
  enable
exit
bridge 5
  vlan 2449
  security-zone trusted
  ip address 192.168.1.3/24 unit 1
  ip address 192.168.1.2/24 unit 2
  vrrp id 2
  vrrp ip 192.168.1.1/32
  vrrp group 1
  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
  spanning-tree disable
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
interface gigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 2/0/2
  mode switchport
  switchport mode trunk
  switchport trunk allowed vlan add 3,2449
exit
interface gigabitethernet 2/0/3
  mode switchport
  spanning-tree disable
exit
interface gigabitethernet 2/0/4
  mode switchport
exit
interface tengigabitethernet 2/0/1
  mode switchport
  switchport access vlan 2
exit
interface tengigabitethernet 2/0/2
  mode switchport
exit

tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  enable
exit

ip failover
  local-address object-group SYNC_SRC
  remote-address object-group SYNC_DST
  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 zone-pair SYNC self
  rule 1
    action permit
    match protocol icmp
    enable
  exit
  rule 2
    action permit
    match protocol vrrp
    enable
  exit
  rule 3
    action permit
    match protocol ah
    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 password
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp server 100.110.0.65
  minpoll 1
  maxpoll 4
exit

crypto-sync
  remote-delete
  enable
```

```
exit
```

Решение:

Создайте профиль адреса сервера из WAN-сети, с которого будет приниматься запросы:

WLC-1

```
wlc-1(config)# object-group network INTERNAL
wlc-1(config-object-group-network)# ip address-range 203.0.113.252
wlc-1(config-object-group-network)# exit
```

Создайте профиль сервиса, доступ к которому будет предоставляться:

WLC-1

```
wlc-1(config)# object-group service SERVER_DMZ
wlc-1(config-object-group-service)# port-range 22
wlc-1(config-object-group-service)# exit
```

Войдите в режим конфигурирования функции DNAT и создайте пул адресов, в которые будут транслироваться адреса пакетов, поступающие на адрес 1.2.3.4 из внешней сети.

WLC-1

```
wlc-1(config)# nat destination
wlc-1(config-dnat)# pool DMZ
wlc-1(config-dnat-pool)# ip address 192.168.1.10
wlc-1(config-dnat-pool)# exit
```

Создайте набор правил «DNAT», в соответствии с которыми будет производиться трансляция адресов. В атрибутах набора укажите, что правила применяются только для пакетов, пришедших из зоны WAN. Набор правил включает в себя требования соответствия данных по адресу и порту назначения (match destination-address, match destination-port) и по протоколу. Кроме этого, в наборе задано действие, применяемое к данным, удовлетворяющим всем правилам (action destination-nat):

WLC-1

```
wlc-1(config-dnat)# ruleset DNAT_SERVER_DMZ
wlc-1(config-dnat-ruleset)# from zone untrusted
wlc-1(config-dnat-ruleset)# rule 1
wlc-1(config-dnat-rule)# match protocol tcp
wlc-1(config-dnat-rule)# match destination-address object-group INTERNAL
wlc-1(config-dnat-rule)# match destination-port object-group SERVER_DMZ
wlc-1(config-dnat-rule)# action destination-nat pool DMZ
wlc-1(config-dnat-rule)# enable
wlc-1(config-dnat-rule)# exit
wlc-1(config-dnat-ruleset)# exit
wlc-1(config-dnat)# exit
```

Добавьте правило, которое проверяет применение правил исключительно к пакетам, поступающим из зоны WAN. Набор правил включает требования соответствия по адресу назначения (match destination-

address) и протоколу. Дополнительно в наборе определено действие (action destination-nat), которое применяется к данным, удовлетворяющим указанным критериям:

WLC-1

```
wlc-1(config)# security zone-pair untrusted trusted
wlc-1(config-security-zone-pair)# rule 1
wlc-1(config-security-zone-pair-rule)# action permit
wlc-1(config-security-zone-pair-rule)# match protocol tcp
wlc-1(config-security-zone-pair-rule)# match destination-port object-group SERVER_DMZ
wlc-1(config-security-zone-pair-rule)# match destination-nat
wlc-1(config-security-zone-pair-rule)# enable
wlc-1(config-security-zone-pair-rule)# exit
wlc-1(config-security-zone-pair)# exit
```

Просмотр таблицы NAT-трансляций осуществляется посредством следующей команды:

WLC-1

```
wlc-1# show ip nat translations
Prot   Inside source           Inside destination      Outside source          Outside
destination     Pkts         Bytes
----   ---------------------   ---------------------   ---------------------
---------------------   ----------   ----------
tcp    203.0.113.1:41296       192.168.1.10:22         203.0.113.1:41296       203.0.113.252:22
       --           --
```

19 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.

20 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.

21 Мониторинг

Данный раздел см. в документации ESR.

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

22 Управление BRAS (Broadband Remote Access Server)

- Алгоритм настройки
- Пример настройки с SoftWLC
- Пример настройки без SoftWLC

Активируется лицензией BRAS.

22.1 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.
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].

Шаг	Описание	Команда	Ключи
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.
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.

Шаг	Описание	Команда	Ключи
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.
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.

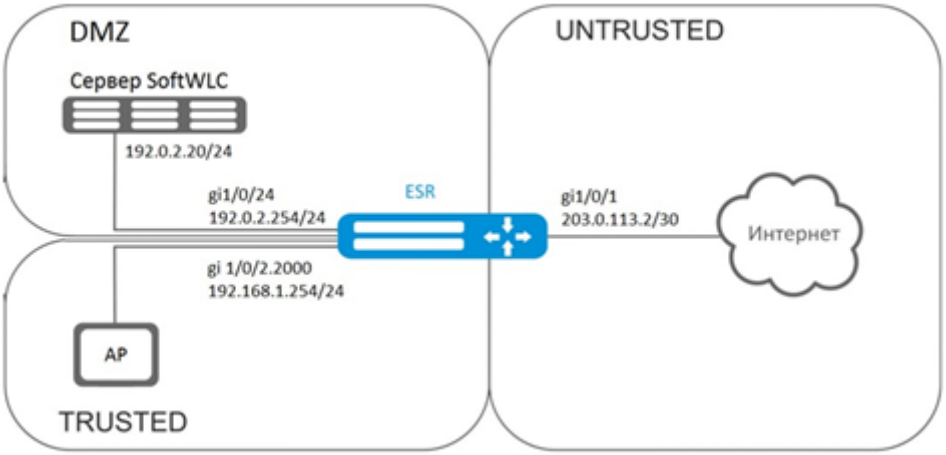
Шаг	Описание	Команда	Ключи
24	Включить перезапрос значения квоты при ее истечении для сервисов пользователя с настроенным ограничением по объему трафика или времени (не обязательно).	**wlc(config-subscriber-control)# quota-expired-reauth**	
25	Включить аутентификацию сессий по IP-адресу (не обязательно).	**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].
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].

Шаг	Описание	Команда	Ключи
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
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

22.2 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 port-range 68
wlc(config-acl-rule)# match destination-port port-range 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 port-range 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 object-group dhcp_client
wlc(config-zone-pair-rule)# match destination-port object-group 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 object-group 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
```

22.3 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 port-range 68
wlc(config-acl-rule)# match destination-port port-range 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 port-range 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 port-range 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 port-range 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 port-range 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 port-range 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     --
```

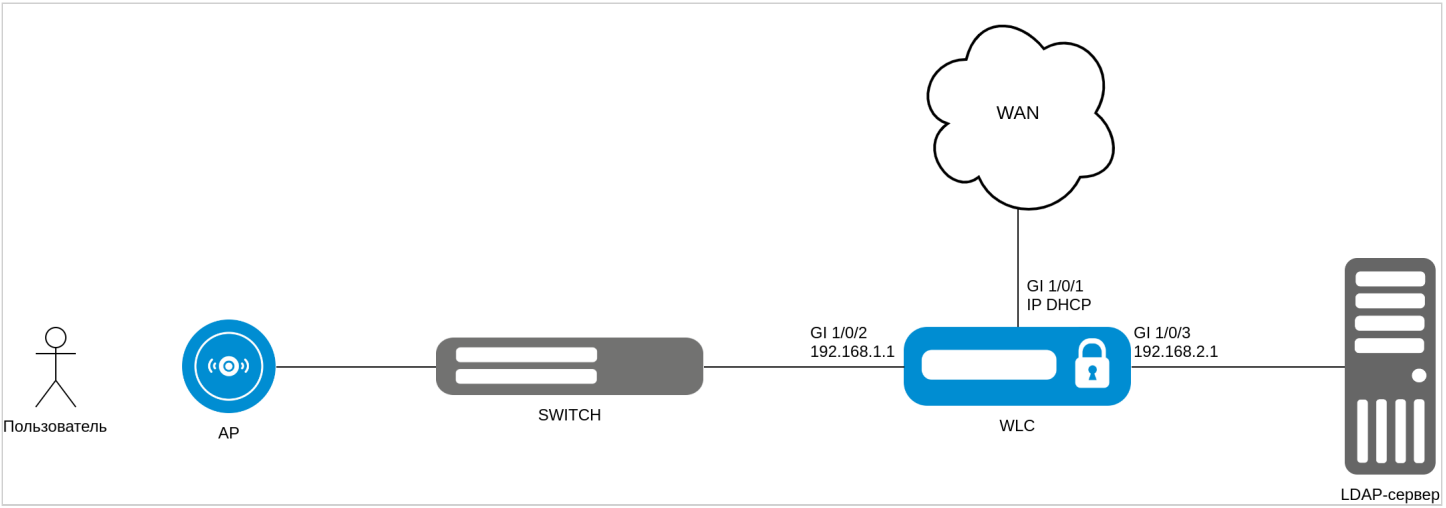
23 Статьи

- LDAP-авторизация
- RADIUS-сервер
- TLS-авторизация
- WIDS/WIPS
- Активация функционала по лицензии
- Анализ отладочной информации протокола RADIUS
- Настройка доступа беспроводных клиентов по MAC-адресам
- Настройка ограничения скорости трафика
- Изменение пути хранения журналов WLC
- Обновление точек доступа
- Портальная авторизация
- Резервирование WLC

23.1 LDAP-авторизация

23.1.1 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.

23.2 RADIUS-сервер

23.2.1 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
```

23.2.2 Настройка проксирования на внешний RADIUS

- Описание
- Логика работы Enterprise-авторизации
  - Успешная авторизация клиента
- Задача
- Решение
  - Пример настройки
    - Полная конфигурация
- Возможные проблемы
  - Запрет доступа по причине неправильного NAS-IP
  - Запрет доступа по причине ошибки аутентификации

Описание

В статье рассматривается настройка проксирования RADIUS-запросов от ТД через контроллер WLC в NAC-систему. ТД является устройством идентификации (NAS-клиент), RADIUS-запросы будут исходить от ТД. Контроллер WLC выполняет роль посредника в общении ТД и NAC-системы.

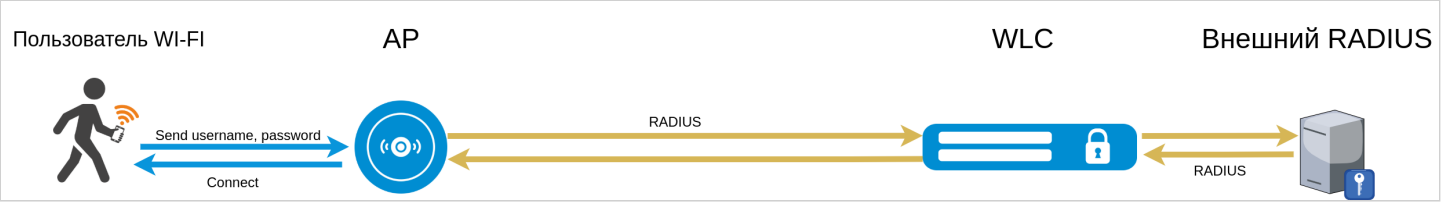


Диаграмма взаимодействия

ТД — самостоятельное устройство идентификации. Возможно несколько схем взаимодействия ТД и RADIUS-сервера:

1. Авторизация на локальном RADIUS-сервере контроллера WLC:
   Список пользователей Wi-Fi хранится в конфигурации контроллера. На контроллере запущен RADIUS-сервер, который выполняет проверку пользователей самостоятельно. Подробное описание представлено в статье Настройка локального RADIUS-сервера.
2. Авторизация на внешнем RADIUS-сервере:
   Список пользователей хранится на внешнем сервере. На контроллере запущен RADIUS-сервер, который выполняет проксирование RADIUS-запросов на вышестоящий сервер.

В статье описана настройка контроллера для проксирования RADIUS-запросов при работе с внешним RADIUS-сервером, т. е. вторая схема.

Проксирование RADIUS-запросов позволяет использовать общее хранилище учетных данных пользователей Wi-Fi.

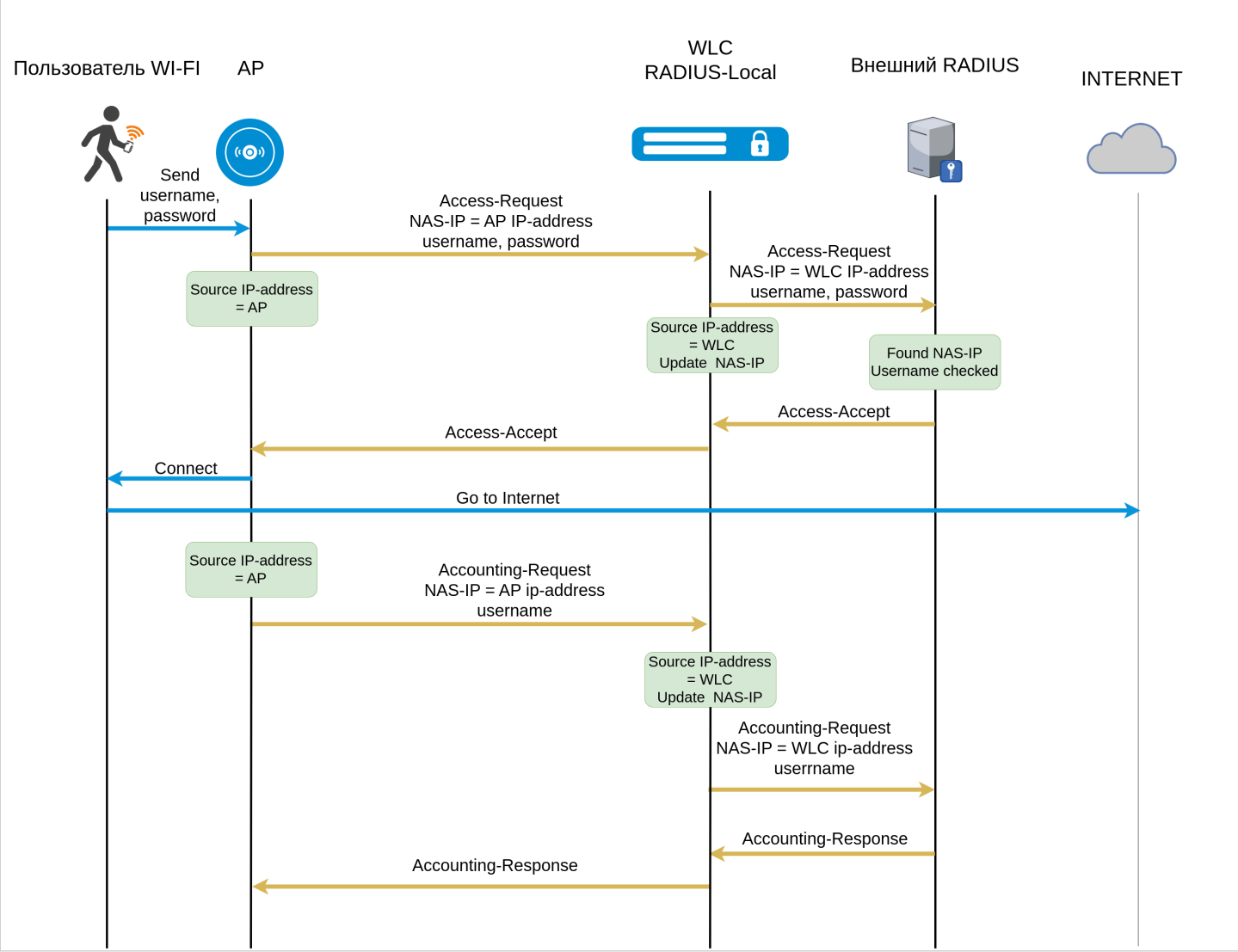
Для успешной авторизации на внешнем RADIUS-сервере необходимо:
- Наличие учетных записей пользователей;
- IP-адреса контроллера WLC нужно прописать в качестве NAS-клиента;
- Настроить подмену NAS-IP в конфигурации WLC. NAS-IP будет меняться в RADIUS-запросах от ТД при прохождении через контроллер. В таком случае на внешнем RADIUS-сервере нужно добавить один NAS-объект, которым является WLC.

Рекомендуется ознакомиться с базовой настройкой подключения ТД к контроллеру WLC, которая описана в разделе Настройка WLC руководства по эксплуатации.

Логика работы Enterprise-авторизации

Успешная авторизация клиента

Рассмотрим поэтапную работу при Enterprise-авторизации. Ниже на диаграмме представлен пример успешной авторизации пользователя с проксированием на внешний RADIUS-сервер.



1. При подключении к SSID клиент вводит учетные данные в виде логина (username) и пароля (password), которые приходят на ТД.
2. ТД отправляет запрос (Access-Request) на RADIUS-сервер WLC, в атрибуте NAS-IP будет задан IP-адрес ТД. На WLC настроено проксирование на внешний RADIUS-сервер.
3. Получив от ТД запрос (Access-Request), WLC подменит NAS-IP на IP-адрес, который указан в конфигурации и отправит запрос на внешний RADIUS-сервер.
4. Внешний RADIUS-сервер проверяет наличие записи NAS-IP WLC в своей конфигурации.
5. Если запись найдена, происходит проверка учетной записи пользователя и в случае успешной проверки, внешний RADIUS-сервер отправляет ответ (Access-Accept) в сторону WLC.
6. WLC, получив ответ от внешнего RADIUS-сервера, пересылает ответ ТД.
7. После успешного подключения клиента ТД отправляет запрос (Accounting-Request) на WLC (если отправка включена в конфигурации).
8. WLC подменяет NAS-IP и пересылает запрос на внешний RADIUS-сервер.
9. Внешний RADIUS-сервер отправляет ответ (Accounting-Response) WLC. WLC пересылает запрос ТД.

Задача

Настроить перенаправление всех RADIUS-запросов от ТД из сети 192.168.1.0/24 на вышестоящий сервер:

- IP-адрес: 10.10.10.12
- Порт для авторизации: 1812
- Порт для аккаунтинга: 1813
- Ключ сервера: password

Производить подмену NAS-IP на 10.10.20.1

Решение

Настройка будет выполнена на базе заводской конфигурации (Factory).

Шаги выполнения:

1. Настроить локальный RADIUS-сервер:
    a. Прописать nas – разрешить прием RADIUS-пакетов от ТД;
    b. Настроить *virtual-server* – включить режим проксирования и настроить подмену NAS-IP;
    c. Настроить *upstream-server* – указать параметры вышестоящего сервера.
2. Настройка в разделе WLC:
    a. Настроить *radius-profile* – настроить radius-profile, который будет использоваться для ТД;
    b. Настроить *ssid-profile* – настроить SSID и выбрать ранее созданный radius-profile;
    c. Включить *ssid-profile* в локацию.
3. Настроить firewall.
4. Применить конфигурацию.

Пример настройки

1. Настройка локального RADIUS-сервера.
   Перейдите в конфигурационный режим:

```
wlc# configure
wlc(config)#
```

   Перейдите в раздел radius-server local:

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

    a. Пропишите NAS.
    Добавьте подсети ТД (адресное пространство ТД, т. е. их IP-адреса), которые будут обслуживаться локальным RADIUS-сервером при Enterprise-авторизации пользователей Wi-Fi в *nas ap*:

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

При схеме подключения ТД через L3-сеть (с SoftGRE-туннелями) в конфигурации должна быть настроена запись для nas *local*, если она отсутствует, то её необходимо добавить:

```
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
```

b. Настройте *virtual-server*.
Настройте *virtual-server* для проксирования RADIUS-запросов на внешний сервер. Задайте имя *virtual-server*:

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

Задайте *nas-ip*.

Подмена NAS-IP

В локальном RADIUS-сервере есть возможность изменять NAS-IP во всех входящих RADIUS-запросах от ТД к WLC.
Если параметр не задан, при пересылке RADIUS-запросов на внешний сервер в атрибуте NAS-IP будет записан адрес ТД. Это может повлечь за собой ошибки в процессе аутентификации, которые подробно рассмотрены в разделе Возможные проблемы при авторизации.

```
wlc(config-radius-vserver)# nas-ip-address 10.10.20.1
```

Включите режим проксирования.

```
wlc(config-radius-vserver)# proxy-mode
```

Включите *virtual-server*.

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

c. Настройте *upstream-server*.
Настройте *upstream-server* доступна из раздела *virtual-server*. Создайте upstream-server для настройки параметров вышестоящего сервера:

```
wlc(config-radius-vserver)# upstream-server eltex
```

Задайте адрес вышестоящего сервера. На этот сервер будут перенаправляться запросы от ТД:

```
wlc(config-radius-upstream-server)# host 10.10.10.12
```

Включите режим проксирования для запросов аутентификации и аккаунтинга.

Типы upstream серверов

Server-type auth – проксирование только запросов аутентификации. Запросы будут проксироваться на порт, указанный в параметре port (по умолчанию – 1812).
Server-type acct – проксирование только аккаунтинга. Проксирование осуществляется на порт, указанный в параметре port (по умолчанию – 1812). При необходимости порт может быть изменен (стандартный порт для аккаунтинга – 1813).
Server-type all – проксирование 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).

Выберите режим all, так как нужно перенаправлять все запросы.

```
wlc(config-radius-upstream-server)# server-type all
```

Задайте ключ для вышестоящего сервера.

```
wlc(config-radius-upstream-server)# key ascii-text password
wlc(config-radius-upstream-server)# exit
wlc(config-radius-vserver)#   exit
```

Конфигурация раздела *radius-server*.

```
radius-server local
  nas local
    key ascii-text encrypted 8CB5107EA7005AFF
    network 127.0.0.1/32
  exit
  nas ap
    key ascii-text encrypted 8CB5107EA7005AFF
    network 192.168.1.0/24
  exit
  virtual-server default
    proxy-mode
    nas-ip-address 10.10.20.1
    upstream-server eltex
      host 10.10.10.12
      server-type all
      key ascii-text password
    exit
  enable
  exit
exit
```

2. Настройка в разделе WLC.
   Перейдите в раздел wlc:

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

   a. Настройте *radius-profile*.
      Настройте профиль *default-radius*:

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

      Поскольку настраивается проксирование запросов аутентификации и аккаунтинга, то в *auth-address* и *acct-address* должен быть указан адрес контроллера, который доступен для ТД. Ключ RADIUS-сервера (*auth-password*/*acct-password*) должен совпадать с ключом, указанным для nas *ap*, который был указан 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
wlc(config-wlc-radius-profile)# acct-address 192.168.1.1
wlc(config-wlc-radius-profile)# acct-password ascii-text password
```

      Если используется проксирование на SoftWLC, необходимо указать домен RADIUS. Этот домен должен совпадать с доменом, в котором созданы учетные записи пользователей Enterprise на SoftWLC.

```
wlc(config-wlc-radius-profile)# domain root
```

      Включите отправку аккаунтинга на RADIUS-сервер.

```
wlc(config-wlc-radius-profile)# acct-enable
```

      Включите добавление идентификатора RADIUS-сессии в запросах аккаунтинга.

```
wlc(config-wlc-radius-profile)# auth-acct-id-send
```

      Задайте временной интервал обновления аккаунтинга.

```
wlc(config-wlc-radius-profile)# acct-interval 600
```

      Конфигурация radius-profile.

```
radius-profile default-radius
  auth-address 192.168.1.1
  auth-password ascii-text password
  auth-acct-id-send
  acct-enable
  acct-address 192.168.1.1
  acct-password ascii-text password
  acct-periodic
  acct-interval 600
exit
```

   b. Создайте ssid-profile.
      Создайте новый профиль SSID:

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

Укажите в *ssid-profile* ранее настроенный профиль *radius-profile*.

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

Задайте имя *SSID*.

```
wlc(config-wlc-ssid-profile)#   ssid "test_enterprise"
```

Задайте режим безопасности.

```
wlc(config-wlc-ssid-profile)#   security-mode WPA2_1X
```

Задайте *VLAN*.

```
wlc(config-wlc-ssid-profile)# vlan-id 3
```

Задать остальные параметры *SSID*.

```
wlc(config-wlc-ssid-profile)# description "SSID  for enterprise users"
wlc(config-wlc-ssid-profile)# 802.11kv
wlc(config-wlc-ssid-profile)# band 2g
wlc(config-wlc-ssid-profile)# band 5g
wlc(config-wlc-ssid-profile)# enable
wlc(config-wlc-ssid-profile)# exit
```

Конфигурация *ssid-profile*.

```
ssid-profile test_enterprise
  description "SSID for enterprise users"
  ssid "test_enterprise"
  radius-profile default-radius
  vlan-id 3
  security-mode WPA2_1X
  802.11kv
  band 2g
  band 5g
  enable
exit
```

c. Включить *ssid-profile* в локацию.
Включите созданный SSID в локацию. ТД получит конфигурацию и начнёт вещать данные SSID. В примере ниже *ssid-profile* включен в локацию *default-location*.

```
ap-location default-location
  ssid-profile test_enterprise
exit
```

Конфигурация раздела *wlc*.

```
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 test_enterprise
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 test_enterprise
  description "SSID for enterprise users"
  ssid "test_enterprise"
  radius-profile default-radius
  vlan-id 3
  security-mode WPA2_1X
  802.11kv
  band 2g
  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
radius-profile default-radius
  description "default-radius"
  auth-address 192.168.1.1
  auth-password ascii-text encrypted 8CB5107EA7005AFF
  auth-acct-id-send
  acct-enable
  acct-address 192.168.1.1
  acct-password ascii-text encrypted 8CB5107EA7005AFF
  acct-periodic
  domain default
exit
wids-profile default-wids
  description "default-wids"
```

```
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit
```

3. Настройка firewall.
   Для приёма аккаунтинга разрешите прохождение UDP-трафика по порту 1813 из зоны *trusted* в зону *self*. В заводской конфигурации порт 1813 закрыт.
   a. Перейдите в конфигурационный режим:

```
wlc# configure
wlc(config)#
```

   b. Создайте группу radius_acct:

```
object-group service radius_acct
  port-range 1813
exit
```

   c. Добавьте правило в *zone-pair trusted self:*

```
security zone-pair trusted self
  rule 91
    action permit
    match protocol udp
    match destination-port object-group radius_acct
    enable
  exit
exit
```

4. Примените и подтвердите конфигурацию.

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

Для настройки внешнего RADIUS-сервера необходимо записать в таблицу NAS внешнего RADIUS-сервера адрес и ключ локального RADIUS-сервера WLC.

Полная конфигурация

Конфигурация устройства:

```
#!/usr/bin/clish
#270
#1.30.0
#2024-12-18
#09:24:58
object-group service ssh
  port-range 22
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
object-group service ntp
  port-range 123
exit
object-group service dns
  port-range 53
exit
object-group service netconf
  port-range 830
exit
object-group service radius_auth
  port-range 1812
exit
object-group service sa
  port-range 8043-8044
exit
object-group service airtune
  port-range 8099
exit
object-group service web
  port-range 443
exit
object-group service radius_acct
  port-range 1813
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
    proxy-mode
    nas-ip-address 10.10.20.1
    upstream-server eltex
      host 10.10.10.12
      server-type all
      key ascii-text encrypted 8CB5107EA7005AFF
    exit
    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 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 untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
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 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
  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 test_enterprise
    description "SSID for enterprise users"
    ssid "test_enterprise"
    radius-profile default-radius
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    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
  radius-profile default-radius
    description "default-radius"
```

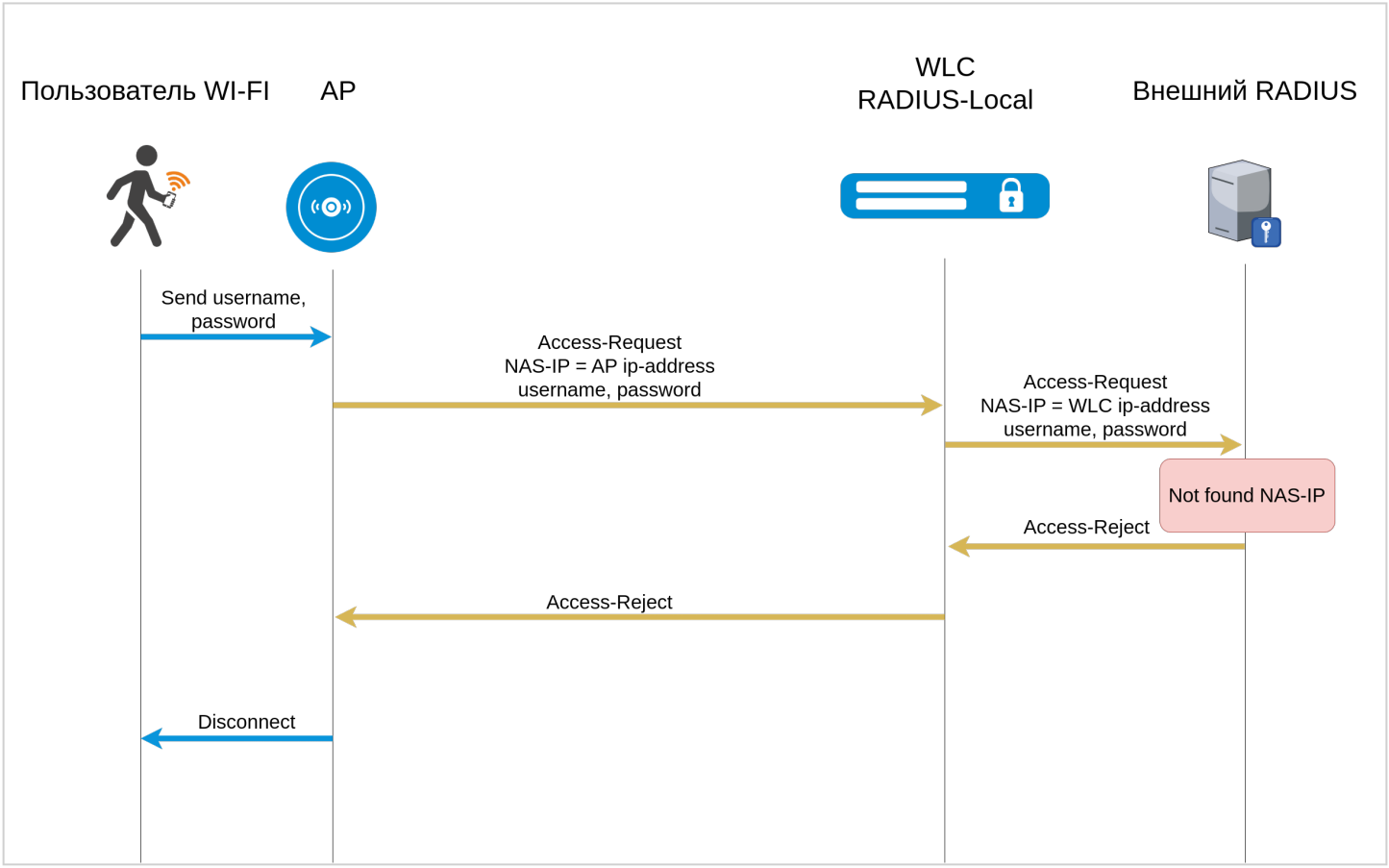
```
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    auth-acct-id-send
    acct-enable
    acct-address 192.168.1.1
    acct-password ascii-text encrypted 8CB5107EA7005AFF
    acct-periodic
    domain default
  exit
  wids-profile default-wids
    description "default-wids"
  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

ip tftp client timeout 45
ntp enable
ntp server 100.110.0.65
exit

ip https server
```

Возможные проблемы

Рассмотрим возможные проблемы при авторизации.

Запрет доступа по причине неправильного NAS-IP

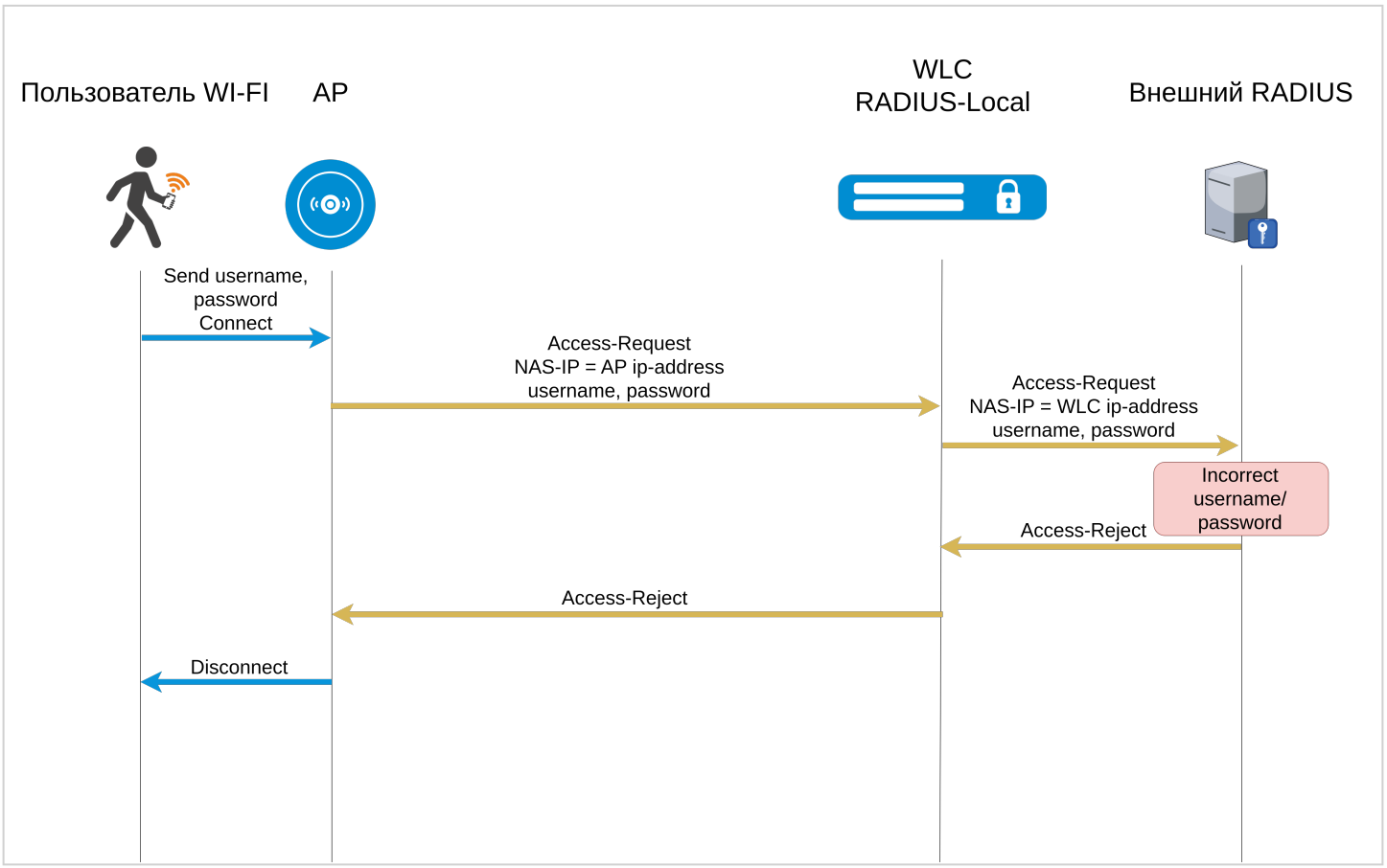
Рассмотрим один из вариантов запрета доступа, где причиной является отсутствие записи NAS-IP в конфигурации внешнего RADIUS-сервера.



В данном примере внешний RADIUS-сервер на входящий запрос (Access-Request), ответит (Access-Reject). Может быть две причины такого ответа.

При настройке проксирования RADIUS запросов на WLC указывается параметр подмены NAS-IP. В случае, если он не указан, запросы будут пересылаться на внешний RADIUS-сервер без подмены NAS-IP. В результате внешний RADIUS-сервер получит запрос с NAS-IP ТД. Если на внешнем RADIUS-сервере включена проверка по NAS-IP, запрос на подключение будет отклонён. Если подмена *NAS-IP* в конфигурации проксирования RADIUS на WLC настроена, но внешний RADIUS-сервер присылает ответ (Access-Reject), необходимо проверить наличие адреса WLC в NAS-клиентах в конфигурации внешнего RADIUS-сервера.

Запрет доступа по причине ошибки аутентификации



Данный пример описывает проблему ответа о запрете доступа (Access-Reject) на запрос (Access-Request).

Причиной такого ответа является отсутствие учетной записи клиента на внешнем RADIUS-сервере. В таком случае необходимо проверить наличие учетной записи клиента в конфигурации внешнего RADIUS-сервера и корректность введенных клиентом данных (логина и пароля).

23.3 TLS-авторизация

- Настройка TLS-авторизации
  - Генерация клиентского сертификата
    - Генерация private-key
    - Генерация csr
    - Генерация сертификата, подписанного CA от RADIUS
    - Генерация сертификата с ограничением срока действия.
    - Создание контейнера PKCS #12 с ключом и сертификатами
  - Настройка radius-server local
  - Настройка SSID и RADIUS-профиля
  - Настройка пользователя
- Установка клиентского сертификата
  - Экспорт сертификата
  - Установка сертификата для устройств с Android версии 11 и выше
  - Установка сертификата в iOS
    - Установка корневого сертификата
    - Установка пользовательского сертификата
  - Установка сертификата в Windows
- Подключение к SSID с поддержкой TLS

- Подключение с Android
- Подключение с Windows
- Подключение с Ubuntu
- Подключение с iOS
- Обновление и замена серверного сертификата

23.3.1 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@w
lc.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
```

При этом по умолчанию будет сгенерирован сертификат сроком действия на 100 лет

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
```

Генерация сертификата с ограничением срока действия.

Для того чтоб ограничить срок действия сертификата, существуют дополнительные параметры:

valid-after <TIME> <DAY> <MONTH> <YEAR>
invalid-after <TIME> <DAY> <MONTH> <YEAR>

valid-after - время и дата, после которых сертификат будет валиден;
invalid-after - время и дата, после которых сертификат будет невалиден;

- <YEAR> – год, принимает значения [1970..2100];
- <MONTH> – месяц, принимает значения [January/February/March/April/May/June/July/August/
- September/October/November/December];
- <DAY> – день месяца, принимает значения [1..31];
- <TIME> – время, задаётся в виде HH:MM:SS, где:
    - HH – часы, принимает значение [0..23];
    - MM – минуты, принимает значение [0 .. 59];
    - SS – секунды, принимает значение [0 .. 59].

Пример команды генерации сертификата с ограничением по сроку действия

```
wlc# crypto generate cert csr tester.csr ca default_ca.pem private-key default_ca_key.pem
valid-after 00:03:00 01 September 2024 invalid-after 06:53:00 02 March 2025 filename tester.crt
```

Пример сгенерированного сертификата

```
wlc# sh crypto certificates cert tester.crt
Version:                                        3
Serial:                                         35:6C:D5:AD:E6:F3:7C:CE:B7:D2:69:3B:E9:32:31:3
0:24:7E:
                                                A9:50
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:                                2024-09-01 00:03:00
    Invalid after:                              2025-03-02 06:53:00
Signature:
    Algorithm:                                  sha256WithRSAEncryption
    Value:                                      49:F2:98:0E:73:84:3C:22:32:6E:19:BF:03:DF:2E:
6E:A9:37:
                                                80:20:33:41:DF:51:0D:46:97:61:F9:05:80:BF:11:
9C:8F:DD:
                                                E8:C0:E4:C2:3E:A4:F9:C6:CF:2F:AE:38:30:47:17:8
9:5F:7F:
                                                2C:CC:D0:9E:13:AF:6F:AA:F2:FD:B0:29:93:04:B5:9
2:DC:8F:
                                                AB:C3:56:F8:47:D3:0C:6F:28:00:E3:6B:2E:64:62:5
2:64:AA:
                                                78:9F:C4:70:18:6B:BE:FB:A9:D7:32:87:06:0E:21:
E3:32:CE:
                                                4F:66:06:02:A3:A7:79:D9:50:DD:33:05:4C:28:40:4
6:F8:64:
                                                EB:31:25:FA:4B:8B:D7:53:46:26:25:16:33:3D:49:
E4:DF:C4:
                                                0B:BA:CB:01:BC:2E:1E:93:DC:81:39:33:D6:29:9B:0
2:39:2E:
                                                7E:F6:F4:31:1C:A0:A6:A8:56:5A:A2:CB:B3:D8:58:
C5:1F:9E:
                                                67:23:E2:FE:D7:5A:FB:A3:B5:E9:ED:4B:8D:C5:93:9
4:C2:1D:
```

```
                                                    62:20:63:5B:FB:62:A1:94:EE:91:F2:0A:AC:E7:1B:
A4:0A:F9:
                                                    2D:03:E8:46:C8:13:99:46:5B:2F:C5:2F:AF:FA:6D:
B2:A5:1B:

BA:CC:E9:8B:6C:B9:8D:E3:4C:F0:7D:FB:E1:B7:C1:B7:1E:3D:
                                                    EE:F7:8F:1E
Public key info:
    Algorithm:                                      RSA
    Key size:                                       4096
    Exponent:                                       65537
    Modulus:                                        00:A3:FE:21:A6:17:66:0E:B1:CA:F3:18:D1:27:3E:9
0:B8:89:
                                                    EE:F3:20:BE:FC:2F:D5:86:C7:F1:DA:25:9D:B2:60:
4A:4E:94:
                                                    AC:57:0E:46:65:A7:75:45:C0:07:EA:2D:8B:D4:08:
CF:FC:FA:
                                                    D2:9D:32:AB:F9:43:85:C8:A3:74:34:CB:F6:D0:A5:8
2:CF:6B:
                                                    10:4B:1D:81:42:68:74:10:7C:E6:E3:60:9C:9E:FD:
C1:0A:52:
                                                    8C:8F:E5:F1:27:72:BC:CC:26:15:1F:1C:C0:EA:AB:
D8:4D:45:
                                                    C6:D2:9D:D3:A9:6A:52:6C:8F:D4:A5:BF:04:C3:5D:
FA:18:2B:
                                                    7D:83:93:B1:B8:84:40:59:80:18:6A:75:96:DB:E4:
7F:D9:F2:
                                                    E7:64:52:AD:FF:60:11:D0:0A:CD:71:99:9A:6A:5B:
F6:42:07:
                                                    83:AF:45:7D:09:E6:DB:A1:63:E2:27:C0:67:54:E1:
CA:7D:F1:
                                                    0F:68:77:6E:C5:31:F5:09:0F:19:F1:FE:46:A9:DB:
0D:DB:B9:
                                                    BC:2F:02:70:86:CD:7F:B2:A2:07:37:F1:48:E4:CB:
9C:34:64:
```

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
```

23.3.2 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.

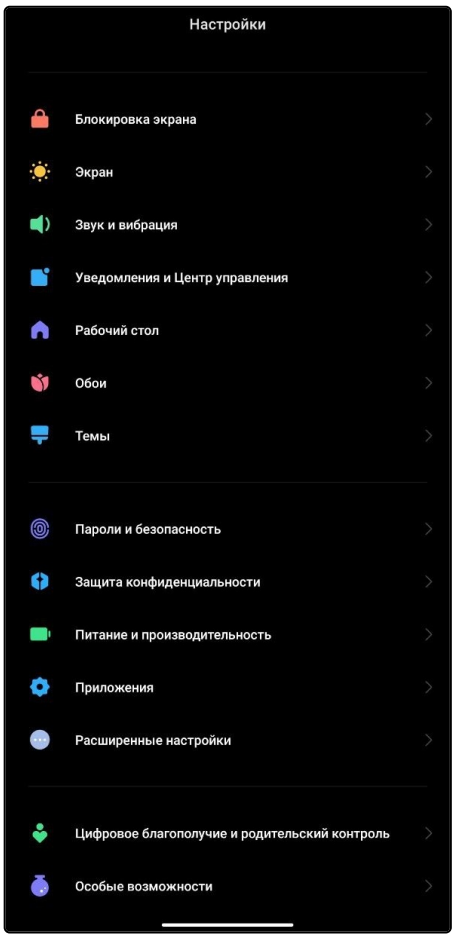
Пример команды экспорта сертификата с помощью tftp

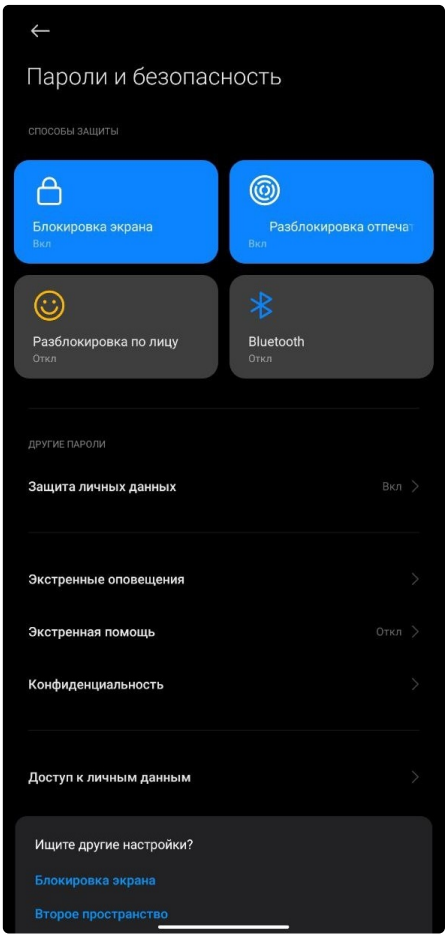
```
wlc# copy crypto:pfx/tester.p12 tftp://100.110.1.79:/tester.p12
|****************************************| 100% (2861B) Success!
```

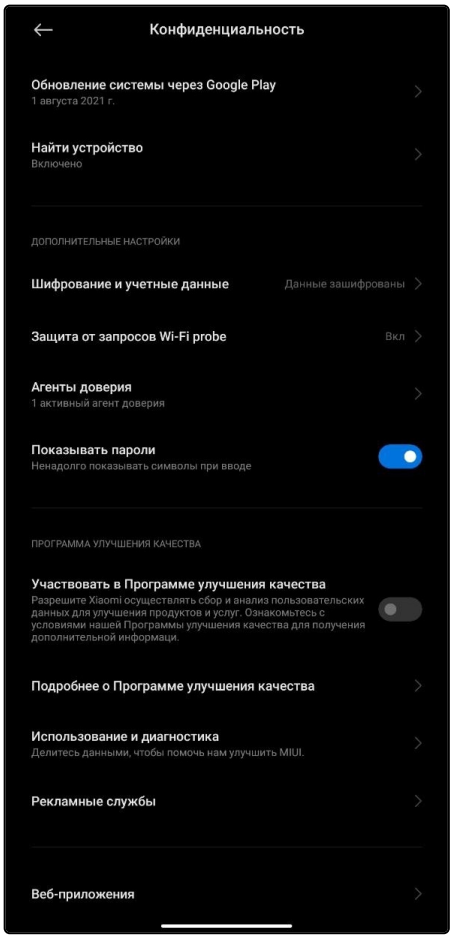
Установка сертификата для устройств с Android версии 11 и выше

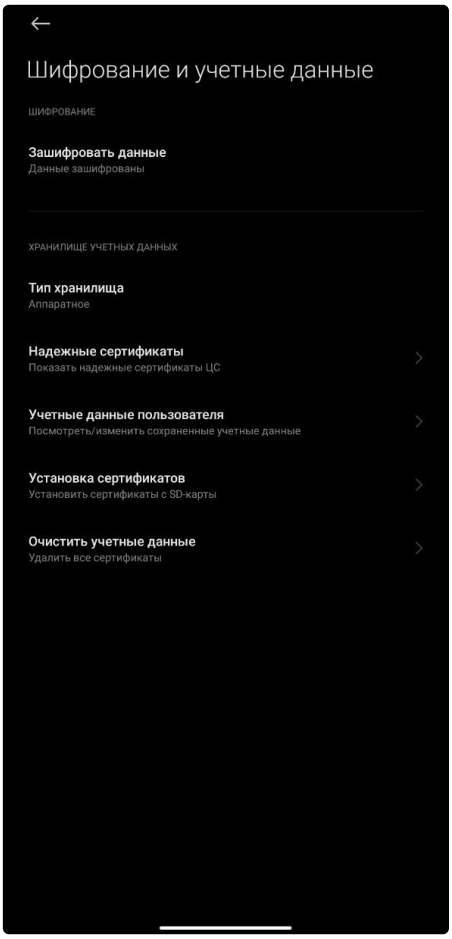
Для установки сертификата на устройство с Android скопируйте содержимое архива на клиентское устройство.

1. Зайдите в настройки устройства и откройте раздел "Пароли и безопасность" → "Конфиденциальность" → "Шифрование и учетные данные";

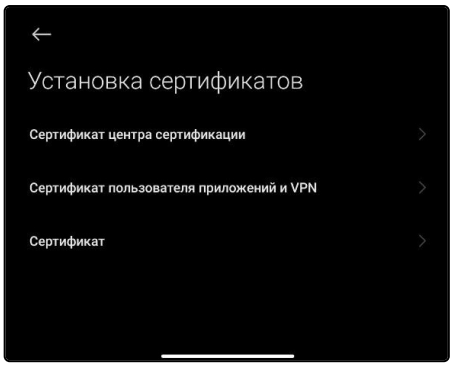






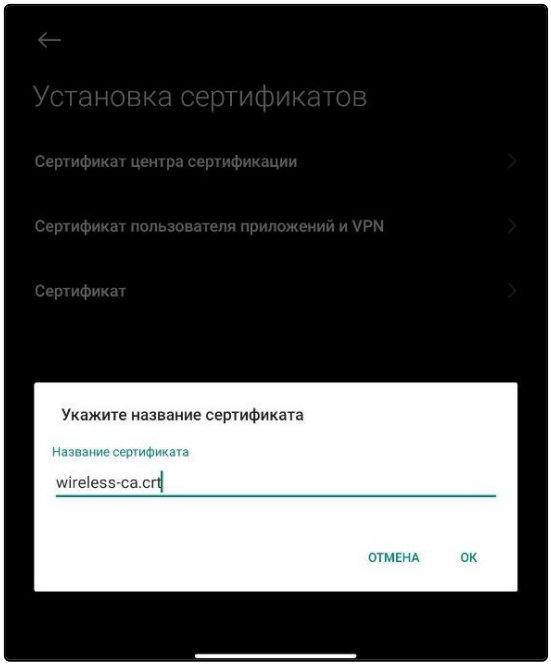


4. Если имеются старые сертификаты, то их можно удалить кнопкой "Очистить учетные данные";
5. Для загрузки новых сертификатов нажмите кнопку "Установка сертификатов";
6. Корневой и пользовательский сертификаты устанавливаются нажатием кнопки "Сертификат".

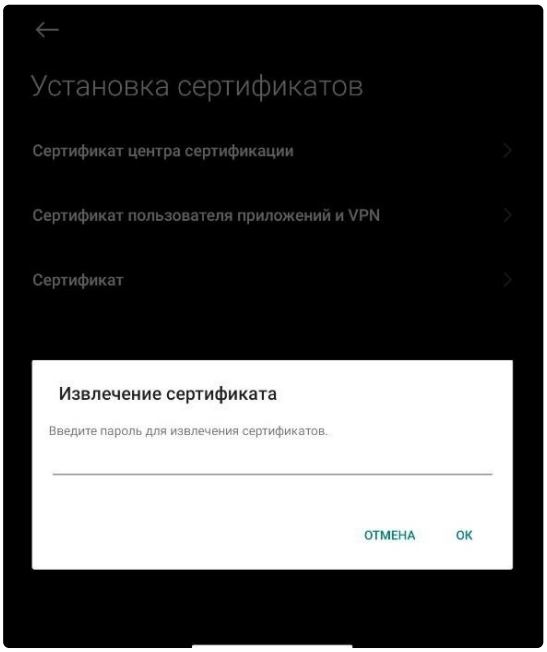


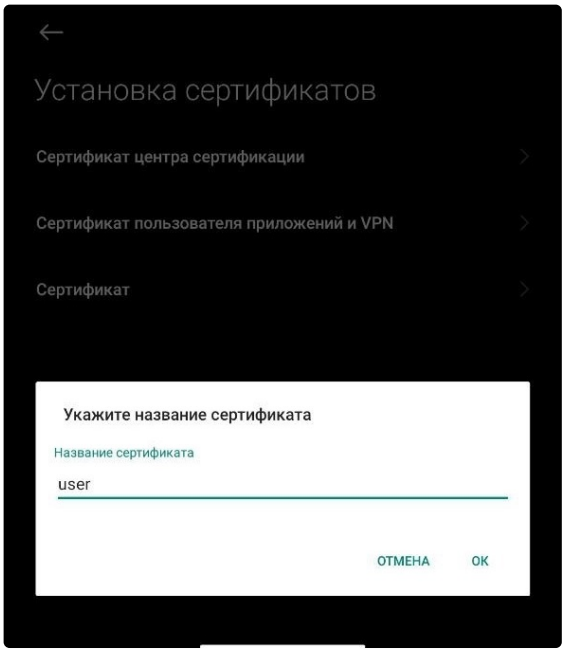
7. Выберите расположение распакованного архива;

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.



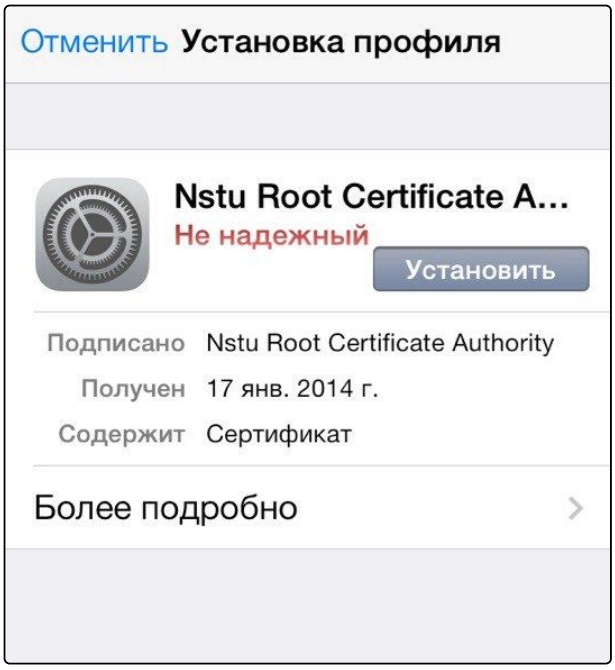


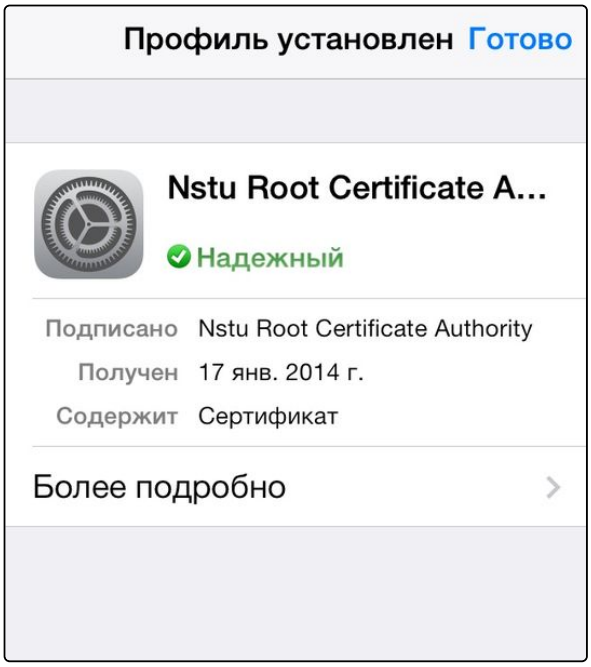
Установка сертификата в iOS

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

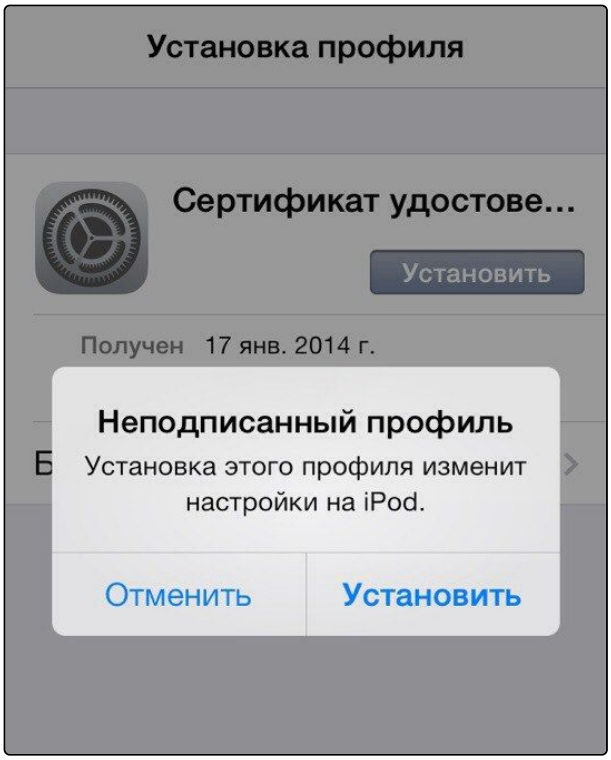
Открыв письмо с вложенным файлом стандартными приложениями iOS (Safari, Mail), нажмите на файл с расширением *.crt. При установке сертификата система будет предупреждать о ненадежности профиля, разрешите установку и сертификат будет успешно установлен.

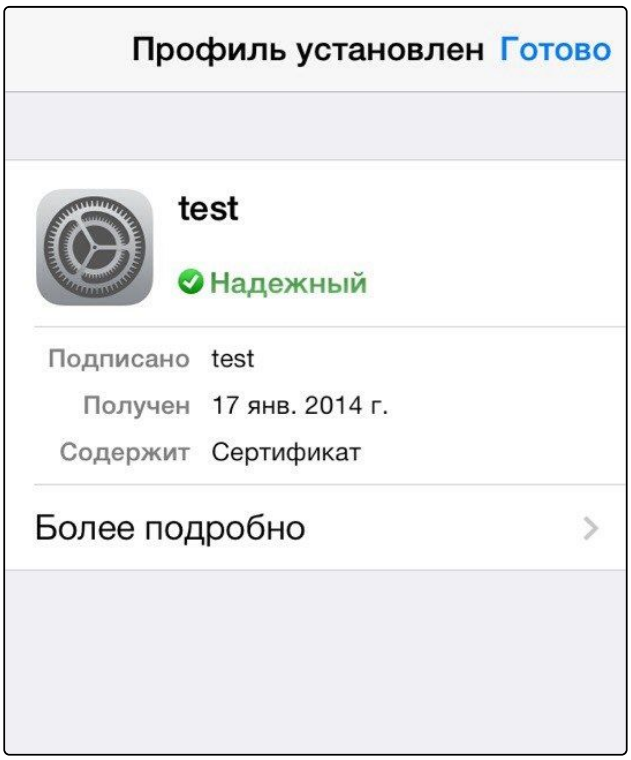


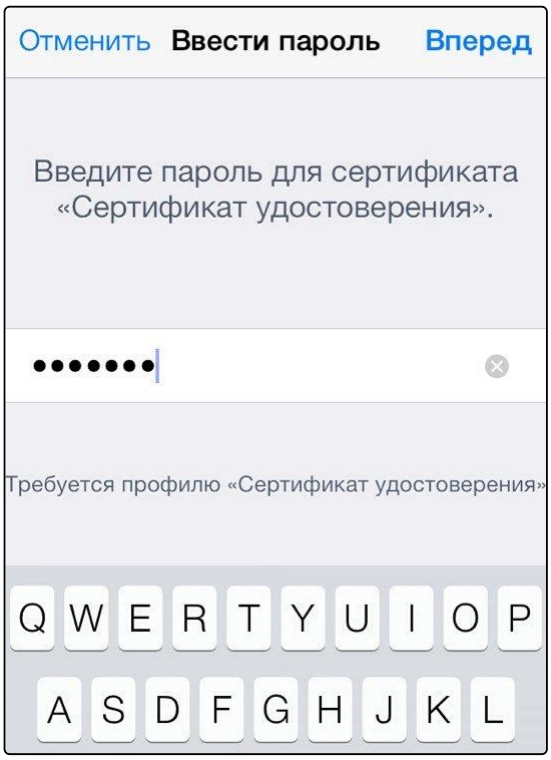


Установка пользовательского сертификата

Установка пользовательского сертификата происходит аналогично установке корневого сертификата. Далее необходимо ввести пароль сертификата. Пароль соответствует параметру сертификата Password, который находится в файле .txt.

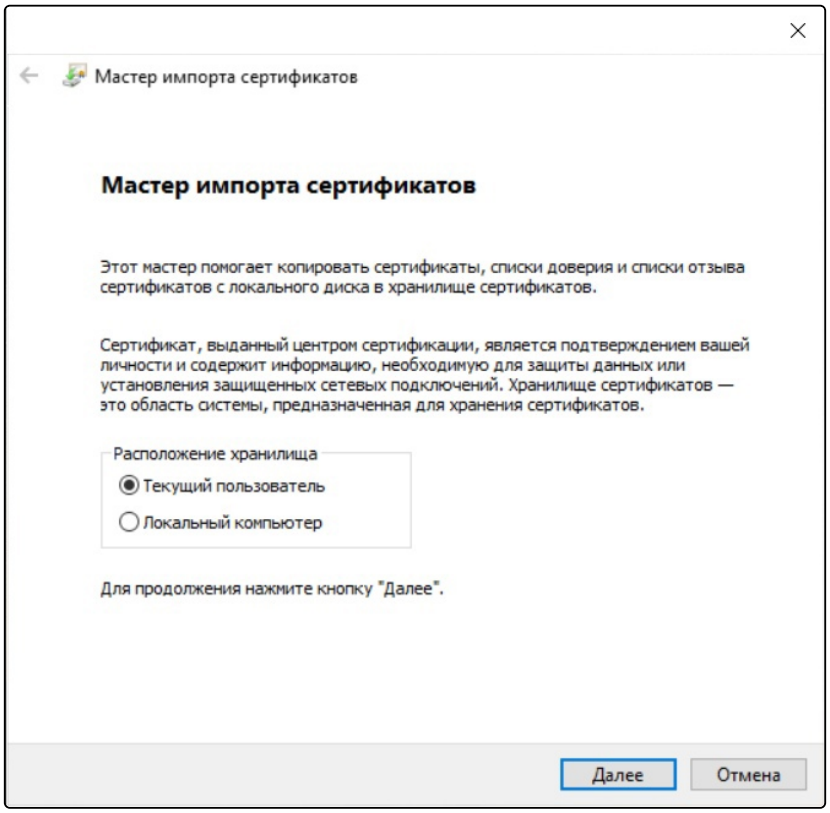

Установка профиля
Сертификат удостове...
Установить
Получен 17 янв. 2014 г.
Неподписанный профиль
Установка этого профиля изменит настройки на iPod.
Отменить
Установить


Профиль установлен
Готово
test
Надежный
Подписано test
Получен 17 янв. 2014 г.
Содержит Сертификат
Более подробно

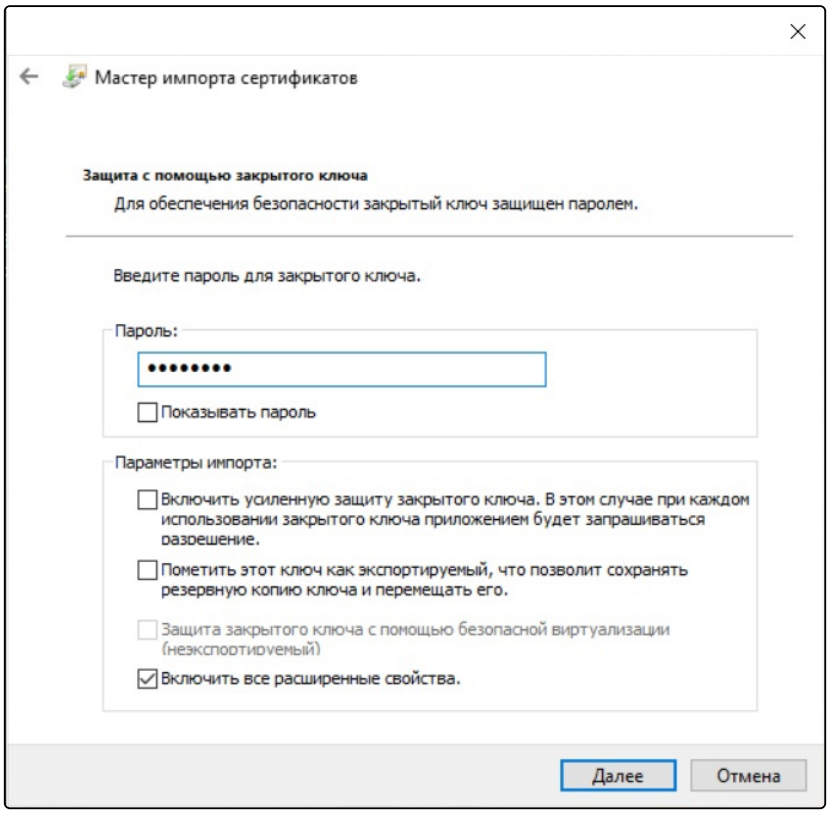

Отменить
Ввести пароль
Вперед
Введите пароль для сертификата «Сертификат удостоверения».
Требуется профилю «Сертификат удостоверения»
Q W E R T Y U I O P
A S D F G H J K L

Установка сертификата в Windows

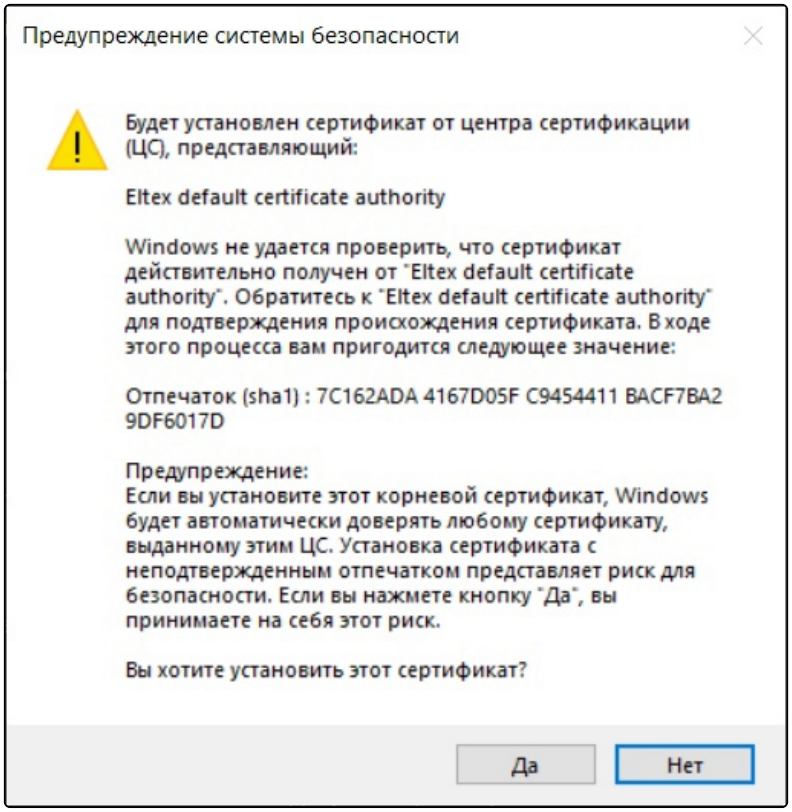
1. Откройте файл .p12. Параметры менять не нужно. Нажмите "Далее".



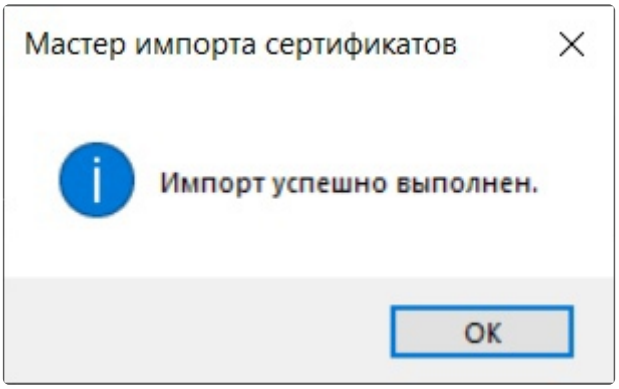
2. Введите пароль. Он соответствует параметру сертификата Password, который вы указали при генерации контейнера на wlc.



3. Подтвердите установку пользовательского сертификата.



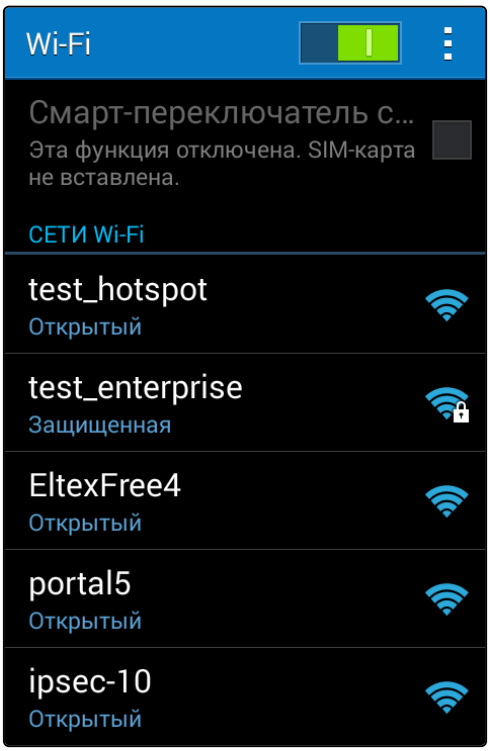
4. При успешной установке пользовательского и корневого сертификата отобразится следующий экран.



23.3.3 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:

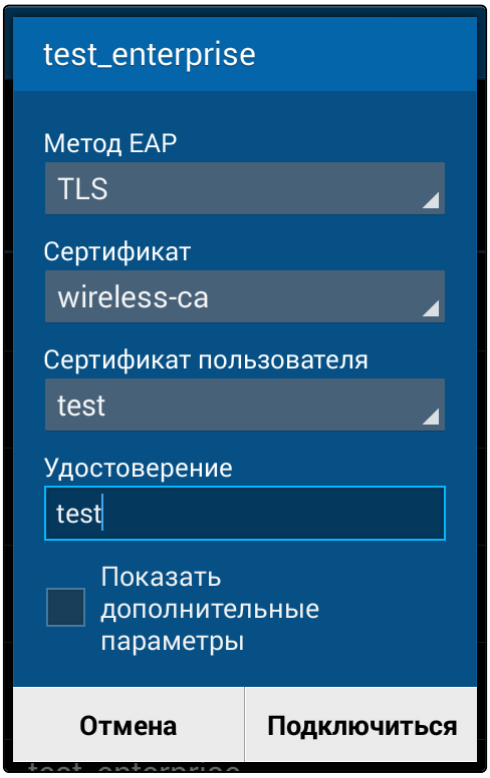
   Метод EAP: TLS

   Сертификат: wireless-ca

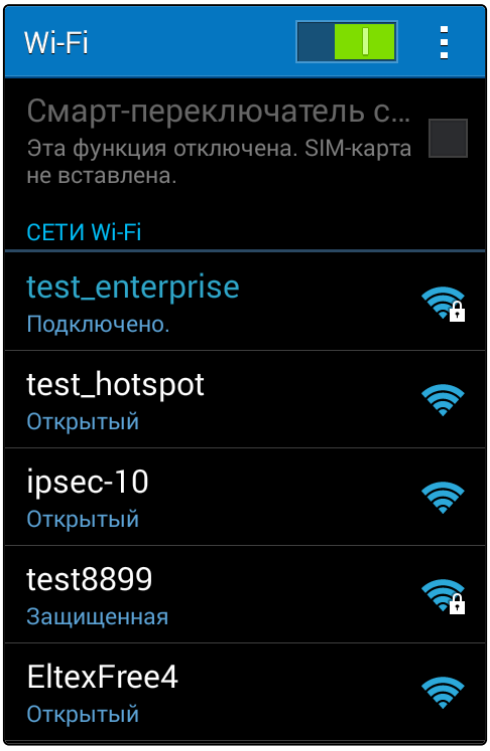
   Сертификат пользователя: test

   Удостоверение: test

   Значение параметра "Удостоверение" задается в соответствии с именем пользователя в сертификате.

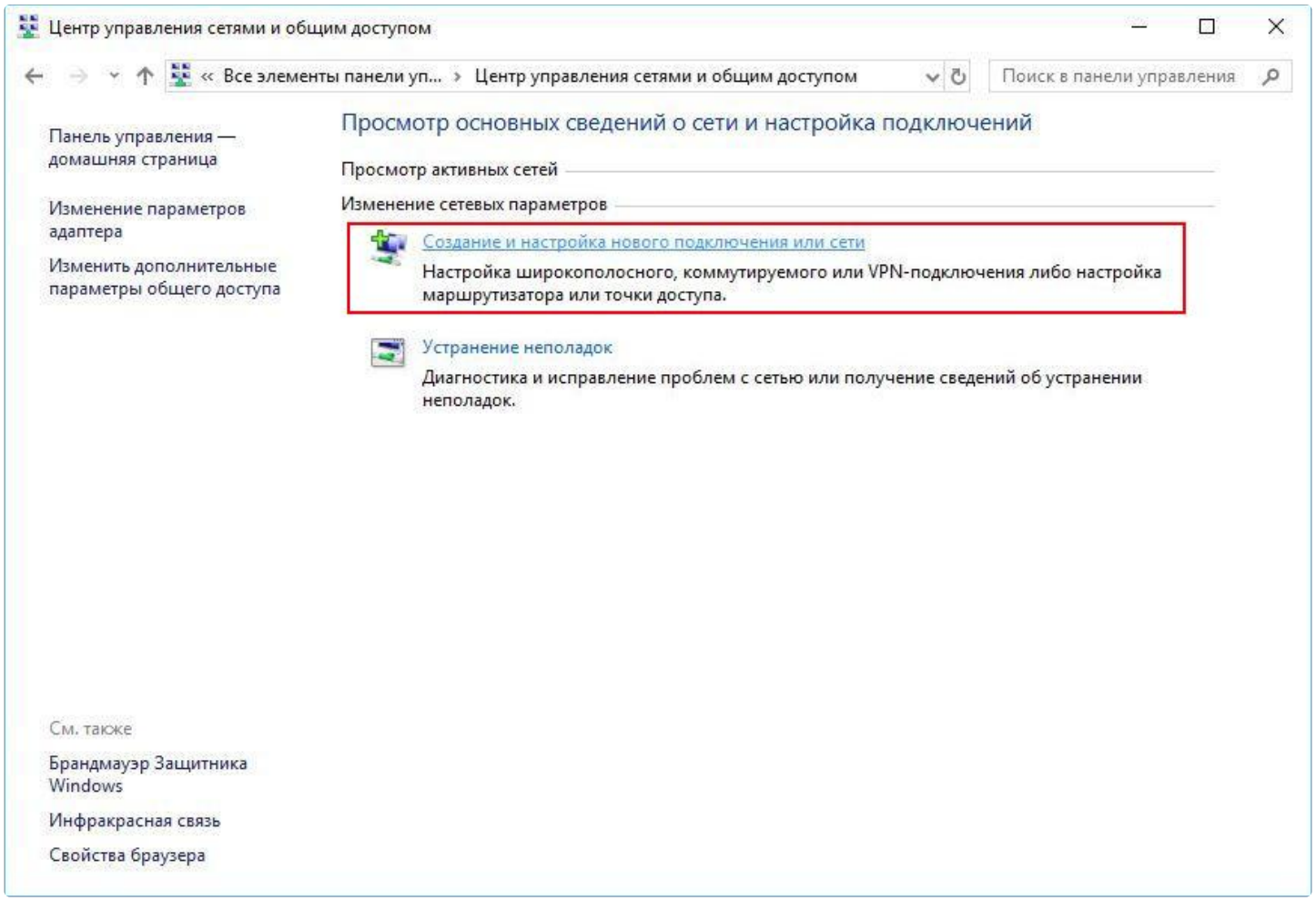


3. Если параметры введены верно, авторизация пройдет успешно.

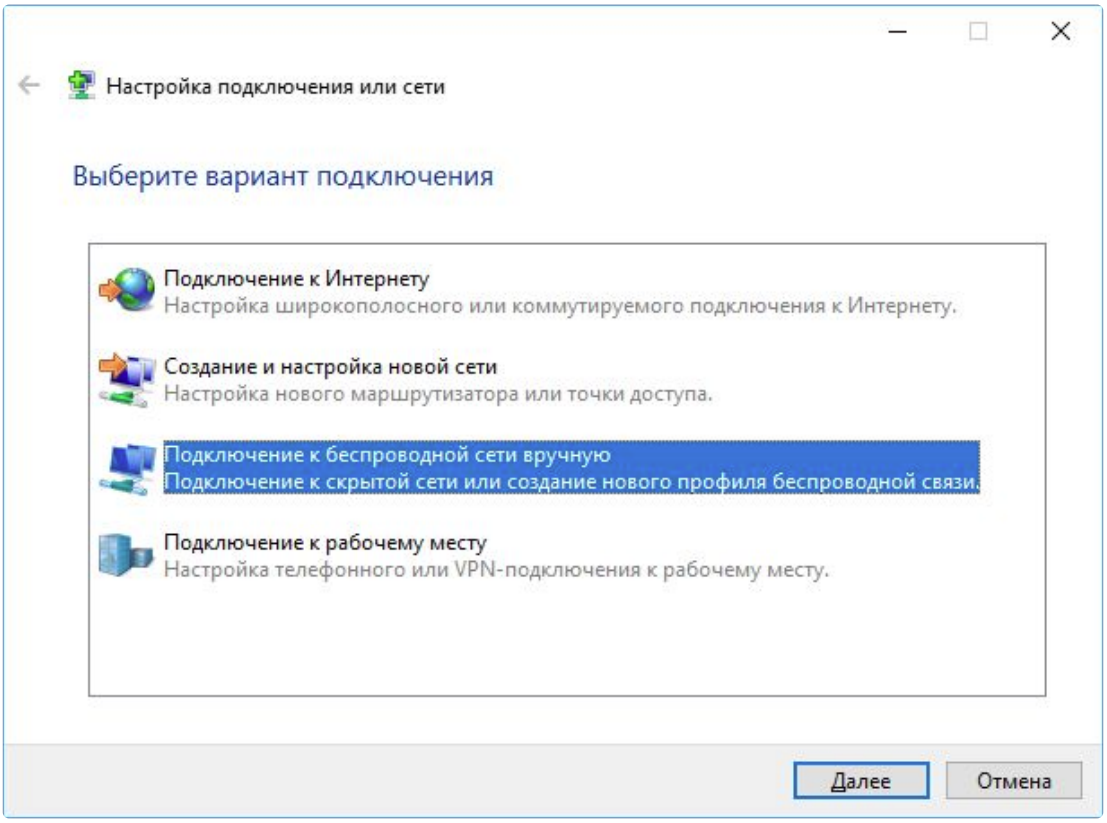


Подключение с Windows

Для создания и настройки нового подключения перейдите в "Центр управления сетями и общим доступом" → "Создание и настройка нового подключения или сети".



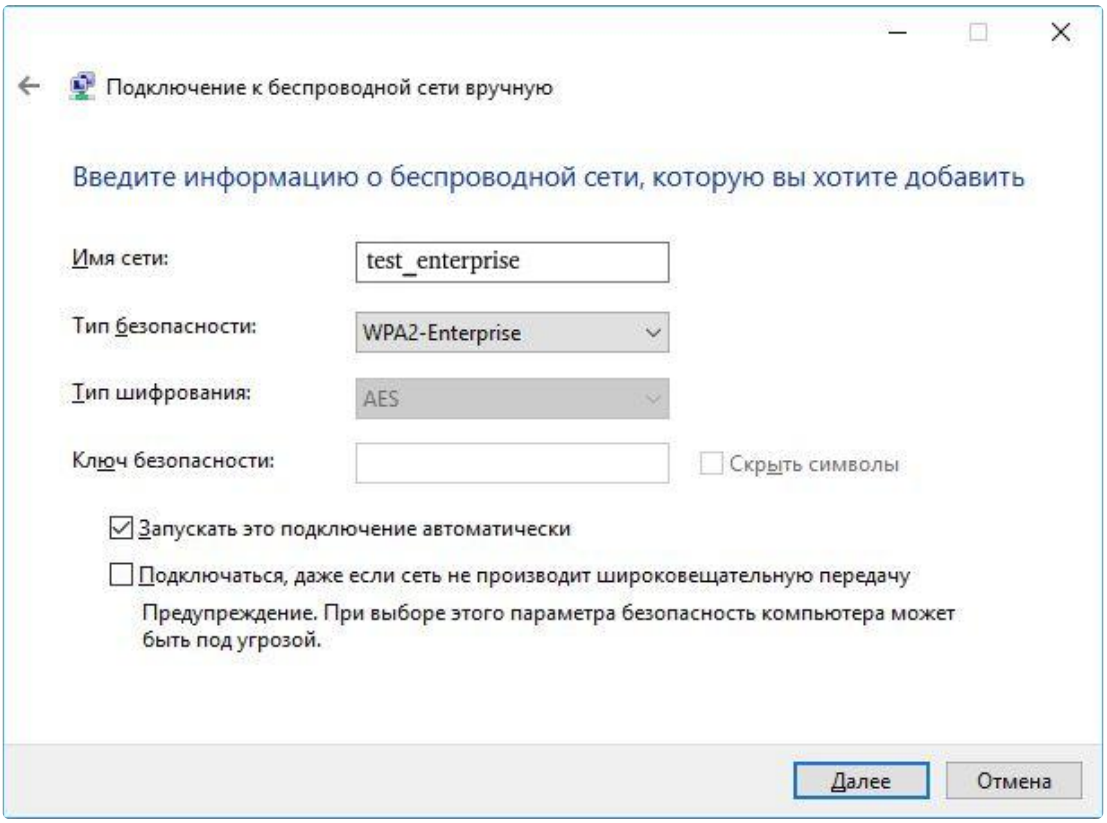
В открывшемся окне выберите пункт "Подключение к беспроводной сети вручную" и нажмите "Далее".



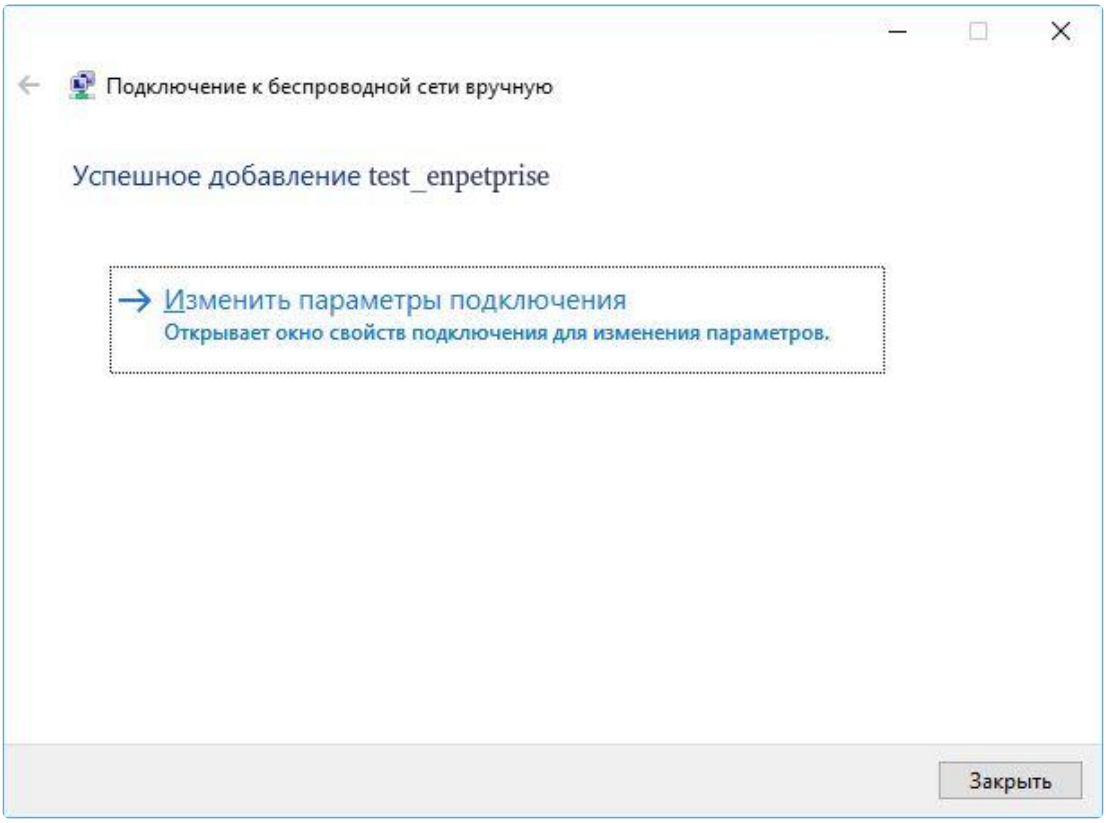
Введите информацию о беспроводной сети:

- Имя сети;
- Тип безопасности: WPA2-Enterprise.

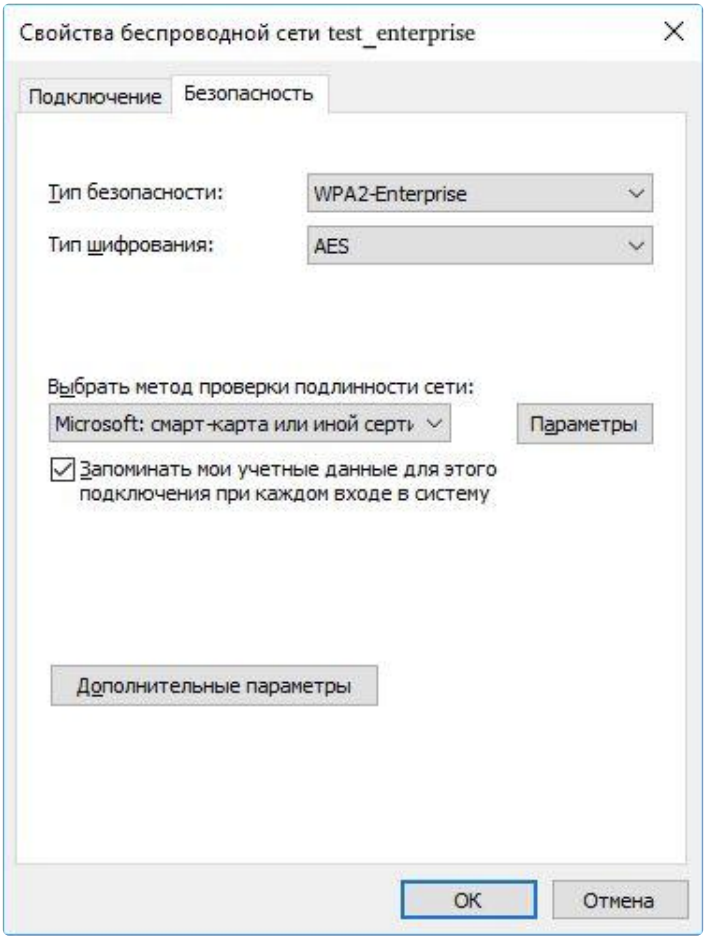
Установите флаг "Запускать это подключение автоматически". Нажмите "Далее".



Сеть успешно добавлена. Далее необходимо настроить параметры подключения.



Откройте раздел "Безопасность", выберите метод проверки подлинности "Microsoft: смарт-карта или иной сертификат". Нажмите кнопку "Параметры".

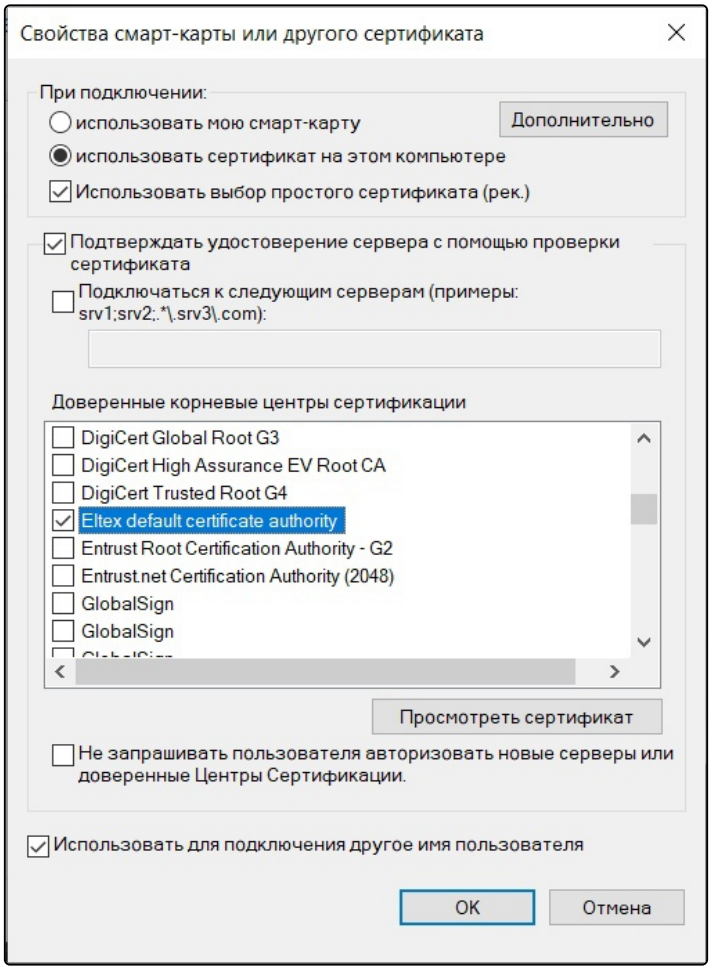


Установите следующие флаги:

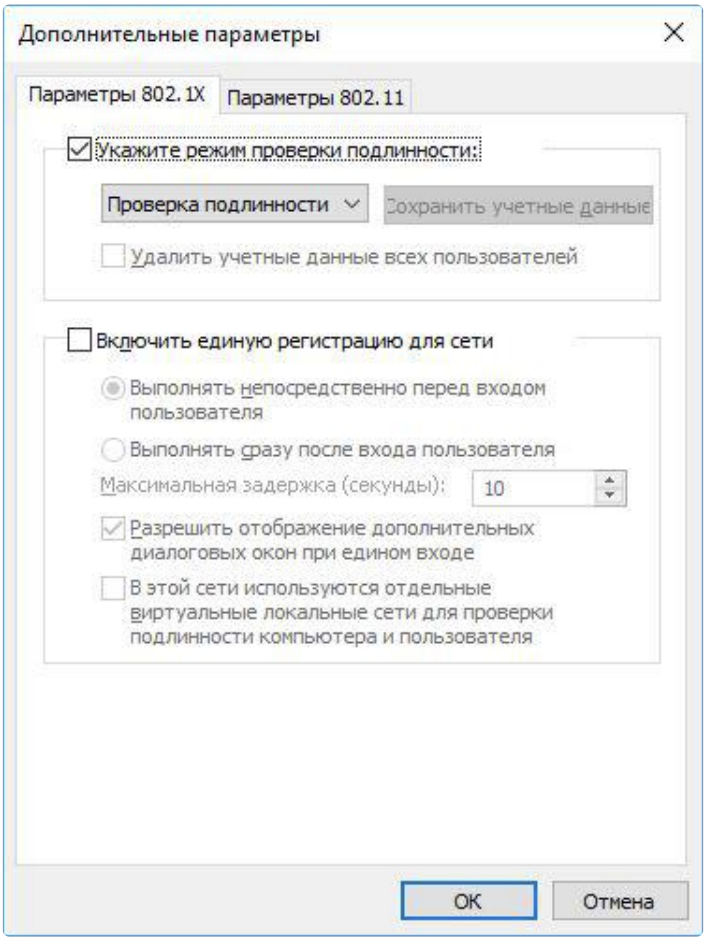
- Использовать сертификат на этом компьютере;
- Использовать выбор простого сертификата;
- Подтверждать удостоверение сервера с помощью проверки сертификата;
- Использовать для подключения другое имя пользователя.

В списке "Доверенных корневых центров сертификации" выберите корневой сертификат "**Eltex default certificate authority**". Это сертификат УЦ, который установился при установке клиентского сертификата.

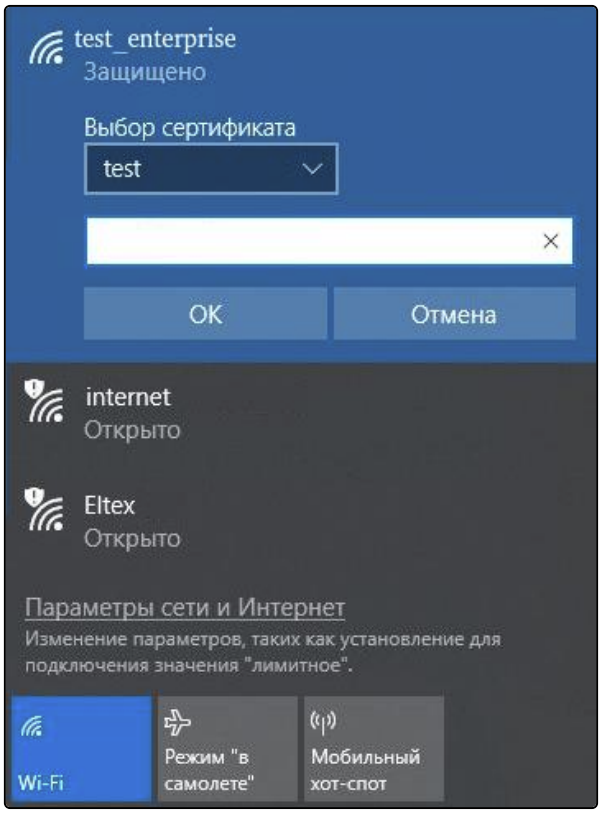
Нажмите кнопку "ОК". В открывшемся окне выберите "Дополнительные параметры".



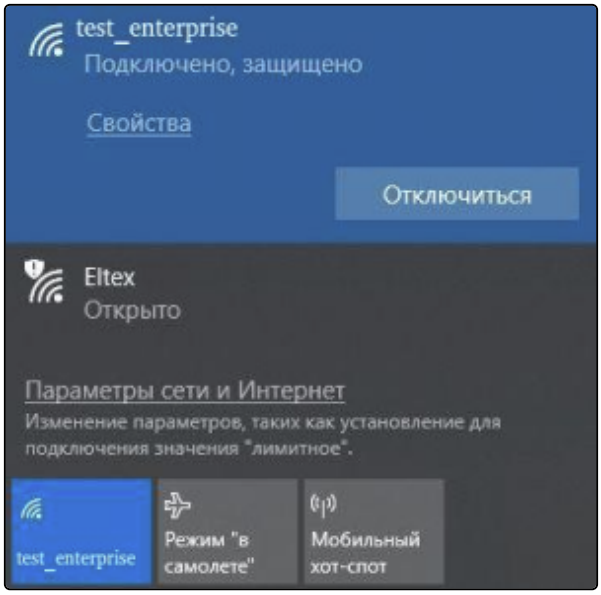
Укажите режим проверки подлинности – "Проверка подлинности пользователя". Нажмите "ОК".



Найдите нужную сеть и нажмите "Подключиться". Выберите пользовательский сертификат для подключения к сети и введите логин пользователя. Нажмите "ОК".

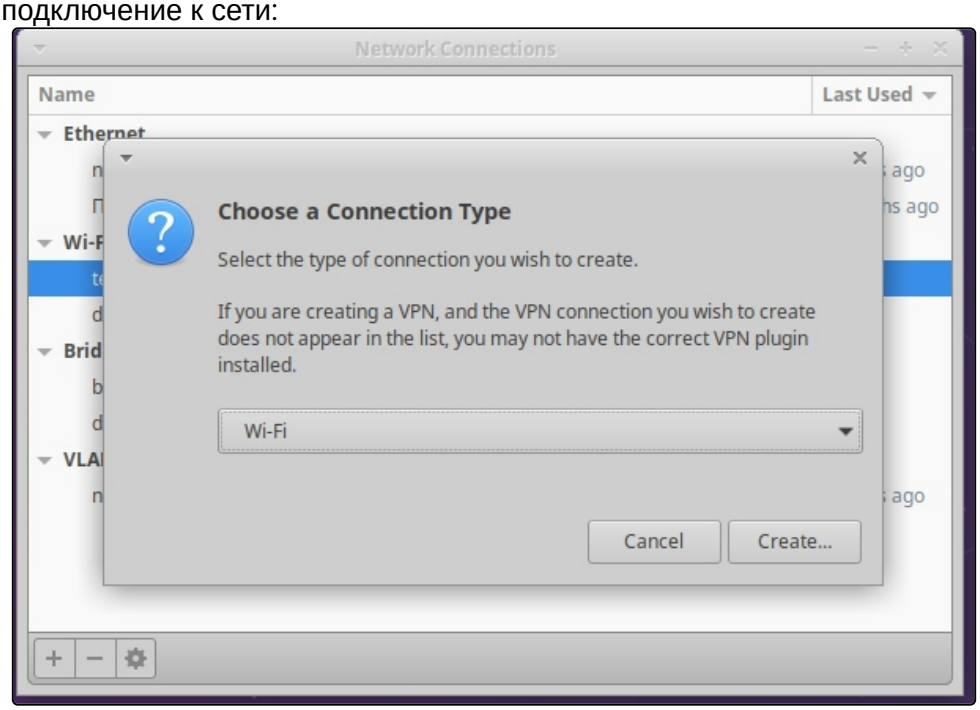


Если параметры введены верно, подключение пройдет успешно.

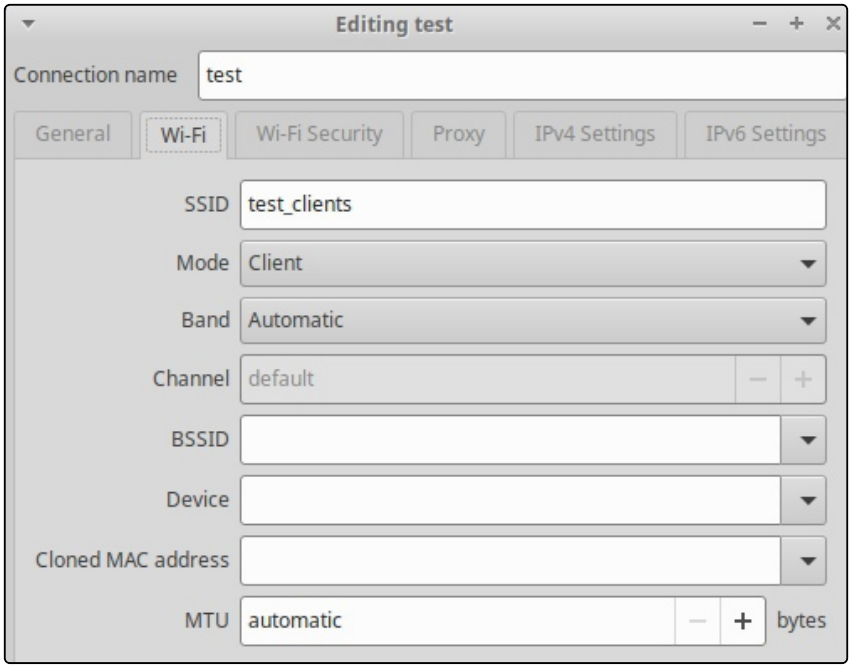


Подключение с Ubuntu

Создайте новое подключение к сети:

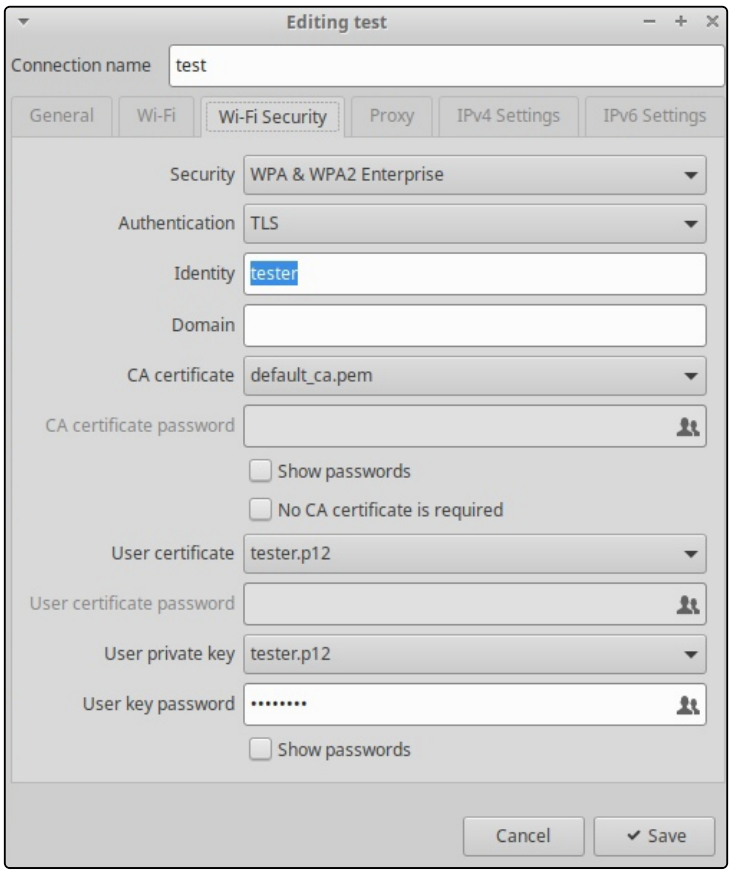


Укажите ssid:



Введите параметры для подключения к сети:

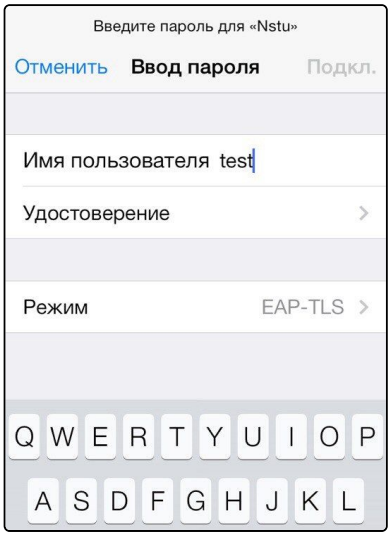
- Security – WPA & WPA2 Enterprice;
- Authentication – TLS;
- Identity – имя пользователя на радиус сервере;
- CA certificate – сертификат УЦ (скачивается с wlc отдельно);
- User certificate – контейнер с сертификатом клиента;
- User private key – контейнер с сертификатом клиента (он также содержит ключ);
- User key password – пароль импорта, заданный при генерации контейнера.

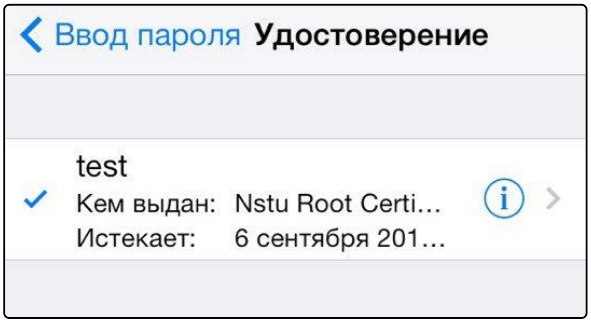


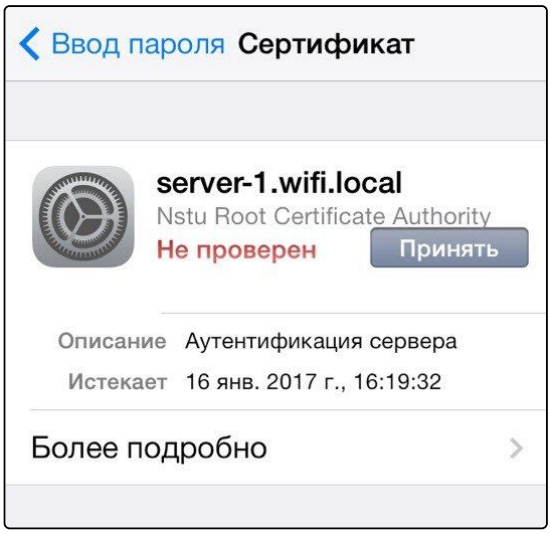
Если параметры введены верно, подключение пройдет успешно.

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".







23.3.4 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.

23.4 WIDS/WIPS

- Описание
- Лицензирование
- Управление
  - Активация сервиса
  - Порядок применения настроек
  - Настройка сервиса на точке доступа и логика работы
    - Атака "Человек посередине" (Man-in-the-Middle, MITM)
      - Обнаружение вредоносных ТД
      - Предотвращение угроз (WIPS)
      - Обнаружение атак деаутентификации клиентов
    - Атака "Отказ в обслуживании" (denial-of-service, DoS)
    - Атака "Перебор паролей" (Bruteforce)

23.4.1 Описание

WIPS/WIDS – внутренний сервис точки доступа (ТД) по обнаружению и предотвращению вторжений в беспроводную сеть.

Функционал WIDS/WIPS доступен на следующих ТД:
WEP-3ax – начиная с версии ПО 1.14.0.
WEP-30L, WEP-30L-Z, WOP-30L, WOP-30LS, WOP-30LI – начиная с версии ПО 2.6.0.
WEP-200L, WOP-20L – начиная с версии ПО 2.7.0.

Данный механизм анализирует трафик в радиоокружении ТД, делает вывод о наличии в сети угроз безопасности, оповещает о них администратора контроллера и, при необходимости, предпринимает действия для подавления этих угроз.

Поддержан следующий функционал WIDS/WIPS:

1. Обнаружение DDoS-атак.
2. Отслеживание перебора паролей.
3. Обнаружение точек доступа, имитирующих SSID.
4. Обнаружение точек доступа, имитирующих MAC-адрес.
5. Отключение клиентов от вражеских ТД.
6. Обнаружение атак деаутентификации клиентов.

23.4.2 Лицензирование

Функционал WIDS/WIPS активируется лицензией WLC-WIDS-WIPS. Информация о загрузке и применении лицензии описана в статье Активация функционала по лицензии.

Проверить наличие лицензии можно с помощью команды **show licence:**

```
wlc# show licence
Feature                          Source     State         Value
Valid from              Expiries
-------------------------------  --------   -----------   --------------------------------
--------------------    --------------------
WLC                              Boot       Active        true
--                      --
WLC                              Boot       Candidate     true
--                      --
WLC-WIDS-WIPS                    File       Active        true
--                      --
WLC-WIDS-WIPS                    File       Candidate     true
--                      --
```

В случае отсутствия лицензии конфигурирование WIDS/WIPS доступно, но функционал не активирован.

23.4.3 Управление

Активация сервиса

Включить сервис можно только в общих настройках WIDS.
Если в общих настройках сервис выключен, то он не работает на всех ТД контроллера и включить его на отдельной ТД или в конкретной локации нельзя.

Предусмотрена возможность выключения сервиса в определенной локации или на конкретной ТД с помощью команды **wids-disable.** При этом команда **no wids-disable** в локации или в индивидуальном профиле ТД не означает, что сервис включен, если одновременно с этим он выключен в общих настройках WIDS.

Для включения сервиса используйте следующие команды:

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# wids
wlc(config-wlc-wids)# enable
wlc(config-wlc-wids)# shared-key ascii-text 0123456789
wlc(config-wlc-wids)# do commit
wlc(config-wlc-wids)# do confirm
```

Для включения сервиса обязательно должен быть задан общий ключ доверенных ТД 'shared-key'.

Все настройки сканирования и детектирования атак содержатся в профиле WIDS. По умолчанию в общих настройках WIDS используется профиль с названием default-wids, это можно увидеть в полной конфигурации контроллера с помощью команды **sh ru full wlc wids:**

```
wlc# sh ru full wlc wids
wids
  wids-profile default-wids
  shared-key ascii-text encrypted CCE5513EE45A1EAC450A
  enable
exit
```

Чтобы проверить параметры профиля используйте команду **sh ru full wlc wids-profile.** В данном случае профиль содержит настройки параметров по умолчанию.

```
wlc# sh ru full wlc wids-profile
wids-profile default-wids
  prevention-mode none
  attack-stats-trap-send-period 10
  scan
    mode none
    interface all
    passive interval 20
    passive time 110
    sentry time 200
  exit
  bruteforce-detection
    threshold 25
    interval 5
    no mac-ban enable
    mac-ban timeout 1800
    no enable
  exit
  dos-detection
    interval 1
    trap-send-period 20
    threshold leap 250
    threshold assoc 500
    threshold reassoc 500
    threshold disassoc 500
    threshold probe 500
    threshold beacon 500
    threshold blockack 500
    threshold blockack-req 500
    threshold ps-poll 500
    threshold auth 500
    threshold deauth 500
    threshold rts 500
    threshold cts 500
    no enable
  exit
exit
```

Порядок применения настроек

Существуют 3 варианта применения настроек:

1. На все ТД контроллера.

2. На ТД локации.

3. На конкретную ТД.

Приоритет применения настроек следующий: настройки индивидуального профиля, настройки локации, общие настройки сервиса.

В общих настройках сервиса задается общий ключ доверенных ТД, выбирается профиль настроек WIDS, а также белые и черные списки для более точной настройки "доверенных" и "вражеских" ТД. Все эти настройки можно переопределить на уровне локации, а также на конкретной ТД через индивидуальный профиль.

Настройка сервиса на точке доступа и логика работы

Атака "Человек посередине" (Man-in-the-Middle, MITM)

Атака, при которой используются методы перехвата данных, позволяющие внедриться в существующее подключение или процесс связи.

Обнаружение вредоносных ТД

Для определения вредоносных точек доступа необходимо настроить сканирование. Сканирование может быть пассивным или активным.

В пассивном режиме сканирования точка доступа периодически (через время, заданное в параметре 'passive interval') и кратковременно (на время, заданное в параметре 'passive time') меняет свой текущий радиоканал, на котором работает с клиентами, на очередной канал из общего списка, чтобы обнаружить другие ТД в эфире. Качество услуги, предоставляемой клиенту в момент сканирования, практически не деградирует.

В активном режиме сканирования не предусмотрена работа ТД с клиентами. ТД всё время сканирует весь список радиоканалов (продолжительность сканирования одного канала задается в параметре 'sentry time') и максимально быстро обнаруживает угрозы.

В результате сканирования ТД распределяет все ТД в эфире на три группы:

1. "Недоверенные" ТД – точки, которые присутствуют в эфире, но о них более ничего не известно;
2. "Доверенные" ТД – точки, которые установлены и управляются оператором;
3. "Вражеские" ТД – точки, которые несут угрозу для остальных ТД в сети – это ТД, которые имитируют MAC-адрес или SSID исходной ТД.

Для однозначного выявления всех "недоверенных" ТД эфире, в Beacon-пакет ТД, использующих сервис WIDS, добавляется динамически изменяющаяся зашифрованная подпись. Расшифровать пакет могут лишь те точки, на которых настроен идентичный общий ключ '*Shared key*' в конфигурации сервиса. Если подписи в пакете нет, либо при его декодировании получен не ожидаемый результат, то ТД, от которой был получен пакет, будет считаться "недоверенной". Иначе – "доверенной".

Если "недоверенная" ТД имеет MAC-адрес или SSID, совпадающий с текущими значениями на сканирующей ТД, то такая точка будет считаться "вражеской", о чем будет сообщено администратору, посредством отправки с ТД соответствующей нотификации на контроллер.

```
wlc# sh wlc journal wids attack mitm detected-rogue
2024-12-02T07:47:59+00:00 AP 68:13:e2:03:00:20 detected rogue AP with MAC e8:28:c1:ed:47:70,
RSSI: -15, channel: 6, SSID: wids_test, AP location: default-location, reason: fake SSID
```

Настройки сканирования выполняются в профиле WIDS. Ниже представлен пример настройки пассивного сканирования со временем сканирования одного канала 110 мс и интервалом между сканированием 30 с, и сканированием в обоих частотных диапазонах:

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# wids-profile test_wids_profile
wlc(config-wlc-wids-profile)# scan
wlc(config-wlc-wids-profile-scan)# mode passive
wlc(config-wlc-wids-profile-scan)# interface all
wlc(config-wlc-wids-profile-scan)# passive time 110
wlc(config-wlc-wids-profile-scan)# passive interval 30
wlc(config-wlc-wids-profile-scan)# do commit
wlc(config-wlc-wids-profile-scan)# do confirm
wlc(config-wlc-wids-profile-scan)#
wlc(config-wlc-wids-profile-scan)# do sh ru wlc wids-profile test_wids_profile
wids-profile test_wids_profile
  scan
    mode passive
    passive interval 30
    passive time 50
  exit
exit
```

Профиль можно применить:

1. На все ТД контроллера. Для этого необходимо указать профиль в общих настройках WIDS.

```
wlc(config)# wlc
wlc(config-wlc)# wids
wlc(config-wlc-wids)# wids-profile test_wids_profile
wlc(config-wlc-wids)# do commit
wlc(config-wlc-wids)# do confirm
wlc(config-wlc-wids)#
```

2. На ТД локации. Для этого необходимо указать профиль в настройках конкретной локации. Если одновременно профиль задан в общих настройках и в локации – будет использоваться профиль из локации.

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# ap-location default-location
wlc(config-wlc-ap-location)# wids
wlc(config-wlc-ap-location-wids)# wids-profile test_wids_profile
wlc(config-wlc-ap-location-wids)#
wlc(config-wlc-ap-location-wids)#
wlc(config-wlc-ap-location-wids)# do commit
wlc(config-wlc-ap-location-wids)# do confirm
wlc(config-wlc-ap-location-wids)#
```

3. На конкретную ТД. Для этого необходимо указать профиль WIDS в индивидуальном профиле ТД. Если одновременно профиль задан в общих настройках и/или в локации и в индивидуальном профиле ТД – будут использоваться настройки из индивидуального профиля ТД.

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# ap 68:13:e2:03:00:10
wlc(config-wlc-ap)# ap-location default-location
wlc(config-wlc-ap)# override wids
wlc(config-wlc-ap-wids-override)# wids-profile default-wids
wlc(config-wlc-ap-wids-override)# do commit
wlc(config-wlc-ap-wids-override)# do confirm
wlc(config-wlc-ap-wids-override)#
```

Для более гибкой работы сервиса, есть возможность явно указать список ТД, которые должны считаться "доверенными" ТД (white-list) или "вражескими"(black-list). Эти списки настраиваются в object-group, а применяются также на 3 уровнях – в общих настройках, в локации или индивидуально на ТД.

Приоритет применения списков следующий: настройки индивидуального профиля, настройки локации, общие настройки сервиса. В случае если на одном уровне задан только список одного вида (белого или черного), противоположный список будет использован со следующего уровня. Например, если в индивидуальном профиле ТД задан только черный список, то белый список будет взят из настроек локации. Если он не задан в локации, то будет взят из общих настроек сервиса.

Ниже представлен пример настройки списков для всех ТД контроллера, в котором в черном списке задан MAC-адрес e4:5a:d4:e8:d9:20 (эта ТД будет считаться "вражеской"), а в белом списке задан MAC-адрес e8:28:c1:d7:3c:20 (эта ТД будет считаться "доверенной"):

```
wlc# configure
wlc(config)# object-group mac AP1
wlc(config-object-group-mac)# mac address e4:5a:d4:e8:d9:20
wlc(config-object-group-mac)# ex
wlc(config)# object-group mac AP2
wlc(config-object-group-mac)# mac address e8:28:c1:d7:3c:20
wlc(config-object-group-mac)# ex
wlc(config)#
wlc(config)# wlc
wlc(config-wlc)# wids
wlc(config-wlc-wids)# black-list AP1
wlc(config-wlc-wids)# white-list AP2
wlc(config-wlc-wids)# do commit
wlc(config-wlc-wids)# do confirm
wlc(config-wlc-wids)#
wlc(config-wlc-wids)# do sh ru object-groups mac
object-group mac AP1
  mac address e4:5a:d4:e8:d9:20 ff:ff:ff:ff:ff:ff
exit
object-group mac AP2
  mac address e8:28:c1:d7:3c:20 ff:ff:ff:ff:ff:ff
exit
wlc(config-wlc-wids)#
wlc(config-wlc-wids)# do sh ru wlc wids
wids
  wids-profile test_wids_profile
  shared-key ascii-text encrypted CCE5513EE45A1EAC450A
  enable
  white-list AP2
```

```
  black-list AP1
exit
```

Если требуется задать пустой список, то необходимо создать пустую группу MAC-адресов и использовать ее на нужном уровне.

Пример настройки пустого списка:

```
wlc# configure
wlc(config)# object-group mac noAP
wlc(config-object-group-mac)# exit
wlc(config)# wlc
wlc(config-wlc)# wids
wlc(config-wlc-wids)# black-list noAP
wlc(config-wlc-wids)# do commit
wlc(config-wlc-wids)# do confirm
 wlc(config-wlc-wids)#
wlc(config-wlc-wids)# do sh ru object-groups mac noAP
object-group mac noAP
exit
wlc(config-wlc-wids)#
wlc(config-wlc-wids)# do sh ru wlc wids
wids
  wids-profile test_wids_profile
  shared-key ascii-text encrypted CCE5513EE45A1EAC450A
  enable
  white-list AP2
  black-list noAP
exit
```

Предотвращение угроз (WIPS)

Для настройки подавления угроз от вредоносных ТД, которые имитируют SSID или MAC-адрес сканирующей ТД, используется параметр prevention-mode. В случае активации режима 'Rogue', исходная ТД будет отправлять пакеты типа 'Deauthentification' от имени "вражеской" ТД ее клиентам. При использовании режима 'All' форсированные пакеты 'Deauthentification' будут отправляться не только "вражеским" ТД, но и всем "недоверенным".

Пример настройки подавления угроз от "вражеских" ТД:

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# wids-profile test_wids_profile
wlc(config-wlc-wids-profile)# prevention-mode rogue
wlc(config-wlc-wids-profile)# do commit
wlc(config-wlc-wids-profile)# do confirm
wlc(config-wlc-wids-profile)#
```

Применить профиль можно в общих настройках WIDS для всех ТД контроллера, в локации или индивидуально на ТД.

При активации режима подавления можно настроить период отправки на контроллер сообщений, содержащих статистику срабатываний функционала подавления угроз (WIPS). Для этого необходимо использовать параметр 'attack-stats-trap-send-period' и задать значение в минутах.

```
wlc(config-wlc-wids-profile)# attack-stats-trap-send-period 10
wlc(config-wlc-wids-profile)# do commit
```

```
wlc(config-wlc-wids-profile)# do confirm
wlc(config-wlc-wids-profile)#
```

При срабатывании функционала WIPS ТД будет отправлять нотификации на контроллер с указанной периодичностью. Сообщения можно увидеть в журнале событий:

```
wlc(config-wlc-wids-profile)# do sh wlc journal wids attack mitm our-attacks-information-update
2024-11-02T20:43:26+07:00 AP 68:13:e2:20:a2:10 attacked AP 68:13:e2:0e:85:51 on channel 1,
interface: wlan0, AP location: default-location1, description: broadcast-count 1012, unicast-
count 1
2024-11-02T20:43:26+07:00 AP 68:13:e2:20:a2:10 attacked AP e0:d9:e3:48:74:90 on channel 1,
interface: wlan0, AP location: default-location1, description: broadcast-count 1012, unicast-
count 1

2024-11-02T20:43:34+07:00 AP e8:28:c1:fc:d4:60 attacked AP e8:28:c1:d7:3c:22 on channel 1,
interface: wlan0, AP location: default-location1, description: broadcast-count 777, unicast-
count 0
2024-11-02T20:43:34+07:00 AP e8:28:c1:fc:d4:60 attacked AP 68:13:e2:21:1e:21 on channel 1,
interface: wlan0, AP location: default-location1, description: broadcast-count 777, unicast-
count 0
```

Обнаружение атак деаутентификации клиентов

В случае, если исходная точка доступа обнаружит отправку пакетов 'Deauthentification' своим клиентам (или широковещательно) от ее имени, она отправит на контроллер нотификацию об обнаружении атаки на себя:

```
wlc# sh wlc journal wids attack mitm detected-deauth-attack
2025-02-28T11:04:47+00:00 AP 68:13:e2:20:a2:70 detected client deauthentification attack on
wlan1 for e0:d9:e3:7b:93:80, VAP MAC: 68:13:e2:20:a2:79, channel: 40, RSSI: -44, AP location:
test
```

Атака "Отказ в обслуживании" (denial-of-service, DoS)

Атака создана для значительного затруднения работы сети или системы путем загрузки служебными запросами, которые исчерпывают ресурсы сети или системы для обслуживания пользователей.

DoS-атака определяется превышением лимита, который задается параметром 'threshold' для управляющих фреймов разных типов в радиоэфире. В профиле также задается интервал времени, в течение которого идет подсчет фреймов (параметр 'interval'). Если за это время заданный лимит превышен, то на контроллер будет сгенерировано и отправлено сообщение об обнаружении атаки. Период отправки таких сообщений настраивается в параметре 'trap-send-period'.

Также администратором задается параметр 'threshold leap', который показывает, насколько должно измениться количество пакетов по сравнению с предыдущим периодом, чтобы было отправлено сообщение о DoS-атаке на контроллер.

Пример настройки профиля WIDS с активацией режима обнаружения DoS-атаки при превышении количества любого типа пакетов 700 на интервале 5 секунд, а также при резком увеличении количества пакетов более чем на 500, с периодом отправки нотификаций – 30 секунд:

```
wlc#
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# wids-profile test_wids_profile
wlc(config-wlc-wids-profile)# dos-detection
wlc(config-wlc-wids-profile-dos-detection)#
wlc(config-wlc-wids-profile-dos-detection)# interval 5
```

```
wlc(config-wlc-wids-profile-dos-detection)# trap-send-period 30
wlc(config-wlc-wids-profile-dos-detection)# threshold leap 500
wlc(config-wlc-wids-profile-dos-detection)# threshold assoc 700
wlc(config-wlc-wids-profile-dos-detection)# threshold reassoc 700
wlc(config-wlc-wids-profile-dos-detection)# threshold disassoc 700
wlc(config-wlc-wids-profile-dos-detection)# threshold probe 700
wlc(config-wlc-wids-profile-dos-detection)# threshold beacon 700
wlc(config-wlc-wids-profile-dos-detection)# threshold blockack 700
wlc(config-wlc-wids-profile-dos-detection)# threshold blockack-req 700
wlc(config-wlc-wids-profile-dos-detection)# threshold ps-poll 700
wlc(config-wlc-wids-profile-dos-detection)# threshold auth 700
wlc(config-wlc-wids-profile-dos-detection)# threshold deauth 700
wlc(config-wlc-wids-profile-dos-detection)# threshold rts 700
wlc(config-wlc-wids-profile-dos-detection)# threshold cts 700
wlc(config-wlc-wids-profile-dos-detection)# enable
wlc(config-wlc-wids-profile-dos-detection)#
wlc(config-wlc-wids-profile-dos-detection)# do commit
wlc(config-wlc-wids-profile-dos-detection)# do confirm
```

Применить профиль можно в общих настройках WIDS для всех ТД контроллера, в локации или индивидуально на ТД.

При обнаружении атаки, в журнале событий WIDS появятся сообщения вида:

```
wlc(config-wlc-wids-profile-dos-detection)# do sh wlc journal wids attack dos
2024-11-02T20:01:43+07:00 AP 68:13:e2:20:a2:70 detected DoS attack on wlan0: a sharp increase
in the number of packets with type 'Probe request' (from 20 to 640), AP location: default-
location. Found 23 attacks for last detection period, attack time from AP:
2024-11-02T17:31:41+04:30
2024-11-02T20:01:43+07:00 AP 68:13:e2:20:a2:70 detected DoS attack on wlan0: too many packets
with type 'Beacon' (count 720 when constraint 700), AP location: default-location. Found 30
attacks for last detection period, attack time from AP: 2024-11-02T17:31:41+04:30
```

Атака "Перебор паролей" (Bruteforce)

Метод атаки с угадыванием паролей учетных данных для входа в систему, ключей шифрования и прочей информации для получения несанкционированного доступ к данным, системам или сетям. Метод заключается в переборе всех возможных комбинаций для получения правильного пароля.

ТД считает количество неудачных попыток авторизации пользователя при Personal- или Enterprise-авторизации в течении периода, определенного в параметре 'interval'. Если общее количество таких попыток за указанное время превышает заданный порог 'threshold', то считается, что производится атака перебора паролей и на контроллер отправляется сообщение о Bruteforce-атаке.

При включении опции mac-ban enable ТД дополнительно считает количество неудачных попыток авторизации для каждого клиента в отдельности и блокирует доступ клиента к сервису по его MAC-адресу, если количество неудачных попыток авторизации для него превышено, а также оповещает об этом контроллер. По истечению времени блокировки, заданному в параметре mac-ban timeout, клиент вновь может делать попытки подключения к ТД, при этом ТД также оповещает контроллер о том, что клиент был разблокирован.

Пример настройки профиля WIDS с активацией режима обнаружения атаки "перебор паролей" при превышении порога 10 попыток на интервале времени 5 секунд, с блокировкой клиентов на 60 секунд:

```
wlc# configure
wlc(config)# wlc
wlc(config-wlc)# wids-profile test_wids_profile
wlc(config-wlc-wids-profile)# bruteforce-detection
wlc(config-wlc-wids-profile-bf-detection)# enable
wlc(config-wlc-wids-profile-bf-detection)# threshold 10
```

```
wlc(config-wlc-wids-profile-bf-detection)# interval 5
wlc(config-wlc-wids-profile-bf-detection)# mac-ban enable
wlc(config-wlc-wids-profile-bf-detection)# mac-ban timeout 60
wlc(config-wlc-wids-profile-bf-detection)# do commit
wlc(config-wlc-wids-profile-bf-detection)# do confirm
```

Применить профиль можно в общих настройках WIDS для всех ТД контроллера, в локации или индивидуально на ТД.

При обнаружении атаки, в журнале событий WIDS появятся сообщения вида:

```
wlc# sh wlc journal wids attack bruteforce too-much-authentication-fail-detected
2024-11-02T19:38:46+07:00 AP e8:28:c1:fc:d4:60 detected too much authorization failed on wlan0-
vap1, SSID: wids_test, last client MAC: 60:ab:67:ba:89:24, AP location: default-location

wlc#  sh wlc journal wids attack bruteforce client-was-banned
2024-11-11T15:14:49+07:00 AP 68:13:e2:20:a2:70 banned client 60:ab:67:ba:89:24, SSID:
wids_test1_Ent, interface: wlan0-va0, auth-method: enterprise, eap-method: PEAP, captive-
portal: disabled, AP location: default-location

wlc#  sh wlc journal wids attack bruteforce client-was-unbanned
2024-11-11T15:15:51+07:00 AP 68:13:e2:20:a2:70 unbanned client 60:ab:67:ba:89:24, SSID:
wids_test1_Ent, interface: wlan0-va0, auth-method: enterprise, eap-method: PEAP, captive-
portal: disabled, AP location: default-location
```

23.5 Активация функционала по лицензии

- Лицензии WLC
- Загрузка и активация файловых лицензий
- Лицензирование через Eltex Licence Manager (ELM)

23.5.1 Лицензии WLC

Виды лицензий, связанные с функционалом контроллера беспроводной сети:

Название лицензии	Функционал
WLC	Управление точками доступа. Требуется для активации функционала на сервисных маршрутизаторах ESR-15, ESR-15R, ESR-30 и ESR-3200. Для контроллеров WLC-15, WLC-30 и WLC-3200 отдельной загрузки не требуется, функционал доступен в заводской конфигурации.
WLC-AP	Расширение числа точек доступа сверх ограничения по умолчанию (с лимитами можно ознакомиться в техническом описании устройства).
WLC-WIDS-WIPS	Обнаружение и предотвращение вторжений в беспроводную сеть.

23.5.2 Загрузка и активация файловых лицензий

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 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:

```
wlc# copy tftp://<server>:/<file_name> system:licence
```

FTP:

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

SCP:

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

SFTP:

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

Пример загрузки лицензии через SCP:

```
wlc# copy scp://adm:password123@192.168.16.168://home/tftp/licence system:licence
|****************************************| 100% (670B) Licence loaded successfully. Please
reboot system to apply changes.
```

Для активации лицензии необходимо перезагрузить устройство:

```
wlc# reload system
```

После перезагрузки проверьте, что лицензия активирована:

```
wlc# show licence
Feature                          Source     State         Value
Valid from             Expiries
-------------------------------  --------   -----------   -------------------------------
--------------------   --------------------
BRAS                             File       Active        true
--                     --
BRAS                             File       Candidate     true
--                     --
WLC                              File       Active        true
--                     --
WLC                              File       Candidate     true
--                     --
WLC-AP                           File       Active        100
--                     --
WLC-AP                           File       Candidate     100
--                     --
```

Статусы лицензий:

Статус	Описание
Active	Лицензия активна.
Candidate	Лицензия будет применена после перезагрузки.
Unsupported	Лицензия не поддерживается в рамках текущей версии ПО или вообще не поддерживается устройством.

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:

```
wlc-15# show licence
Feature                          Source     State          Value
Valid from             Expiries
--------------------------------   --------   -----------
--------------------------------   --------------------   --------------------
BRAS                             File       Active         true
--                     --
WLC                              File       Active         true
--                     --
WLC                              File       Candidate      true
--                     --
WLC-AP                           File       Active         100
--                     --
```

В примере выше после перезагрузки устройства будет заблокирован доступ к функционалу под лицензией BRAS и WLC-AP.
У лицензий **BRAS** и **WLC-AP** отсутствует статус **Candidate** и присутствует **Active**. Значит они активны на момент вывода команды **show licence**, но после перезагрузки функционал перестанут работать.
Лицензия **WLC** находится одновременно в статусе **Active** и **Candidate**. Значит лицензия активна на момент вывода команды **show licence** и будет активна после перезагрузки.
В случае расширения списка доступного функционала, при обращении в техническую поддержку или коммерческий отдел компании ЭЛТЕКС необходимо сообщать информацию **show system** и **show licence.**

23.5.3 Лицензирование через Eltex Licence Manager (ELM)

Для того, чтобы получить лицензию с помощью Eltex Licence Manager необходимо выполнить следующие шаги:

1. Настроить подключение к серверу лицензирования и применить конфигурацию.

```
wlc# configure
wlc(config)# licence-manager
wlc(config-licence-manager)# host address elm.eltex-co.ru
wlc(config-licence-manager)# enable
wlc(config-licence-manager)# end
wlc#commit
wlc#confirm
```

Для программного контроллера vWLC необходимо дополнительно указать параметр **licence-key.**

2. Выполнить команду update licence-manager licence.

```
wlc# update licence-manager licence
wlc# 2024-12-07T10:42:09+07:00 %LICENCE-W-EVENT: Licence recieved from Eltex Licence Manager
server
```

3. Проверить, что лицензия получена и находится в статусе **Active**:

```
#пример получение 2-х лицензий WLC-AP-SUPPORT-EXT и WLC-WIDS-WIPS через ELM
wlc# show licence
Feature                          Source     State         Value
Valid from             Expiries
-------------------------------  --------   -----------   --------------------------------
--------------------   --------------------
BRAS                             File       Active        true
--                     --
BRAS                             File       Candidate     true
--                     --
WLC                              File       Active        true
--                     --
WLC                              File       Candidate     true
--                     --
WLC-AP-SUPPORT-EXT               ELM        Active        110
--                     --
WLC-WIDS-WIPS                    ELM        Active        true
--                     --
```

Для активации лицензии перезагрузка устройства не требуется, лицензия будет работать сразу после получения.

23.6 Анализ отладочной информации протокола RADIUS

Данный функционал доступен начиная с версии ПО 1.30.0 для устройств WLC-15/30/3200, ESR-15/15R/30/3200 и программного контроллера vWLC.

- Введение
- Команда show radius debug
  - Опции
    - file
    - ip-address
    - timeout
    - user
- Примеры вывода команды show radius debug
  - При успешном подключении клиента с авторизацией на локальном RADIUS-сервере
  - При неуспешном подключении клиента с авторизацией на локальном RADIUS-сервере
  - Сохранение вывода в файл на flash:data/ и выгрузка по tftp
  - Сохранение вывода в файл на внешний USB

23.6.1 Введение

Начиная с версии 1.30.0 появилась возможность оперативно производить troubleshooting RADIUS-пакетов в таких схемах, как:

- Локальный RADIUS-сервер
- Проксирование запросов на внешний RADIUS-сервер

- TLS-авторизация

23.6.2 Команда show radius debug

Команда расположена в debug view.

Запуск команды без каких либо опций выводит всю отладочную информацию RADIUS с таймаутом 60 секунд.

Для того чтобы принудительно остановить работу команды, необходимо нажать комбинацию клавиш Ctrl+C.

Есть возможность использовать опции.

```
wlc-15# debug
wlc-15(debug)# show
  brasd          Show BRAS
  configuration  Show configuration information
  cpu            Show CPU related statistics
  debug          Show debug configuration parameters
  ipc-hub        Show IPC-HUB information
  licence        Show licence inforamtion
  memory         Show memory related information
  radius-debug   Show raddebug information       <<<---------------------------

wlc-15(debug)# show radius-debug
```

Опции

file

Данная опция позволяет записать результат выполнения команды в файл с произвольным названием и сохранить его для последующего анализа.

При использовании данной опции отсутствует вывод отладочной информации в терминал, информация записывается **только в файл**.

Файл возможно сохранить в:

- **flash:data/** – встроенный flash-накопитель устройства;
- **usb://usb_name:/** – внешний USB-накопитель;
- **mmc://mmc_name:/** – внешний MicroSD-накопитель;
- **hdd://hdd_name:/** – внешний SSD/HDD-накопитель, форм-фактора 2.5 дюйма.

MicroSD-слот поддержан на устройствах WLC-30, WLC-3200, ESR-3200.
SSD/HDD-накопитель форм-фактора 2.5 дюйма, поддержан на устройствах WLC-15, WLC-30, WLC-3200.

Пример опции file

```
#Запись отладочной информации RADIUS в файл с названием test-file на внутренний flash-
накопитель устройства

wlc-30(debug)# show radius-debug file flash:data/test-file.txt
Total lines written: 1339
File saved
```

```
wlc-30# dir flash:data/
Name                                                        Type         Size            Last
modified
----------------------------------------------------------  ----------   --------   --
-------------------------
test-file.txt                                               File         106.64     KB   Thu
Nov 21 12:07:29 2024

#Выгрузка файла на tftp-сервер для последующего анализа

wlc-30r# copy flash:data/test-file.txt tftp://100.110.0.214:/test-file.txt
|****************************************| 100% (106kB) Success!
```

ip-address

Данная опция позволяет осуществлять вывод отладочной RADIUS-информации от конкретного IPv4-адреса RADIUS-клиента.

Опция ip-address задается в формате A.B.C.D.

Пример опции ip-address

```
wlc-30(debug)# show radius-debug ip-address
  A.B.C.D  IP address of client

wlc-30-failover(debug)# show radius-debug ip-address 100.129.56.1
```

timeout

Данная опция задает таймаут выполнения команды show radius debug. Работа команды автоматически завершается по истечении заданного времени.

Опция timeout задается в диапазоне 0-1200 сек.

В случае если опция не указана, значение по умолчанию 60 сек.

Если задать значение timeout = 0, команда будет выполнятся бесконечно.
Для завершения выполнения команды необходимо нажать комбинацию клавиш Ctrl+C.

Пример опции timeout

```
#Выполнение команды с опцией timeout, равной 600 сек
wlc-30(debug)# show radius-debug timeout 600
```

user

Данная опция позволяет осуществлять вывод отладочной RADIUS-информации конкретного пользователя (атрибут User-Name).

Опция username задается строкой от 1 до 50 символов.

Пример опции username

```
#Вывод radius-debug для пользователя tester
wlc-30(debug)#show radius-debug username tester
```

23.6.3 Примеры вывода команды show radius debug

При успешном подключении клиента с авторизацией на локальном RADIUS-сервере

```
wlc-15#
wlc-15# debug
wlc-15(debug)# show radius-debug username tester ip-address 100.129.56.1 timeout 600
(33) Thu Nov 21 15:34:09 2024: Debug: Received Access-Request Id 31 from 100.129.56.1:37236 to
100.129.58.1:1812 length 259
(33) Thu Nov 21 15:34:09 2024: Debug:   User-Name = "tester"
(33) Thu Nov 21 15:34:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(33) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Domain = "default"
(33) Thu Nov 21 15:34:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(33) Thu Nov 21 15:34:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(33) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(33) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Id = "10"
(33) Thu Nov 21 15:34:09 2024: Debug:   Service-Type = Framed-User
(33) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port = 1
(33) Thu Nov 21 15:34:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(33) Thu Nov 21 15:34:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(33) Thu Nov 21 15:34:09 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(33) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(33) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(33) Thu Nov 21 15:34:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(33) Thu Nov 21 15:34:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(33) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1400
(33) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message = 0x0285000b01746573746572
(33) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x204ffb9b5a0f9dcf0b9e1ca3cd13c639
(33) Thu Nov 21 15:34:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(33) Thu Nov 21 15:34:09 2024: Debug:   authorize {
(33) Thu Nov 21 15:34:09 2024: Debug:     policy filter_username {
(33) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name) {
(33) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  -> TRUE
(33) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /) {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(33) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(33) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
```

```
(33) Thu Nov 21 15:34:09 2024: Debug:       } # if (&User-Name)  = notfound
(33) Thu Nov 21 15:34:09 2024: Debug:     } # policy filter_username = notfound
(33) Thu Nov 21 15:34:09 2024: Debug:     [preprocess] = ok
(33) Thu Nov 21 15:34:09 2024: Debug:     [chap] = noop
(33) Thu Nov 21 15:34:09 2024: Debug:     [mschap] = noop
(33) Thu Nov 21 15:34:09 2024: Debug:     [digest] = noop
(33) Thu Nov 21 15:34:09 2024: Debug: suffix: Checking for suffix after "@"
(33) Thu Nov 21 15:34:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(33) Thu Nov 21 15:34:09 2024: Debug: suffix: No such realm "NULL"
(33) Thu Nov 21 15:34:09 2024: Debug:     [suffix] = noop
(33) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(33) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(33) Thu Nov 21 15:34:09 2024: Debug:     [files_multi] = ok
(33) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(33) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(33) Thu Nov 21 15:34:09 2024: Debug:     else {
(33) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 133 length 11
(33) Thu Nov 21 15:34:09 2024: Debug: eap: EAP-Identity reply, returning 'ok' so we can short-
circuit the rest of authorize
(33) Thu Nov 21 15:34:09 2024: Debug:       [eap] = ok
(33) Thu Nov 21 15:34:09 2024: Debug:     } # else = ok
(33) Thu Nov 21 15:34:09 2024: Debug:     if (ok) {
(33) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  -> TRUE
(33) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  {
(33) Thu Nov 21 15:34:09 2024: Debug:       return
(33) Thu Nov 21 15:34:09 2024: Debug:     } # if (ok)  = ok
(33) Thu Nov 21 15:34:09 2024: Debug:   } # authorize = ok
(33) Thu Nov 21 15:34:09 2024: Debug: Found Auth-Type = eap
(33) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(33) Thu Nov 21 15:34:09 2024: Debug:   authenticate {
(33) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent packet with method EAP Identity (1)
(33) Thu Nov 21 15:34:09 2024: Debug: eap: Calling submodule eap_peap to process data
(33) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Initiating new session
(33) Thu Nov 21 15:34:09 2024: Debug: eap: Sending EAP Request (code 1) ID 134 length 6
(33) Thu Nov 21 15:34:09 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d640c1da
(33) Thu Nov 21 15:34:09 2024: Debug:     [eap] = handled
(33) Thu Nov 21 15:34:09 2024: Debug:   } # authenticate = handled
(33) Thu Nov 21 15:34:09 2024: Debug: Using Post-Auth-Type Challenge
(33) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(33) Thu Nov 21 15:34:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(33) Thu Nov 21 15:34:09 2024: Debug: session-state: Saving cached attributes
(33) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1004
(33) Thu Nov 21 15:34:09 2024: Debug: Sent Access-Challenge Id 31 from 100.129.58.1:1812 to
100.129.56.1:37236 length 76
(33) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Tls-Enabled = 0
(33) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message = 0x018600061920
(33) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(33) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d640c1da517e6b54cde2f128
(33) Thu Nov 21 15:34:09 2024: Debug: Finished request
(34) Thu Nov 21 15:34:09 2024: Debug: Received Access-Request Id 32 from 100.129.56.1:37236 to
100.129.58.1:1812 length 427
(34) Thu Nov 21 15:34:09 2024: Debug:   User-Name = "tester"
(34) Thu Nov 21 15:34:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(34) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Domain = "default"
(34) Thu Nov 21 15:34:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(34) Thu Nov 21 15:34:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
```

```
(34) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(34) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Id = "10"
(34) Thu Nov 21 15:34:09 2024: Debug:   Service-Type = Framed-User
(34) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port = 1
(34) Thu Nov 21 15:34:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(34) Thu Nov 21 15:34:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(34) Thu Nov 21 15:34:09 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(34) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(34) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(34) Thu Nov 21 15:34:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(34) Thu Nov 21 15:34:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(34) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1400
(34) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message =
0x028600a11980000000971603010092010000 8e0303673ef08120eff9f8ebe08572c925c8194ba8df959e2ec704e89
33241538475fe00002c00ffc02cc02bc024c023c00ac009c008c030c02fc00
(34) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d640c1da517e6b54cde2f128
(34) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0xe9d462619fab68ba99b3766d0517073d
(34) Thu Nov 21 15:34:09 2024: Debug: Restoring &session-state
(34) Thu Nov 21 15:34:09 2024: Debug:   &session-state:Framed-MTU = 1004
(34) Thu Nov 21 15:34:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(34) Thu Nov 21 15:34:09 2024: Debug:   authorize {
(34) Thu Nov 21 15:34:09 2024: Debug:     policy filter_username {
(34) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name) {
(34) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  -> TRUE
(34) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /) {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(34) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(34) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:       } # if (&User-Name)  = notfound
(34) Thu Nov 21 15:34:09 2024: Debug:     } # policy filter_username = notfound
(34) Thu Nov 21 15:34:09 2024: Debug:     [preprocess] = ok
(34) Thu Nov 21 15:34:09 2024: Debug:     [chap] = noop
(34) Thu Nov 21 15:34:09 2024: Debug:     [mschap] = noop
(34) Thu Nov 21 15:34:09 2024: Debug:     [digest] = noop
(34) Thu Nov 21 15:34:09 2024: Debug: suffix: Checking for suffix after "@"
(34) Thu Nov 21 15:34:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(34) Thu Nov 21 15:34:09 2024: Debug: suffix: No such realm "NULL"
(34) Thu Nov 21 15:34:09 2024: Debug:     [suffix] = noop
(34) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(34) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(34) Thu Nov 21 15:34:09 2024: Debug:     [files_multi] = ok
(34) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(34) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(34) Thu Nov 21 15:34:09 2024: Debug:     else {
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 134 length 161
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Continuing tunnel setup
(34) Thu Nov 21 15:34:09 2024: Debug:       [eap] = ok
```

```
(34) Thu Nov 21 15:34:09 2024: Debug:     } # else = ok
(34) Thu Nov 21 15:34:09 2024: Debug:     if (ok) {
(34) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  -> TRUE
(34) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  {
(34) Thu Nov 21 15:34:09 2024: Debug:       return
(34) Thu Nov 21 15:34:09 2024: Debug:     } # if (ok)  = ok
(34) Thu Nov 21 15:34:09 2024: Debug:   } # authorize = ok
(34) Thu Nov 21 15:34:09 2024: Debug: Found Auth-Type = eap
(34) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(34) Thu Nov 21 15:34:09 2024: Debug:   authenticate {
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Expiring EAP session with state 0xba2ef008bae3e943
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d640c1da
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d640c1da
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d640c1da, released from the list
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Calling submodule eap_peap to process data
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) EAP Peer says that the final record size
will be 151 bytes
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) EAP Got all data (151 bytes)
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - before/accept
initialization
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server before/accept
initialization
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client hello A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
server hello A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
certificate A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write key
exchange A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
server done A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 flush data
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client certificate A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Server : Need to read more data: SSLv3
read client key exchange A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Server : Need to read more data: SSLv3
read client key exchange A
(34) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) In Handshake Phase
(34) Thu Nov 21 15:34:09 2024: Debug: eap: Sending EAP Request (code 1) ID 135 length 1014
(34) Thu Nov 21 15:34:09 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d741c1da
(34) Thu Nov 21 15:34:09 2024: Debug:     [eap] = handled
(34) Thu Nov 21 15:34:09 2024: Debug:   } # authenticate = handled
(34) Thu Nov 21 15:34:09 2024: Debug: Using Post-Auth-Type Challenge
(34) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(34) Thu Nov 21 15:34:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(34) Thu Nov 21 15:34:09 2024: Debug: session-state: Saving cached attributes
(34) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1004
(34) Thu Nov 21 15:34:09 2024: Debug: Sent Access-Challenge Id 32 from 100.129.58.1:1812 to
100.129.56.1:37236 length 1092
(34) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Tls-Enabled = 0
(34) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message =
0x018703f619c00000090f160303003902000035030305 6c34d7a2cd4443bf84fdb3787baa9f1292763bb392ba21349
1760b839487e900c03000000dff01000100000b000403000102 16030307710
(34) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
```

```
(34) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d741c1da517e6b54cde2f128
(34) Thu Nov 21 15:34:09 2024: Debug: Finished request
(35) Thu Nov 21 15:34:09 2024: Debug: Received Access-Request Id 33 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
(35) Thu Nov 21 15:34:09 2024: Debug:   User-Name = "tester"
(35) Thu Nov 21 15:34:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(35) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Domain = "default"
(35) Thu Nov 21 15:34:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(35) Thu Nov 21 15:34:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(35) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(35) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Id = "10"
(35) Thu Nov 21 15:34:09 2024: Debug:   Service-Type = Framed-User
(35) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port = 1
(35) Thu Nov 21 15:34:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(35) Thu Nov 21 15:34:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(35) Thu Nov 21 15:34:09 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(35) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(35) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(35) Thu Nov 21 15:34:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(35) Thu Nov 21 15:34:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(35) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1400
(35) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message = 0x028700061900
(35) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d741c1da517e6b54cde2f128
(35) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x9211bd5236d0093375733c66b58cd3c9
(35) Thu Nov 21 15:34:09 2024: Debug: Restoring &session-state
(35) Thu Nov 21 15:34:09 2024: Debug:   &session-state:Framed-MTU = 1004
(35) Thu Nov 21 15:34:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(35) Thu Nov 21 15:34:09 2024: Debug:   authorize {
(35) Thu Nov 21 15:34:09 2024: Debug:     policy filter_username {
(35) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name) {
(35) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  -> TRUE
(35) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /) {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(35) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(35) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:       } # if (&User-Name)  = notfound
(35) Thu Nov 21 15:34:09 2024: Debug:     } # policy filter_username = notfound
(35) Thu Nov 21 15:34:09 2024: Debug:     [preprocess] = ok
(35) Thu Nov 21 15:34:09 2024: Debug:     [chap] = noop
(35) Thu Nov 21 15:34:09 2024: Debug:     [mschap] = noop
(35) Thu Nov 21 15:34:09 2024: Debug:     [digest] = noop
(35) Thu Nov 21 15:34:09 2024: Debug: suffix: Checking for suffix after "@"
(35) Thu Nov 21 15:34:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(35) Thu Nov 21 15:34:09 2024: Debug: suffix: No such realm "NULL"
(35) Thu Nov 21 15:34:09 2024: Debug:     [suffix] = noop
(35) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
```

```
(35) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(35) Thu Nov 21 15:34:09 2024: Debug:     [files_multi] = ok
(35) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(35) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(35) Thu Nov 21 15:34:09 2024: Debug:     else {
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 135 length 6
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Continuing tunnel setup
(35) Thu Nov 21 15:34:09 2024: Debug:       [eap] = ok
(35) Thu Nov 21 15:34:09 2024: Debug:     } # else = ok
(35) Thu Nov 21 15:34:09 2024: Debug:     if (ok) {
(35) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  -> TRUE
(35) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  {
(35) Thu Nov 21 15:34:09 2024: Debug:       return
(35) Thu Nov 21 15:34:09 2024: Debug:     } # if (ok)  = ok
(35) Thu Nov 21 15:34:09 2024: Debug:   } # authorize = ok
(35) Thu Nov 21 15:34:09 2024: Debug: Found Auth-Type = eap
(35) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(35) Thu Nov 21 15:34:09 2024: Debug:   authenticate {
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d741c1da
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d741c1da
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d741c1da, released from the list
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Calling submodule eap_peap to process data
(35) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment
(35) Thu Nov 21 15:34:09 2024: Debug: eap: Sending EAP Request (code 1) ID 136 length 1010
(35) Thu Nov 21 15:34:09 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d44ec1da
(35) Thu Nov 21 15:34:09 2024: Debug:     [eap] = handled
(35) Thu Nov 21 15:34:09 2024: Debug:   } # authenticate = handled
(35) Thu Nov 21 15:34:09 2024: Debug: Using Post-Auth-Type Challenge
(35) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(35) Thu Nov 21 15:34:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(35) Thu Nov 21 15:34:09 2024: Debug: session-state: Saving cached attributes
(35) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1004
(35) Thu Nov 21 15:34:09 2024: Debug: Sent Access-Challenge Id 33 from 100.129.58.1:1812 to
100.129.56.1:37236 length 1086
(35) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Tls-Enabled = 0
(35) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message =
0x018803f21940300d06092a864886f70d01010b0500308181310b3009060355040613025255310f300d06035504080
c0652757373696131143012060355040 70c0b4e6f766f7369626972736b314
(35) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(35) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d44ec1da517e6b54cde2f128
(35) Thu Nov 21 15:34:09 2024: Debug: Finished request
(36) Thu Nov 21 15:34:09 2024: Debug: Received Access-Request Id 34 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
(36) Thu Nov 21 15:34:09 2024: Debug:   User-Name = "tester"
(36) Thu Nov 21 15:34:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(36) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Domain = "default"
(36) Thu Nov 21 15:34:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(36) Thu Nov 21 15:34:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(36) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(36) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port-Id = "10"
(36) Thu Nov 21 15:34:09 2024: Debug:   Service-Type = Framed-User
(36) Thu Nov 21 15:34:09 2024: Debug:   NAS-Port = 1
(36) Thu Nov 21 15:34:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(36) Thu Nov 21 15:34:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(36) Thu Nov 21 15:34:09 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
```

```
(36) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(36) Thu Nov 21 15:34:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(36) Thu Nov 21 15:34:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(36) Thu Nov 21 15:34:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(36) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1400
(36) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message = 0x028800061900
(36) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d44ec1da517e6b54cde2f128
(36) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x4bf2d8459c4ec1c30e777a67d2369bc6
(36) Thu Nov 21 15:34:09 2024: Debug: Restoring &session-state
(36) Thu Nov 21 15:34:09 2024: Debug:   &session-state:Framed-MTU = 1004
(36) Thu Nov 21 15:34:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(36) Thu Nov 21 15:34:09 2024: Debug:   authorize {
(36) Thu Nov 21 15:34:09 2024: Debug:     policy filter_username {
(36) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name) {
(36) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  -> TRUE
(36) Thu Nov 21 15:34:09 2024: Debug:       if (&User-Name)  {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /) {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(36) Thu Nov 21 15:34:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(36) Thu Nov 21 15:34:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:       } # if (&User-Name)  = notfound
(36) Thu Nov 21 15:34:09 2024: Debug:     } # policy filter_username = notfound
(36) Thu Nov 21 15:34:09 2024: Debug:     [preprocess] = ok
(36) Thu Nov 21 15:34:09 2024: Debug:     [chap] = noop
(36) Thu Nov 21 15:34:09 2024: Debug:     [mschap] = noop
(36) Thu Nov 21 15:34:09 2024: Debug:     [digest] = noop
(36) Thu Nov 21 15:34:09 2024: Debug: suffix: Checking for suffix after "@"
(36) Thu Nov 21 15:34:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(36) Thu Nov 21 15:34:09 2024: Debug: suffix: No such realm "NULL"
(36) Thu Nov 21 15:34:09 2024: Debug:     [suffix] = noop
(36) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(36) Thu Nov 21 15:34:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(36) Thu Nov 21 15:34:09 2024: Debug:     [files_multi] = ok
(36) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(36) Thu Nov 21 15:34:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(36) Thu Nov 21 15:34:09 2024: Debug:     else {
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 136 length 6
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Continuing tunnel setup
(36) Thu Nov 21 15:34:09 2024: Debug:       [eap] = ok
(36) Thu Nov 21 15:34:09 2024: Debug:     } # else = ok
(36) Thu Nov 21 15:34:09 2024: Debug:     if (ok) {
(36) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  -> TRUE
(36) Thu Nov 21 15:34:09 2024: Debug:     if (ok)  {
(36) Thu Nov 21 15:34:09 2024: Debug:       return
(36) Thu Nov 21 15:34:09 2024: Debug:     } # if (ok)  = ok
(36) Thu Nov 21 15:34:09 2024: Debug:   } # authorize = ok
(36) Thu Nov 21 15:34:09 2024: Debug: Found Auth-Type = eap
```

```
(36) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(36) Thu Nov 21 15:34:09 2024: Debug:   authenticate {
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d44ec1da
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d44ec1da
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d44ec1da, released from the list
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Calling submodule eap_peap to process data
(36) Thu Nov 21 15:34:09 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment
(36) Thu Nov 21 15:34:09 2024: Debug: eap: Sending EAP Request (code 1) ID 137 length 317
(36) Thu Nov 21 15:34:09 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d54fc1da
(36) Thu Nov 21 15:34:09 2024: Debug:     [eap] = handled
(36) Thu Nov 21 15:34:09 2024: Debug:   } # authenticate = handled
(36) Thu Nov 21 15:34:09 2024: Debug: Using Post-Auth-Type Challenge
(36) Thu Nov 21 15:34:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(36) Thu Nov 21 15:34:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(36) Thu Nov 21 15:34:09 2024: Debug: session-state: Saving cached attributes
(36) Thu Nov 21 15:34:09 2024: Debug:   Framed-MTU = 1004
(36) Thu Nov 21 15:34:09 2024: Debug: Sent Access-Challenge Id 34 from 100.129.58.1:1812 to
100.129.56.1:37236 length 389
(36) Thu Nov 21 15:34:09 2024: Debug:   Eltex-Tls-Enabled = 0
(36) Thu Nov 21 15:34:09 2024: Debug:   EAP-Message =
0x0189013d1900e90c33a738cccf02dda76e56ee53e2d612e830debd251974be17a02cf62e886c47c93fc1456ba2751
23e040101005b94113a376be5c27367f6df21134e38b494e5442b45800d7a0
(36) Thu Nov 21 15:34:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(36) Thu Nov 21 15:34:09 2024: Debug:   State = 0xd6c6d814d54fc1da517e6b54cde2f128
(36) Thu Nov 21 15:34:09 2024: Debug: Finished request
(37) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 35 from 100.129.56.1:37236 to
100.129.58.1:1812 length 402
(37) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(37) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(37) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(37) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(37) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(37) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(37) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(37) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(37) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(37) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(37) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(37) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(37) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(37) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(37) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(37) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(37) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(37) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x02890088198000000007e160303004610000042410406 2f114b734c6fa21c06e87a7576c15cbf6f7f8dbf30c1c52d6
f726e78f24d06bd1b075797550030c6117b5d1ce0f5b9a41b13705938f833d
(37) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d54fc1da517e6b54cde2f128
(37) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0xef09f27e663784fbc4d7fb0b23be3fdd
(37) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(37) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(37) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(37) Thu Nov 21 15:34:14 2024: Debug:   authorize {
```

```
(37) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(37) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(37) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(37) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(37) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(37) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(37) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(37) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(37) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(37) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(37) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(37) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(37) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(37) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(37) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(37) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(37) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(37) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(37) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(37) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(37) Thu Nov 21 15:34:14 2024: Debug:     else {
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 137 length 136
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(37) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(37) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(37) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(37) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(37) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(37) Thu Nov 21 15:34:14 2024: Debug:       return
(37) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(37) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(37) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(37) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(37) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d54fc1da
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d54fc1da
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d54fc1da, released from the list
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Peer says that the final record size
will be 126 bytes
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Got all data (126 bytes)
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client key exchange A
```

```
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
certificate verify A
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
finished A
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
change cipher spec A
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
finished A
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 flush data
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Handshake state - SSL negotiation
finished successfully
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Connection Established
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-
GCM-SHA384"
(37) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   TLS-Session-Version = "TLS 1.2"
(37) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 138 length 57
(37) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d24cc1da
(37) Thu Nov 21 15:34:14 2024: Debug:     [eap] = handled
(37) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = handled
(37) Thu Nov 21 15:34:14 2024: Debug: Using Post-Auth-Type Challenge
(37) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(37) Thu Nov 21 15:34:14 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(37) Thu Nov 21 15:34:14 2024: Debug: session-state: Saving cached attributes
(37) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1004
(37) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(37) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(37) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Challenge Id 35 from 100.129.58.1:1812 to
100.129.56.1:37236 length 127
(37) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(37) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018a00391900140303000101160303002889966e719344ac9746988eefda7798137249678c7732156f51c4a631258
1ae9dfb5cab5b1ab182eb
(37) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(37) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d24cc1da517e6b54cde2f128
(37) Thu Nov 21 15:34:14 2024: Debug: Finished request
(38) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 36 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
(38) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(38) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(38) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(38) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(38) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(38) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(38) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(38) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(38) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(38) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(38) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(38) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(38) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(38) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(38) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(38) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(38) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(38) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message = 0x028a00061900
(38) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d24cc1da517e6b54cde2f128
```

```
(38) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x55540bd1180d2b71ccb2613611147157
(38) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(38) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(38) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(38) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(38) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(38) Thu Nov 21 15:34:14 2024: Debug:   authorize {
(38) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(38) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(38) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(38) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(38) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(38) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(38) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(38) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(38) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(38) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(38) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(38) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(38) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(38) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(38) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(38) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(38) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(38) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(38) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(38) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(38) Thu Nov 21 15:34:14 2024: Debug:     else {
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 138 length 6
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(38) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(38) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(38) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(38) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(38) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(38) Thu Nov 21 15:34:14 2024: Debug:       return
(38) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(38) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(38) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(38) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(38) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d24cc1da
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d24cc1da
```

```
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d24cc1da, released from the list
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(38) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment.
handshake is finished
(38) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(38) Thu Nov 21 15:34:14 2024: Debug: eap_peap: PEAP state TUNNEL ESTABLISHED
(38) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 139 length 40
(38) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d34dc1da
(38) Thu Nov 21 15:34:14 2024: Debug:     [eap] = handled
(38) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = handled
(38) Thu Nov 21 15:34:14 2024: Debug: Using Post-Auth-Type Challenge
(38) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(38) Thu Nov 21 15:34:14 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(38) Thu Nov 21 15:34:14 2024: Debug: session-state: Saving cached attributes
(38) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1004
(38) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(38) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(38) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Challenge Id 36 from 100.129.58.1:1812 to
100.129.56.1:37236 length 110
(38) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(38) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018b00281900170303001d89966e719344ac98f850f361870d173ed36fe65f614390b1e5ab900f07
(38) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(38) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d34dc1da517e6b54cde2f128
(38) Thu Nov 21 15:34:14 2024: Debug: Finished request
(39) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 37 from 100.129.56.1:37236 to
100.129.58.1:1812 length 308
(39) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(39) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(39) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(39) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(39) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(39) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(39) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(39) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(39) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(39) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x028b002a1900170303001f126f9cc4d1f2f8310e2667957637c36ced32de7781959f814e57e1addc11c0
(39) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d34dc1da517e6b54cde2f128
(39) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0xd7700cfe8a99e9b13bb7d67c602ad766
(39) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(39) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(39) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(39) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
```

```
(39) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(39) Thu Nov 21 15:34:14 2024: Debug:   authorize {
(39) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(39) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(39) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(39) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(39) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(39) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(39) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(39) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(39) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(39) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(39) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(39) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(39) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(39) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(39) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(39) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:     else {
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 139 length 42
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(39) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(39) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(39) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(39) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(39) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(39) Thu Nov 21 15:34:14 2024: Debug:       return
(39) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(39) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(39) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(39) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(39) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814d34dc1da
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d34dc1da
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d34dc1da, released from the list
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
```

```
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: PEAP state WAITING FOR INNER IDENTITY
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Identity - tester
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got inner identity 'tester'
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Setting default EAP type for tunneled EAP
session
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled request
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message = 0x028b000b01746573746572
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Setting User-Name to tester
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Sending tunneled request to inner-tunnel
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message = 0x028b000b01746573746572
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   User-Name = "tester"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-IP-Address = 100.129.56.1
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Domain = "default"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Identifier = "68:13:E2:35:D2:20"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-
SSID-WLC-15"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Type = Wireless-802.11
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Id = "10"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Service-Type = Framed-User
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port = 1
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Connect-Info = "CONNECT 24Mbps 802.11a"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Acct-Session-Id = "073DA111-08E53DB2"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Pairwise-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Group-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-AKM-Suite = 1027073
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-AP-Domain = "with-gre"
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Framed-MTU = 1400
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Event-Timestamp = "Nov 21 2024 15:34:14
GMT+7"
(39) Thu Nov 21 15:34:14 2024: Debug: Virtual server inner-tunnel received request
(39) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message = 0x028b000b01746573746572
(39) Thu Nov 21 15:34:14 2024: Debug:   FreeRADIUS-Proxied-To = 127.0.0.1
(39) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(39) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(39) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(39) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(39) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(39) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(39) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(39) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(39) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(39) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(39) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(39) Thu Nov 21 15:34:14 2024: Debug:   Event-Timestamp = "Nov 21 2024 15:34:14 GMT+7"
(39) Thu Nov 21 15:34:14 2024: WARNING: Outer and inner identities are the same.  User privacy
is compromised.
(39) Thu Nov 21 15:34:14 2024: Debug: server inner-tunnel {
(39) Thu Nov 21 15:34:14 2024: Debug:   # Executing section authorize from file /etc/raddb/
sites-enabled/inner-tunnel
(39) Thu Nov 21 15:34:14 2024: Debug:     authorize {
(39) Thu Nov 21 15:34:14 2024: Debug:       policy filter_username {
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name) {
```

```
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  -> TRUE
(39) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /) {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /)  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ ) {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ ) {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ )  -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))  {
(39) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)  {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)  {
(39) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)   -> FALSE
(39) Thu Nov 21 15:34:14 2024: Debug:         } # if (&User-Name)  = notfound
(39) Thu Nov 21 15:34:14 2024: Debug:       } # policy filter_username = notfound
(39) Thu Nov 21 15:34:14 2024: Debug:       [chap] = noop
(39) Thu Nov 21 15:34:14 2024: Debug:       [mschap] = noop
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(39) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(39) Thu Nov 21 15:34:14 2024: Debug:       [suffix] = noop
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 139 length 11
(39) Thu Nov 21 15:34:14 2024: Debug: eap: EAP-Identity reply, returning 'ok' so we can short-
circuit the rest of authorize
(39) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(39) Thu Nov 21 15:34:14 2024: Debug:     } # authorize = ok
(39) Thu Nov 21 15:34:14 2024: Debug:   Found Auth-Type = eap
(39) Thu Nov 21 15:34:14 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(39) Thu Nov 21 15:34:14 2024: Debug:     authenticate {
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP Identity (1)
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_mschapv2 to process data
(39) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2: Issuing Challenge
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 140 length 43
(39) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0x73c34f14734f5598
(39) Thu Nov 21 15:34:14 2024: Debug:       [eap] = handled
(39) Thu Nov 21 15:34:14 2024: Debug:     } # authenticate = handled
(39) Thu Nov 21 15:34:14 2024: Debug: } # server inner-tunnel
(39) Thu Nov 21 15:34:14 2024: Debug: Virtual server sending reply
(39) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018c002b1a018c00261029f35ca9eb06d27f3cb6a0fcbfbc9f986672656572616469757 32d332e302e3235
(39) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(39) Thu Nov 21 15:34:14 2024: Debug:   State = 0x73c34f14734f5598209f4f525a078ea5
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled reply code 11
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message =
0x018c002b1a018c00261029f35ca9eb06d27f3cb6a0fcbfbc9f986672656572616469757 32d332e302e3235
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Message-Authenticator =
0x00000000000000000000000000000000
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   State = 0x73c34f14734f5598209f4f525a078ea5
(39) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled Access-Challenge
(39) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 140 length 74
(39) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d04ac1da
(39) Thu Nov 21 15:34:14 2024: Debug:     [eap] = handled
(39) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = handled
(39) Thu Nov 21 15:34:14 2024: Debug: Using Post-Auth-Type Challenge
```

```
(39) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(39) Thu Nov 21 15:34:14 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(39) Thu Nov 21 15:34:14 2024: Debug: session-state: Saving cached attributes
(39) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1004
(39) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(39) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(39) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Challenge Id 37 from 100.129.58.1:1812 to
100.129.56.1:37236 length 144
(39) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(39) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018c004a1900170303003f89966e719344ac99e939d773930e064bd033b593033706bea8aec6d4cd24d0bf543cbad
16b9719d94345c1eab84515cb6dd852bb943f855b6f710a6337cb1d
(39) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(39) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d04ac1da517e6b54cde2f128
(39) Thu Nov 21 15:34:14 2024: Debug: Finished request
(40) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 38 from 100.129.56.1:37236 to
100.129.58.1:1812 length 362
(40) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(40) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(40) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(40) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(40) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(40) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(40) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(40) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x028c00601900170303005512 6f9cc4d1f2f83261a51a42029098784c64cb1d267f8fc01cc65f9eae5cc6ffb7b2ad1
e394575d739bf9f12051c16b587a1247b3c1ba27b02d868c470842e31031dc
(40) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d04ac1da517e6b54cde2f128
(40) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x3c5f1f1b33a3d189d133901ba166f8e4
(40) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(40) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(40) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(40) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(40) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(40) Thu Nov 21 15:34:14 2024: Debug:   authorize {
(40) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(40) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(40) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(40) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
```

```
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(40) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(40) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(40) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(40) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(40) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(40) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(40) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(40) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(40) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(40) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(40) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(40) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:     else {
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 140 length 96
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(40) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(40) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(40) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(40) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(40) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(40) Thu Nov 21 15:34:14 2024: Debug:       return
(40) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(40) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(40) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(40) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(40) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0x73c34f14734f5598
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d04ac1da
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d04ac1da, released from the list
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: PEAP state phase2
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: EAP method MSCHAPv2 (26)
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled request
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message =
0x028c00411a028c003c31f49491c79b94785aea350343b0b0e191000000000000000c5ae22e446e2f7e9a56cfd03b
5a5fd6d08ca17d41d1a5f0300746573746572
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Setting User-Name to tester
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Sending tunneled request to inner-tunnel
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message =
0x028c00411a028c003c31f49491c79b94785aea350343b0b0e191000000000000000c5ae22e446e2f7e9a56cfd03b
5a5fd6d08ca17d41d1a5f0300746573746572
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
```

```
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   User-Name = "tester"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   State = 0x73c34f14734f5598209f4f525a078ea5
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-IP-Address = 100.129.56.1
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Domain = "default"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Identifier = "68:13:E2:35:D2:20"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-
SSID-WLC-15"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Type = Wireless-802.11
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Id = "10"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Service-Type = Framed-User
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port = 1
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Connect-Info = "CONNECT 24Mbps 802.11a"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Acct-Session-Id = "073DA111-08E53DB2"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Pairwise-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Group-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-AKM-Suite = 1027073
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-AP-Domain = "with-gre"
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Framed-MTU = 1400
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Event-Timestamp = "Nov 21 2024 15:34:14
GMT+7"
(40) Thu Nov 21 15:34:14 2024: Debug: Virtual server inner-tunnel received request
(40) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x028c00411a028c003c31f49491c79b94785aea350343b0b0e191000000000000000c5ae22e446e2f7e9a56cfd03b
5a5fd6d08ca17d41d1a5f0300746573746572
(40) Thu Nov 21 15:34:14 2024: Debug:   FreeRADIUS-Proxied-To = 127.0.0.1
(40) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(40) Thu Nov 21 15:34:14 2024: Debug:   State = 0x73c34f14734f5598209f4f525a078ea5
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(40) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(40) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(40) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(40) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(40) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(40) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(40) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(40) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(40) Thu Nov 21 15:34:14 2024: Debug:   Event-Timestamp = "Nov 21 2024 15:34:14 GMT+7"
(40) Thu Nov 21 15:34:14 2024: WARNING: Outer and inner identities are the same.  User privacy
is compromised.
(40) Thu Nov 21 15:34:14 2024: Debug: server inner-tunnel {
(40) Thu Nov 21 15:34:14 2024: Debug:   session-state: No cached attributes
(40) Thu Nov 21 15:34:14 2024: Debug:   # Executing section authorize from file /etc/raddb/
sites-enabled/inner-tunnel
(40) Thu Nov 21 15:34:14 2024: Debug:     authorize {
(40) Thu Nov 21 15:34:14 2024: Debug:       policy filter_username {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name) {
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  -> TRUE
(40) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /) {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /)  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ ) {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
```

```
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ ) {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ )  -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))  {
(40) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)  {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)  {
(40) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)   -> FALSE
(40) Thu Nov 21 15:34:14 2024: Debug:         } # if (&User-Name)  = notfound
(40) Thu Nov 21 15:34:14 2024: Debug:       } # policy filter_username = notfound
(40) Thu Nov 21 15:34:14 2024: Debug:       [chap] = noop
(40) Thu Nov 21 15:34:14 2024: Debug:       [mschap] = noop
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(40) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(40) Thu Nov 21 15:34:14 2024: Debug:       [suffix] = noop
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 140 length 65
(40) Thu Nov 21 15:34:14 2024: Debug: eap: No EAP Start, assuming it's an on-going EAP
conversation
(40) Thu Nov 21 15:34:14 2024: Debug:       [eap] = updated
(40) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(40) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(40) Thu Nov 21 15:34:14 2024: Debug:       [files_multi] = ok
(40) Thu Nov 21 15:34:14 2024: Debug:       [expiration] = noop
(40) Thu Nov 21 15:34:14 2024: Debug:       [logintime] = noop
(40) Thu Nov 21 15:34:14 2024: WARNING: pap: Auth-Type already set.  Not setting to PAP
(40) Thu Nov 21 15:34:14 2024: Debug:       [pap] = noop
(40) Thu Nov 21 15:34:14 2024: Debug:     } # authorize = updated
(40) Thu Nov 21 15:34:14 2024: Debug:   Found Auth-Type = eap
(40) Thu Nov 21 15:34:14 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(40) Thu Nov 21 15:34:14 2024: Debug:     authenticate {
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0x73c34f14734f5598
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0x73c34f14734f5598
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0x73c34f14734f5598, released from the list
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP MSCHAPv2 (26)
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_mschapv2 to process data
(40) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2: # Executing group from file /etc/raddb/
sites-enabled/inner-tunnel
(40) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2:   authenticate {
(40) Thu Nov 21 15:34:14 2024: Debug: mschap: Found Cleartext-Password, hashing to create NT-
Password
(40) Thu Nov 21 15:34:14 2024: Debug: mschap: Creating challenge hash with username: tester
(40) Thu Nov 21 15:34:14 2024: Debug: mschap: Client is using MS-CHAPv2
(40) Thu Nov 21 15:34:14 2024: Debug: mschap: Adding MS-CHAPv2 MPPE keys
(40) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2:     [mschap] = ok
(40) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2:   } # authenticate = ok
(40) Thu Nov 21 15:34:14 2024: Debug: eap_mschapv2: MSCHAP Success
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 141 length 51
(40) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0x73c34f14724e5598
(40) Thu Nov 21 15:34:14 2024: Debug:       [eap] = handled
(40) Thu Nov 21 15:34:14 2024: Debug:     } # authenticate = handled
(40) Thu Nov 21 15:34:14 2024: Debug: } # server inner-tunnel
(40) Thu Nov 21 15:34:14 2024: Debug: Virtual server sending reply
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
```

```
(40) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018d00331a038c002e533d39354232443738333534413844394239323646343137334234443336433636443346353
239323633
(40) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(40) Thu Nov 21 15:34:14 2024: Debug:   State = 0x73c34f14724e5598209f4f525a078ea5
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled reply code 11
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Tls-Enabled = 0
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message =
0x018d00331a038c002e533d39354232443738333534413844394239323646343137334234443336433636443346353
239323633
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Message-Authenticator =
0x00000000000000000000000000000000
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   State = 0x73c34f14724e5598209f4f525a078ea5
(40) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled Access-Challenge
(40) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 141 length 82
(40) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814d14bc1da
(40) Thu Nov 21 15:34:14 2024: Debug:     [eap] = handled
(40) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = handled
(40) Thu Nov 21 15:34:14 2024: Debug: Using Post-Auth-Type Challenge
(40) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(40) Thu Nov 21 15:34:14 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(40) Thu Nov 21 15:34:14 2024: Debug: session-state: Saving cached attributes
(40) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1004
(40) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(40) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(40) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Challenge Id 38 from 100.129.58.1:1812 to
100.129.56.1:37236 length 152
(40) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(40) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018d00521900170303004789966e719344ac9af15a53fdbc7ddd326dbb2077c4408506c914b95ba44cd77fbb7e6cb
22459ac676effd3c6f5765c6bd5c649e3c1d850390aa630ee9738d0ebfcae8
(40) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(40) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d14bc1da517e6b54cde2f128
(40) Thu Nov 21 15:34:14 2024: Debug: Finished request
(41) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 39 from 100.129.56.1:37236 to
100.129.58.1:1812 length 303
(41) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(41) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(41) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(41) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(41) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(41) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(41) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(41) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x028d00251900170303001a126f9cc4d1f2f833c2f45c7003974c78f59be6590bd4cd7aef19
(41) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814d14bc1da517e6b54cde2f128
```

```
(41) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0xdf7e4ecdc69f4f27b35460f818113c1b
(41) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(41) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(41) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(41) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(41) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(41) Thu Nov 21 15:34:14 2024: Debug:   authorize {
(41) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(41) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(41) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(41) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(41) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(41) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(41) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(41) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(41) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(41) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(41) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(41) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(41) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(41) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(41) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(41) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:     else {
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 141 length 37
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(41) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(41) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(41) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(41) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(41) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(41) Thu Nov 21 15:34:14 2024: Debug:       return
(41) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(41) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(41) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(41) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(41) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0x73c34f14724e5598
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814d14bc1da
```

```
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814d14bc1da, released from the list
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: PEAP state phase2
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: EAP method MSCHAPv2 (26)
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled request
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message = 0x028d00061a03
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Setting User-Name to tester
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Sending tunneled request to inner-tunnel
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message = 0x028d00061a03
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   User-Name = "tester"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   State = 0x73c34f14724e5598209f4f525a078ea5
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-IP-Address = 100.129.56.1
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Domain = "default"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Identifier = "68:13:E2:35:D2:20"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-
SSID-WLC-15"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Type = Wireless-802.11
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port-Id = "10"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Service-Type = Framed-User
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   NAS-Port = 1
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Connect-Info = "CONNECT 24Mbps 802.11a"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Acct-Session-Id = "073DA111-08E53DB2"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Pairwise-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-Group-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   WLAN-AKM-Suite = 1027073
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-AP-Domain = "with-gre"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Framed-MTU = 1400
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Event-Timestamp = "Nov 21 2024 15:34:14
GMT+7"
(41) Thu Nov 21 15:34:14 2024: Debug: Virtual server inner-tunnel received request
(41) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message = 0x028d00061a03
(41) Thu Nov 21 15:34:14 2024: Debug:   FreeRADIUS-Proxied-To = 127.0.0.1
(41) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(41) Thu Nov 21 15:34:14 2024: Debug:   State = 0x73c34f14724e5598209f4f525a078ea5
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(41) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(41) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(41) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(41) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(41) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(41) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(41) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(41) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(41) Thu Nov 21 15:34:14 2024: Debug:   Event-Timestamp = "Nov 21 2024 15:34:14 GMT+7"
(41) Thu Nov 21 15:34:14 2024: WARNING: Outer and inner identities are the same.  User privacy
is compromised.
```

```
(41) Thu Nov 21 15:34:14 2024: Debug: server inner-tunnel {
(41) Thu Nov 21 15:34:14 2024: Debug:   session-state: No cached attributes
(41) Thu Nov 21 15:34:14 2024: Debug:   # Executing section authorize from file /etc/raddb/
sites-enabled/inner-tunnel
(41) Thu Nov 21 15:34:14 2024: Debug:     authorize {
(41) Thu Nov 21 15:34:14 2024: Debug:       policy filter_username {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name) {
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  -> TRUE
(41) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name)  {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /) {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ / /)  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ ) {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ ) {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.\./ )  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))  {
(41) Thu Nov 21 15:34:14 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)  {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /\.$/)   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)  {
(41) Thu Nov 21 15:34:14 2024: Debug:           if (&User-Name =~ /@\./)   -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:         } # if (&User-Name)  = notfound
(41) Thu Nov 21 15:34:14 2024: Debug:       } # policy filter_username = notfound
(41) Thu Nov 21 15:34:14 2024: Debug:       [chap] = noop
(41) Thu Nov 21 15:34:14 2024: Debug:       [mschap] = noop
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(41) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(41) Thu Nov 21 15:34:14 2024: Debug:       [suffix] = noop
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 141 length 6
(41) Thu Nov 21 15:34:14 2024: Debug: eap: No EAP Start, assuming it's an on-going EAP
conversation
(41) Thu Nov 21 15:34:14 2024: Debug:       [eap] = updated
(41) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(41) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(41) Thu Nov 21 15:34:14 2024: Debug:       [files_multi] = ok
(41) Thu Nov 21 15:34:14 2024: Debug:       [expiration] = noop
(41) Thu Nov 21 15:34:14 2024: Debug:       [logintime] = noop
(41) Thu Nov 21 15:34:14 2024: WARNING: pap: Auth-Type already set.  Not setting to PAP
(41) Thu Nov 21 15:34:14 2024: Debug:       [pap] = noop
(41) Thu Nov 21 15:34:14 2024: Debug:     } # authorize = updated
(41) Thu Nov 21 15:34:14 2024: Debug:   Found Auth-Type = eap
(41) Thu Nov 21 15:34:14 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(41) Thu Nov 21 15:34:14 2024: Debug:     authenticate {
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0x73c34f14724e5598
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0x73c34f14724e5598
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0x73c34f14724e5598, released from the list
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP MSCHAPv2 (26)
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_mschapv2 to process data
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Success (code 3) ID 141 length 4
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Freeing handler
(41) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(41) Thu Nov 21 15:34:14 2024: Debug:     } # authenticate = ok
(41) Thu Nov 21 15:34:14 2024: Debug:   # Executing section post-auth from file /etc/raddb/
sites-enabled/inner-tunnel
(41) Thu Nov 21 15:34:14 2024: Debug:     post-auth {
```

```
(41) Thu Nov 21 15:34:14 2024: Debug:       if (0) {
(41) Thu Nov 21 15:34:14 2024: Debug:       if (0)  -> FALSE
(41) Thu Nov 21 15:34:14 2024: Debug:     } # post-auth = noop
(41) Thu Nov 21 15:34:14 2024: Debug: } # server inner-tunnel
(41) Thu Nov 21 15:34:14 2024: Debug: Virtual server sending reply
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(41) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Encryption-Policy = Encryption-Allowed
(41) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Encryption-Types = RC4-40or128-bit-Allowed
(41) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Send-Key = 0xa1b0f8364771b07393ee9c7191c09627
(41) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Recv-Key = 0xcf76ef2300c319b73c9c69ad346871db
(41) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message = 0x038d0004
(41) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(41) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Got tunneled reply code 2
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Tls-Enabled = 0
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   MS-MPPE-Encryption-Policy = Encryption-
Allowed
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   MS-MPPE-Encryption-Types = RC4-40or128-bit-
Allowed
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   MS-MPPE-Send-Key =
0xa1b0f8364771b07393ee9c7191c09627
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   MS-MPPE-Recv-Key =
0xcf76ef2300c319b73c9c69ad346871db
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   EAP-Message = 0x038d0004
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Message-Authenticator =
0x00000000000000000000000000000000
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   User-Name = "tester"
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Tunneled authentication was successful
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: SUCCESS
(41) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Saving tunneled attributes for later
(41) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Request (code 1) ID 142 length 46
(41) Thu Nov 21 15:34:14 2024: Debug: eap: EAP session adding &reply:State = 0xd6c6d814de48c1da
(41) Thu Nov 21 15:34:14 2024: Debug:     [eap] = handled
(41) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = handled
(41) Thu Nov 21 15:34:14 2024: Debug: Using Post-Auth-Type Challenge
(41) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(41) Thu Nov 21 15:34:14 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(41) Thu Nov 21 15:34:14 2024: Debug: session-state: Saving cached attributes
(41) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1004
(41) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(41) Thu Nov 21 15:34:14 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(41) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Challenge Id 39 from 100.129.58.1:1812 to
100.129.56.1:37236 length 116
(41) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(41) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x018e002e1900170303002389966e719344ac9b8267c67f9750e7bb519cb3f6257935d203dc4994d8e9d0d2b36a60
(41) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(41) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814de48c1da517e6b54cde2f128
(41) Thu Nov 21 15:34:14 2024: Debug: Finished request
(42) Thu Nov 21 15:34:14 2024: Debug: Received Access-Request Id 40 from 100.129.56.1:37236 to
100.129.58.1:1812 length 312
(42) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(42) Thu Nov 21 15:34:14 2024: Debug:   NAS-IP-Address = 100.129.56.1
(42) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Domain = "default"
(42) Thu Nov 21 15:34:14 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(42) Thu Nov 21 15:34:14 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
```

```
(42) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Type = Wireless-802.11
(42) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port-Id = "10"
(42) Thu Nov 21 15:34:14 2024: Debug:   Service-Type = Framed-User
(42) Thu Nov 21 15:34:14 2024: Debug:   NAS-Port = 1
(42) Thu Nov 21 15:34:14 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(42) Thu Nov 21 15:34:14 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(42) Thu Nov 21 15:34:14 2024: Debug:   Acct-Session-Id = "073DA111-08E53DB2"
(42) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(42) Thu Nov 21 15:34:14 2024: Debug:   WLAN-Group-Cipher = 1027076
(42) Thu Nov 21 15:34:14 2024: Debug:   WLAN-AKM-Suite = 1027073
(42) Thu Nov 21 15:34:14 2024: Debug:   Eltex-AP-Domain = "with-gre"
(42) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU = 1400
(42) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message =
0x028e002e19001703030023126f9cc4d1f2f83408287a1e257f531796457aef03f619f341ea20ffc3f42c04759a27
(42) Thu Nov 21 15:34:14 2024: Debug:   State = 0xd6c6d814de48c1da517e6b54cde2f128
(42) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x48ba664f6a34ca3f75cf6dc1827a2fea
(42) Thu Nov 21 15:34:14 2024: Debug: Restoring &session-state
(42) Thu Nov 21 15:34:14 2024: Debug:   &session-state:Framed-MTU = 1004
(42) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(42) Thu Nov 21 15:34:14 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(42) Thu Nov 21 15:34:14 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(42) Thu Nov 21 15:34:14 2024: Debug:   authorize {
(42) Thu Nov 21 15:34:14 2024: Debug:     policy filter_username {
(42) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name) {
(42) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  -> TRUE
(42) Thu Nov 21 15:34:14 2024: Debug:       if (&User-Name)  {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /) {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(42) Thu Nov 21 15:34:14 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)  {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)  {
(42) Thu Nov 21 15:34:14 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:       } # if (&User-Name)  = notfound
(42) Thu Nov 21 15:34:14 2024: Debug:     } # policy filter_username = notfound
(42) Thu Nov 21 15:34:14 2024: Debug:     [preprocess] = ok
(42) Thu Nov 21 15:34:14 2024: Debug:     [chap] = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     [mschap] = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     [digest] = noop
(42) Thu Nov 21 15:34:14 2024: Debug: suffix: Checking for suffix after "@"
(42) Thu Nov 21 15:34:14 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(42) Thu Nov 21 15:34:14 2024: Debug: suffix: No such realm "NULL"
(42) Thu Nov 21 15:34:14 2024: Debug:     [suffix] = noop
(42) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(42) Thu Nov 21 15:34:14 2024: Debug: files_multi: users: Matched entry tester at line 5
(42) Thu Nov 21 15:34:14 2024: Debug:     [files_multi] = ok
(42) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(42) Thu Nov 21 15:34:14 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:     else {
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent EAP Response (code 2) ID 142 length 46
```

```
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Continuing tunnel setup
(42) Thu Nov 21 15:34:14 2024: Debug:       [eap] = ok
(42) Thu Nov 21 15:34:14 2024: Debug:     } # else = ok
(42) Thu Nov 21 15:34:14 2024: Debug:     if (ok) {
(42) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  -> TRUE
(42) Thu Nov 21 15:34:14 2024: Debug:     if (ok)  {
(42) Thu Nov 21 15:34:14 2024: Debug:       return
(42) Thu Nov 21 15:34:14 2024: Debug:     } # if (ok)  = ok
(42) Thu Nov 21 15:34:14 2024: Debug:   } # authorize = ok
(42) Thu Nov 21 15:34:14 2024: Debug: Found Auth-Type = eap
(42) Thu Nov 21 15:34:14 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(42) Thu Nov 21 15:34:14 2024: Debug:   authenticate {
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Expiring EAP session with state 0xd6c6d814de48c1da
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Finished EAP session with state 0xd6c6d814de48c1da
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Previous EAP request found for state
0xd6c6d814de48c1da, released from the list
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Calling submodule eap_peap to process data
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: PEAP state send tlv success
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Received EAP-TLV response
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Success
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap: Using saved attributes from the original
Access-Accept
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   Eltex-Tls-Enabled = 0
(42) Thu Nov 21 15:34:14 2024: Debug: eap_peap:   User-Name = "tester"
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Sending EAP Success (code 3) ID 142 length 4
(42) Thu Nov 21 15:34:14 2024: Debug: eap: Freeing handler
(42) Thu Nov 21 15:34:14 2024: Debug:     [eap] = ok
(42) Thu Nov 21 15:34:14 2024: Debug:   } # authenticate = ok
(42) Thu Nov 21 15:34:14 2024: Debug: # Executing section post-auth from file /etc/raddb/sites-
enabled/_default
(42) Thu Nov 21 15:34:14 2024: Debug:   post-auth {
(42) Thu Nov 21 15:34:14 2024: Debug:     if (session-state:User-Name && reply:User-Name &&
request:User-Name && (reply:User-Name == request:User-Name)) {
(42) Thu Nov 21 15:34:14 2024: Debug:     if (session-state:User-Name && reply:User-Name &&
request:User-Name && (reply:User-Name == request:User-Name))  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:     update {
(42) Thu Nov 21 15:34:14 2024: Debug:     } # update = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     [exec] = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     policy remove_reply_message_if_eap {
(42) Thu Nov 21 15:34:14 2024: Debug:       if (&reply:EAP-Message && &reply:Reply-Message) {
(42) Thu Nov 21 15:34:14 2024: Debug:       if (&reply:EAP-Message && &reply:Reply-Message)  ->
FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:       else {
(42) Thu Nov 21 15:34:14 2024: Debug:         [noop] = noop
(42) Thu Nov 21 15:34:14 2024: Debug:       } # else = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     } # policy remove_reply_message_if_eap = noop
(42) Thu Nov 21 15:34:14 2024: Debug:     if (EAP-Key-Name && &reply:EAP-Session-Id) {
(42) Thu Nov 21 15:34:14 2024: Debug:     if (EAP-Key-Name && &reply:EAP-Session-Id)  -> FALSE
(42) Thu Nov 21 15:34:14 2024: Debug:     update reply {
(42) Thu Nov 21 15:34:14 2024: Debug:     } # update reply = noop
(42) Thu Nov 21 15:34:14 2024: Debug:   } # post-auth = noop
(42) Thu Nov 21 15:34:14 2024: Debug: Sent Access-Accept Id 40 from 100.129.58.1:1812 to
100.129.56.1:37236 length 198   <------------------------------------------- Access-Accept
пользователь успешно авторизован
(42) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
(42) Thu Nov 21 15:34:14 2024: Debug:   Eltex-Tls-Enabled = 0
```

```
(42) Thu Nov 21 15:34:14 2024: Debug:   User-Name = "tester"
(42) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Recv-Key =
0xf396c52ff7d711df6e4a0d232d3224dc45afe1533f7042754905fe2081b10869
(42) Thu Nov 21 15:34:14 2024: Debug:   MS-MPPE-Send-Key =
0x37006c121c188e56215bda352b9806ea837ecd042cae84dfb7cc7815d5f15802
(42) Thu Nov 21 15:34:14 2024: Debug:   EAP-Message = 0x038e0004
(42) Thu Nov 21 15:34:14 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(42) Thu Nov 21 15:34:14 2024: Debug:   Framed-MTU += 1004
(42) Thu Nov 21 15:34:14 2024: Debug: Finished request
(33) Thu Nov 21 15:34:14 2024: Debug: Cleaning up request packet ID 31 with timestamp +8808
(34) Thu Nov 21 15:34:14 2024: Debug: Cleaning up request packet ID 32 with timestamp +8808
(35) Thu Nov 21 15:34:14 2024: Debug: Cleaning up request packet ID 33 with timestamp +8808
(36) Thu Nov 21 15:34:14 2024: Debug: Cleaning up request packet ID 34 with timestamp +8808
(37) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 35 with timestamp +8813
(38) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 36 with timestamp +8813
(39) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 37 with timestamp +8813
(40) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 38 with timestamp +8813
(41) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 39 with timestamp +8813
(42) Thu Nov 21 15:34:19 2024: Debug: Cleaning up request packet ID 40 with timestamp +8813
```

При неуспешном подключении клиента с авторизацией на локальном RADIUS-сервере

```
wlc-15#
wlc-15# debug
wlc-15(debug)# show radius-debug username tester ip-address 100.129.56.1 timeout 600
(43) Thu Nov 21 15:38:09 2024: Debug: Received Access-Request Id 41 from 100.129.56.1:37236 to
100.129.58.1:1812 length 259
(43) Thu Nov 21 15:38:09 2024: Debug:   User-Name = "tester"
(43) Thu Nov 21 15:38:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(43) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Domain = "default"
(43) Thu Nov 21 15:38:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(43) Thu Nov 21 15:38:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(43) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(43) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Id = "10"
(43) Thu Nov 21 15:38:09 2024: Debug:   Service-Type = Framed-User
(43) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port = 1
(43) Thu Nov 21 15:38:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(43) Thu Nov 21 15:38:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(43) Thu Nov 21 15:38:09 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(43) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(43) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(43) Thu Nov 21 15:38:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(43) Thu Nov 21 15:38:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(43) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1400
(43) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message = 0x0246000b01746573746572
(43) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x8052997bb00c324abe23685055e7e121
(43) Thu Nov 21 15:38:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(43) Thu Nov 21 15:38:09 2024: Debug:   authorize {
(43) Thu Nov 21 15:38:09 2024: Debug:     policy filter_username {
(43) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name) {
(43) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  -> TRUE
(43) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  {
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /) {
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
```

```
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(43) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(43) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:       } # if (&User-Name)  = notfound
(43) Thu Nov 21 15:38:09 2024: Debug:     } # policy filter_username = notfound
(43) Thu Nov 21 15:38:09 2024: Debug:     [preprocess] = ok
(43) Thu Nov 21 15:38:09 2024: Debug:     [chap] = noop
(43) Thu Nov 21 15:38:09 2024: Debug:     [mschap] = noop
(43) Thu Nov 21 15:38:09 2024: Debug:     [digest] = noop
(43) Thu Nov 21 15:38:09 2024: Debug: suffix: Checking for suffix after "@"
(43) Thu Nov 21 15:38:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(43) Thu Nov 21 15:38:09 2024: Debug: suffix: No such realm "NULL"
(43) Thu Nov 21 15:38:09 2024: Debug:     [suffix] = noop
(43) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(43) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(43) Thu Nov 21 15:38:09 2024: Debug:     [files_multi] = ok
(43) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(43) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(43) Thu Nov 21 15:38:09 2024: Debug:     else {
(43) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 70 length 11
(43) Thu Nov 21 15:38:09 2024: Debug: eap: EAP-Identity reply, returning 'ok' so we can short-
circuit the rest of authorize
(43) Thu Nov 21 15:38:09 2024: Debug:       [eap] = ok
(43) Thu Nov 21 15:38:09 2024: Debug:     } # else = ok
(43) Thu Nov 21 15:38:09 2024: Debug:     if (ok) {
(43) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  -> TRUE
(43) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  {
(43) Thu Nov 21 15:38:09 2024: Debug:       return
(43) Thu Nov 21 15:38:09 2024: Debug:     } # if (ok)  = ok
(43) Thu Nov 21 15:38:09 2024: Debug:   } # authorize = ok
(43) Thu Nov 21 15:38:09 2024: Debug: Found Auth-Type = eap
(43) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(43) Thu Nov 21 15:38:09 2024: Debug:   authenticate {
(43) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent packet with method EAP Identity (1)
(43) Thu Nov 21 15:38:09 2024: Debug: eap: Calling submodule eap_peap to process data
(43) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Initiating new session
(43) Thu Nov 21 15:38:09 2024: Debug: eap: Sending EAP Request (code 1) ID 71 length 6
(43) Thu Nov 21 15:38:09 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8e935dca6
(43) Thu Nov 21 15:38:09 2024: Debug:     [eap] = handled
(43) Thu Nov 21 15:38:09 2024: Debug:   } # authenticate = handled
(43) Thu Nov 21 15:38:09 2024: Debug: Using Post-Auth-Type Challenge
(43) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(43) Thu Nov 21 15:38:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(43) Thu Nov 21 15:38:09 2024: Debug: session-state: Saving cached attributes
(43) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1004
(43) Thu Nov 21 15:38:09 2024: Debug: Sent Access-Challenge Id 41 from 100.129.58.1:1812 to
100.129.56.1:37236 length 76
(43) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Tls-Enabled = 0
(43) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message = 0x014700061920
```

```
(43) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(43) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8e935dca62745240ad035bf82
(43) Thu Nov 21 15:38:09 2024: Debug: Finished request
(44) Thu Nov 21 15:38:09 2024: Debug: Received Access-Request Id 42 from 100.129.56.1:37236 to
100.129.58.1:1812 length 427
(44) Thu Nov 21 15:38:09 2024: Debug:   User-Name = "tester"
(44) Thu Nov 21 15:38:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(44) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Domain = "default"
(44) Thu Nov 21 15:38:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(44) Thu Nov 21 15:38:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(44) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(44) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Id = "10"
(44) Thu Nov 21 15:38:09 2024: Debug:   Service-Type = Framed-User
(44) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port = 1
(44) Thu Nov 21 15:38:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(44) Thu Nov 21 15:38:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(44) Thu Nov 21 15:38:09 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(44) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(44) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(44) Thu Nov 21 15:38:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(44) Thu Nov 21 15:38:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(44) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1400
(44) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message =
0x024700a11980000000097160301009201000008e0303673ef170064c92e3d9f914a8c17727c881d308d40f531afb93b
aaaf9f565df9700002c00ffc02cc02bc024c023c00ac009c008c030c02fc00
(44) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8e935dca62745240ad035bf82
(44) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0xeb9ce4f152d26f14fe009617feb33a71
(44) Thu Nov 21 15:38:09 2024: Debug: Restoring &session-state
(44) Thu Nov 21 15:38:09 2024: Debug:   &session-state:Framed-MTU = 1004
(44) Thu Nov 21 15:38:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(44) Thu Nov 21 15:38:09 2024: Debug:   authorize {
(44) Thu Nov 21 15:38:09 2024: Debug:     policy filter_username {
(44) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name) {
(44) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  -> TRUE
(44) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /) {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(44) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(44) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:       } # if (&User-Name)  = notfound
(44) Thu Nov 21 15:38:09 2024: Debug:     } # policy filter_username = notfound
(44) Thu Nov 21 15:38:09 2024: Debug:     [preprocess] = ok
(44) Thu Nov 21 15:38:09 2024: Debug:     [chap] = noop
(44) Thu Nov 21 15:38:09 2024: Debug:     [mschap] = noop
(44) Thu Nov 21 15:38:09 2024: Debug:     [digest] = noop
(44) Thu Nov 21 15:38:09 2024: Debug: suffix: Checking for suffix after "@"
```

```
(44) Thu Nov 21 15:38:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(44) Thu Nov 21 15:38:09 2024: Debug: suffix: No such realm "NULL"
(44) Thu Nov 21 15:38:09 2024: Debug:     [suffix] = noop
(44) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(44) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(44) Thu Nov 21 15:38:09 2024: Debug:     [files_multi] = ok
(44) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(44) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(44) Thu Nov 21 15:38:09 2024: Debug:     else {
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 71 length 161
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Continuing tunnel setup
(44) Thu Nov 21 15:38:09 2024: Debug:       [eap] = ok
(44) Thu Nov 21 15:38:09 2024: Debug:     } # else = ok
(44) Thu Nov 21 15:38:09 2024: Debug:     if (ok) {
(44) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  -> TRUE
(44) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  {
(44) Thu Nov 21 15:38:09 2024: Debug:       return
(44) Thu Nov 21 15:38:09 2024: Debug:     } # if (ok)  = ok
(44) Thu Nov 21 15:38:09 2024: Debug:   } # authorize = ok
(44) Thu Nov 21 15:38:09 2024: Debug: Found Auth-Type = eap
(44) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(44) Thu Nov 21 15:38:09 2024: Debug:   authenticate {
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8e935dca6
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Finished EAP session with state 0xe972c5d8e935dca6
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8e935dca6, released from the list
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Calling submodule eap_peap to process data
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) EAP Peer says that the final record size
will be 151 bytes
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) EAP Got all data (151 bytes)
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - before/accept
initialization
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server before/accept
initialization
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client hello A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
server hello A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
certificate A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write key
exchange A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
server done A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 flush data
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client certificate A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Server : Need to read more data: SSLv3
read client key exchange A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Server : Need to read more data: SSLv3
read client key exchange A
(44) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) In Handshake Phase
(44) Thu Nov 21 15:38:09 2024: Debug: eap: Sending EAP Request (code 1) ID 72 length 1014
(44) Thu Nov 21 15:38:09 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8e83adca6
(44) Thu Nov 21 15:38:09 2024: Debug:     [eap] = handled
(44) Thu Nov 21 15:38:09 2024: Debug:   } # authenticate = handled
(44) Thu Nov 21 15:38:09 2024: Debug: Using Post-Auth-Type Challenge
```

```
(44) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(44) Thu Nov 21 15:38:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(44) Thu Nov 21 15:38:09 2024: Debug: session-state: Saving cached attributes
(44) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1004
(44) Thu Nov 21 15:38:09 2024: Debug: Sent Access-Challenge Id 42 from 100.129.58.1:1812 to
100.129.56.1:37236 length 1092
(44) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Tls-Enabled = 0
(44) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message =
0x014803f619c00000090f160303003902000035030 3ca841ca7fba6fa59e4b8f03b2de4c392f99af02b133d18a559f
4ca89b0e0c3ca00c03000000dff01000100000b000403000102160303077 10
(44) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(44) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8e83adca62745240ad035bf82
(44) Thu Nov 21 15:38:09 2024: Debug: Finished request
(45) Thu Nov 21 15:38:09 2024: Debug: Received Access-Request Id 43 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
(45) Thu Nov 21 15:38:09 2024: Debug:   User-Name = "tester"
(45) Thu Nov 21 15:38:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(45) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Domain = "default"
(45) Thu Nov 21 15:38:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(45) Thu Nov 21 15:38:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(45) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(45) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Id = "10"
(45) Thu Nov 21 15:38:09 2024: Debug:   Service-Type = Framed-User
(45) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port = 1
(45) Thu Nov 21 15:38:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(45) Thu Nov 21 15:38:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(45) Thu Nov 21 15:38:09 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(45) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(45) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(45) Thu Nov 21 15:38:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(45) Thu Nov 21 15:38:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(45) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1400
(45) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message = 0x024800061900
(45) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8e83adca62745240ad035bf82
(45) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x79778347b42853902dd172864da20b91
(45) Thu Nov 21 15:38:09 2024: Debug: Restoring &session-state
(45) Thu Nov 21 15:38:09 2024: Debug:   &session-state:Framed-MTU = 1004
(45) Thu Nov 21 15:38:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(45) Thu Nov 21 15:38:09 2024: Debug:   authorize {
(45) Thu Nov 21 15:38:09 2024: Debug:     policy filter_username {
(45) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name) {
(45) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  -> TRUE
(45) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  {
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /) {
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(45) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)  {
```

```
(45) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:       } # if (&User-Name)  = notfound
(45) Thu Nov 21 15:38:09 2024: Debug:     } # policy filter_username = notfound
(45) Thu Nov 21 15:38:09 2024: Debug:     [preprocess] = ok
(45) Thu Nov 21 15:38:09 2024: Debug:     [chap] = noop
(45) Thu Nov 21 15:38:09 2024: Debug:     [mschap] = noop
(45) Thu Nov 21 15:38:09 2024: Debug:     [digest] = noop
(45) Thu Nov 21 15:38:09 2024: Debug: suffix: Checking for suffix after "@"
(45) Thu Nov 21 15:38:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(45) Thu Nov 21 15:38:09 2024: Debug: suffix: No such realm "NULL"
(45) Thu Nov 21 15:38:09 2024: Debug:     [suffix] = noop
(45) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(45) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(45) Thu Nov 21 15:38:09 2024: Debug:     [files_multi] = ok
(45) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(45) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(45) Thu Nov 21 15:38:09 2024: Debug:     else {
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 72 length 6
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Continuing tunnel setup
(45) Thu Nov 21 15:38:09 2024: Debug:       [eap] = ok
(45) Thu Nov 21 15:38:09 2024: Debug:     } # else = ok
(45) Thu Nov 21 15:38:09 2024: Debug:     if (ok) {
(45) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  -> TRUE
(45) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  {
(45) Thu Nov 21 15:38:09 2024: Debug:       return
(45) Thu Nov 21 15:38:09 2024: Debug:     } # if (ok)  = ok
(45) Thu Nov 21 15:38:09 2024: Debug:   } # authorize = ok
(45) Thu Nov 21 15:38:09 2024: Debug: Found Auth-Type = eap
(45) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(45) Thu Nov 21 15:38:09 2024: Debug:   authenticate {
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8e83adca6
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Finished EAP session with state 0xe972c5d8e83adca6
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8e83adca6, released from the list
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Calling submodule eap_peap to process data
(45) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment
(45) Thu Nov 21 15:38:09 2024: Debug: eap: Sending EAP Request (code 1) ID 73 length 1010
(45) Thu Nov 21 15:38:09 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8eb3bdca6
(45) Thu Nov 21 15:38:09 2024: Debug:     [eap] = handled
(45) Thu Nov 21 15:38:09 2024: Debug:   } # authenticate = handled
(45) Thu Nov 21 15:38:09 2024: Debug: Using Post-Auth-Type Challenge
(45) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(45) Thu Nov 21 15:38:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(45) Thu Nov 21 15:38:09 2024: Debug: session-state: Saving cached attributes
(45) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1004
(45) Thu Nov 21 15:38:09 2024: Debug: Sent Access-Challenge Id 43 from 100.129.58.1:1812 to
100.129.56.1:37236 length 1086
(45) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Tls-Enabled = 0
(45) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message =
0x014903f21940300d06092a864886f70d01010b0500308181310b3009060355040613025255310f300d06035504080
c0652757373696131143012060355040 70c0b4e6f766f7369626972736b314
(45) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(45) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8eb3bdca62745240ad035bf82
(45) Thu Nov 21 15:38:09 2024: Debug: Finished request
(46) Thu Nov 21 15:38:09 2024: Debug: Received Access-Request Id 44 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
```

```
(46) Thu Nov 21 15:38:09 2024: Debug:   User-Name = "tester"
(46) Thu Nov 21 15:38:09 2024: Debug:   NAS-IP-Address = 100.129.56.1
(46) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Domain = "default"
(46) Thu Nov 21 15:38:09 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(46) Thu Nov 21 15:38:09 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(46) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Type = Wireless-802.11
(46) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port-Id = "10"
(46) Thu Nov 21 15:38:09 2024: Debug:   Service-Type = Framed-User
(46) Thu Nov 21 15:38:09 2024: Debug:   NAS-Port = 1
(46) Thu Nov 21 15:38:09 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(46) Thu Nov 21 15:38:09 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(46) Thu Nov 21 15:38:09 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(46) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(46) Thu Nov 21 15:38:09 2024: Debug:   WLAN-Group-Cipher = 1027076
(46) Thu Nov 21 15:38:09 2024: Debug:   WLAN-AKM-Suite = 1027073
(46) Thu Nov 21 15:38:09 2024: Debug:   Eltex-AP-Domain = "with-gre"
(46) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1400
(46) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message = 0x024900061900
(46) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8eb3bdca62745240ad035bf82
(46) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0xf6921fdf077bcefe93465d0622df347d
(46) Thu Nov 21 15:38:09 2024: Debug: Restoring &session-state
(46) Thu Nov 21 15:38:09 2024: Debug:   &session-state:Framed-MTU = 1004
(46) Thu Nov 21 15:38:09 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(46) Thu Nov 21 15:38:09 2024: Debug:   authorize {
(46) Thu Nov 21 15:38:09 2024: Debug:     policy filter_username {
(46) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name) {
(46) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  -> TRUE
(46) Thu Nov 21 15:38:09 2024: Debug:       if (&User-Name)  {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /) {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(46) Thu Nov 21 15:38:09 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)  {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)  {
(46) Thu Nov 21 15:38:09 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(46) Thu Nov 21 15:38:09 2024: Debug:       } # if (&User-Name)  = notfound
(46) Thu Nov 21 15:38:09 2024: Debug:     } # policy filter_username = notfound
(46) Thu Nov 21 15:38:09 2024: Debug:     [preprocess] = ok
(46) Thu Nov 21 15:38:09 2024: Debug:     [chap] = noop
(46) Thu Nov 21 15:38:09 2024: Debug:     [mschap] = noop
(46) Thu Nov 21 15:38:09 2024: Debug:     [digest] = noop
(46) Thu Nov 21 15:38:09 2024: Debug: suffix: Checking for suffix after "@"
(46) Thu Nov 21 15:38:09 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(46) Thu Nov 21 15:38:09 2024: Debug: suffix: No such realm "NULL"
(46) Thu Nov 21 15:38:09 2024: Debug:     [suffix] = noop
(46) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(46) Thu Nov 21 15:38:09 2024: Debug: files_multi: users: Matched entry tester at line 5
(46) Thu Nov 21 15:38:09 2024: Debug:     [files_multi] = ok
(46) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(46) Thu Nov 21 15:38:09 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
```

```
(46) Thu Nov 21 15:38:09 2024: Debug:     else {
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent EAP Response (code 2) ID 73 length 6
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Continuing tunnel setup
(46) Thu Nov 21 15:38:09 2024: Debug:       [eap] = ok
(46) Thu Nov 21 15:38:09 2024: Debug:     } # else = ok
(46) Thu Nov 21 15:38:09 2024: Debug:     if (ok) {
(46) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  -> TRUE
(46) Thu Nov 21 15:38:09 2024: Debug:     if (ok)  {
(46) Thu Nov 21 15:38:09 2024: Debug:       return
(46) Thu Nov 21 15:38:09 2024: Debug:     } # if (ok)  = ok
(46) Thu Nov 21 15:38:09 2024: Debug:   } # authorize = ok
(46) Thu Nov 21 15:38:09 2024: Debug: Found Auth-Type = eap
(46) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(46) Thu Nov 21 15:38:09 2024: Debug:   authenticate {
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8eb3bdca6
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Finished EAP session with state 0xe972c5d8eb3bdca6
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8eb3bdca6, released from the list
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Calling submodule eap_peap to process data
(46) Thu Nov 21 15:38:09 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment
(46) Thu Nov 21 15:38:09 2024: Debug: eap: Sending EAP Request (code 1) ID 74 length 317
(46) Thu Nov 21 15:38:09 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8ea38dca6
(46) Thu Nov 21 15:38:09 2024: Debug:     [eap] = handled
(46) Thu Nov 21 15:38:09 2024: Debug:   } # authenticate = handled
(46) Thu Nov 21 15:38:09 2024: Debug: Using Post-Auth-Type Challenge
(46) Thu Nov 21 15:38:09 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(46) Thu Nov 21 15:38:09 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(46) Thu Nov 21 15:38:09 2024: Debug: session-state: Saving cached attributes
(46) Thu Nov 21 15:38:09 2024: Debug:   Framed-MTU = 1004
(46) Thu Nov 21 15:38:09 2024: Debug: Sent Access-Challenge Id 44 from 100.129.58.1:1812 to
100.129.56.1:37236 length 389
(46) Thu Nov 21 15:38:09 2024: Debug:   Eltex-Tls-Enabled = 0
(46) Thu Nov 21 15:38:09 2024: Debug:   EAP-Message =
0x014a013d1900a271db240af40070d8383b0d1499a92f76240efa2e5f0b75bd61c25c5693938ffab6c28685e5a9a7e
9ff04010100ace6e0163e6295adb6a28327b5c00395e2f0feb4841f3283a70
(46) Thu Nov 21 15:38:09 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(46) Thu Nov 21 15:38:09 2024: Debug:   State = 0xe972c5d8ea38dca62745240ad035bf82
(46) Thu Nov 21 15:38:09 2024: Debug: Finished request
(47) Thu Nov 21 15:38:12 2024: Debug: Received Access-Request Id 45 from 100.129.56.1:37236 to
100.129.58.1:1812 length 402
(47) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(47) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(47) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(47) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(47) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(47) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(47) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(47) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(47) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(47) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(47) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(47) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(47) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(47) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(47) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(47) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
```

```
(47) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(47) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x024a008819800000007e160303004610000042410423f5d337b5ef95bd6246a2ed3b77f78a23b18c6bd143580437c
050474e879456d5b30c5455791886532fda426c319f25f52de4bb73688c706
(47) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ea38dca62745240ad035bf82
(47) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x4fbfe35b822dd4f23cd00967ab5c653a
(47) Thu Nov 21 15:38:12 2024: Debug: Restoring &session-state
(47) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Framed-MTU = 1004
(47) Thu Nov 21 15:38:12 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(47) Thu Nov 21 15:38:12 2024: Debug:   authorize {
(47) Thu Nov 21 15:38:12 2024: Debug:     policy filter_username {
(47) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name) {
(47) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  -> TRUE
(47) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /) {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(47) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)  {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)  {
(47) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:       } # if (&User-Name)  = notfound
(47) Thu Nov 21 15:38:12 2024: Debug:     } # policy filter_username = notfound
(47) Thu Nov 21 15:38:12 2024: Debug:     [preprocess] = ok
(47) Thu Nov 21 15:38:12 2024: Debug:     [chap] = noop
(47) Thu Nov 21 15:38:12 2024: Debug:     [mschap] = noop
(47) Thu Nov 21 15:38:12 2024: Debug:     [digest] = noop
(47) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(47) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(47) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(47) Thu Nov 21 15:38:12 2024: Debug:     [suffix] = noop
(47) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(47) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(47) Thu Nov 21 15:38:12 2024: Debug:     [files_multi] = ok
(47) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(47) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(47) Thu Nov 21 15:38:12 2024: Debug:     else {
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 74 length 136
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Continuing tunnel setup
(47) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(47) Thu Nov 21 15:38:12 2024: Debug:     } # else = ok
(47) Thu Nov 21 15:38:12 2024: Debug:     if (ok) {
(47) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  -> TRUE
(47) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  {
(47) Thu Nov 21 15:38:12 2024: Debug:       return
(47) Thu Nov 21 15:38:12 2024: Debug:     } # if (ok)  = ok
(47) Thu Nov 21 15:38:12 2024: Debug:   } # authorize = ok
(47) Thu Nov 21 15:38:12 2024: Debug: Found Auth-Type = eap
(47) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(47) Thu Nov 21 15:38:12 2024: Debug:   authenticate {
```

```
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8ea38dca6
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0xe972c5d8ea38dca6
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8ea38dca6, released from the list
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_peap to process data
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) EAP Peer says that the final record size
will be 126 bytes
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) EAP Got all data (126 bytes)
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
client key exchange A
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
certificate verify A
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 read
finished A
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
change cipher spec A
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 write
finished A
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - Server SSLv3 flush data
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Handshake state - SSL negotiation
finished successfully
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Connection Established
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-
GCM-SHA384"
(47) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   TLS-Session-Version = "TLS 1.2"
(47) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Request (code 1) ID 75 length 57
(47) Thu Nov 21 15:38:12 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8ed39dca6
(47) Thu Nov 21 15:38:12 2024: Debug:     [eap] = handled
(47) Thu Nov 21 15:38:12 2024: Debug:   } # authenticate = handled
(47) Thu Nov 21 15:38:12 2024: Debug: Using Post-Auth-Type Challenge
(47) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(47) Thu Nov 21 15:38:12 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(47) Thu Nov 21 15:38:12 2024: Debug: session-state: Saving cached attributes
(47) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1004
(47) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(47) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(47) Thu Nov 21 15:38:12 2024: Debug: Sent Access-Challenge Id 45 from 100.129.58.1:1812 to
100.129.56.1:37236 length 127
(47) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Tls-Enabled = 0
(47) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x014b00391900140303000101160303002849b195ac8c59a1d46333e916107a84e292a43db7f6e5836b59c8c37cb7d
0dfcd69f685b829e7ab69
(47) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(47) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ed39dca62745240ad035bf82
(47) Thu Nov 21 15:38:12 2024: Debug: Finished request
(48) Thu Nov 21 15:38:12 2024: Debug: Received Access-Request Id 46 from 100.129.56.1:37236 to
100.129.58.1:1812 length 272
(48) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(48) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(48) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(48) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(48) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(48) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(48) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(48) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(48) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
```

```
(48) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(48) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(48) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(48) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(48) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(48) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(48) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
(48) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(48) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message = 0x024b00061900
(48) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ed39dca62745240ad035bf82
(48) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x82dd95a5c92c2f3fc07f730d829f740f
(48) Thu Nov 21 15:38:12 2024: Debug: Restoring &session-state
(48) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Framed-MTU = 1004
(48) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(48) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(48) Thu Nov 21 15:38:12 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(48) Thu Nov 21 15:38:12 2024: Debug:   authorize {
(48) Thu Nov 21 15:38:12 2024: Debug:     policy filter_username {
(48) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name) {
(48) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  -> TRUE
(48) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /) {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(48) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)  {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)  {
(48) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:       } # if (&User-Name)  = notfound
(48) Thu Nov 21 15:38:12 2024: Debug:     } # policy filter_username = notfound
(48) Thu Nov 21 15:38:12 2024: Debug:     [preprocess] = ok
(48) Thu Nov 21 15:38:12 2024: Debug:     [chap] = noop
(48) Thu Nov 21 15:38:12 2024: Debug:     [mschap] = noop
(48) Thu Nov 21 15:38:12 2024: Debug:     [digest] = noop
(48) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(48) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(48) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(48) Thu Nov 21 15:38:12 2024: Debug:     [suffix] = noop
(48) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(48) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(48) Thu Nov 21 15:38:12 2024: Debug:     [files_multi] = ok
(48) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(48) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(48) Thu Nov 21 15:38:12 2024: Debug:     else {
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 75 length 6
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Continuing tunnel setup
(48) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(48) Thu Nov 21 15:38:12 2024: Debug:     } # else = ok
(48) Thu Nov 21 15:38:12 2024: Debug:     if (ok) {
(48) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  -> TRUE
```

```
(48) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  {
(48) Thu Nov 21 15:38:12 2024: Debug:       return
(48) Thu Nov 21 15:38:12 2024: Debug:     } # if (ok)  = ok
(48) Thu Nov 21 15:38:12 2024: Debug:   } # authorize = ok
(48) Thu Nov 21 15:38:12 2024: Debug: Found Auth-Type = eap
(48) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(48) Thu Nov 21 15:38:12 2024: Debug:   authenticate {
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8ed39dca6
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0xe972c5d8ed39dca6
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8ed39dca6, released from the list
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_peap to process data
(48) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) Peer ACKed our handshake fragment.
handshake is finished
(48) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(48) Thu Nov 21 15:38:12 2024: Debug: eap_peap: PEAP state TUNNEL ESTABLISHED
(48) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Request (code 1) ID 76 length 40
(48) Thu Nov 21 15:38:12 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8ec3edca6
(48) Thu Nov 21 15:38:12 2024: Debug:     [eap] = handled
(48) Thu Nov 21 15:38:12 2024: Debug:   } # authenticate = handled
(48) Thu Nov 21 15:38:12 2024: Debug: Using Post-Auth-Type Challenge
(48) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(48) Thu Nov 21 15:38:12 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(48) Thu Nov 21 15:38:12 2024: Debug: session-state: Saving cached attributes
(48) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1004
(48) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(48) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(48) Thu Nov 21 15:38:12 2024: Debug: Sent Access-Challenge Id 46 from 100.129.58.1:1812 to
100.129.56.1:37236 length 110
(48) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Tls-Enabled = 0
(48) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x014c00281900170303001d49b195ac8c59a1d55225d2729e22fe21d9a67c0216924b115c80a1327d
(48) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(48) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ec3edca62745240ad035bf82
(48) Thu Nov 21 15:38:12 2024: Debug: Finished request
(49) Thu Nov 21 15:38:12 2024: Debug: Received Access-Request Id 47 from 100.129.56.1:37236 to
100.129.58.1:1812 length 308
(49) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(49) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(49) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(49) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(49) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(49) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(49) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(49) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
(49) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
```

```
(49) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x024c002a1900170303001ff8975c28e091e730066e4f736163e372fca19ec6aae10f9d73fabe9f52ebcf
(49) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ec3edca62745240ad035bf82
(49) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x97ee747668e390335d3a23fd13637129
(49) Thu Nov 21 15:38:12 2024: Debug: Restoring &session-state
(49) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Framed-MTU = 1004
(49) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(49) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(49) Thu Nov 21 15:38:12 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(49) Thu Nov 21 15:38:12 2024: Debug:   authorize {
(49) Thu Nov 21 15:38:12 2024: Debug:     policy filter_username {
(49) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name) {
(49) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  -> TRUE
(49) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /) {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(49) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)  {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)  {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:       } # if (&User-Name)  = notfound
(49) Thu Nov 21 15:38:12 2024: Debug:     } # policy filter_username = notfound
(49) Thu Nov 21 15:38:12 2024: Debug:     [preprocess] = ok
(49) Thu Nov 21 15:38:12 2024: Debug:     [chap] = noop
(49) Thu Nov 21 15:38:12 2024: Debug:     [mschap] = noop
(49) Thu Nov 21 15:38:12 2024: Debug:     [digest] = noop
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(49) Thu Nov 21 15:38:12 2024: Debug:     [suffix] = noop
(49) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(49) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(49) Thu Nov 21 15:38:12 2024: Debug:     [files_multi] = ok
(49) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(49) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:     else {
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 76 length 42
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Continuing tunnel setup
(49) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(49) Thu Nov 21 15:38:12 2024: Debug:     } # else = ok
(49) Thu Nov 21 15:38:12 2024: Debug:     if (ok) {
(49) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  -> TRUE
(49) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  {
(49) Thu Nov 21 15:38:12 2024: Debug:       return
(49) Thu Nov 21 15:38:12 2024: Debug:     } # if (ok)  = ok
(49) Thu Nov 21 15:38:12 2024: Debug:   } # authorize = ok
(49) Thu Nov 21 15:38:12 2024: Debug: Found Auth-Type = eap
(49) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
```

```
(49) Thu Nov 21 15:38:12 2024: Debug:   authenticate {
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8ec3edca6
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0xe972c5d8ec3edca6
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8ec3edca6, released from the list
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_peap to process data
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: PEAP state WAITING FOR INNER IDENTITY
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Identity - tester
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got inner identity 'tester'
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Setting default EAP type for tunneled EAP
session
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got tunneled request
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message = 0x024c000b01746573746572
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Setting User-Name to tester
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Sending tunneled request to inner-tunnel
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message = 0x024c000b01746573746572
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   User-Name = "tester"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-IP-Address = 100.129.56.1
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Eltex-Domain = "default"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Identifier = "68:13:E2:35:D2:20"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-
SSID-WLC-15"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port-Type = Wireless-802.11
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port-Id = "10"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Service-Type = Framed-User
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port = 1
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Connect-Info = "CONNECT 24Mbps 802.11a"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-Pairwise-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-Group-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-AKM-Suite = 1027073
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Eltex-AP-Domain = "with-gre"
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Framed-MTU = 1400
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Event-Timestamp = "Nov 21 2024 15:38:12
GMT+7"
(49) Thu Nov 21 15:38:12 2024: Debug: Virtual server inner-tunnel received request
(49) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message = 0x024c000b01746573746572
(49) Thu Nov 21 15:38:12 2024: Debug:   FreeRADIUS-Proxied-To = 127.0.0.1
(49) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(49) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(49) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(49) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(49) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(49) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(49) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(49) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(49) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(49) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
```

```
(49) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(49) Thu Nov 21 15:38:12 2024: Debug:   Event-Timestamp = "Nov 21 2024 15:38:12 GMT+7"
(49) Thu Nov 21 15:38:12 2024: WARNING: Outer and inner identities are the same.  User privacy
is compromised.
(49) Thu Nov 21 15:38:12 2024: Debug: server inner-tunnel {
(49) Thu Nov 21 15:38:12 2024: Debug:   # Executing section authorize from file /etc/raddb/
sites-enabled/inner-tunnel
(49) Thu Nov 21 15:38:12 2024: Debug:     authorize {
(49) Thu Nov 21 15:38:12 2024: Debug:       policy filter_username {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name) {
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name)  -> TRUE
(49) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name)  {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ / /) {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ / /)  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@[^@]*@/ ) {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.\./ ) {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.\./ )  -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))  {
(49) Thu Nov 21 15:38:12 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.$/)  {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.$/)   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@\./)  {
(49) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@\./)   -> FALSE
(49) Thu Nov 21 15:38:12 2024: Debug:         } # if (&User-Name)  = notfound
(49) Thu Nov 21 15:38:12 2024: Debug:       } # policy filter_username = notfound
(49) Thu Nov 21 15:38:12 2024: Debug:       [chap] = noop
(49) Thu Nov 21 15:38:12 2024: Debug:       [mschap] = noop
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(49) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(49) Thu Nov 21 15:38:12 2024: Debug:       [suffix] = noop
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 76 length 11
(49) Thu Nov 21 15:38:12 2024: Debug: eap: EAP-Identity reply, returning 'ok' so we can short-
circuit the rest of authorize
(49) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(49) Thu Nov 21 15:38:12 2024: Debug:     } # authorize = ok
(49) Thu Nov 21 15:38:12 2024: Debug:   Found Auth-Type = eap
(49) Thu Nov 21 15:38:12 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(49) Thu Nov 21 15:38:12 2024: Debug:     authenticate {
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP Identity (1)
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_mschapv2 to process data
(49) Thu Nov 21 15:38:12 2024: Debug: eap_mschapv2: Issuing Challenge
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Request (code 1) ID 77 length 43
(49) Thu Nov 21 15:38:12 2024: Debug: eap: EAP session adding &reply:State = 0x39415d07390c47ca
(49) Thu Nov 21 15:38:12 2024: Debug:       [eap] = handled
(49) Thu Nov 21 15:38:12 2024: Debug:     } # authenticate = handled
(49) Thu Nov 21 15:38:12 2024: Debug: } # server inner-tunnel
(49) Thu Nov 21 15:38:12 2024: Debug: Virtual server sending reply
(49) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x014d002b1a014d002610e2e14d5f0898922ab87af7edb2f2ee9b667265657261646975732d332e302e3235
(49) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(49) Thu Nov 21 15:38:12 2024: Debug:   State = 0x39415d07390c47ca233427c848ccd003
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got tunneled reply code 11
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message =
0x014d002b1a014d002610e2e14d5f0898922ab87af7edb2f2ee9b667265657261646975732d332e302e3235
```

```
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Message-Authenticator =
0x00000000000000000000000000000000
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   State = 0x39415d07390c47ca233427c848ccd003
(49) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got tunneled Access-Challenge
(49) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Request (code 1) ID 77 length 74
(49) Thu Nov 21 15:38:12 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8ef3fdca6
(49) Thu Nov 21 15:38:12 2024: Debug:     [eap] = handled
(49) Thu Nov 21 15:38:12 2024: Debug:   } # authenticate = handled
(49) Thu Nov 21 15:38:12 2024: Debug: Using Post-Auth-Type Challenge
(49) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(49) Thu Nov 21 15:38:12 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(49) Thu Nov 21 15:38:12 2024: Debug: session-state: Saving cached attributes
(49) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1004
(49) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(49) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(49) Thu Nov 21 15:38:12 2024: Debug: Sent Access-Challenge Id 47 from 100.129.58.1:1812 to
100.129.56.1:37236 length 144
(49) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Tls-Enabled = 0
(49) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x014d004a1900170303003f49b195ac8c59a1d654f33dca05bf20250b88cddeebc0c09887f71b8ff66130ef7a8826f
1b8a520a6a2f7813901df73eba9f66ddbc6ff7e0ad4b8e944b839eb
(49) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(49) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ef3fdca62745240ad035bf82
(49) Thu Nov 21 15:38:12 2024: Debug: Finished request
(50) Thu Nov 21 15:38:12 2024: Debug: Received Access-Request Id 48 from 100.129.56.1:37236 to
100.129.58.1:1812 length 362
(50) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(50) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(50) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(50) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(50) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(50) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(50) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(50) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
(50) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(50) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x024d00601900170303005f8975c28e091e7313eb8678aa99ad357b0caf84c03afe5d765d6edcbc7f2a5241dfed39
306b35428a04356f0b8c6da22c8941bc2f57eb2bc410888f59bbe7450557ec
(50) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ef3fdca62745240ad035bf82
(50) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0xad80263807a5eb7abd7d2bba1f3c679d
(50) Thu Nov 21 15:38:12 2024: Debug: Restoring &session-state
(50) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Framed-MTU = 1004
(50) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(50) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(50) Thu Nov 21 15:38:12 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(50) Thu Nov 21 15:38:12 2024: Debug:   authorize {
```

```
(50) Thu Nov 21 15:38:12 2024: Debug:     policy filter_username {
(50) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name) {
(50) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  -> TRUE
(50) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /) {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(50) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)  {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)  {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:       } # if (&User-Name)  = notfound
(50) Thu Nov 21 15:38:12 2024: Debug:     } # policy filter_username = notfound
(50) Thu Nov 21 15:38:12 2024: Debug:     [preprocess] = ok
(50) Thu Nov 21 15:38:12 2024: Debug:     [chap] = noop
(50) Thu Nov 21 15:38:12 2024: Debug:     [mschap] = noop
(50) Thu Nov 21 15:38:12 2024: Debug:     [digest] = noop
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(50) Thu Nov 21 15:38:12 2024: Debug:     [suffix] = noop
(50) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(50) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(50) Thu Nov 21 15:38:12 2024: Debug:     [files_multi] = ok
(50) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(50) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:     else {
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 77 length 96
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Continuing tunnel setup
(50) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(50) Thu Nov 21 15:38:12 2024: Debug:     } # else = ok
(50) Thu Nov 21 15:38:12 2024: Debug:     if (ok) {
(50) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  -> TRUE
(50) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  {
(50) Thu Nov 21 15:38:12 2024: Debug:       return
(50) Thu Nov 21 15:38:12 2024: Debug:     } # if (ok)  = ok
(50) Thu Nov 21 15:38:12 2024: Debug:   } # authorize = ok
(50) Thu Nov 21 15:38:12 2024: Debug: Found Auth-Type = eap
(50) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(50) Thu Nov 21 15:38:12 2024: Debug:   authenticate {
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0x39415d07390c47ca
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0xe972c5d8ef3fdca6
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8ef3fdca6, released from the list
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_peap to process data
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: PEAP state phase2
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: EAP method MSCHAPv2 (26)
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got tunneled request
```

```
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message =
0x024d00411a024d003c31307984efc4700161597ce2539f3e0434000000000000000857df15fd3dd3b9cd17cadd24
bddbdbe25b1d02854c7371000746573746572
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Setting User-Name to tester
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Sending tunneled request to inner-tunnel
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message =
0x024d00411a024d003c31307984efc4700161597ce2539f3e0434000000000000000857df15fd3dd3b9cd17cadd24
bddbdbe25b1d02854c7371000746573746572
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   FreeRADIUS-Proxied-To = 127.0.0.1
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   User-Name = "tester"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   State = 0x39415d07390c47ca233427c848ccd003
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-IP-Address = 100.129.56.1
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Eltex-Domain = "default"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Identifier = "68:13:E2:35:D2:20"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-
SSID-WLC-15"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port-Type = Wireless-802.11
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port-Id = "10"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Service-Type = Framed-User
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   NAS-Port = 1
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Connect-Info = "CONNECT 24Mbps 802.11a"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-Pairwise-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-Group-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   WLAN-AKM-Suite = 1027073
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Eltex-AP-Domain = "with-gre"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Framed-MTU = 1400
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Event-Timestamp = "Nov 21 2024 15:38:12
GMT+7"
(50) Thu Nov 21 15:38:12 2024: Debug: Virtual server inner-tunnel received request
(50) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x024d00411a024d003c31307984efc4700161597ce2539f3e0434000000000000000857df15fd3dd3b9cd17cadd24
bddbdbe25b1d02854c7371000746573746572
(50) Thu Nov 21 15:38:12 2024: Debug:   FreeRADIUS-Proxied-To = 127.0.0.1
(50) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(50) Thu Nov 21 15:38:12 2024: Debug:   State = 0x39415d07390c47ca233427c848ccd003
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(50) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
(50) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(50) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(50) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(50) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(50) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(50) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(50) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(50) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
(50) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(50) Thu Nov 21 15:38:12 2024: Debug:   Event-Timestamp = "Nov 21 2024 15:38:12 GMT+7"
(50) Thu Nov 21 15:38:12 2024: WARNING: Outer and inner identities are the same.  User privacy
is compromised.
(50) Thu Nov 21 15:38:12 2024: Debug: server inner-tunnel {
(50) Thu Nov 21 15:38:12 2024: Debug:   session-state: No cached attributes
(50) Thu Nov 21 15:38:12 2024: Debug:   # Executing section authorize from file /etc/raddb/
sites-enabled/inner-tunnel
```

```
(50) Thu Nov 21 15:38:12 2024: Debug:     authorize {
(50) Thu Nov 21 15:38:12 2024: Debug:       policy filter_username {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name) {
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name)  -> TRUE
(50) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name)  {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ / /) {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ / /)  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@[^@]*@/ ) {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.\./ ) {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.\./ )  -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))  {
(50) Thu Nov 21 15:38:12 2024: Debug:           if ((&User-Name =~ /@/) && (&User-Name !~ /@(.
+)\.(.+)$/))   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.$/)  {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /\.$/)   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@\./)  {
(50) Thu Nov 21 15:38:12 2024: Debug:           if (&User-Name =~ /@\./)   -> FALSE
(50) Thu Nov 21 15:38:12 2024: Debug:         } # if (&User-Name)  = notfound
(50) Thu Nov 21 15:38:12 2024: Debug:       } # policy filter_username = notfound
(50) Thu Nov 21 15:38:12 2024: Debug:       [chap] = noop
(50) Thu Nov 21 15:38:12 2024: Debug:       [mschap] = noop
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(50) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(50) Thu Nov 21 15:38:12 2024: Debug:       [suffix] = noop
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 77 length 65
(50) Thu Nov 21 15:38:12 2024: Debug: eap: No EAP Start, assuming it's an on-going EAP
conversation
(50) Thu Nov 21 15:38:12 2024: Debug:       [eap] = updated
(50) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(50) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(50) Thu Nov 21 15:38:12 2024: Debug:       [files_multi] = ok
(50) Thu Nov 21 15:38:12 2024: Debug:       [expiration] = noop
(50) Thu Nov 21 15:38:12 2024: Debug:       [logintime] = noop
(50) Thu Nov 21 15:38:12 2024: WARNING: pap: Auth-Type already set.  Not setting to PAP
(50) Thu Nov 21 15:38:12 2024: Debug:       [pap] = noop
(50) Thu Nov 21 15:38:12 2024: Debug:     } # authorize = updated
(50) Thu Nov 21 15:38:12 2024: Debug:   Found Auth-Type = eap
(50) Thu Nov 21 15:38:12 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(50) Thu Nov 21 15:38:12 2024: Debug:     authenticate {
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0x39415d07390c47ca
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0x39415d07390c47ca
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0x39415d07390c47ca, released from the list
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP MSCHAPv2 (26)
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_mschapv2 to process data
(50) Thu Nov 21 15:38:12 2024: Debug: eap_mschapv2: # Executing group from file /etc/raddb/
sites-enabled/inner-tunnel
(50) Thu Nov 21 15:38:12 2024: Debug: eap_mschapv2:   authenticate {
(50) Thu Nov 21 15:38:12 2024: Debug: mschap: Found Cleartext-Password, hashing to create NT-
Password
(50) Thu Nov 21 15:38:12 2024: Debug: mschap: Creating challenge hash with username: tester
(50) Thu Nov 21 15:38:12 2024: Debug: mschap: Client is using MS-CHAPv2
(50) Thu Nov 21 15:38:12 2024: ERROR: mschap: MS-CHAP2-Response is incorrect
(50) Thu Nov 21 15:38:12 2024: Debug: eap_mschapv2:     [mschap] = reject
(50) Thu Nov 21 15:38:12 2024: Debug: eap_mschapv2:   } # authenticate = reject
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Failure (code 4) ID 77 length 4
```

```
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Freeing handler
(50) Thu Nov 21 15:38:12 2024: Debug:       [eap] = reject
(50) Thu Nov 21 15:38:12 2024: Debug:     } # authenticate = reject
(50) Thu Nov 21 15:38:12 2024: Debug:   Failed to authenticate the user
(50) Thu Nov 21 15:38:12 2024: Debug:   Using Post-Auth-Type Reject
(50) Thu Nov 21 15:38:12 2024: Debug:   # Executing group from file /etc/raddb/sites-enabled/
inner-tunnel
(50) Thu Nov 21 15:38:12 2024: Debug:     Post-Auth-Type REJECT {
(50) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject: EXPAND %{User-Name}
(50) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject:    --> tester
(50) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject: Matched entry DEFAULT at line
11
(50) Thu Nov 21 15:38:12 2024: Debug:       [attr_filter.access_reject] = updated
(50) Thu Nov 21 15:38:12 2024: Debug:       update outer.session-state {
(50) Thu Nov 21 15:38:12 2024: Debug:       } # update outer.session-state = noop
(50) Thu Nov 21 15:38:12 2024: Debug:     } # Post-Auth-Type REJECT = updated
(50) Thu Nov 21 15:38:12 2024: Debug: } # server inner-tunnel
(50) Thu Nov 21 15:38:12 2024: Debug: Virtual server sending reply
(50) Thu Nov 21 15:38:12 2024: Debug:   MS-CHAP-Error = "ME=691 R=1
C=b1c57ec11acb98cafda3f21162e8c4d8 V=3 M=Authentication rejected"
(50) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message = 0x044d0004
(50) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Got tunneled reply code 3
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   MS-CHAP-Error = "ME=691 R=1
C=b1c57ec11acb98cafda3f21162e8c4d8 V=3 M=Authentication rejected"
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   EAP-Message = 0x044d0004
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Message-Authenticator =
0x00000000000000000000000000000000
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Tunneled authentication was rejected
(50) Thu Nov 21 15:38:12 2024: Debug: eap_peap: FAILURE
(50) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Request (code 1) ID 78 length 46
(50) Thu Nov 21 15:38:12 2024: Debug: eap: EAP session adding &reply:State = 0xe972c5d8ee3cdca6
(50) Thu Nov 21 15:38:12 2024: Debug:     [eap] = handled
(50) Thu Nov 21 15:38:12 2024: Debug:   } # authenticate = handled
(50) Thu Nov 21 15:38:12 2024: Debug: Using Post-Auth-Type Challenge
(50) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(50) Thu Nov 21 15:38:12 2024: Debug:   Challenge { ... } # empty sub-section is ignored
(50) Thu Nov 21 15:38:12 2024: Debug: session-state: Saving cached attributes
(50) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1004
(50) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-
SHA384"
(50) Thu Nov 21 15:38:12 2024: Debug:   TLS-Session-Version = "TLS 1.2"
(50) Thu Nov 21 15:38:12 2024: Debug:   Module-Failure-Message := "mschap: MS-CHAP2-Response is
incorrect"
(50) Thu Nov 21 15:38:12 2024: Debug: Sent Access-Challenge Id 48 from 100.129.58.1:1812 to
100.129.56.1:37236 length 116
(50) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Tls-Enabled = 0
(50) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x014e002e1900170303002349b195ac8c59a1d798bd355a6f14ba67c4d53f463ad1801366b41b485e42ff0ad36c50
(50) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(50) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ee3cdca62745240ad035bf82
(50) Thu Nov 21 15:38:12 2024: Debug: Finished request
(51) Thu Nov 21 15:38:12 2024: Debug: Received Access-Request Id 49 from 100.129.56.1:37236 to
100.129.58.1:1812 length 312
(51) Thu Nov 21 15:38:12 2024: Debug:   User-Name = "tester"
(51) Thu Nov 21 15:38:12 2024: Debug:   NAS-IP-Address = 100.129.56.1
(51) Thu Nov 21 15:38:12 2024: Debug:   Eltex-Domain = "default"
(51) Thu Nov 21 15:38:12 2024: Debug:   NAS-Identifier = "68:13:E2:35:D2:20"
```

```
(51) Thu Nov 21 15:38:12 2024: Debug:   Called-Station-Id = "68-13-E2-35-D2-20:TEST-SSID-
WLC-15"
(51) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Type = Wireless-802.11
(51) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port-Id = "10"
(51) Thu Nov 21 15:38:12 2024: Debug:   Service-Type = Framed-User
(51) Thu Nov 21 15:38:12 2024: Debug:   NAS-Port = 1
(51) Thu Nov 21 15:38:12 2024: Debug:   Calling-Station-Id = "DA-A7-8A-41-68-F5"
(51) Thu Nov 21 15:38:12 2024: Debug:   Connect-Info = "CONNECT 24Mbps 802.11a"
(51) Thu Nov 21 15:38:12 2024: Debug:   Acct-Session-Id = "FA94FFC0-B7DB1A4A"
(51) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Pairwise-Cipher = 1027076
(51) Thu Nov 21 15:38:12 2024: Debug:   WLAN-Group-Cipher = 1027076
(51) Thu Nov 21 15:38:12 2024: Debug:   WLAN-AKM-Suite = 1027073
(51) Thu Nov 21 15:38:12 2024: Debug:   Eltex-AP-Domain = "with-gre"
(51) Thu Nov 21 15:38:12 2024: Debug:   Framed-MTU = 1400
(51) Thu Nov 21 15:38:12 2024: Debug:   EAP-Message =
0x024e002e19001703030023f8975c28e091e732883ca2d06dc3ca29c0cd107d25060443fde1b3547ef8345092780d
(51) Thu Nov 21 15:38:12 2024: Debug:   State = 0xe972c5d8ee3cdca62745240ad035bf82
(51) Thu Nov 21 15:38:12 2024: Debug:   Message-Authenticator =
0x6772704783a0e9f5592c63afe8b7a042
(51) Thu Nov 21 15:38:12 2024: Debug: Restoring &session-state
(51) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Framed-MTU = 1004
(51) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-
AES256-GCM-SHA384"
(51) Thu Nov 21 15:38:12 2024: Debug:   &session-state:TLS-Session-Version = "TLS 1.2"
(51) Thu Nov 21 15:38:12 2024: Debug:   &session-state:Module-Failure-Message := "mschap: MS-
CHAP2-Response is incorrect"
(51) Thu Nov 21 15:38:12 2024: Debug: # Executing section authorize from file /etc/raddb/sites-
enabled/_default
(51) Thu Nov 21 15:38:12 2024: Debug:   authorize {
(51) Thu Nov 21 15:38:12 2024: Debug:     policy filter_username {
(51) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name) {
(51) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  -> TRUE
(51) Thu Nov 21 15:38:12 2024: Debug:       if (&User-Name)  {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /) {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ / /)  -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ ) {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@[^@]*@/ )  -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ ) {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.\./ )  -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))  {
(51) Thu Nov 21 15:38:12 2024: Debug:         if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)
\.(.+)$/))   -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)  {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /\.$/)   -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)  {
(51) Thu Nov 21 15:38:12 2024: Debug:         if (&User-Name =~ /@\./)   -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:       } # if (&User-Name)  = notfound
(51) Thu Nov 21 15:38:12 2024: Debug:     } # policy filter_username = notfound
(51) Thu Nov 21 15:38:12 2024: Debug:     [preprocess] = ok
(51) Thu Nov 21 15:38:12 2024: Debug:     [chap] = noop
(51) Thu Nov 21 15:38:12 2024: Debug:     [mschap] = noop
(51) Thu Nov 21 15:38:12 2024: Debug:     [digest] = noop
(51) Thu Nov 21 15:38:12 2024: Debug: suffix: Checking for suffix after "@"
(51) Thu Nov 21 15:38:12 2024: Debug: suffix: No '@' in User-Name = "tester", looking up realm
NULL
(51) Thu Nov 21 15:38:12 2024: Debug: suffix: No such realm "NULL"
(51) Thu Nov 21 15:38:12 2024: Debug:     [suffix] = noop
(51) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry DEFAULT at line 1
(51) Thu Nov 21 15:38:12 2024: Debug: files_multi: users: Matched entry tester at line 5
(51) Thu Nov 21 15:38:12 2024: Debug:     [files_multi] = ok
```

```
(51) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1) {
(51) Thu Nov 21 15:38:12 2024: Debug:     if (&reply:Eltex-Tls-Enabled == 1)  -> FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:     else {
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent EAP Response (code 2) ID 78 length 46
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Continuing tunnel setup
(51) Thu Nov 21 15:38:12 2024: Debug:       [eap] = ok
(51) Thu Nov 21 15:38:12 2024: Debug:     } # else = ok
(51) Thu Nov 21 15:38:12 2024: Debug:     if (ok) {
(51) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  -> TRUE
(51) Thu Nov 21 15:38:12 2024: Debug:     if (ok)  {
(51) Thu Nov 21 15:38:12 2024: Debug:       return
(51) Thu Nov 21 15:38:12 2024: Debug:     } # if (ok)  = ok
(51) Thu Nov 21 15:38:12 2024: Debug:   } # authorize = ok
(51) Thu Nov 21 15:38:12 2024: Debug: Found Auth-Type = eap
(51) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(51) Thu Nov 21 15:38:12 2024: Debug:   authenticate {
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Expiring EAP session with state 0xe972c5d8ee3cdca6
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Finished EAP session with state 0xe972c5d8ee3cdca6
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Previous EAP request found for state
0xe972c5d8ee3cdca6, released from the list
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Peer sent packet with method EAP PEAP (25)
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Calling submodule eap_peap to process data
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap: (TLS) EAP Done initial handshake
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Session established.  Decoding tunneled
attributes
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap: PEAP state send tlv failure
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap: Received EAP-TLV response
(51) Thu Nov 21 15:38:12 2024: ERROR: eap_peap:   The users session was previously rejected:
returning reject (again.)
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   This means you need to read the PREVIOUS
messages in the debug output
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   to find out the reason why the user was
rejected
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   Look for "reject" or "fail".  Those earlier
messages will tell you
(51) Thu Nov 21 15:38:12 2024: Debug: eap_peap:   what went wrong, and how to fix the problem
(51) Thu Nov 21 15:38:12 2024: ERROR: eap: Failed continuing EAP PEAP (25) session.  EAP sub-
module failed
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Sending EAP Failure (code 4) ID 78 length 4
(51) Thu Nov 21 15:38:12 2024: Debug: eap: Failed in EAP select
(51) Thu Nov 21 15:38:12 2024: Debug:     [eap] = invalid
(51) Thu Nov 21 15:38:12 2024: Debug:   } # authenticate = invalid
(51) Thu Nov 21 15:38:12 2024: Debug: Failed to authenticate the user
<<<------------------------------------------------------------------------
Пользователь не прошел аутентификацию
(51) Thu Nov 21 15:38:12 2024: Debug: Using Post-Auth-Type Reject
(51) Thu Nov 21 15:38:12 2024: Debug: # Executing group from file /etc/raddb/sites-enabled/
_default
(51) Thu Nov 21 15:38:12 2024: Debug:   Post-Auth-Type REJECT {
(51) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject: EXPAND %{User-Name}
(51) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject:    --> tester
(51) Thu Nov 21 15:38:12 2024: Debug: attr_filter.access_reject: Matched entry DEFAULT at line
11
(51) Thu Nov 21 15:38:12 2024: Debug:     [attr_filter.access_reject] = updated
(51) Thu Nov 21 15:38:12 2024: Debug:     [eap] = noop
(51) Thu Nov 21 15:38:12 2024: Debug:     policy remove_reply_message_if_eap {
(51) Thu Nov 21 15:38:12 2024: Debug:       if (&reply:EAP-Message && &reply:Reply-Message) {
(51) Thu Nov 21 15:38:12 2024: Debug:       if (&reply:EAP-Message && &reply:Reply-Message)  ->
FALSE
(51) Thu Nov 21 15:38:12 2024: Debug:       else {
```

```
(51) Thu Nov 21 15:38:12 2024: Debug:         [noop] = noop
(51) Thu Nov 21 15:38:12 2024: Debug:       } # else = noop
(51) Thu Nov 21 15:38:12 2024: Debug:     } # policy remove_reply_message_if_eap = noop
(51) Thu Nov 21 15:38:12 2024: Debug:   } # Post-Auth-Type REJECT = updated
(51) Thu Nov 21 15:38:12 2024: Debug: Delaying response for 1.000000 seconds
(51) Thu Nov 21 15:38:13 2024: Debug: Sending delayed response
(51) Thu Nov 21 15:38:13 2024: Debug: Sent Access-Reject Id 49 from 100.129.58.1:1812 to
100.129.56.1:37236 length 44
<<<------------------------------------------------------------------------------ Acess-
Reject
(51) Thu Nov 21 15:38:13 2024: Debug:   EAP-Message = 0x044e0004
(51) Thu Nov 21 15:38:13 2024: Debug:   Message-Authenticator =
0x00000000000000000000000000000000
(43) Thu Nov 21 15:38:14 2024: Debug: Cleaning up request packet ID 41 with timestamp +9048
(44) Thu Nov 21 15:38:14 2024: Debug: Cleaning up request packet ID 42 with timestamp +9048
(45) Thu Nov 21 15:38:14 2024: Debug: Cleaning up request packet ID 43 with timestamp +9048
(46) Thu Nov 21 15:38:14 2024: Debug: Cleaning up request packet ID 44 with timestamp +9048
(47) Thu Nov 21 15:38:17 2024: Debug: Cleaning up request packet ID 45 with timestamp +9051
(48) Thu Nov 21 15:38:17 2024: Debug: Cleaning up request packet ID 46 with timestamp +9051
(49) Thu Nov 21 15:38:17 2024: Debug: Cleaning up request packet ID 47 with timestamp +9051
(50) Thu Nov 21 15:38:17 2024: Debug: Cleaning up request packet ID 48 with timestamp +9051
(51) Thu Nov 21 15:38:17 2024: Debug: Cleaning up request packet ID 49 with timestamp +9051
```

Сохранение вывода в файл на flash:data/ и выгрузка по tftp

```
wlc-15(debug)# show radius-debug username tester timeout 600  file flash:data/radius_debug.txt
Total lines written: 2678
File saved
wlc-15(debug)# end
wlc-15# copy flash:data/radius_debug.txt tftp://100.110.0.214:/radius_debug.txt
|****************************************| 100% (210kB) Success!
```

Сохранение вывода в файл на внешний USB

```
wlc-15(debug)# show radius-debug username tester timeout 600 file usb://103F-2D94:/
test_radius_debug_usb.txt
Total lines written: 1329
File saved
wlc-15(debug)# end
wlc-15# show storage-devices usb
Name                            Filesystem   Total, MB    Used, MB     Free, MB
------------------------------  ----------   ----------   ----------   ----------
103F-2D94                       vfat         7771.80      834.25       6937.55

wlc-15# dir usb://103F-2D94:/
Name                                                      Type         Size            Last
modified
--------------------------------------------------------  ----------   --------   --
-------------------------
test_radius_debug_usb.txt                                 File         105.24     KB   Thu
Nov 21 16:44:22 2024
```

23.7 Настройка доступа беспроводных клиентов по MAC-адресам

- Настройка доступа беспроводных клиентов по локальным спискам на ТД
- Настройка MAC аутентификации на локальном RADIUS-сервере

Поддержано начиная с версий:
Устройства: WLC-15/30/3200, ESR-15/15R/30/3200
Версия ПО WLC/ESR: 1.26.0
Программный контроллер vWLC:
Версия ПО vWLC: 1.27.0
Точки доступа: WEP-1L, WEP-200L, WEP-2L, WEP-30L, WEP-30L-Z, WEP-3L, WOP-20L, WOP-2L, WOP-30L, WOP-30LI, WOP-30LS
Версия ПО ТД: 2.5.0
Точка доступа: WEP-3ax
Версия ПО ТД: 1.8.0
Точки доступа: WEP-2ac, WEP-2ac Smart, WOP-2ac, WOP-2ac rev.B, WOP-2ac rev.C
Версия ПО ТД: 1.25.0

Таблица поддержки функционала на различных моделях ТД:

Модель ТД	По локальным спискам	Через RADIUS
WEP-1L	Да	Да
WEP-2L	Да	Да
WEP-3L	Да	Нет
WEP-200L	Да	Да
WEP-30L	Да	Да
WEP-30L-Z	Да	Да
WOP-2L	Да	Да
WOP-20L	Да	Да
WOP-30L	Да	Да
WOP-30LI	Да	Да
WOP-30LS	Да	Да
WEP-3ax	Нет	Да
WEP-2ac	Да	Да
WEP-2ac Smart	Да	Да
WOP-2ac	Да	Да
WOP-2ac:rev.B	Да	Да
WOP-2ac:rev.C	Да	Да

Настройка осуществляется в SSID-профиле. Существует 2 способа ограничения доступа:

- По локальным спискам на ТД;
- По записям на RADIUS-сервере.

```
wlc(config-wlc-ssid-profile)# mac-auth mode
  local   Set MAC authentication local mode
  radius  Set MAC authentication radius mode
```

23.7.1 Настройка доступа беспроводных клиентов по локальным спискам на ТД

Для авторизации по локальным спискам на ТД 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. 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 устройствам;
mac-auth mode local policy deny any – запретить доступ всем устройствам;
mac-auth mode local policy deny test_mac_auth – запретить доступ для устройств, у которых MAC-адрес указан в object group test_mac_auth.

23.7.2 Настройка MAC аутентификации на локальном RADIUS-сервере

Для MAC-аутентификации на локальном RADIUS-сервере требуется:

1. Добавить пользователя на локальный RADIUS-сервер в домен, который будет использоваться для авторизации. В данном примере создается запись для пользователя **6C-E8-5C-4E-97-1E** с паролем **NOPASSWORD** в домене **default**.

```
wlc# configure
wlc(config)# radius-server local
wlc(config-radius)# domain default
wlc(config-radius-domain)# user 6C-E8-5C-4E-97-1E
wlc(config-radius-user)# password ascii-text NOPASSWORD
wlc(config-radius-user)# exit
wlc(config-radius-domain)# exit
wlc(config-radius)# exit
```

В поле "**user**" необходимо задать **MAC-адрес** клиента в формате: **XX-XX-XX-XX-XX-XX**. **Важно использовать верхний регистр формата MAC-адреса с разделителем "-".**
В поле "**password**" необходимо задать пароль: **NOPASSWORD** (точка доступа по умолчанию подставляет в RADIUS аттрибут User-Password значение: 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.

```
wlc(config)# wlc
wlc(config-wlc)# ssid-profile default-ssid
wlc(config-wlc-ssid-profile)# mac-auth mode radius policy permit
```

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.

3. Применить изменения.

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

Пример пакета **Acess-Request** от ТД в процессе MAC-аутентификации через локальный **RADIUS-сервер**:

```
(56) Fri Dec  6 07:13:11 2024: Debug: Received Access-Request Id 0 from
100.129.48.1:56038 to 100.129.58.1:1812 length 210
(56) Fri Dec  6 07:13:11 2024: Debug:   User-Name = "6C-E8-5C-4E-97-1E"
 <<------------------- формат MAC-адреса клиента в верхнем регистре
(56) Fri Dec  6 07:13:11 2024: Debug:   Eltex-Domain = "default"
(56) Fri Dec  6 07:13:11 2024: Debug:   User-Password = "NOPASSWORD"
 <<------------------- в качестве значения аттрибута User-Password ТД по умолчанию
подставляет значение NOPASSWORD
(56) Fri Dec  6 07:13:11 2024: Debug:   NAS-IP-Address = 100.129.48.1
(56) Fri Dec  6 07:13:11 2024: Debug:   NAS-Identifier = "E0-D9-E3-73-07-62"
(56) Fri Dec  6 07:13:11 2024: Debug:   NAS-Port-Id = "2"
(56) Fri Dec  6 07:13:11 2024: Debug:   Called-Station-Id = "E0-D9-
E3-73-07-60:WLC_ENTERPRICE"
(56) Fri Dec  6 07:13:11 2024: Debug:   Calling-Station-Id = "6C-E8-5C-4E-97-1E"
(56) Fri Dec  6 07:13:11 2024: Debug:   NAS-Port-Type = Wireless-802.11
(56) Fri Dec  6 07:13:11 2024: Debug:   Connect-Info = "CONNECT 11Mbps 802.11b"
(56) Fri Dec  6 07:13:11 2024: Debug:   Message-Authenticator =
0x8ede933ed54795333b6a35ae73020088
```

Начиная с версии ПО **2.8.0** на точках доступа WEP-30L, WEP-30L-Z, WOP-30L, WOP-30LI, WOP-30LS с помощью настройки **session password mac** возможно подставлять значение MAC-адреса клиента в атрибут **User-Password** и настраивать его формат. Настройка выполняется в профиле RADIUS, который используется в соответствующем SSID. В этом случае, в учетной записи пользователя на RADIUS-сервере, в качестве пароля, также необходимо задать MAC-адрес клиента в соответствующем формате.

Пример пакета **Acess-Request** от ТД в процессе MAC-аутентификации через локальный **RADIUS-сервер** с настроенным параметром **session password mac uppercase-separator-dash**:

```
(0) Wed May 14 12:35:52 2025: Debug: Received Access-Request Id 0 from 192.168.1.2:60054
to 192.168.1.1:1812 length 223
(0) Wed May 14 12:35:52 2025: Debug:   User-Name = "B6-9A-E6-CC-62-3A"
(0) Wed May 14 12:35:52 2025: Debug:   User-Password = "B6-9A-E6-CC-62-3A"
 <<------------------- Значение MAC-адреса клиента в формате XX-XX-XX-XX-XX-XX
(0) Wed May 14 12:35:52 2025: Debug:   NAS-IP-Address = 192.168.1.2
(0) Wed May 14 12:35:52 2025: Debug:   Eltex-Domain = "default"
(0) Wed May 14 12:35:52 2025: Debug:   NAS-Identifier = "68-13-E2-C2-F7-40"
(0) Wed May 14 12:35:52 2025: Debug:   Called-Station-Id = "68-13-E2-C2-
F7-40:WLC_ENTERPRICE"
(0) Wed May 14 12:35:52 2025: Debug:   NAS-Port-Type = Wireless-802.11
(0) Wed May 14 12:35:52 2025: Debug:   NAS-Port-Id = "8"
(0) Wed May 14 12:35:52 2025: Debug:   Calling-Station-Id = "B6-9A-E6-CC-62-3A"
(0) Wed May 14 12:35:52 2025: Debug:   Connect-Info = "CONNECT 11Mbps 802.11b"
(0) Wed May 14 12:35:52 2025: Debug:   Service-Type = Call-Check
(0) Wed May 14 12:35:52 2025: Debug:   Message-Authenticator =
0xcfd079fe6d97930bbc9ba8cf341e60e6
```

Если список пользователей находится на внешнем сервере, необходимо настроить проксирование (см. статью Настройка проксирования на внешний RADIUS).

23.8 Настройка ограничения скорости трафика

- Описание
- Задача
- Решение

23.8.1 Описание

Ограничение скорости реализуется на ТД и применимо для всех схем включения L2/L3.

Поддержано начиная с версий:
Устройства: WLC-15/30/3200, ESR-15/15R/30/3200
Версия ПО WLC\ESR: 1.30.0
Программный контроллер: vWLC
Версия ПО vWLC: 1.30.0
Точки доступа: WEP-1L, WEP-200L, WEP-2L, WEP-30L, WEP-30L-Z, WEP-3L, WOP-20L, WOP-2L, WOP-30L, WOP-30LI, WOP-30LS
Версия ПО ТД: 2.6.0
Точка доступа: WEP-3ax
Версия ПО ТД: 1.14.0

Ниже представлена развернутая таблица поддержки функционала ограничения трафика на различных моделях ТД.

Модель ТД	VAP	Клиент	Broadcast	Multicast
WEP-1L	Да	Да	Да	Да

Модель ТД	VAP	Клиент	Broadcast	Multicast
WEP-2L	Да	Да	Да	Да
WEP-3L	Да	Да	Да	Да
WEP-200L	Да	Да	Да	Да
WEP-30L	Да	Да	Да	Да
WEP-30L-Z	Да	Да	Да	Да
WOP-2L	Да	Да	Да	Да
WOP-20L	Да	Да	Да	Да
WOP-30L	Да	Да	Да	Да
WOP-30LI	Да	Да	Да	Да
WOP-30LS	Да	Да	Да	Да
WEP-3ax	Да	Да	Нет	Нет
WEP-2ac	Нет	Нет	Нет	Нет
WEP-2ac Smart	Нет	Нет	Нет	Нет
WOP-2ac	Нет	Нет	Нет	Нет
WOP-2ac:rev.B	Нет	Нет	Нет	Нет
WOP-2ac:rev.C	Нет	Нет	Нет	Нет

Профиль ограничения скорости содержит настройки ограничения скорости для разных видов трафика.

- *VAP* – ограничение скорости на SSID, т.е. суммарное ограничение скорости в заданном диапазоне;
- *Station* – ограничение скорости на клиента;
- *Broadcast* – ограничение broadcast-трафика на SSID в заданном диапазоне;
- *Multicast* – ограничение multicast-трафика на SSID в заданном диапазоне.

Направление трафика:

- *Output* – трафик от ТД до клиента;
- *Input* – трафик от клиента к ТД.

Выставить значение ограничения скорости можно в двух единицах измерения:

- *kbps* – в килобитах в секунду (Кбит/с);
- *pps* – в пакетах в секунду.

23.8.2 Задача

Настроить ограничение скорости на SSID:

- Задать ограничение для broadcast в 150 Кбит/с для всех направлений;
- Задать ограничение в 100 пакетов в секунду на VAP для исходящего от клиента трафика;
- Задать ограничение в 200 пакетов в секунду на VAP для входящего к клиенту трафика;
- Ограничение должно работать только в 5 ГГц.

Настройка SSID не рассмотрена в примере: принято, что он уже создан и предоставляет сервис.

23.8.3 Решение

Для решения поставленной задачи нужно создать профиль ограничения скорости policy-profile:

```
wlc(config-wlc)# policy-profile ap test-policy-profile
```

Настроить ограничение в 150 Кбит/с для широковещательного трафика во всех направлениях, 100 пакетов в секунду — для исходящего трафика со стороны всех клиентов VAP и 200 пакетов в секунду — для входящего трафика.

Выбрать вид трафика, который нужно ограничить, его направление и единицы измерения ограничения:

```
wlc(config-wlc-policy-profile-ap)# rate-limit broadcast output kbps 150
wlc(config-wlc-policy-profile-ap)# rate-limit broadcast input kbps 150
wlc(config-wlc-policy-profile-ap)# rate-limit vap output pps 100
wlc(config-wlc-policy-profile-ap)# rate-limit vap input pps 200
```

Указать описание профиля:

```
wlc(config-wlc-policy-profile-ap)# description test-policy-profile
wlc(config-wlc-policy-profile-ap)# exit
```

Привязать к SSID-профилю созданный профиль ограничения скорости. Выбрать, для какого диапазона будет действовать профиль, возможны варианты: 2.4 ГГц (2g), 5 ГГц (5g) или для двух сразу (all). Выбрать 5g:

```
wlc(config-wlc)# ssid-profile default-ssid
wlc(config-wlc-ssid-profile)# policy-profile ap band 5g test-policy-profile
```

Ограничения скорости можно выключить командой **no policy-profile ap** в ssid-profile:

```
wlc(config-wlc-ssid-profile)# no policy-profile ap
wlc(config-wlc-ssid-profile)# exit
```

Применить изменения:

```
wlc(config-wlc-ssid-profile)# end
wlc# commit
wlc# confirm
```

23.9 Изменение пути хранения журналов WLC

- Описание
- Требования к внешнему диску
- Первичное подключение диска
- Перенос журналов с Flash на Disk
- Переключение с Disk на Flash
- Корректное извлечение диска
- Форматирование диска средствами устройства

23.9.1 Описание

Начиная с версии ПО 1.30.2 для устройств WLC-15, WLC-30, WLC-3200, появилась возможность переноса журналов show wlc journal clients/ap/wids на внешний диск.

Данный функционал позволяет:

- Увеличить объем информации, которая может хранится в журналах
- Существенно увеличить скорость чтения/записи, в случае использования SSD

> Перенос (миграция) журналов происходит только с внутренней flash-памяти устройства на внешний диск.
> Перенос журналов с внешнего диска на flash не поддерживается, в связи с тем, что в определенных ситуациях размер журналов может превышать размер flash-памяти на устройстве.

23.9.2 Требования к внешнему диску

Требования:

- Интерфейс подключения: SATA-3
- Формат диска: 2.5
- Минимальный рекомендуемый размер диска: 128 ГБ
- Файловая система: ext4

> Рекомендуется использовать SSD-диск вместо HDD в связи с большей производительностью.

23.9.3 Первичное подключение диска

> - При первичном подключение нового диска он не размечен, поэтому, он **не будет** отображаться в выводах команды show storage-device hdd.
> - Устройства WLC-15, WLC-30, WLC-3200 имеют только 1 слот для диска, поэтому при форматировании диска средствами устройства, используя команду clear storage device, <SLOT_NUMBER> всегда равен 1.

1. Подключить диск к устройству в разъем для установки диска. Проверить, что загорелся зеленый индикатор. Подробная информация представлена в разделе "Описание изделий".
2. Форматировать диск средствами устройства, используя команду **clear storage device hdd-dev://1 <hdd_name>.**

```
wlc-30# clear storage-device hdd-dev://1 MYDISK
Formatting will erase all data on this device
Do you really want to continue? (y/N): y
mke2fs 1.43.1 (08-Jun-2016)
Device clear success.
```

3. Выполнить команду show storage-device hdd и убедиться, что диск успешно отформатирован и корректно определяется устройством.

```
wlc-30# show storage-devices hdd
Name                            Filesystem   Total, MB    Used, MB     Free, MB
------------------------------  ----------   ----------   ----------   ----------
```

```
MYDISK                          ext4          234601.75     60.02         234541.72
```

23.9.4 Перенос журналов с Flash на Disk

1. Зайти в конфигурационный режим устройства, выполнить настройки **wlc-jounral storage hdd://<hdd_name>:/<dir>** и выполнить команды **commit** и **confirm.**
   - **<hdd_name>** – имя внешнего диска.
   - **<dir>** – директория, в которую будут перенесены журналы.

Пример конфигурации переноса журналов на SSD "MYDISK" в директорию SSD-JOURNAL

```
wlc#
wlc# configure
wlc(config)# wlc-journal storage hdd://MYDISK:/SSD-JOURNAL
wlc(config)# do commit
2025-02-19T15:05:50+07:00 %SYS-W-EVENT: WARNING!!! the database will be moving to SATA storage
device after reboot hardware
Configuration has been successfully applied and saved to flash. Commit timer started, changes
will be reverted in 600 seconds.
2025-02-19T15:05:53+07:00 %CLI-I-CRIT: user techsupport from console  input: do commit
wlc(config)# do confirm
Configuration has been confirmed. Commit timer canceled.
```

⚠
- Директория для хранения журналов, создается автоматически после выполнения команды **commit,** при условии, что она отсутствует на диске. В случае, если директория с данным для журналов уже существует, то после перезагрузки будет использоваться она.
- Вложенные директории не поддерживаются. Только один уровень вложенности.

2. Проверить, что директория успешно создана командой dir.

Проверка создания директории на внешнем диске

```
wlc# dir hdd://MYDISK:/
Name                                                        Type         Size            Last
modified
----------------------------------------------------------  -----------  --------  --
-------------------------
SSD-JOURNAL                                                 Directory    0.00       B    Wed
Feb 19 15:05:50 2025
```

3. Перезагрузить устройство командой **reload system.**

Пезагрузка устойства

```
wlc-30# reload system
```

4. Проверить выводы команд **show wlc journal ap/clients/wids** и убедиться, что данные журналов успешно перенесены с flash-памяти устройства.

```
wlc# show wlc journal clients
wlc# show wlc journal ap
```

```
wlc# show wlc journal wids
```

⚠ После переноса на disk данные журналов, которые были на flash удаляются.

23.9.5 Переключение с Disk на Flash

1. Зайти в конфигурационный режим устройства, выполнить настройки **wlc-jounral storage flash:wlc_database**, выполнить команды **commit** и **confirm** и перезагрузить устройство командой **reload system**.

```
wlc-30-failover# configure
wlc-30-failover(config)# wlc-journal storage flash:wlc_database
wlc-30-failover(config)# do commit
2025-02-20T16:58:13+07:00 %SYS-W-EVENT: WARNING!!! the database will be placed on the
FLASH after reboot hardware
Configuration has been successfully applied and saved to flash. Commit timer started,
changes will be reverted in 600 seconds.
2025-02-20T16:58:17+07:00 %CLI-I-CRIT: user techsupport from console  input: do commit
wlc-30-failover(config)#
```

⚠ После перезагрузки устройства на flash будет создана директория для хранения журналов, в случае если она отсутствует. Данные в журналах будут отсутствовать.
В случае, если директория с данными для журналов уже присутствует на flash-памяти устройства, то после перезагрузки устройства она будет использоваться.

2. Проверить выводы команд **show wlc journal ap/clients/wids.**

23.9.6 Корректное извлечение диска

⛔ Не рекомендуется отключать диск на "Горячую" без использования команды unmount storage-device**,** если в текущем состояние устройство использует диск для хранения данных журналов.

Для того чтобы корректно извлечь внешний диск из устройства, необходимо использовать команду unmount storage-device**.**

Пример команды unmount

```
wlc# unmount storage-device hdd-dev://1
```

В случае, если устройство использует внешний диск для хранения журналов (выполнены шаги из подраздела "Перенос журналов с Flash на Disk"), команда unmount storage-device не выполнится.

Для выполнения команды unmount storage-device в данном случае, необходимо выполнить следующие шаги:

- Переключить хранение журналов с disk на flash, выполнить команды **commit** и **confirm**, перезагрузить устройство командой **reload system.**

```
wlc# configure
wlc(config)# wlc-journal storage flash:wlc_database
wlc(config)# do commit
2025-02-20T10:13:33+07:00 %SYS-W-EVENT: WARNING!!! the database will be placed on the
FLASH after reboot hardware
```

```
wlc(config)#
wlc(config)# do confirm
Configuration has been confirmed. Commit timer canceled
wlc# reload system
Do you really want to reload system now? (y/N): y
```

- Выполнить команду **unmount storage-device.**

```
wlc# unmount storage-device hdd://MYDISK1
2025-02-20T11:59:36+07:00 %FILE_MGR-I-INFO: operation started: 'unmout storage-device
hdd://MYDISK1' (index: 1, origin: CLI)
Device unmount
Do you really want to continue? (y/N): y
2025-02-20T11:59:51+07:00 %HDD-I-CHANGE: 'MYDISK1' has been removed!
2025-02-20T11:59:52+07:00 %FILE_MGR-I-INFO: operation is finished: 'unmout storage-device
hdd://MYDISK1' (index: 1, origin: CLI)
Device unmount success.
```

- Извлечь диск из устройства.

23.9.7 Форматирование диска средствами устройства

Для того чтобы форматировать диск, необходимо выполнить команду clear storage-device.

После форматирование диск будет с одним разделом, имя которого задал пользователь и файловой системой ext4.

Пример использования команды clear storage-device

```
wlc# clear storage-device hdd-dev://1 MYDISK2
```

В случае, если устройство, использует внешний диск для хранения журналов (выполнены шаги из подраздела "Перенос журналов с Flash на Disk"), форматировать диск командой clear storage-device не получится.

Для выполнения команды clear storage-device в данном случае, необходимо выполнить шаги:

- Переключить хранение журналов с disk на flash, выполнить команды **commit** и **confirm**, перезагрузить устройство командой **reload system.**

```
wlc# configure
wlc(config)# wlc-journal storage flash:wlc_database
wlc(config)# do commit
2025-02-20T10:13:33+07:00 %SYS-W-EVENT: WARNING!!! the database will be placed on the
FLASH after reboot hardware
wlc(config)#
wlc(config)# do confirm
Configuration has been confirmed. Commit timer canceled
wlc# reload system
Do you really want to reload system now? (y/N): y
```

- Выполнить команду **clear storage-device.**

```
wlc# clear storage-device hdd-dev://1 MYDISK2
Formatting will erase all data on this device
Do you really want to continue? (y/N): y
mke2fs 1.43.1 (08-Jun-2016)
```

```
Device clear success.
```

- Выполнить команду **show storage-device hdd** и убедиться, что диск успешно отформатирован и корректно определяется устройством.

```
 wlc# show storage-devices hdd
Name                            Filesystem   Total, MB    Used, MB     Free, MB
------------------------------  ----------   ----------   ----------   ----------
MYDISK                          ext4         234601.75    60.02        234541.72
```

23.10 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

  , то актуальным будет ПО 1.6.0_build_50.tar.gz.

23.10.1 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
```

23.10.2 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 только после переподключения к контроллеру, если менеджер обновления отключен. Принудительно переподключить точку доступа к контроллеру можно с помощью команды:

```
wlc# clear wlc ap HH:HH:HH:HH:HH:HH
# где
# HH:HH:HH:HH:HH:HH – MAC адрес точки доступа
```

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 четырех 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);
- allow-update-with-clients – включение возможности обновления точек доступа, к которым на момент обновления подключены клиенты. Значение по умолчанию: no allow-update-with-clients (запрещено обновлять точки доступа с клиентами).

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.
# Запрещено обновлять точки с клиентами (настройка не требуется, включено по умолчанию).
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 1.30.4 указаны в таблице ниже:

Модель точки доступа	Минимальная версия ПО
WEP-1L	2.5.6
WEP-2L	2.5.6
WEP-3L	2.5.3
WEP-200L	2.7.0
WEP-30L	2.6.0
WEP-30L-Z	2.6.0
WEP-3ax	1.14.0
WOP-2L	2.5.6
WOP-20L	2.7.0
WOP-30L	2.6.0
WOP-30LS	2.6.0
WOP-30LI	2.6.0
WEP-2ac	1.25.2
WEP-2ac Smart	1.25.2
WOP-2ac	1.25.2
WOP-2ac rev.B	1.25.2
WOP-2ac rev.C	1.25.2

Начиная с версии ПО 1.30.0 добавлена команда **show wlc ap firmware**, которая содержит вывод о минимальной версии ПО точки доступа для работы с контроллером. Описание команды **show wlc ap firmware** можно посмотреть по следующей ссылке.

Версии ПО точек доступа, для которых поддержано взаимодействие с контроллером WLC предыдущих версий

Версии ПО точек доступа, для которых поддержано взаимодействие с контроллером WLC версий 1.30.0 указаны в таблице ниже:

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-1L	2.5.6	2.5.x
WEP-2L	2.5.6	2.5.x
WEP-3L	2.5.3	2.5.x
WEP-200L	2.6.0	2.6.x
WEP-30L	2.6.0	2.6.x
WEP-30L-Z	2.6.0	2.6.x
WEP-3ax	1.14.0	1.14.x
WOP-2L	2.5.6	2.5.x
WOP-20L	2.6.0	2.6.x
WOP-30L	2.6.0	2.6.x
WOP-30LS	2.6.0	2.6.x
WOP-30LI	2.6.0	2.6.x
WEP-2ac	1.25.2	1.25.x
WEP-2ac Smart	1.25.2	1.25.x
WOP-2ac	1.25.2	1.25.x
WOP-2ac rev.B	1.25.2	1.25.x
WOP-2ac rev.C	1.25.2	1.25.x

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

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
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
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

Модель точки доступа	Минимальная версия ПО	Максимальная версия ПО
WEP-200L	1.6.0	2.2.x
WEP-2L	1.6.0	2.2.x
WEP-30L	2.1.0	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
WOP-30L	2.1.0	2.2.x

23.11 Портальная авторизация

23.11.1 Авторизация через Cisco ISE

- Взаимодействие контроллера с порталом Cisco ISE
- Настройка на WLC
  - Настройка RADIUS-сервера
  - Настройка портальной авторизации
    - Использование сертификатов
  - Суммарные изменения в конфигурации
- Настройка Cisco ISE
  - Отладочная информация RADIUS

Взаимодействие контроллера с порталом Cisco ISE

1. При первом подключении клиента ТД пытается пройти MAB-авторизацию на NAC-сервере, подставляя MAC-адрес клиента в атрибуты User-Name и User-Password запроса access-request к RADIUS-серверу WLC. Контроллер проксирует запрос на внешний RADIUS-сервер Cisco ISE. Так как ISE ничего не известно о данном клиенте, он присылает access-reject на WLC, тот, в свою очередь, на ТД.
2. После того как ТД получила access-reject, она отправляет клиенту ссылку перенаправления на гостевой портал ISE-формата, при этом дополняя ACL с доступом только до гостевого портала. Пример ссылки: https://100.110.0.161:8443/portal/PortalSetup.action?portal=10968c1f-36fe-4e5c-96ff-9d74f689b29b?action_url=http%3A%2F%2Fredirect%2Eloc%3A10081%2F&ap_mac=68%3A13%3AE2%3A0E%3A85%3A50&client_mac=a2%3A13%3A66%3A1b%3Ac7%3A8e&redirect=http%3A%2F%2Fconnectivitycheck%2Egstatic%2Ecom%2Fgenerate%5F204
3. После авторизации пользователя на гостевом портале клиенту возвращается ссылка редиректа на ТД, содержащая в себе адрес сайта, на который клиент хотел попасть изначально, логин и пароль, под которым клиент успешно прошёл аутентификацию на гостевом портале. Пример ссылки: http://redirect.loc:10081/?token=NAI4PU5HK6O007V0KMYS37M800GOZW97&buttonClicked=4&err_flag=0&err_msg=&info_flag=0&info_msg=&redirect_url=http%3A%2F%2Fconnectivitycheck.gstatic.com%2Fgenerate_204&username=login&password=Password

4. Когда клиент переходит по этой ссылке, ТД считывает из нее логин и пароль и подставляет в атрибуты User-Name и User-Password запроса access-request, RADIUS успешно авторизует клиента, и ТД снимает ACL на доступ клиента и перенаправляет на изначально запрашиваемый пользователем портал.
5. После отключения от SSID и подключения заново или подключения к другой ТД (к тому же SSID), авторизация будет проходить по MAC-адресу (так как этот сценарий реализован в логике ТД «external portal» и срабатывает при подключении к SSID, если ТД не помнит клиента). Редирект пользователя на портал происходить не будет до тех пор, пока учетная запись клиента не будет удалена из базы, вручную или автоматически (по настроенной логике).

Пример страницы гостевого портала:

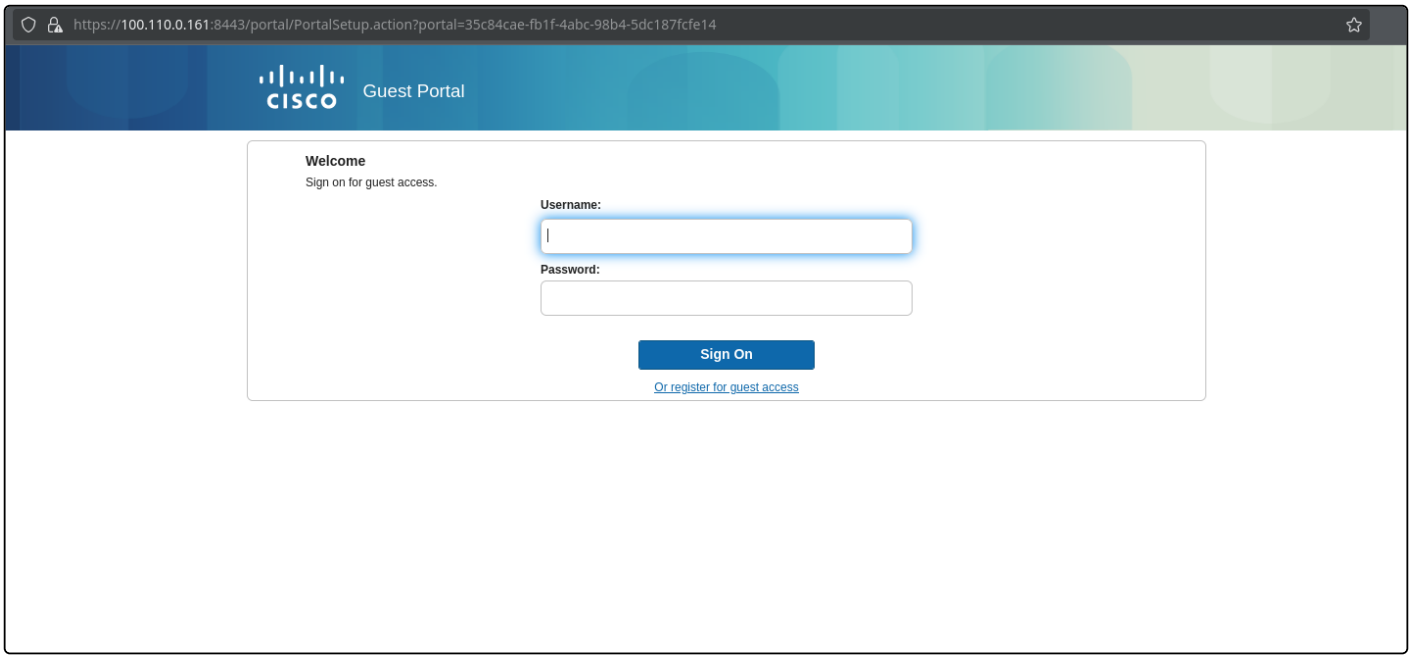
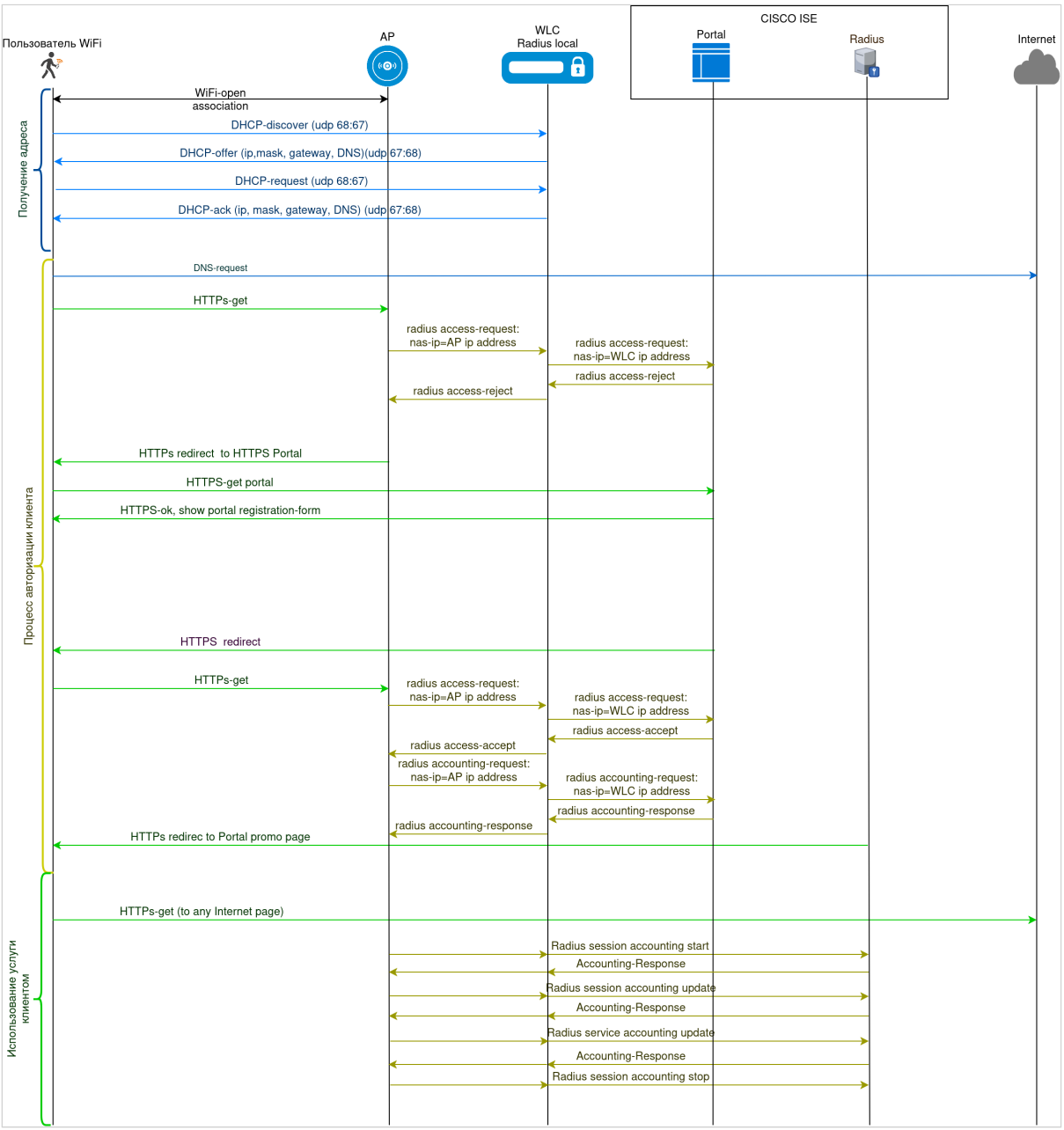


Схема процесса авторизации нового клиента по логину и паролю:



Настройка на WLC

В данном разделе описана настройка внешней портальной авторизации на WLC.

За основу взята заводская конфигурация Factory (подробнее в инструкции Quickstart):

```
object-group service ssh
  port-range 22
exit
object-group service dhcp_server
  port-range 67
exit
object-group service dhcp_client
  port-range 68
exit
```

```
object-group service ntp
  port-range 123
exit
object-group service dns
  port-range 53
exit
object-group service netconf
  port-range 830
exit
object-group service radius_auth
  port-range 1812
exit
object-group service sa
  port-range 8043-8044
exit
object-group service airtune
  port-range 8099
exit
object-group service web
  port-range 443
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
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 untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
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 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
  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
  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
  radius-profile default-radius
    description "default-radius"
    auth-address 192.168.1.1
    auth-password ascii-text encrypted 8CB5107EA7005AFF
    domain default
  exit
  wids-profile default-wids
    description "default-wids"
  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

ip tftp client timeout 45
ntp enable
ntp broadcast-client enable

ip https server
```

Различие конфигурации устройств

Физическая конфигурация интерфейсов устройств WLC-15, WLC-30 и WLC-3200 различается между собой. Попытка применения настроек для одной модели устройства на другую может вызвать ошибку инициализации интерфейсов.

Внесение дополнений в конфигурацию:

Ниже рассмотрен пример настройки RADIUS-сервера и проксирования RADIUS-запросов ТД на внешний RADIUS-сервер (подробнее в инструкции Настройка проксирования на внешний RADIUS):

Настройка RADIUS-сервера

Настройте локальный RADIUS-сервер:

```
radius-server local
  nas ap
    key ascii-text password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  virtual-server default
    proxy-mode
    nas-ip-address 100.109.1.246 <-- WLC UPLINK IP BRIDGE 2
    upstream-server cisco-ise
      host 100.110.0.161
      server-type all
      key ascii-text password
    exit
    enable
  exit
  enable
exit
```

Настройте локальный RADIUS-профиль:

```
radius-server host 127.0.0.1
  key ascii-text password
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit
```

Настройка портальной авторизации

Настройте портальную авторизацию (общий принцип работы описан в статье Авторизация через RADIUS).

В конфигурацию WLC необходимо внести настройки:

```
wlc
  portal-profile default-portal
```

```
    redirect-url-custom "https://100.110.0.161:8443/portal/PortalSetup.action?
portal=10968c1f-36fe-4e5c-96ff-9d74f689b29b?
action_url=<SWITCH_URL>&redirect=<ORIGINAL_URL>&ap_mac=<AP_MAC>"
    age-timeout 10
    verification-mode external-portal
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text password
    auth-acct-id-send
    acct-enable
    acct-address 192.168.1.1
    acct-password ascii-text password
    acct-periodic
  exit
exit
```

⚠ Значение параметра *redirect-url-custom* в профиле портала требуется указывать в двойных кавычках.

Параметр wlc>portal-profile>redirect-url-custom содержит URL портала и атрибуты, указанные после символа "?". Между собой атрибуты разделяются символом "&".

Таблица 1 — Атрибуты URL-шаблона для внешней портальной авторизации

Параметр	Описание
<NAS_ID>	Идентификатор ТД. Когда параметр не задан, то в качестве NAS ID в RADIUS-пакетах и строке редиректа будет использоваться MAC-адрес ТД. NAS ID возможно задать в конфигурации wlc → radius-profile <name> → nas-id. В данном примере NAS ID не задается.
<SWITCH_URL>	Доменное имя, которое получает клиент при перенаправлении
<AP_MAC>	MAC-адрес точки доступа
<CLIENT_MAC>	MAC-адрес клиента
<SSID>	SSID
<ORIGINAL_URL>	URL, который изначально запрашивал клиент
<NAS_IP>	IP-адрес точки доступа

Настройте SSID-профиль:

```
wlc
  ssid-profile default-ssid
    ssid "default-ssid_cisco_ise"
    radius-profile default-radius
    portal-enable
    portal-profile default-portal
    vlan-id 3
```

```
    802.11kv
    band 2g
    band 5g
    enable
  exit
exit
```

Использование сертификатов

Для повышения безопасности передачи данных между клиентом и ТД необходимо обеспечить шифрование трафика с использованием SSL. Для этого требуется:

- SSL-сертификат (формат PEM);
- Приватный ключ (формат PEM).

На ТД возможно использовать RSA-сертификаты. ECDSA-сертификаты не поддержаны.

Для защиты приватного ключа в схеме с портальной авторизацией рекомендуется использовать пароль.

Стандартный процесс выпуска сертификатов не предусматривает автоматическое шифрование приватного ключа. Однако это можно выполнить вручную с помощью утилиты **OpenSSL**.

Команда для шифрования ключа:

```
openssl rsa -aes256 -in private_key.pem -out private_key_encrypted.pem
```

Параметры:

- `-aes256` – алгоритм шифрования (можно заменить на `-aes128` или `-aes192`);
- `-in private_key.pem` – исходный незашифрованный ключ;
- `-out private_key_encrypted.pem` – зашифрованный ключ.

После выполнения команды OpenSSL запросит пароль, который будет использоваться для защиты ключа.

Этот подход обеспечит дополнительный уровень защиты приватного ключа от несанкционированного доступа.

Данная процедура проводится вне процесса выпуска сертификата и является дополнительной мерой безопасности.

После шифрования ключа его необходимо добавить к сертификату, например через текстовый редактор. Файл сертификата с шифрованным ключом должен иметь вид:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----

-----END ENCRYPTED PRIVATE KEY-----
```

Загрузите файл сертификата с шифрованным ключом на контроллер WLC в директорию *crypto:cert/*

Настройте проверку сертификата и включите режим HTTPs:

```
wlc
```

```
  ap-profile default-ap
    captive-portal
      ap-ip-alias certificate_alias
      crypto cert certificate_encrypted.pem
      crypto private-key-password ascii-text password
      proxy-https
    exit
```

Перед применением конфигурации произойдёт проверка псевдонима сертификата и пароля шифрованного ключа.

Допустимо использовать сертификат без шифрованного ключа. В таком случае приватный ключ добавляется к сертификату. Настройка **crypto private-key-password** не требуется.

Формат файла для сертификата без шифрованного ключа:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----
```

Конфигурация:

```
wlc
  ap-profile default-ap
    captive-portal
      ap-ip-alias certificate_alias
      crypto cert certificate.pem
      proxy-https
    exit
```

Суммарные изменения в конфигурации

Изменения в конфигурации WLC:

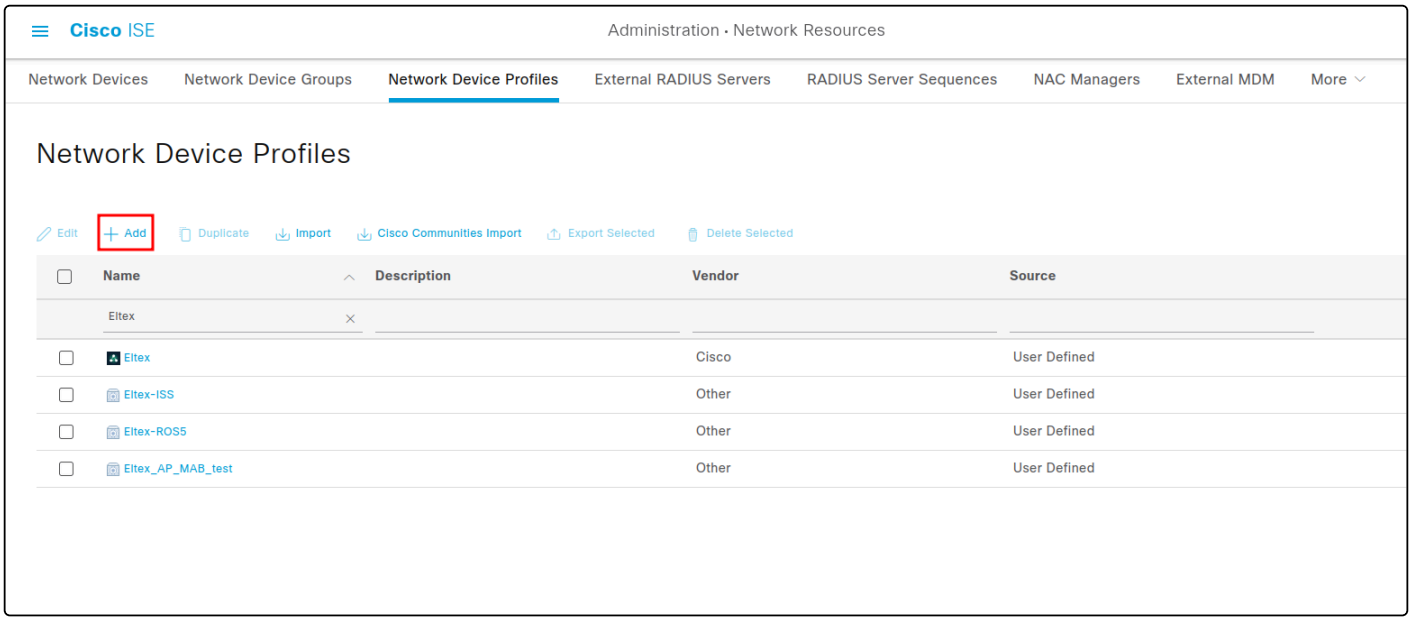
```
radius-server local
  nas ap
    key ascii-text password
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text password
    network 127.0.0.1/32
  exit
  virtual-server default
    proxy-mode
    nas-ip-address 100.109.1.246
    upstream-server cisco-ise
      host 100.110.0.161
      server-type all
      key ascii-text password
    exit
    enable
  exit
  enable
exit
```

```
radius-server host 127.0.0.1
  key ascii-text password
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit

wlc
  outside-address 192.168.1.1
  service-activator
    aps join auto
  exit
  airtune
    enable
  exit
  ap-location default-location
    mode tunnel
    ap-profile default-ap
    airtune-profile default_airtune
    ssid-profile default-ssid
  exit
  airtune-profile default_airtune
    description "default_airtune"
  exit
  ssid-profile default-ssid
    ssid "default-ssid_cisco_ise"
    radius-profile default-radius
    portal-enable
    portal-profile default-portal
    vlan-id 3
    security-mode WPA2_1X
    802.11kv
    band 2g
    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
    password ascii-text password
    captive-portal
      ap-ip-alias wlc.ddns.net
      crypto cert certificate_encrypted.pem
      crypto private-key-password ascii-text password
      proxy-https
    exit
  exit
  portal-profile default-portal
    redirect-url-custom "https://100.110.0.161:8443/portal/PortalSetup.action?
portal=10968c1f-36fe-4e5c-96ff-9d74f689b29b?
action_url=<SWITCH_URL>&redirect=<ORIGINAL_URL>&ap_mac=<AP_MAC>"
    age-timeout 10
    verification-mode external-portal
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
```

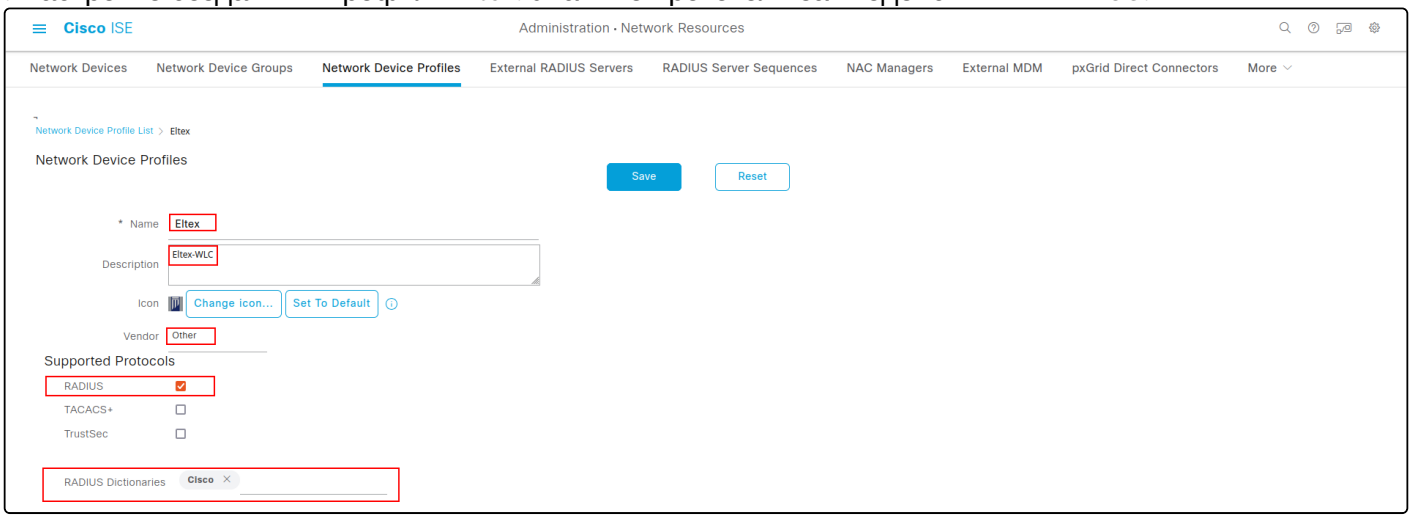
```
    auth-password ascii-text password
    auth-acct-id-send
    acct-enable
    acct-address 192.168.1.1
    acct-password ascii-text password
    acct-periodic
    domain default
  exit
  ip-pool default-ip-pool
    description "default-ip-pool"
    ap-location default-location
  exit
  enable
exit
```

Настройка Cisco ISE

1. В Cisco ISE создайте *Network Device Profile — Eltex* с помощью кнопки **Add**:



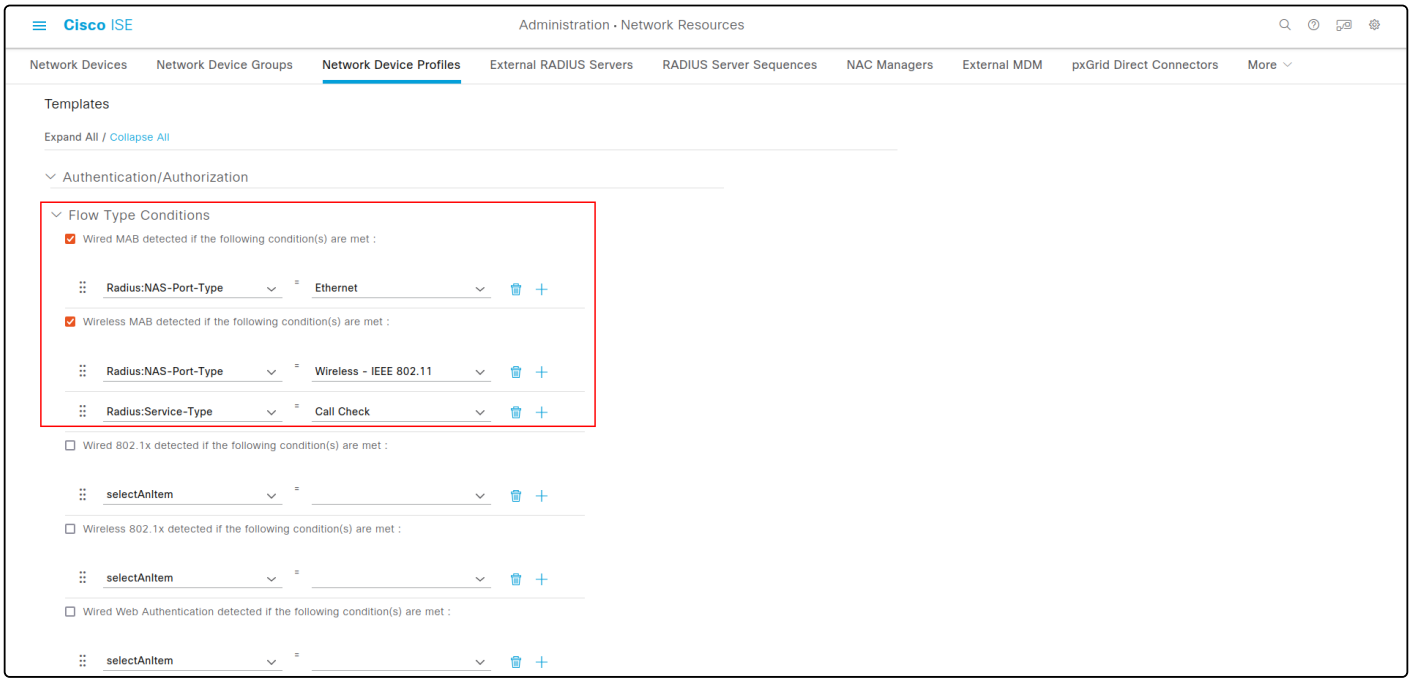
2. Настройте созданный профиль *Eltex*. Укажите протокол взаимодействия — *RADIUS*:



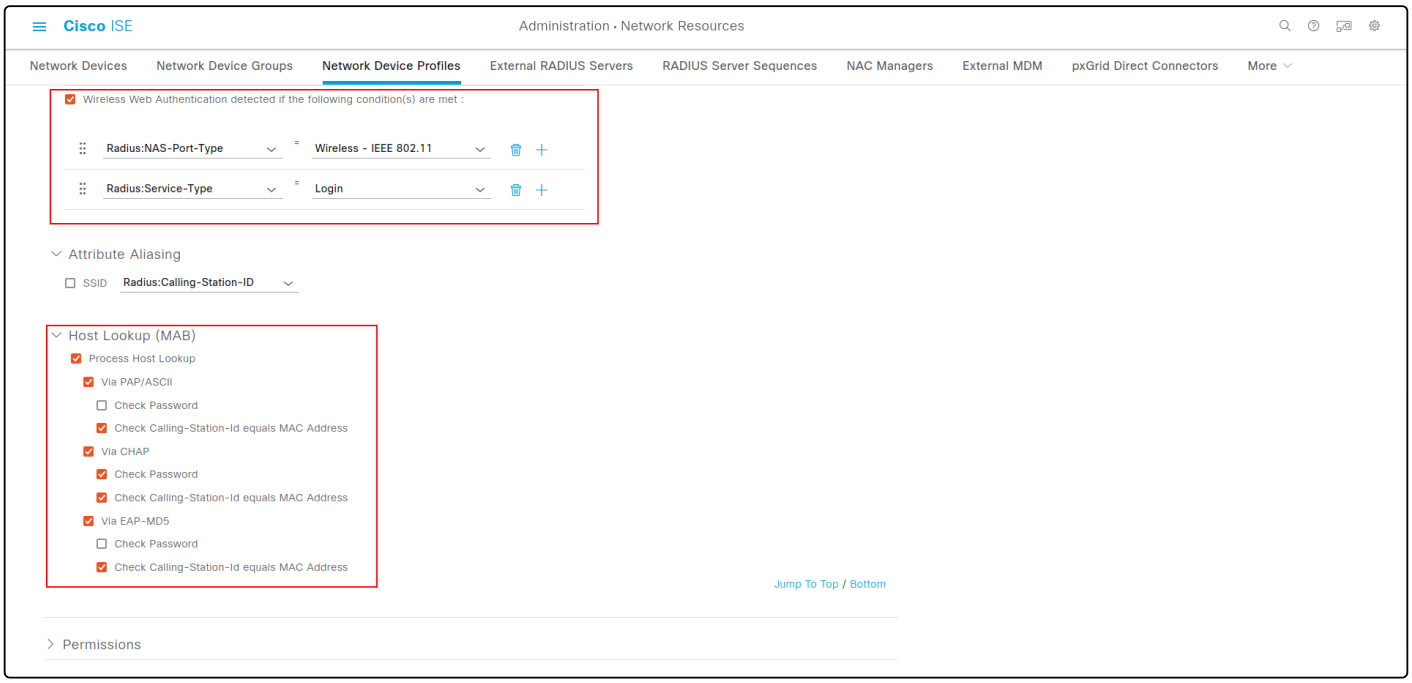
В параметрах укажите атрибуты RADIUS, по которым ISE будет определять типы Authentication/ Authorization. Для этого в выпадающем списке необходимо настроить *Flow Type Conditions*:

- *Wireless MAB detected;*
- *Wireless Web Authentication detected.*

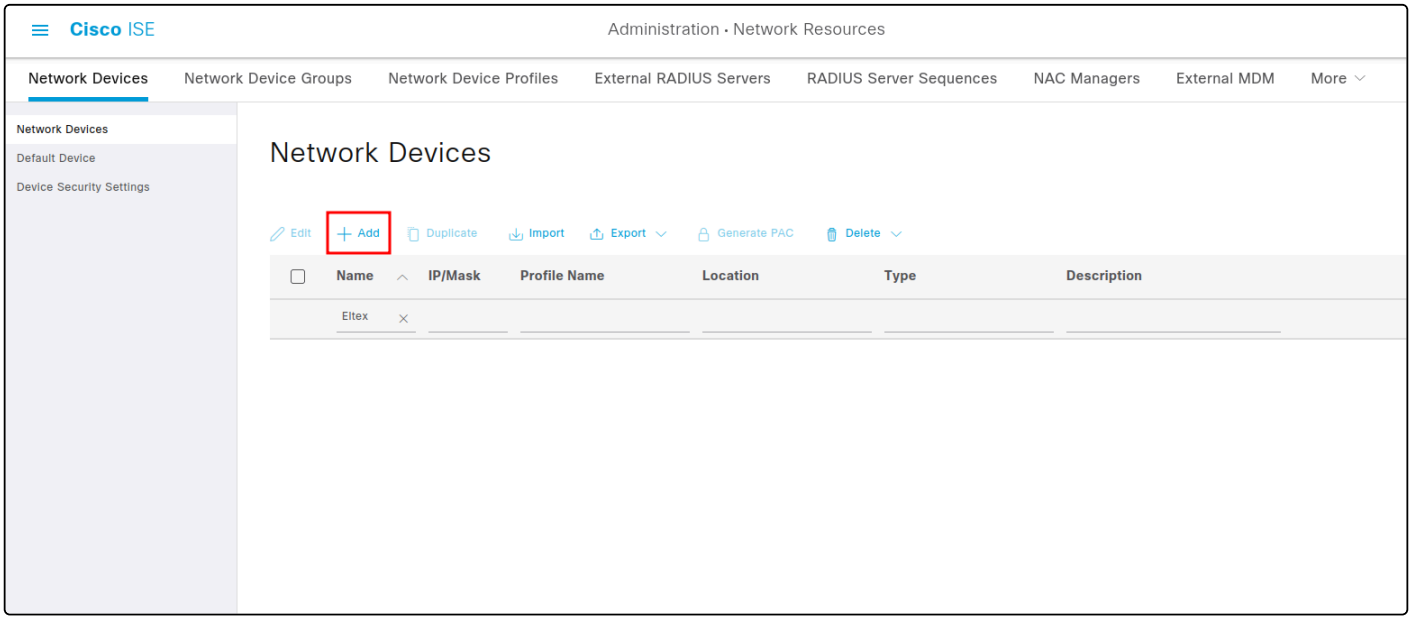
Для всех Wireless-подключений атрибут идентификации *Radius:NAS-Port-Type* будет одинаков *Wireless - IEEE 802.11*.
В Wireless MAB detected необходимо добавить еще один атрибут — *Radius:Service-Type* со значением *Call Check*.
В *Wireless Web Authentication detected* необходимо добавить еще один атрибут — *Radius:Service-Type* со значением *Login*.



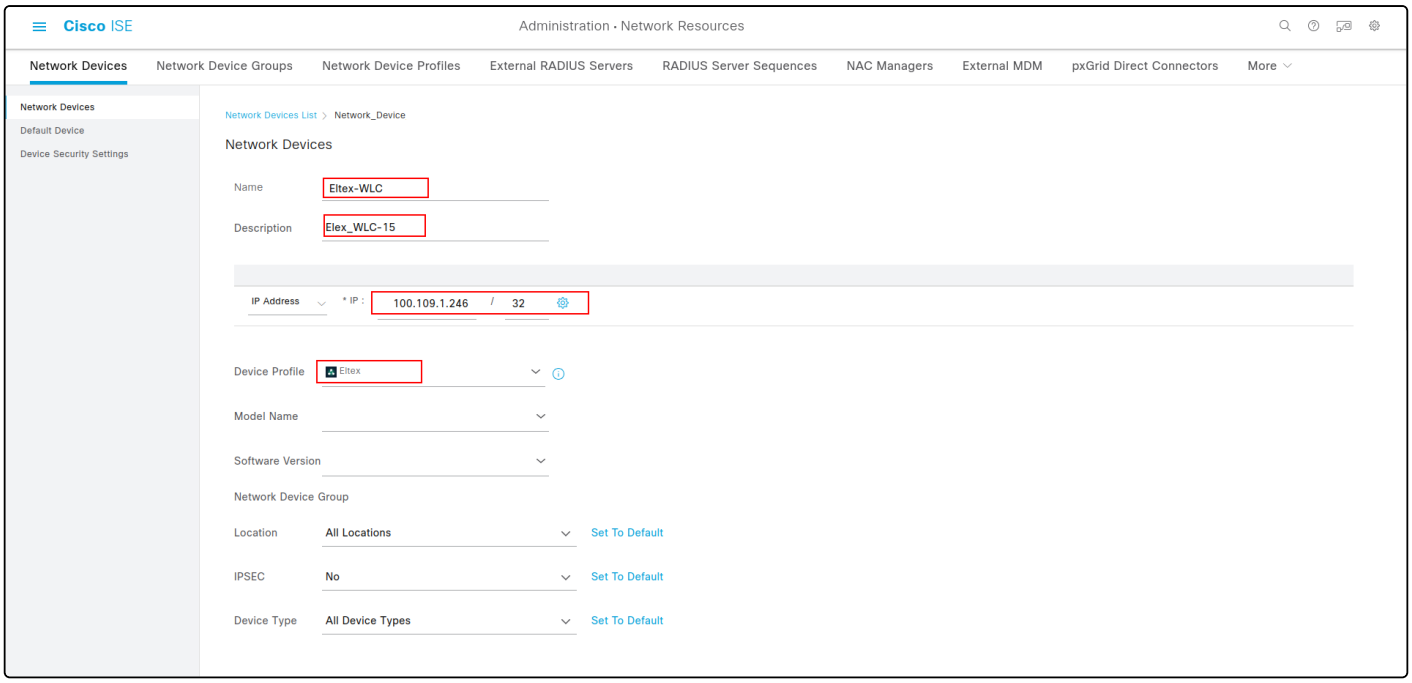
В *Host Lookup (MAB)* установите флаг на пункте *Process Host Lookup*, включите используемый ТД протокол обмена подтверждениями, отключите *Check Password* в разделах *Via PAP/ASCII* и *Via EAP-MD5*:



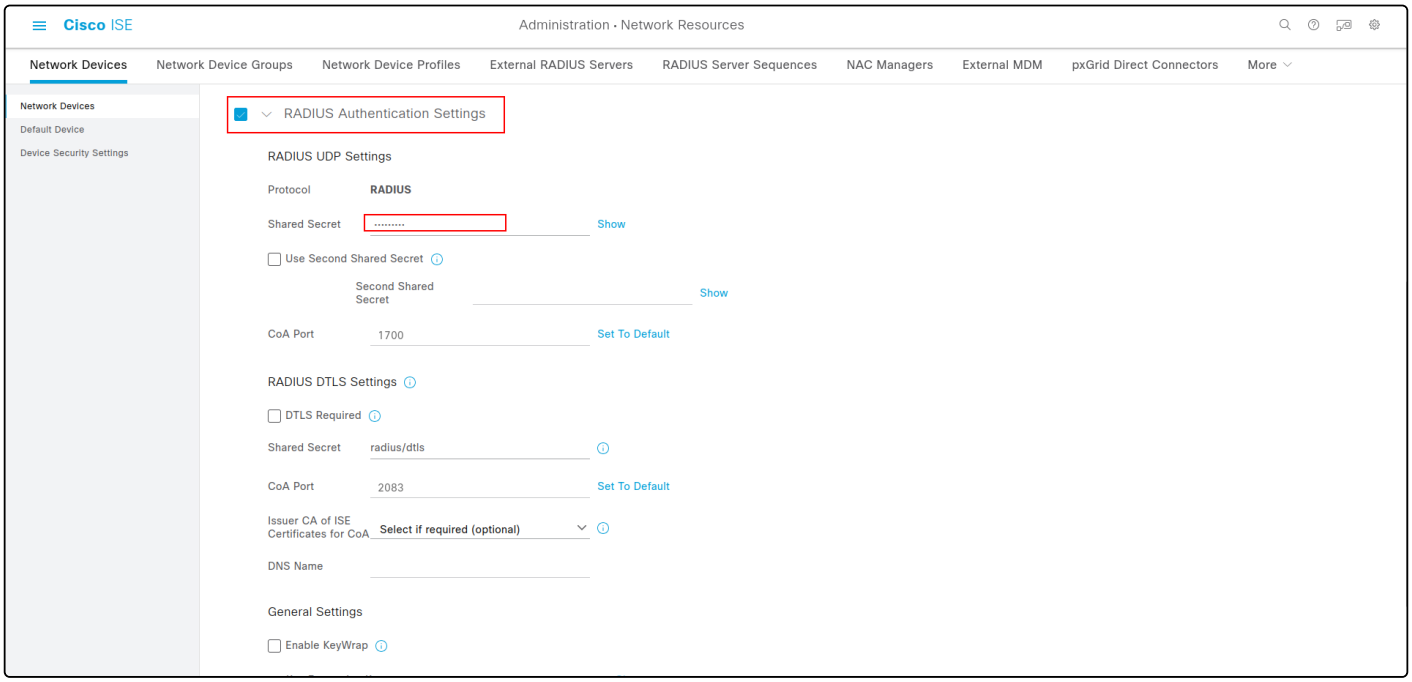
3. Создайте новое сетевое устройство, в примере ниже — *Eltex-WLC*:



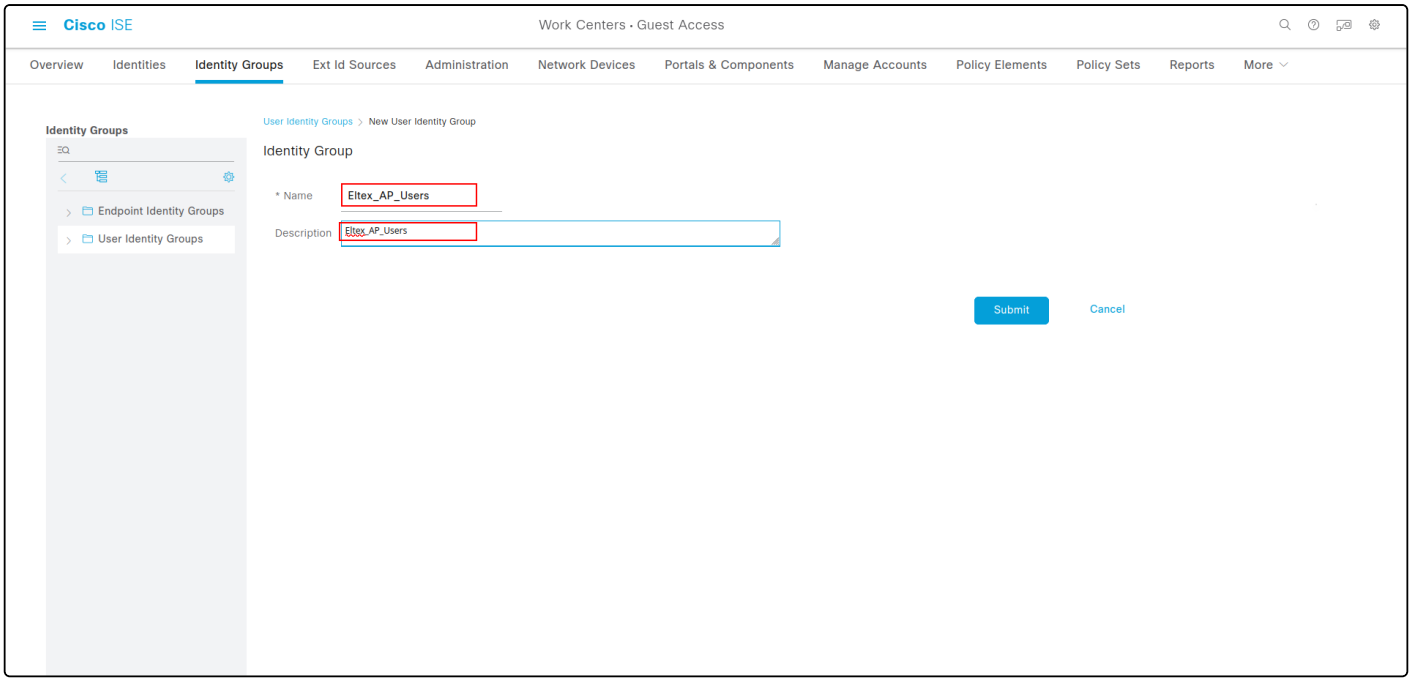
4. Настройте взаимодействие по протоколу RADIUS. Укажите адрес и подсеть **контроллера WLC** (в примере это один контроллер и подсеть 100.109.1.246/32), в поле *Device Profile* выберите ранее созданный профиль *Eltex*:



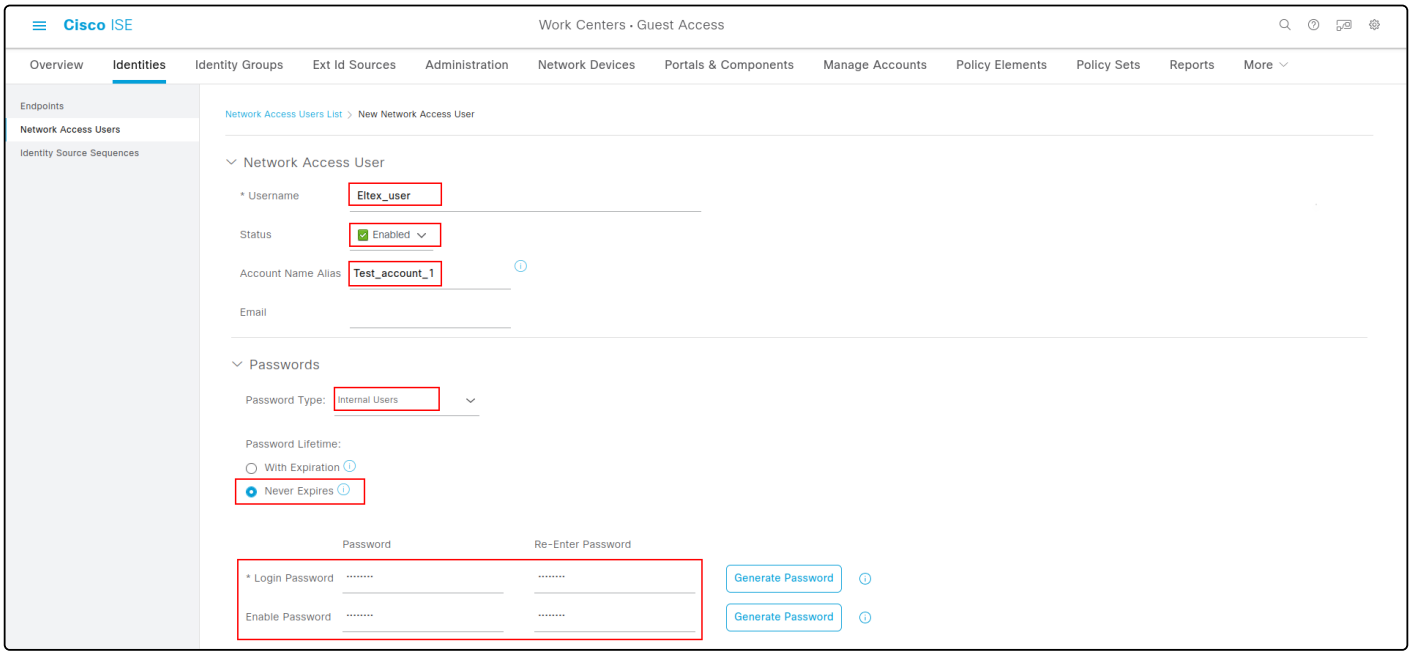
Укажите *secret key* для протокола RADIUS, настроенный на контроллере WLC в разделе radius-server → virtual-server → upstream-server → key:

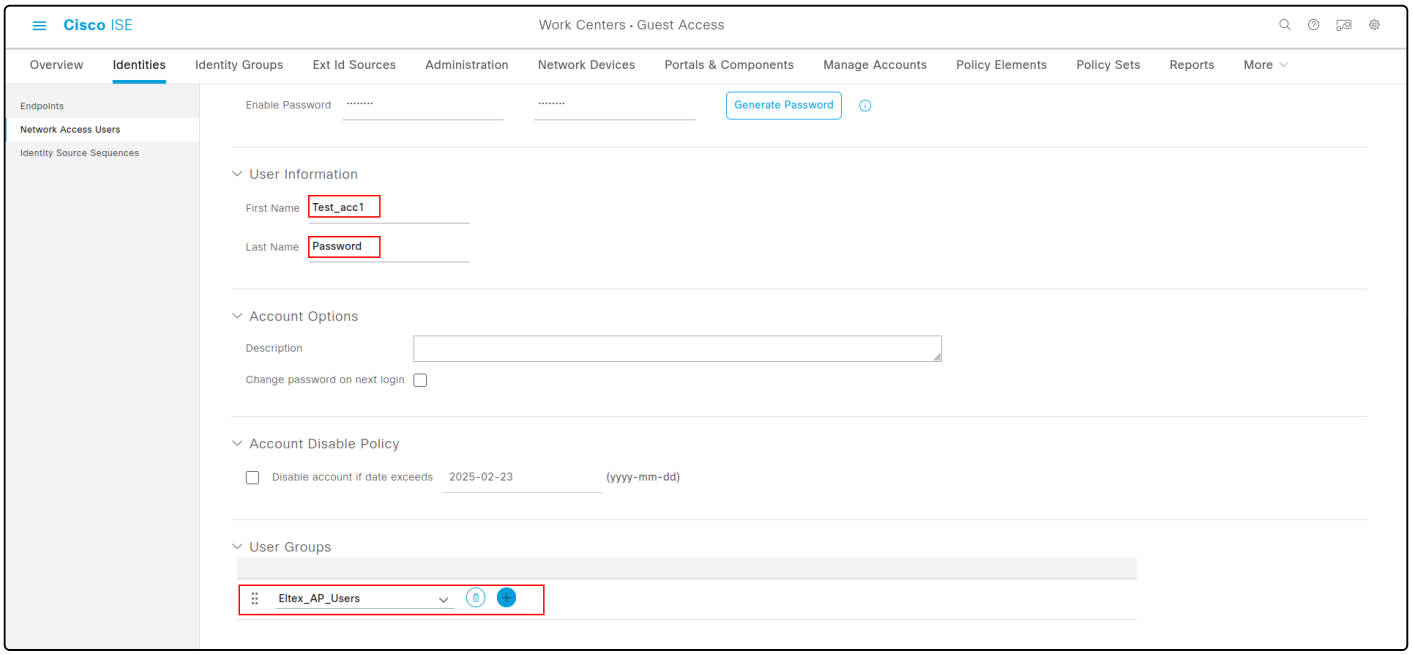


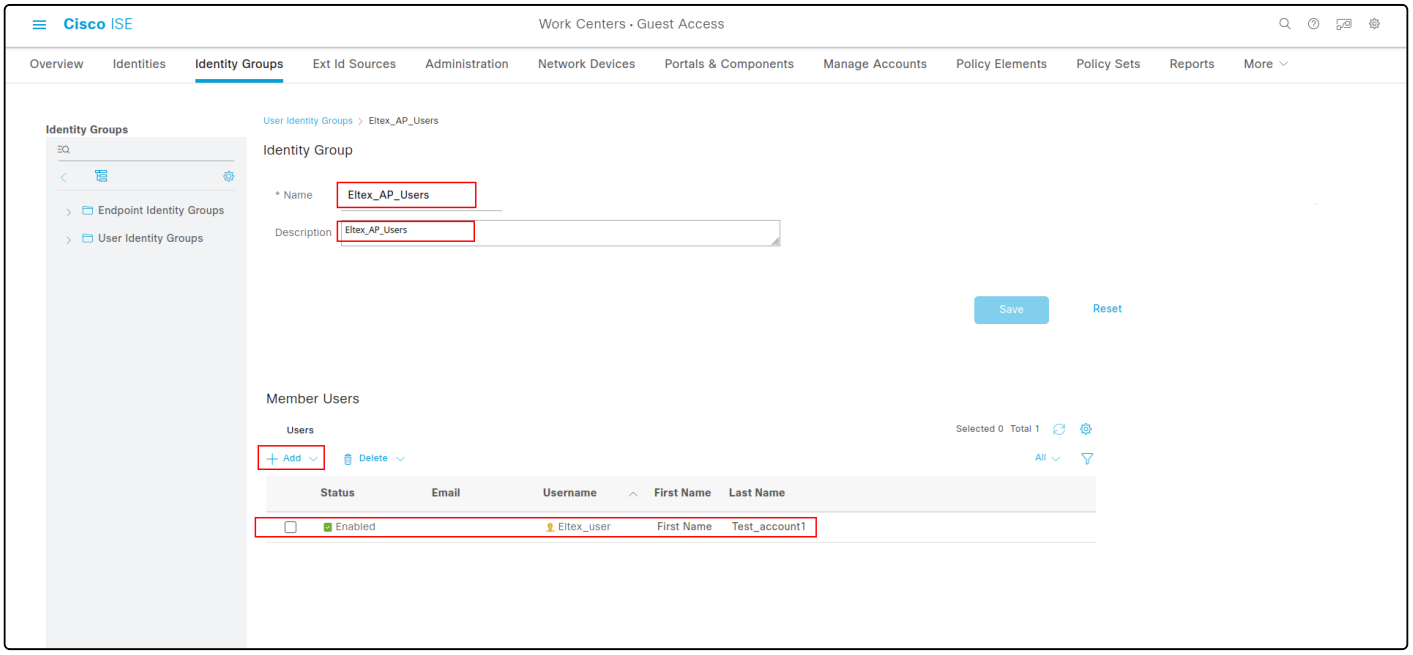
5. Создайте группу встроенных гостевых учетных записей, в примере ниже это *Eltex_AP_Users*:



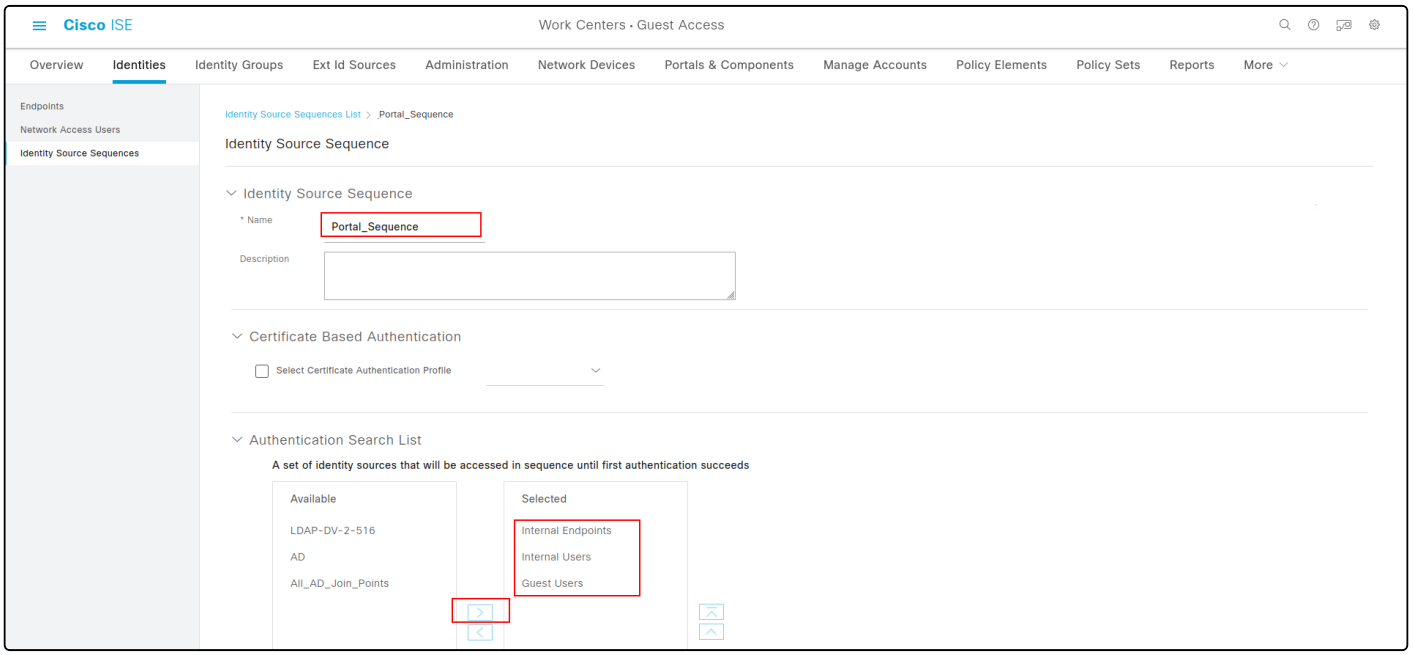
В этой группе необходимо создать учетные записи, задать для каждой логин и пароль. Пример создания учетной записи:

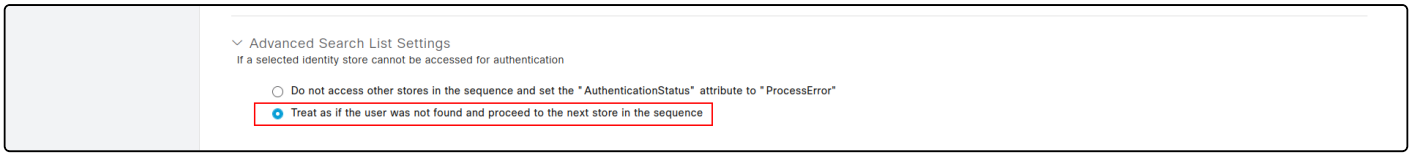

Cisco ISE
Work Centers · Guest Access
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
More
Endpoints
Network Access Users
Identity Source Sequences
Network Access Users List > New Network Access User
Network Access User
* Username
Eltex_user
Status
Enabled
Account Name Alias
Test_account_1
Email
Passwords
Password Type:
Internal Users
Password Lifetime:
With Expiration
Never Expires
Password
Re-Enter Password
* Login Password
Enable Password
Generate Password
Generate Password


Cisco ISE
Work Centers · Guest Access
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
More
Endpoints
Network Access Users
Identity Source Sequences
Enable Password
Generate Password
User Information
First Name
Test_acc1
Last Name
Password
Account Options
Description
Change password on next login
Account Disable Policy
Disable account if date exceeds
2025-02-23
(yyyy-mm-dd)
User Groups
Eltex_AP_Users

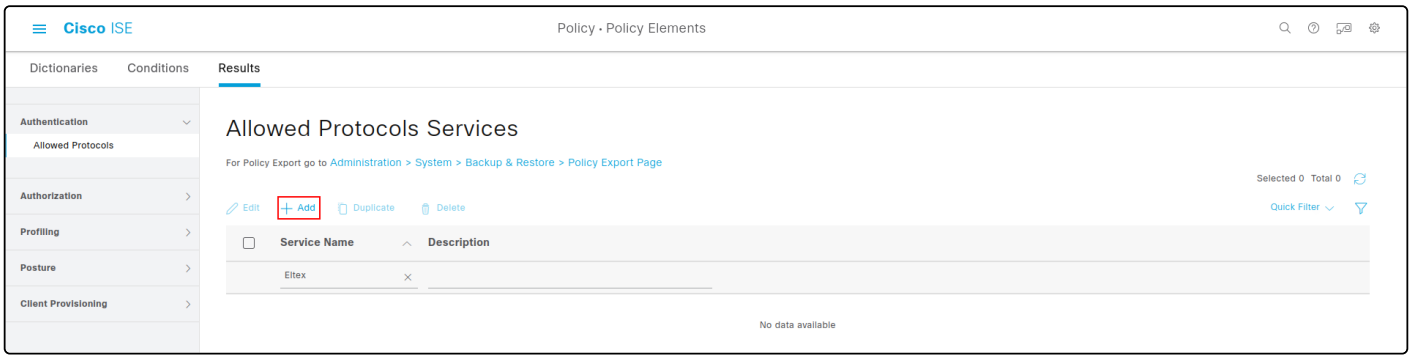

Cisco ISE
Work Centers · Guest Access
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
More
Identity Groups
Endpoint Identity Groups
User Identity Groups
User Identity Groups > Eltex_AP_Users
Identity Group
* Name
Eltex_AP_Users
Description
Eltex_AP_Users
Save
Reset
Member Users
Users
Selected 0 Total 1
Add
Delete
All
Status
Email
Username
First Name
Last Name
Enabled
Eltex_user
First Name
Test_account1

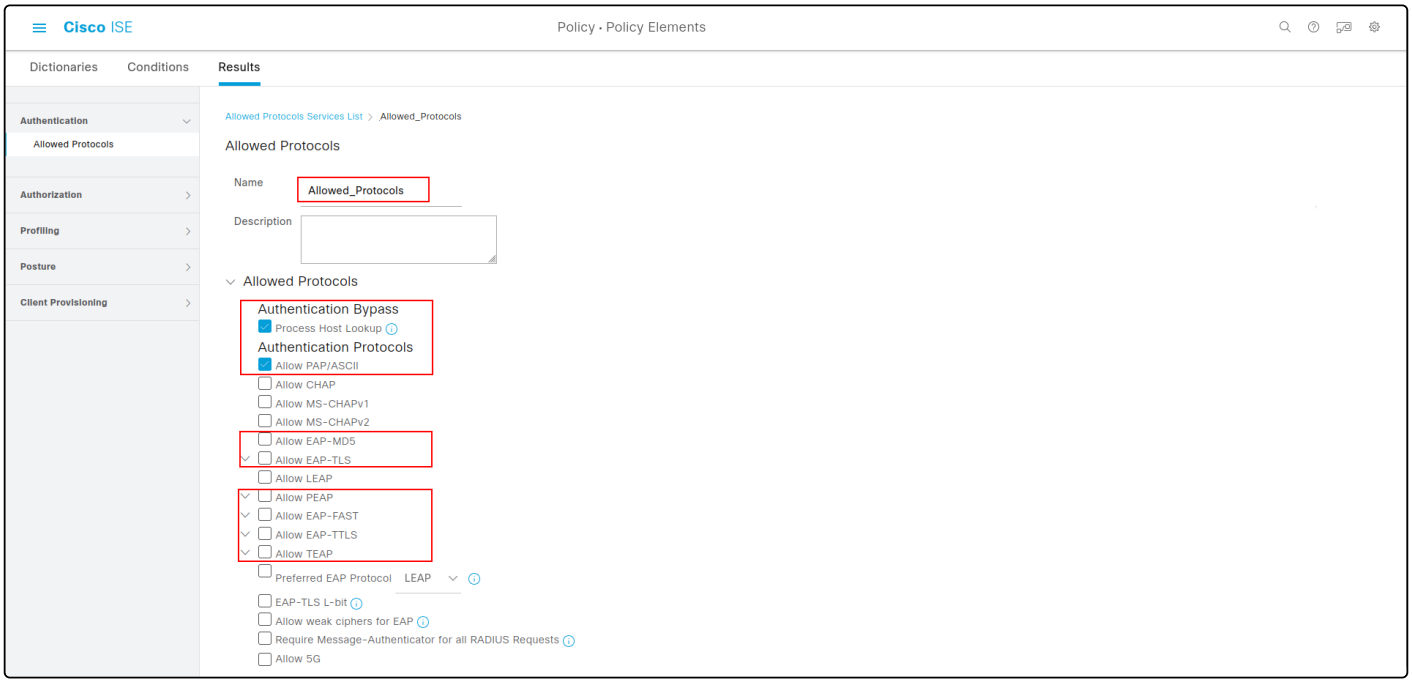
6. Настройте последовательность действий для гостевого портала (*Guest Portal Sequence*). Перейдите в настройки *Work Centers → Guest Access → Identities → Identity Source Sequence → Guest Portal Sequence* — это предустановленная последовательность аутентификации гостевых пользователей. В поле *Authentication Search List* выберите порядок аутентификации пользователей. В примере ниже установлен следующий порядок: *Internal Endpoints (MAB) → Internal Users* (встроенные учетные записи) *→ Guest Users* (учетные записи созданные пользователем самостоятельно на гостевом портале):



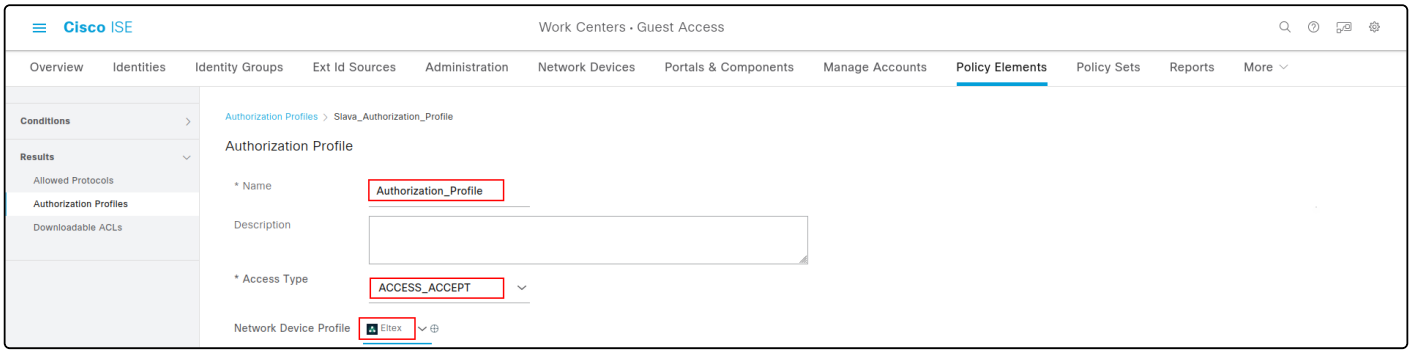


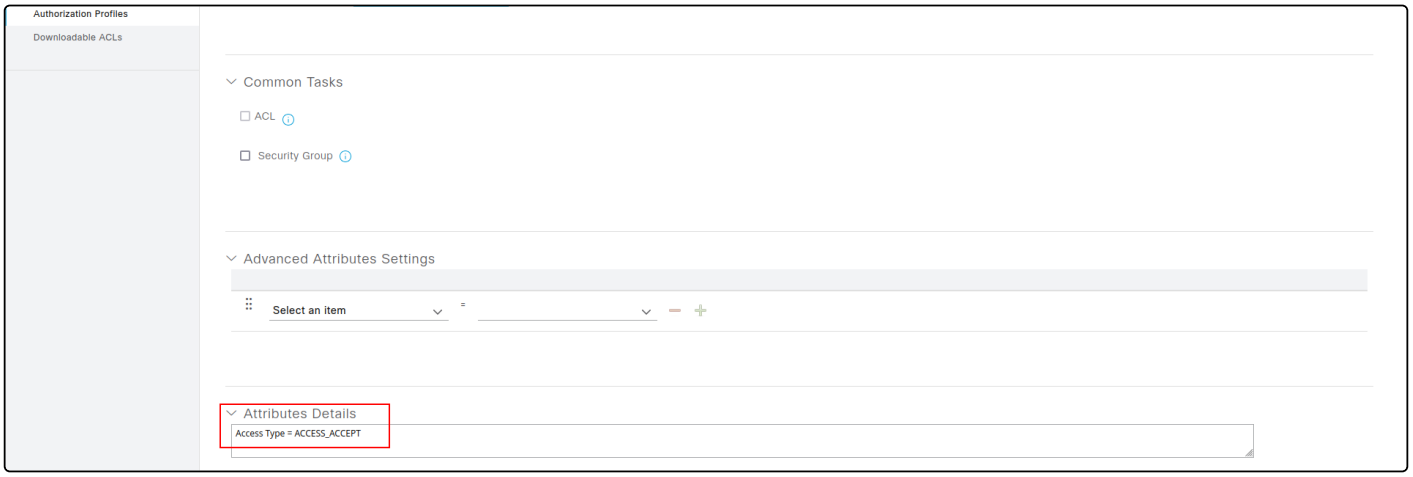
7. Создайте правило с разрешенными протоколами, в примере это *Allowed_Protocols*. Установите необходимые разрешения в пунктах *Authentication Bypass — Process Host Lookup* и в *Authentication Protocols — Allow PAP/ASCII*.



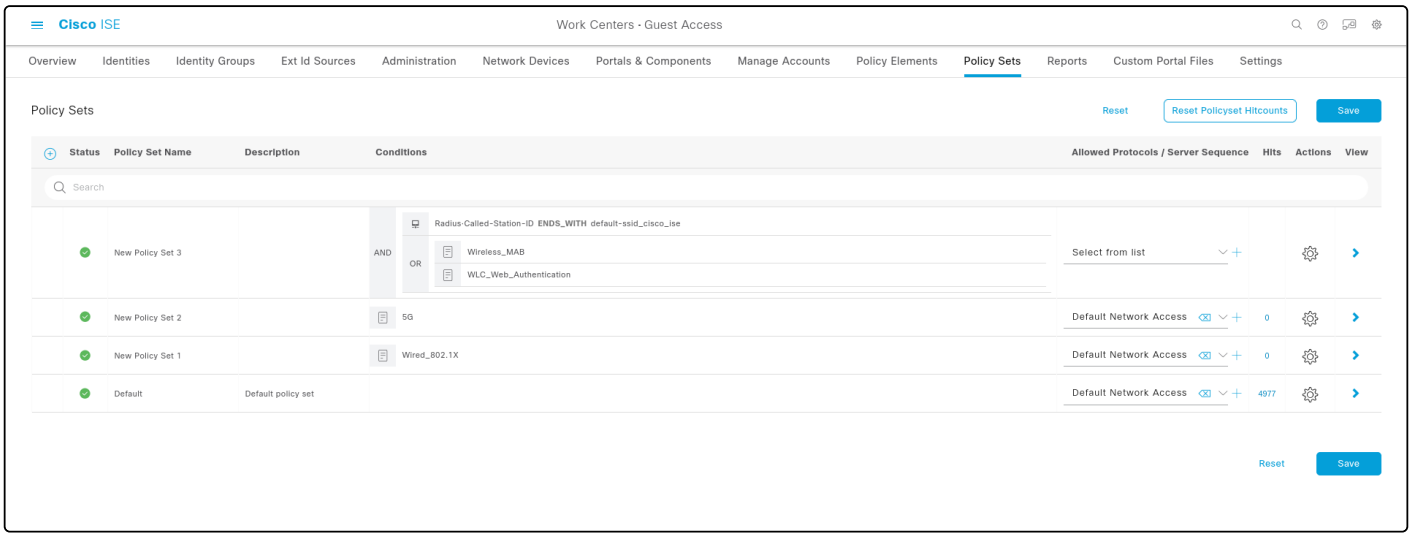


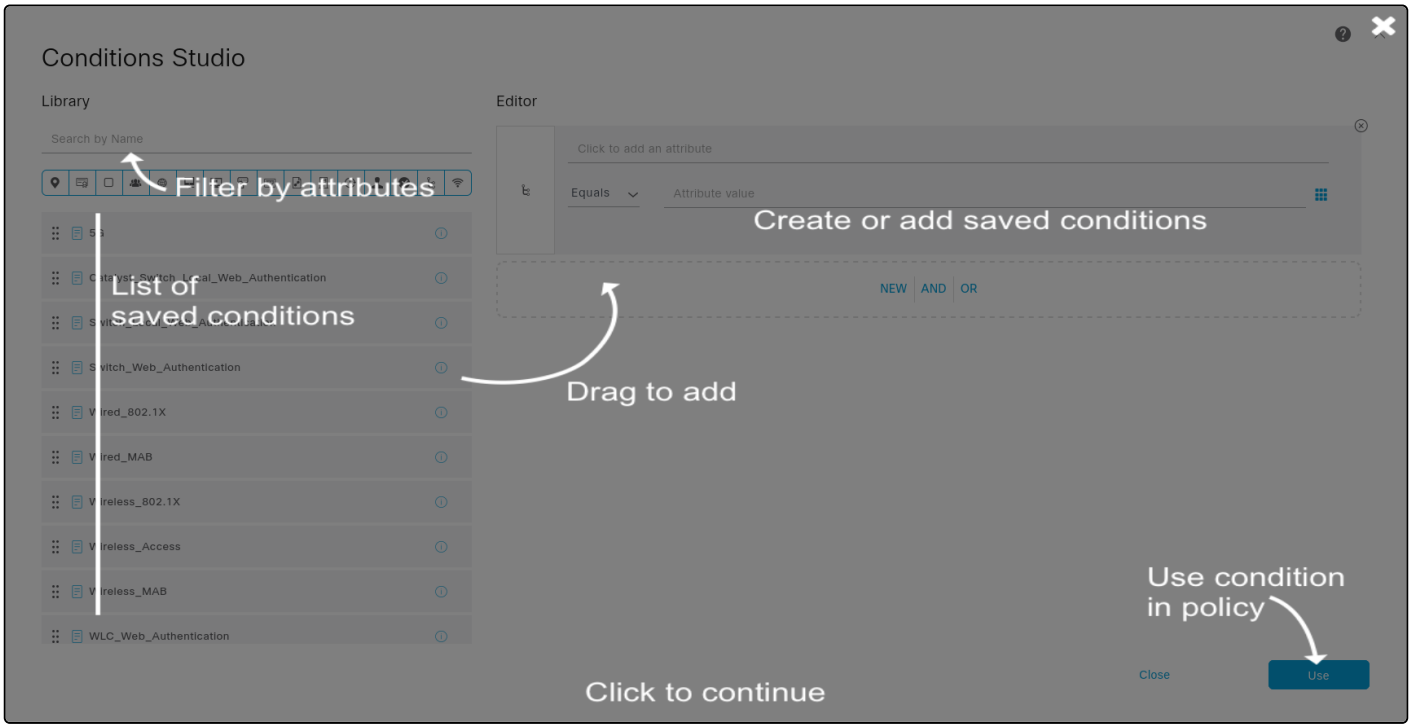
8. Настройте *Authorization Profiles*. На вкладке *Work Centers → Guest Access → Policy Elements → Results → Authorization Profiles → Add* создайте профиль авторизации под ранее созданный *Network Device Profile*. В данный сценарий можно включать параметры авторизации клиента, такие как CVLAN, ACL, shaper и т. п. через добавление различных атрибутов, которые поддерживают ТД ELTEX:

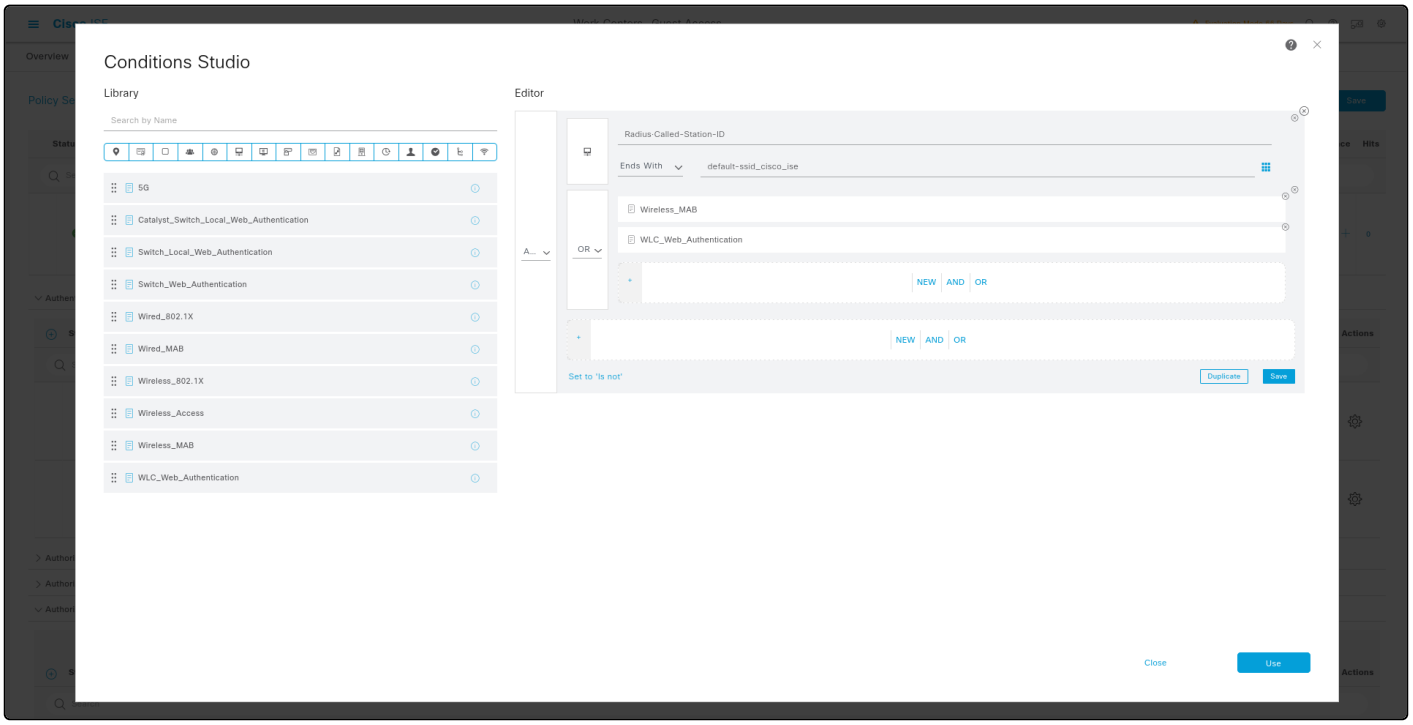




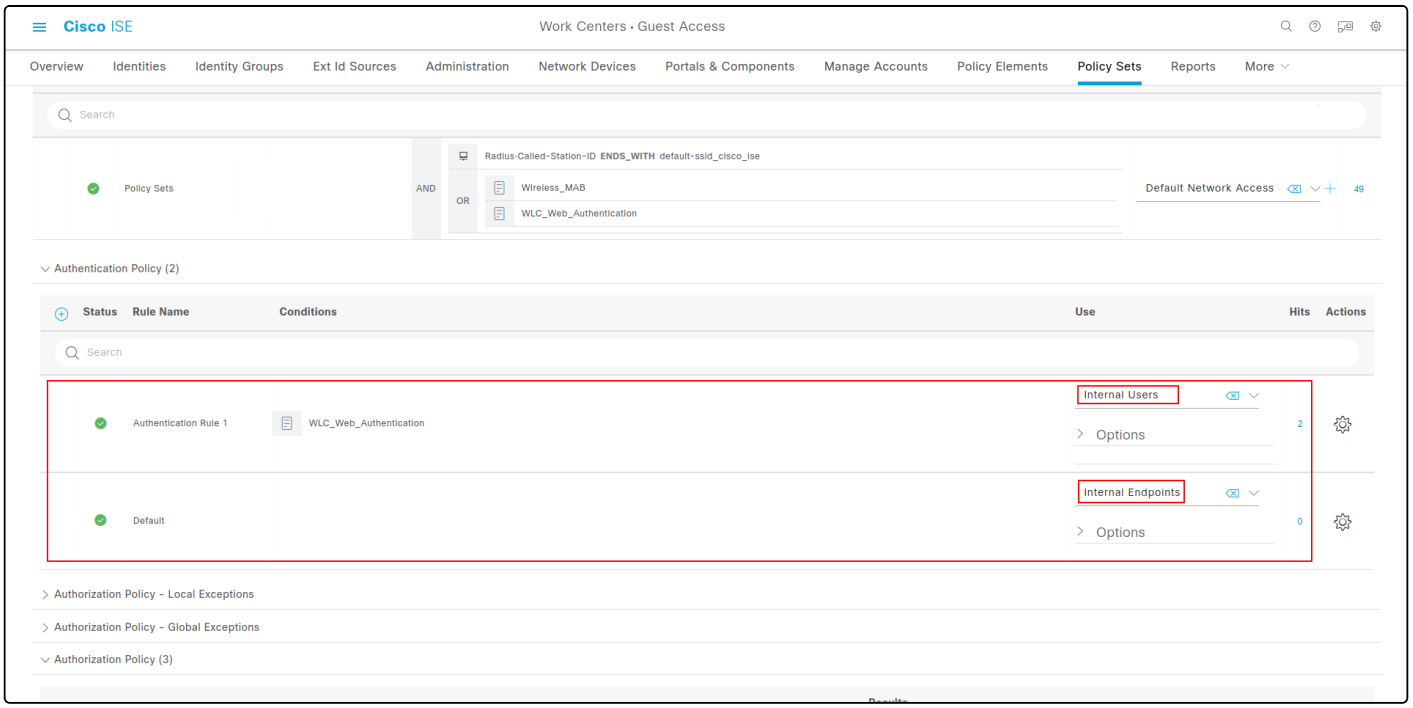
9. Настройте *Policy Sets*. На вкладке *Work Centers → Guest Access → Policy Sets* создайте политику доступа для Wi-Fi пользователей. В примере ниже создана политика доступа с названием *Policy Sets*. В эту политику попадают клиенты, приходящие с SSID *default-ssid_cisco_ise, Flow Type Conditions* соответствуют *Wirelles_MAB* или *WLC_WEB_Authentication*:

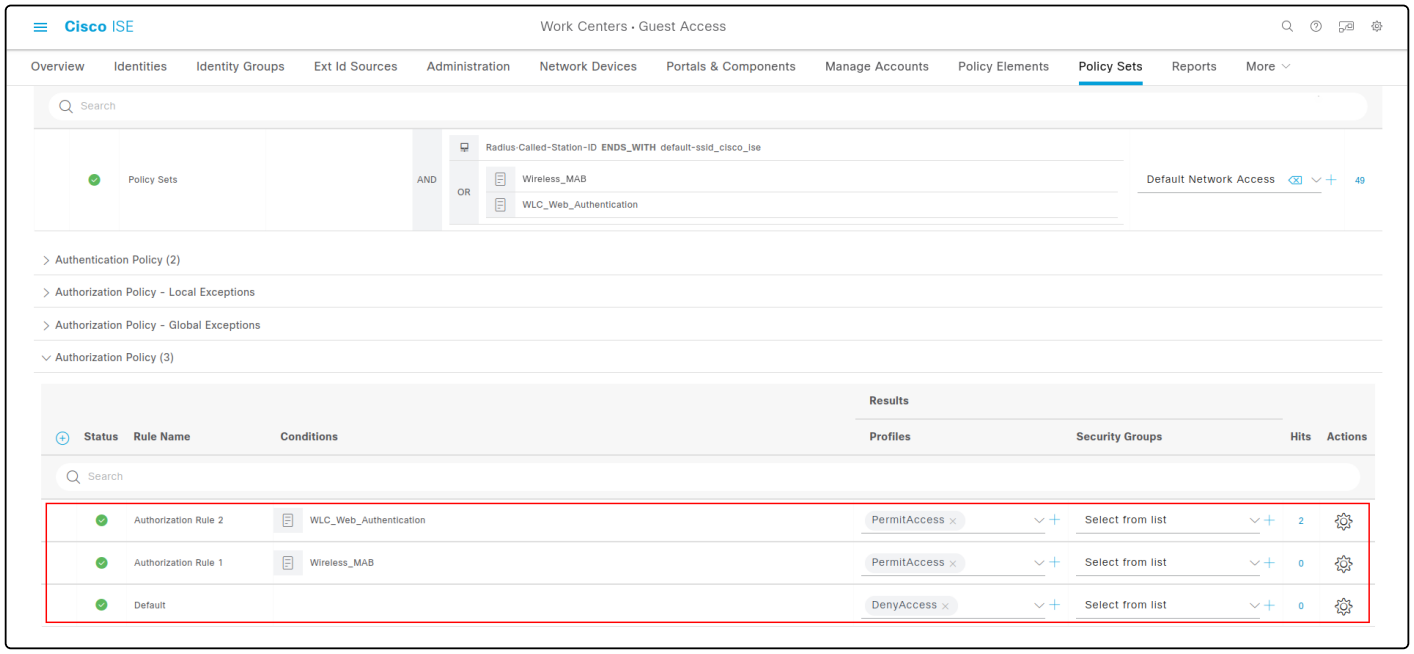




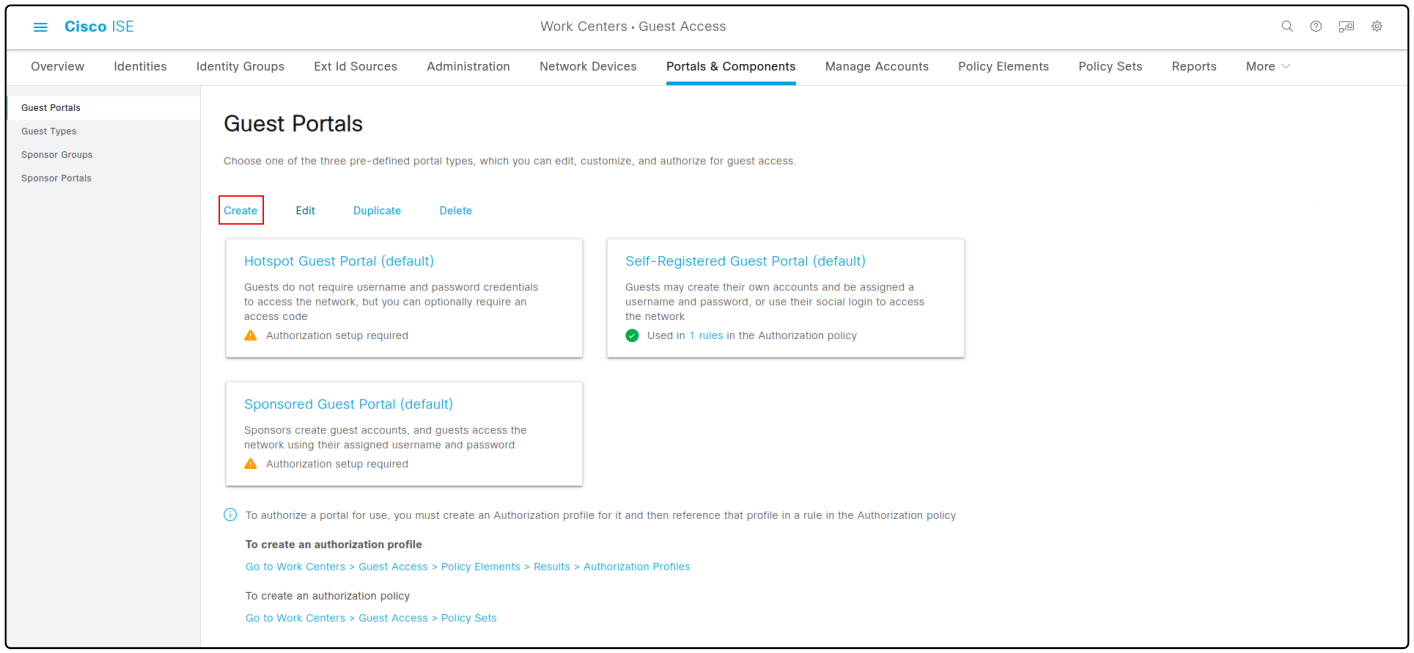


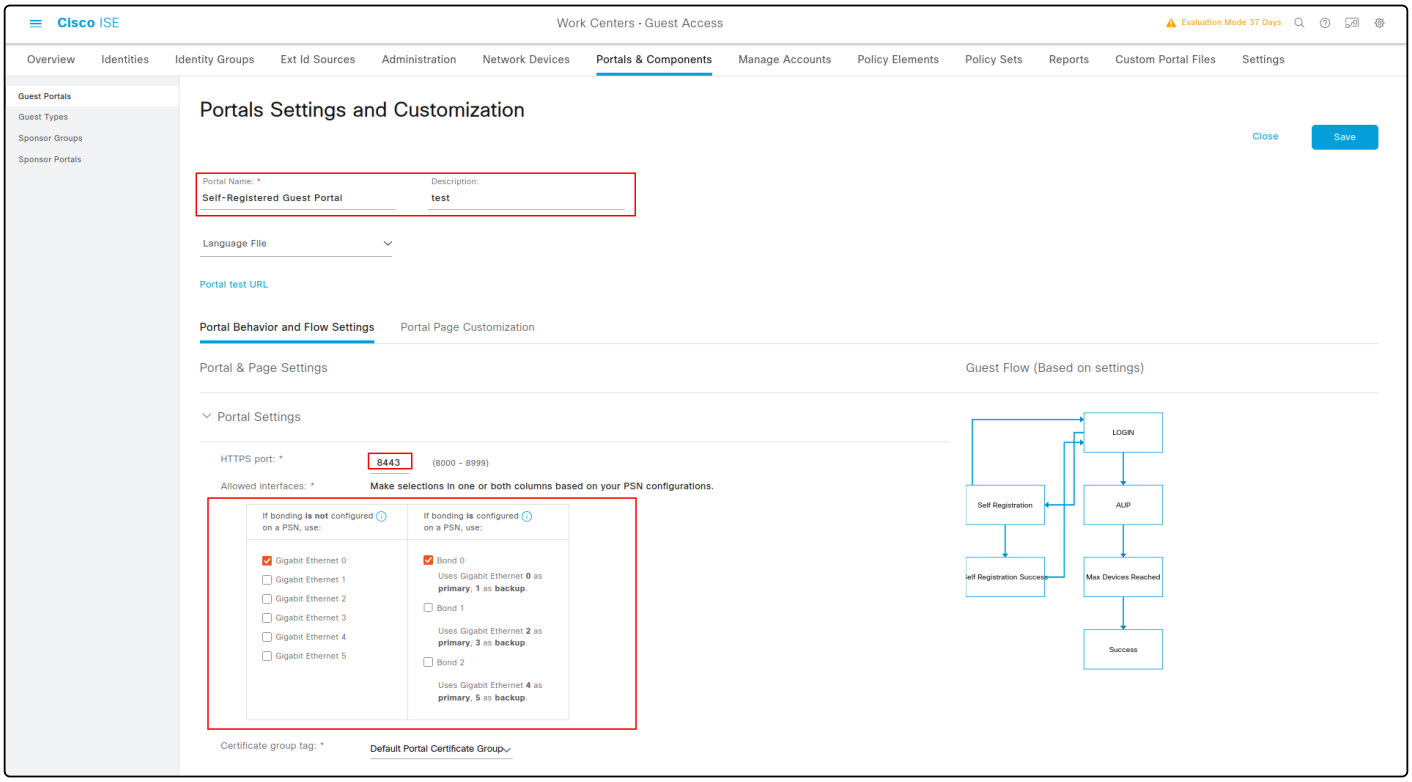
10. В созданной политике настройте правила аутентификации и авторизации.
В правиле аутентификации сначала идет проверка пользователя по логину и паролю в базе *Internal Users*. Далее, если не сработала проверка по логину и паролю, проверяется MAC-адрес в базе *EndPoints (MAB)*.
В правиле авторизации сначала идет проверка пользователя по логину и паролю в базе *Internal Users*. Далее, если не сработала проверка по логину и паролю, проверяется MAC-адрес в базе *EndPoints (MAB)*.
В примере при успешной проверке применяется действие *PermitAccess*.

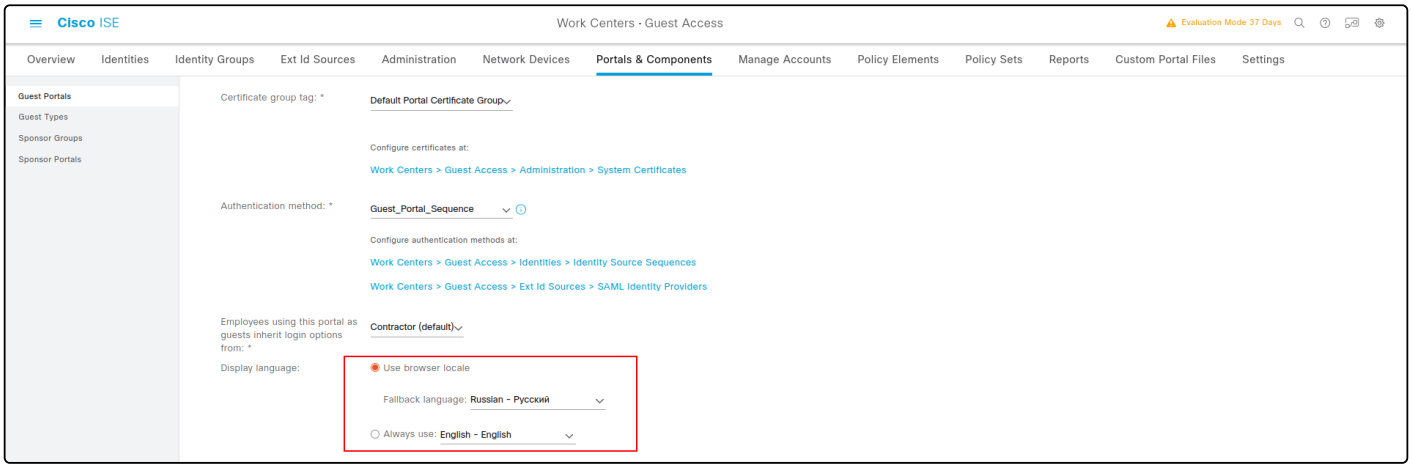


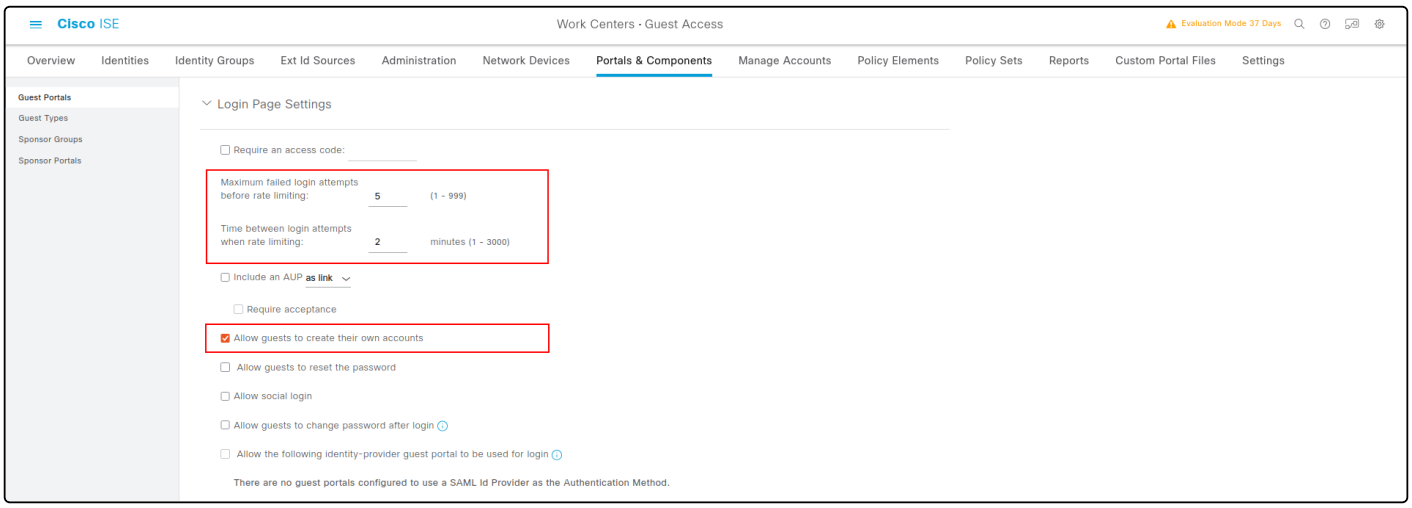


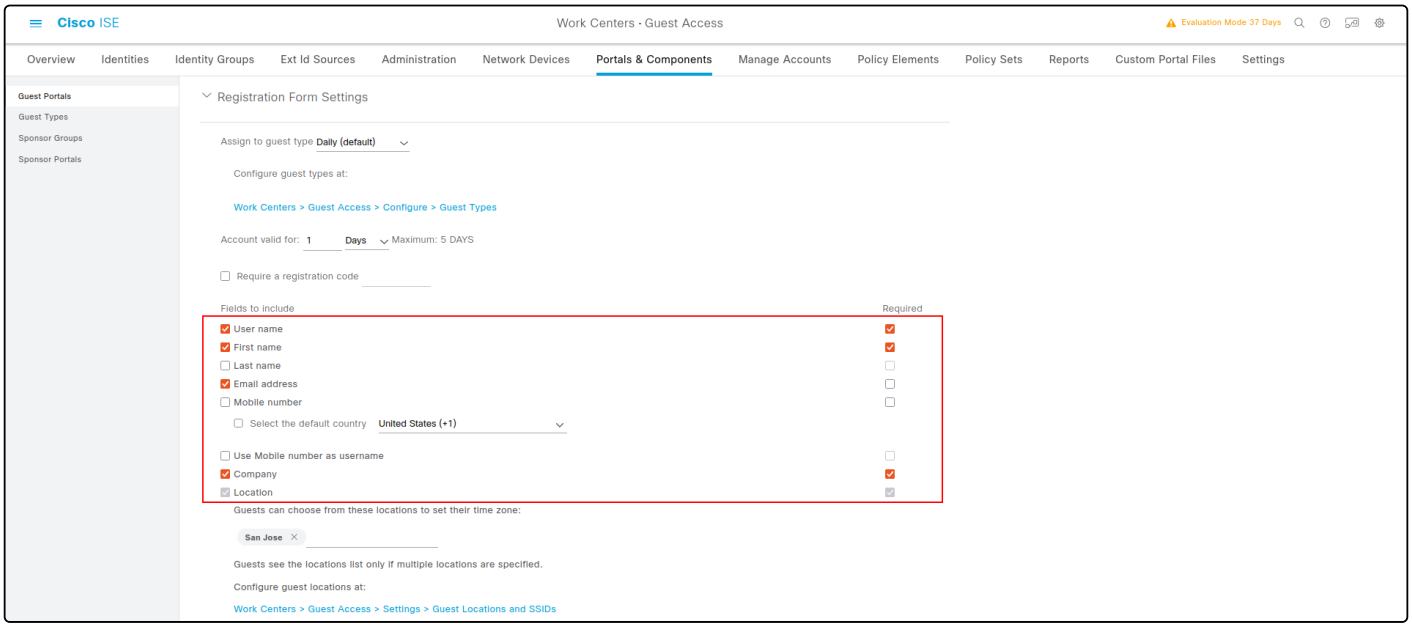
11. Настройте гостевой портал. Ниже приведен пример настройки портала.

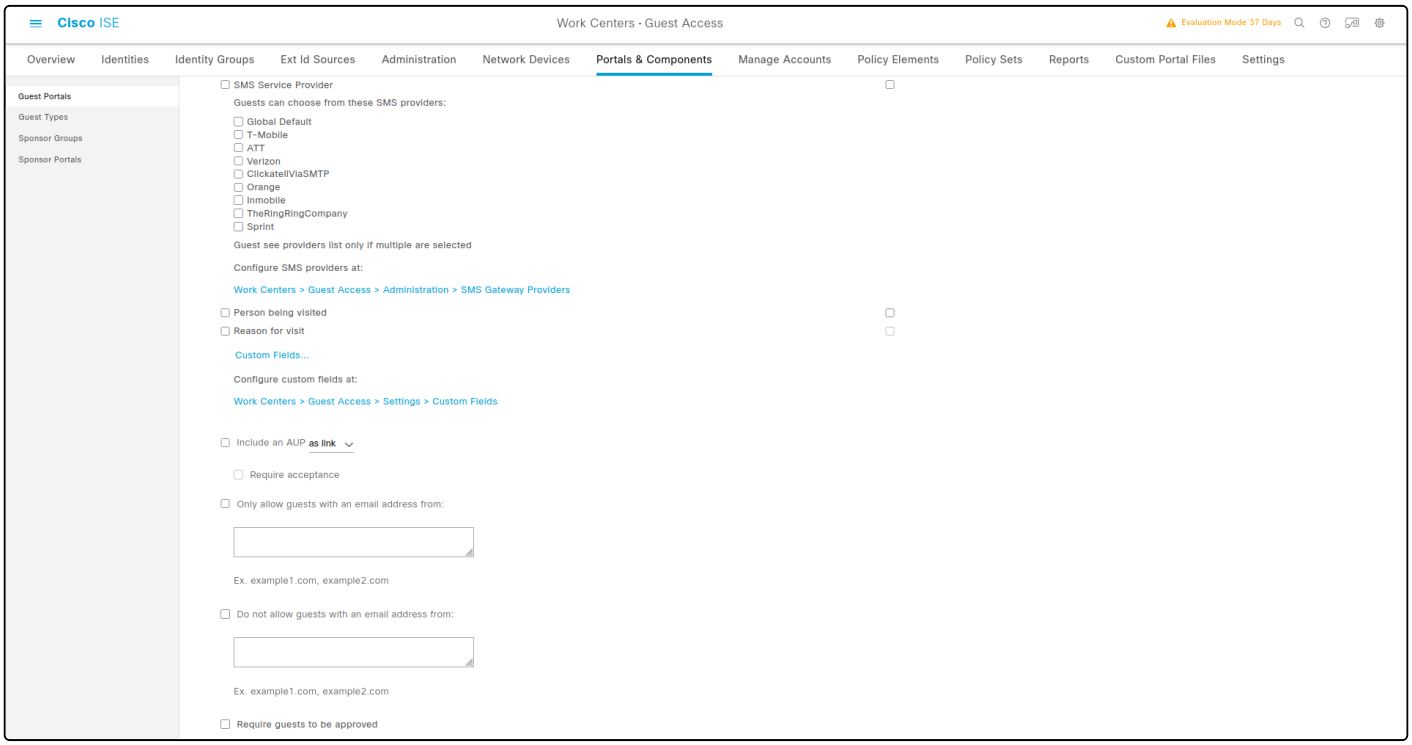


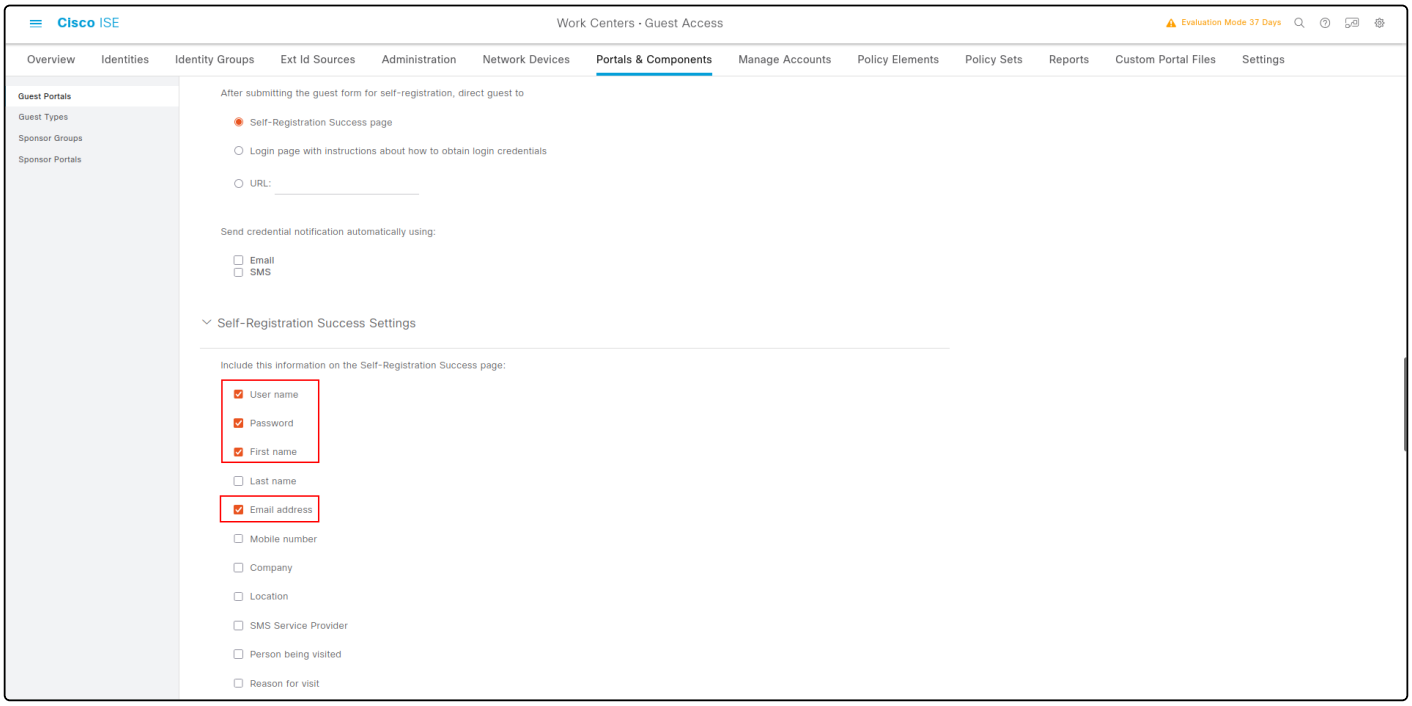

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Portals Settings and Customization
Close
Save
Portal Name: *
Self-Registered Guest Portal
Description:
test
Language File
Portal test URL
Portal Behavior and Flow Settings
Portal Page Customization
Portal & Page Settings
Guest Flow (Based on settings)
Portal Settings
HTTPS port: *
8443
(8000 - 8999)
Allowed interfaces: *
Make selections in one or both columns based on your PSN configurations.
If bonding is not configured on a PSN, use:
If bonding is configured on a PSN, use:
Gigabit Ethernet 0
Gigabit Ethernet 1
Gigabit Ethernet 2
Gigabit Ethernet 3
Gigabit Ethernet 4
Gigabit Ethernet 5
Bond 0
Uses Gigabit Ethernet 0 as primary, 1 as backup.
Bond 1
Uses Gigabit Ethernet 2 as primary, 3 as backup.
Bond 2
Uses Gigabit Ethernet 4 as primary, 5 as backup.
Certificate group tag: *
Default Portal Certificate Group
LOGIN
Self Registration
AUP
Max Devices Reached
Success

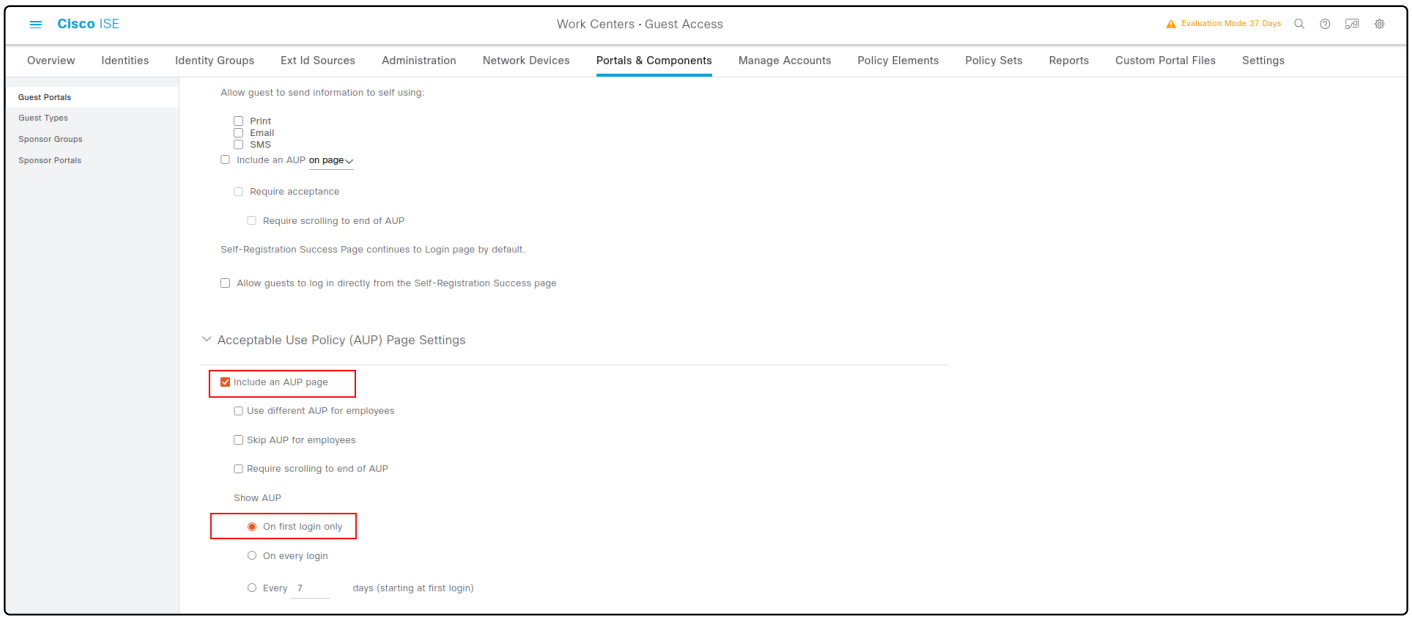

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Certificate group tag: *
Default Portal Certificate Group
Configure certificates at:
Work Centers > Guest Access > Administration > System Certificates
Authentication method: *
Guest_Portal_Sequence
Configure authentication methods at:
Work Centers > Guest Access > Identities > Identity Source Sequences
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers
Employees using this portal as guests inherit login options from: *
Contractor (default)
Display language:
Use browser locale
Fallback language: Russian - Русский
Always use: English - English

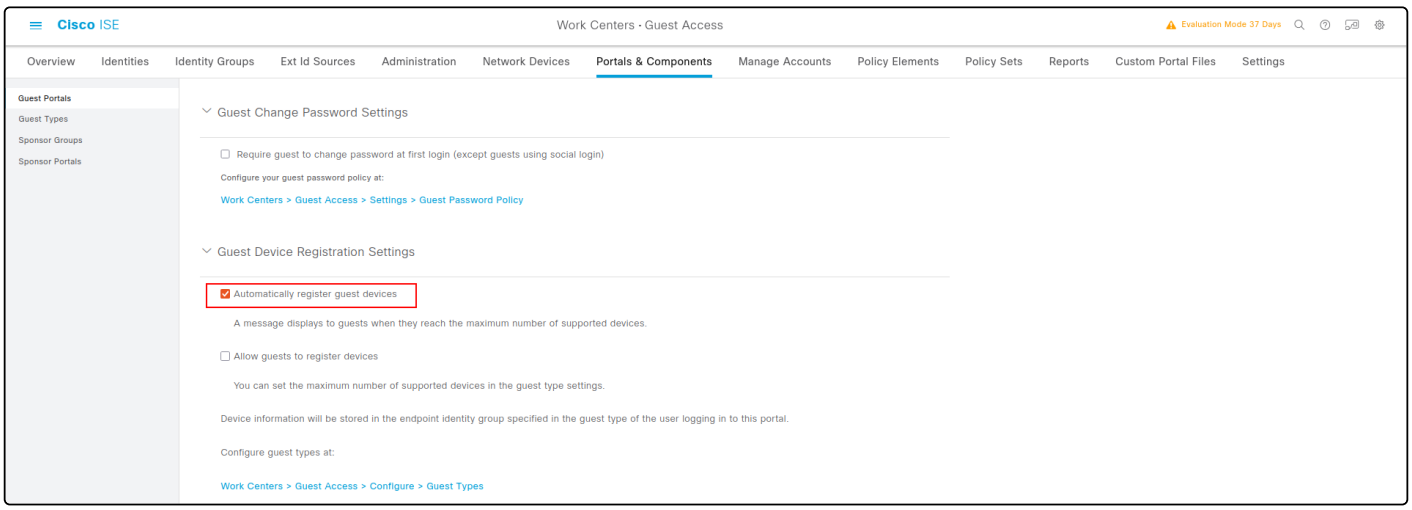

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Login Page Settings
Require an access code:
Maximum failed login attempts before rate limiting:
5
(1 - 999)
Time between login attempts when rate limiting:
2
minutes (1 - 3000)
Include an AUP as link
Require acceptance
Allow guests to create their own accounts
Allow guests to reset the password
Allow social login
Allow guests to change password after login
Allow the following identity-provider guest portal to be used for login
There are no guest portals configured to use a SAML Id Provider as the Authentication Method.

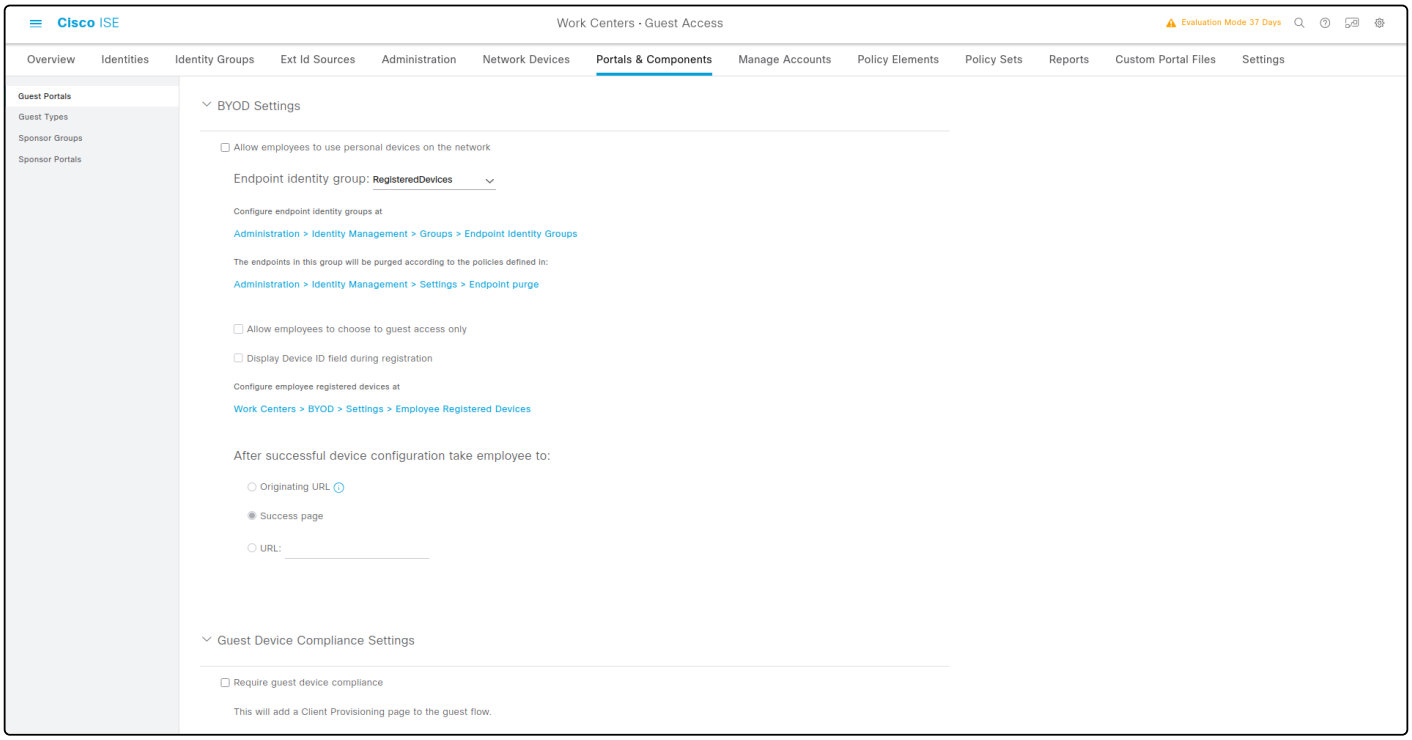

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Registration Form Settings
Assign to guest type Daily (default)
Configure guest types at:
Work Centers > Guest Access > Configure > Guest Types
Account valid for: 1 Days Maximum: 5 DAYS
Require a registration code
Fields to include
Required
User name
First name
Last name
Email address
Mobile number
Select the default country United States (+1)
Use Mobile number as username
Company
Location
Guests can choose from these locations to set their time zone:
San Jose
Guests see the locations list only if multiple locations are specified.
Configure guest locations at:
Work Centers > Guest Access > Settings > Guest Locations and SSIDs

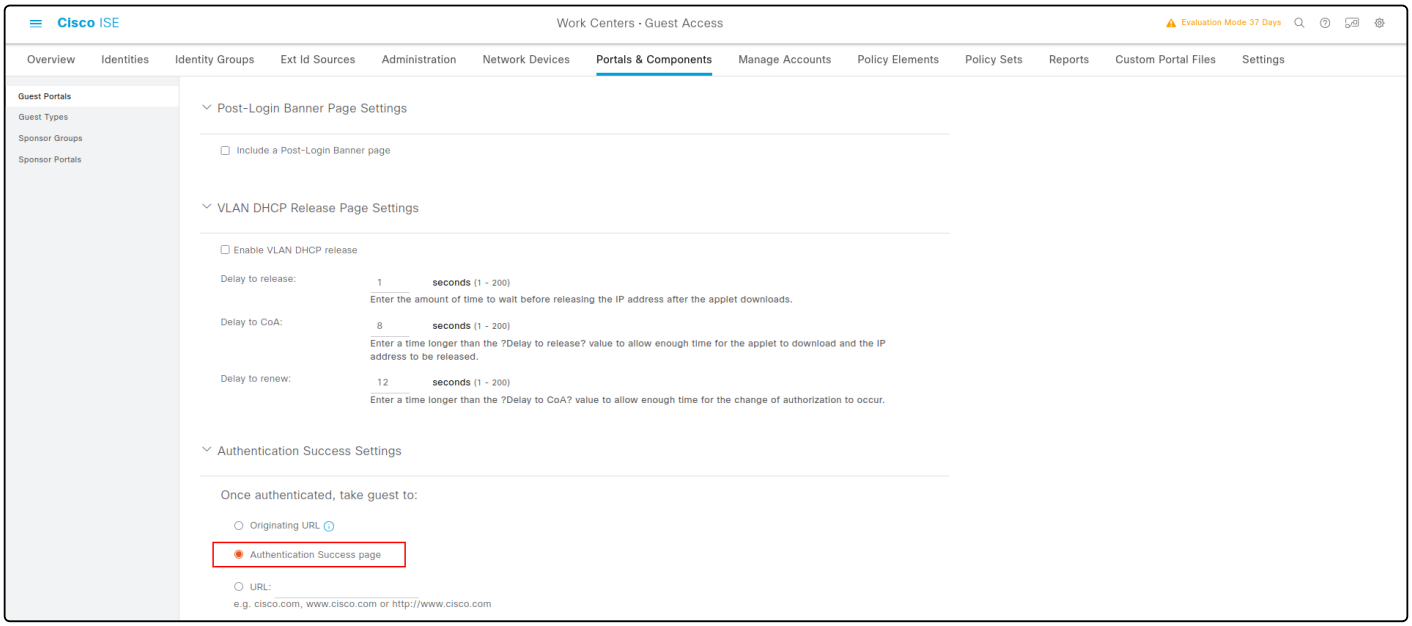

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
SMS Service Provider
Guests can choose from these SMS providers:
Global Default
T-Mobile
ATT
Verizon
ClickatellViaSMTP
Orange
Inmobile
TheRingRingCompany
Sprint
Guest see providers list only if multiple are selected
Configure SMS providers at:
Work Centers > Guest Access > Administration > SMS Gateway Providers
Person being visited
Reason for visit
Custom Fields...
Configure custom fields at:
Work Centers > Guest Access > Settings > Custom Fields
Include an AUP as link
Require acceptance
Only allow guests with an email address from:
Ex. example1.com, example2.com
Do not allow guests with an email address from:
Ex. example1.com, example2.com
Require guests to be approved

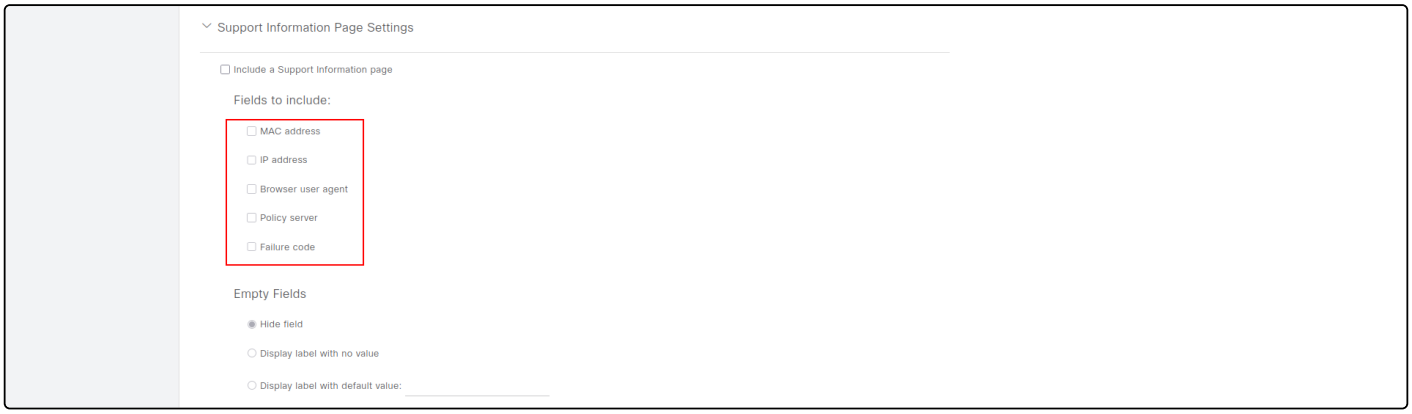

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
After submitting the guest form for self-registration, direct guest to
Self-Registration Success page
Login page with instructions about how to obtain login credentials
URL:
Send credential notification automatically using:
Email
SMS
Self-Registration Success Settings
Include this information on the Self-Registration Success page:
User name
Password
First name
Last name
Email address
Mobile number
Company
Location
SMS Service Provider
Person being visited
Reason for visit


Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Allow guest to send information to self using:
Print
Email
SMS
Include an AUP on page
Require acceptance
Require scrolling to end of AUP
Self-Registration Success Page continues to Login page by default.
Allow guests to log in directly from the Self-Registration Success page
Acceptable Use Policy (AUP) Page Settings
Include an AUP page
Use different AUP for employees
Skip AUP for employees
Require scrolling to end of AUP
Show AUP
On first login only
On every login
Every 7 days (starting at first login)

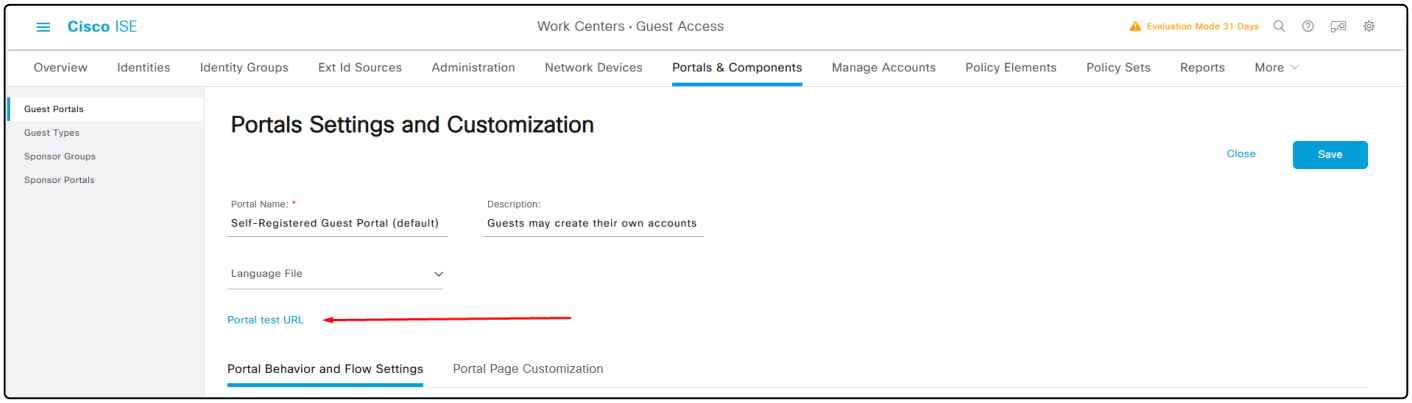

Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Guest Change Password Settings
Require guest to change password at first login (except guests using social login)
Configure your guest password policy at:
Work Centers > Guest Access > Settings > Guest Password Policy
Guest Device Registration Settings
Automatically register guest devices
A message displays to guests when they reach the maximum number of supported devices.
Allow guests to register devices
You can set the maximum number of supported devices in the guest type settings.
Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.
Configure guest types at:
Work Centers > Guest Access > Configure > Guest Types


Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
BYOD Settings
Allow employees to use personal devices on the network
Endpoint identity group: RegisteredDevices
Configure endpoint identity groups at
Administration > Identity Management > Groups > Endpoint Identity Groups
The endpoints in this group will be purged according to the policies defined in:
Administration > Identity Management > Settings > Endpoint purge
Allow employees to choose to guest access only
Display Device ID field during registration
Configure employee registered devices at
Work Centers > BYOD > Settings > Employee Registered Devices
After successful device configuration take employee to:
Originating URL
Success page
URL:
Guest Device Compliance Settings
Require guest device compliance
This will add a Client Provisioning page to the guest flow.


Cisco ISE
Work Centers · Guest Access
Evaluation Mode 37 Days
Overview
Identities
Identity Groups
Ext Id Sources
Administration
Network Devices
Portals & Components
Manage Accounts
Policy Elements
Policy Sets
Reports
Custom Portal Files
Settings
Guest Portals
Guest Types
Sponsor Groups
Sponsor Portals
Post-Login Banner Page Settings
Include a Post-Login Banner page
VLAN DHCP Release Page Settings
Enable VLAN DHCP release
Delay to release: 1 seconds (1 - 200)
Enter the amount of time to wait before releasing the IP address after the applet downloads.
Delay to CoA: 8 seconds (1 - 200)
Enter a time longer than the ?Delay to release? value to allow enough time for the applet to download and the IP address to be released.
Delay to renew: 12 seconds (1 - 200)
Enter a time longer than the ?Delay to CoA? value to allow enough time for the change of authorization to occur.
Authentication Success Settings
Once authenticated, take guest to:
Originating URL
Authentication Success page
URL:
e.g. cisco.com, www.cisco.com or http://www.cisco.com

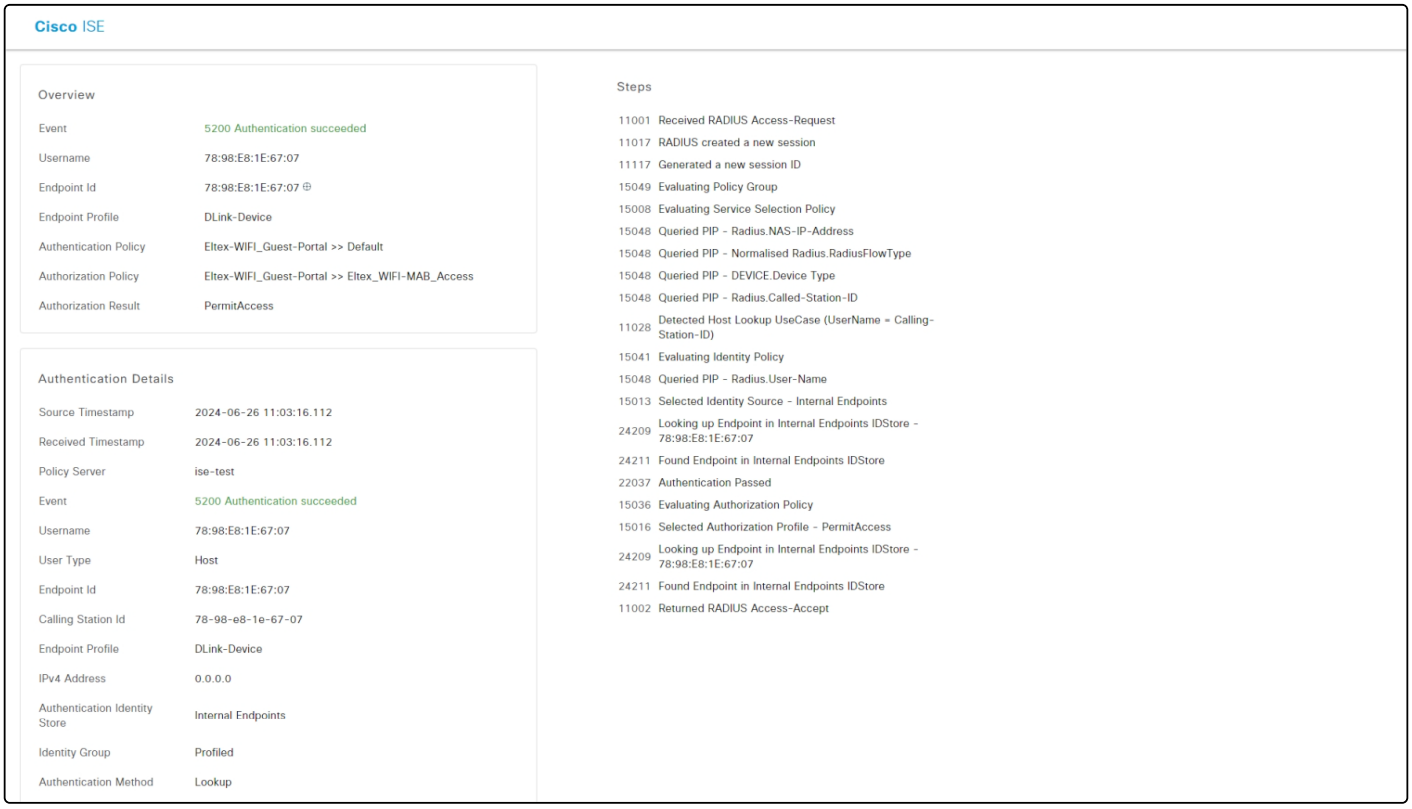

Support Information Page Settings
Include a Support Information page
Fields to include:
MAC address
IP address
Browser user agent
Policy server
Failure code
Empty Fields
Hide field
Display label with no value
Display label with default value:

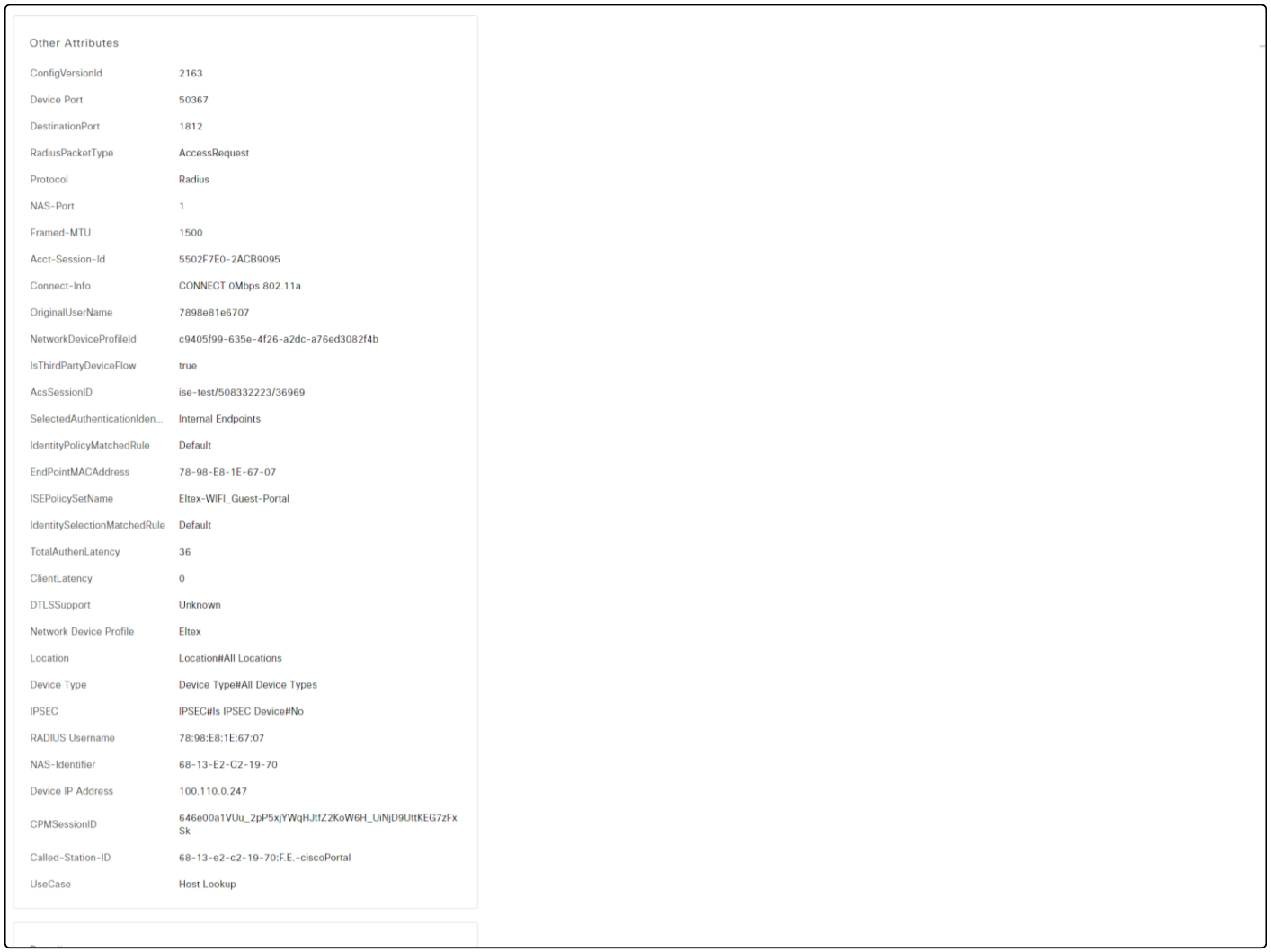
12. Адрес портала для настройки ссылки редиректа возможно получить по ссылке *Portal test URL:*



Отладочная информация RADIUS

В разделе Operations → RADIUS → Live Logs находится запись журнала с отладочной информацией RADIUS.

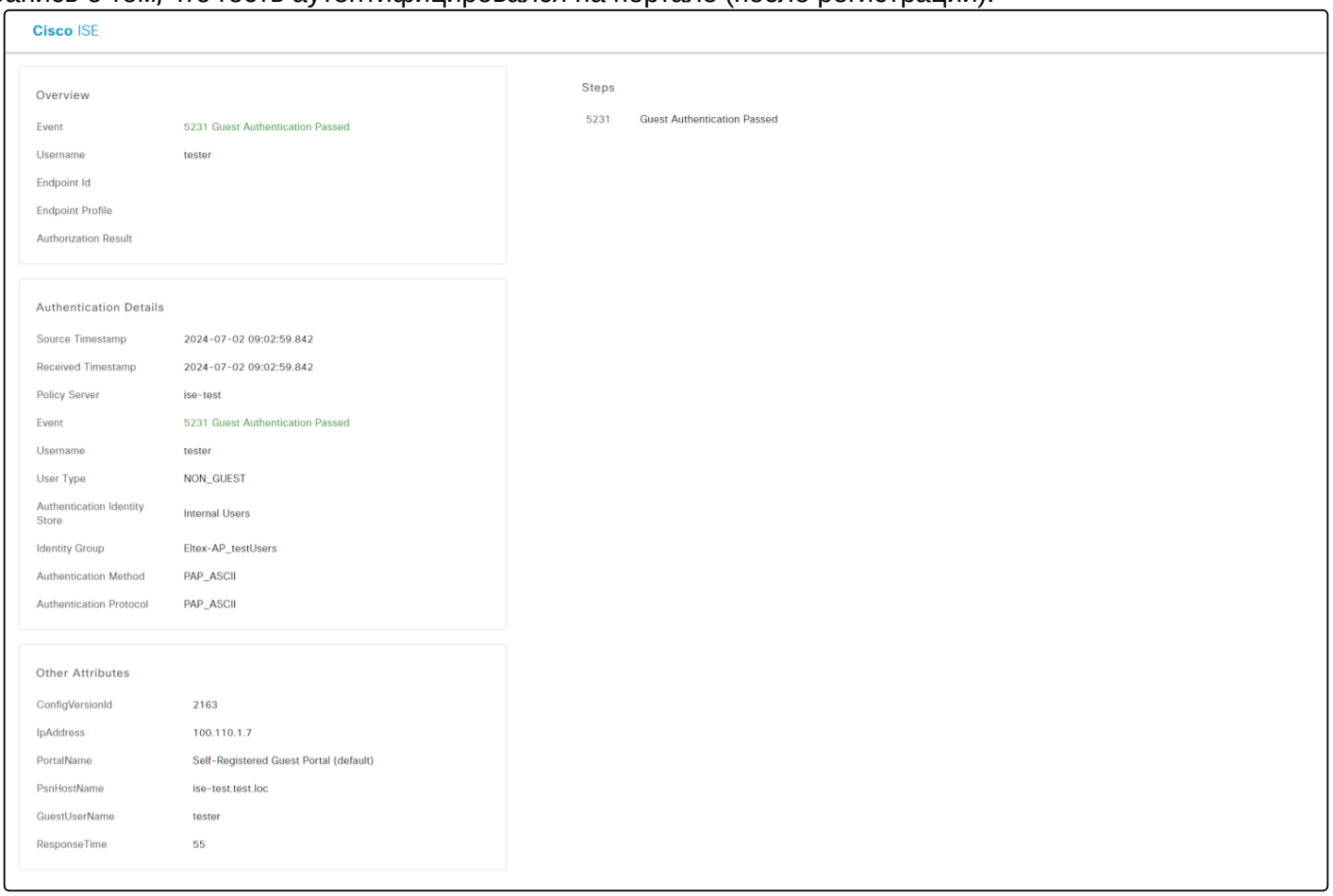




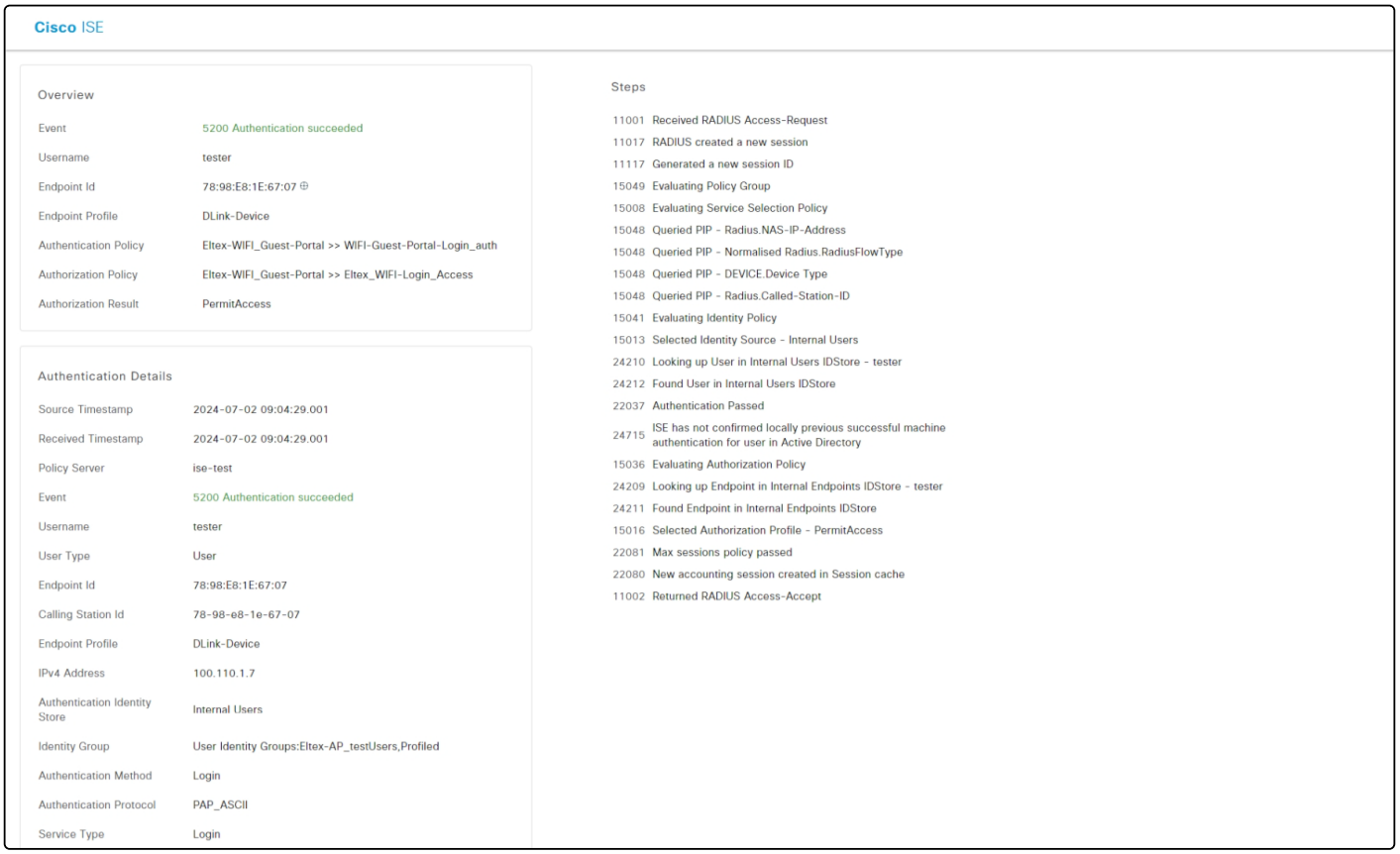
Other Attributes

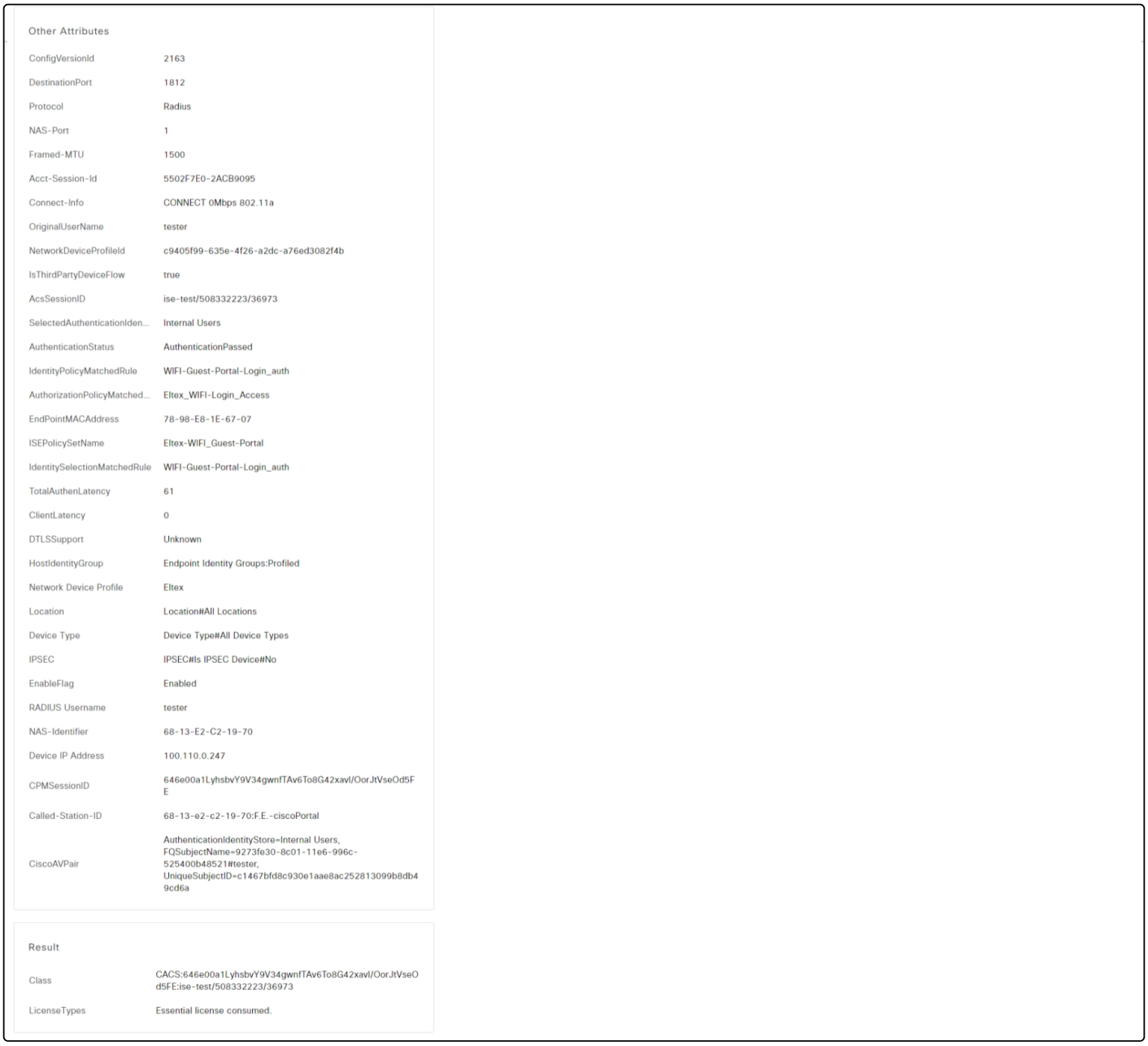
ConfigVersionId	2163
Device Port	50367
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	1
Framed-MTU	1500
Acct-Session-Id	5502F7E0-2ACB9095
Connect-Info	CONNECT 0Mbps 802.11a
OriginalUserName	7898e81e6707
NetworkDeviceProfileId	c9405f99-635e-4f26-a2dc-a76ed3082f4b
IsThirdPartyDeviceFlow	true
AcsSessionID	ise-test/508332223/36969
SelectedAuthenticationIden...	Internal Endpoints
IdentityPolicyMatchedRule	Default
EndPointMACAddress	78-98-E8-1E-67-07
ISEPolicySetName	Eltex-WIFI_Guest-Portal
IdentitySelectionMatchedRule	Default
TotalAuthenLatency	36
ClientLatency	0
DTLSSupport	Unknown
Network Device Profile	Eltex
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	78:98:E8:1E:67:07
NAS-Identifier	68-13-E2-C2-19-70
Device IP Address	100.110.0.247
CPMSessionID	646e00a1VUu_2pP5xjYWqHJtfZ2KoW6H_UiNjD9UttKEG7zFxSk
Called-Station-ID	68-13-e2-c2-19-70:F.E.-ciscoPortal
UseCase	Host Lookup

Запись о том, что гость аутентифицировался на портале (после регистрации).



Запись о том, что пользователь успешно аутентифицировался и авторизовался через RADIUS по логину и паролю.





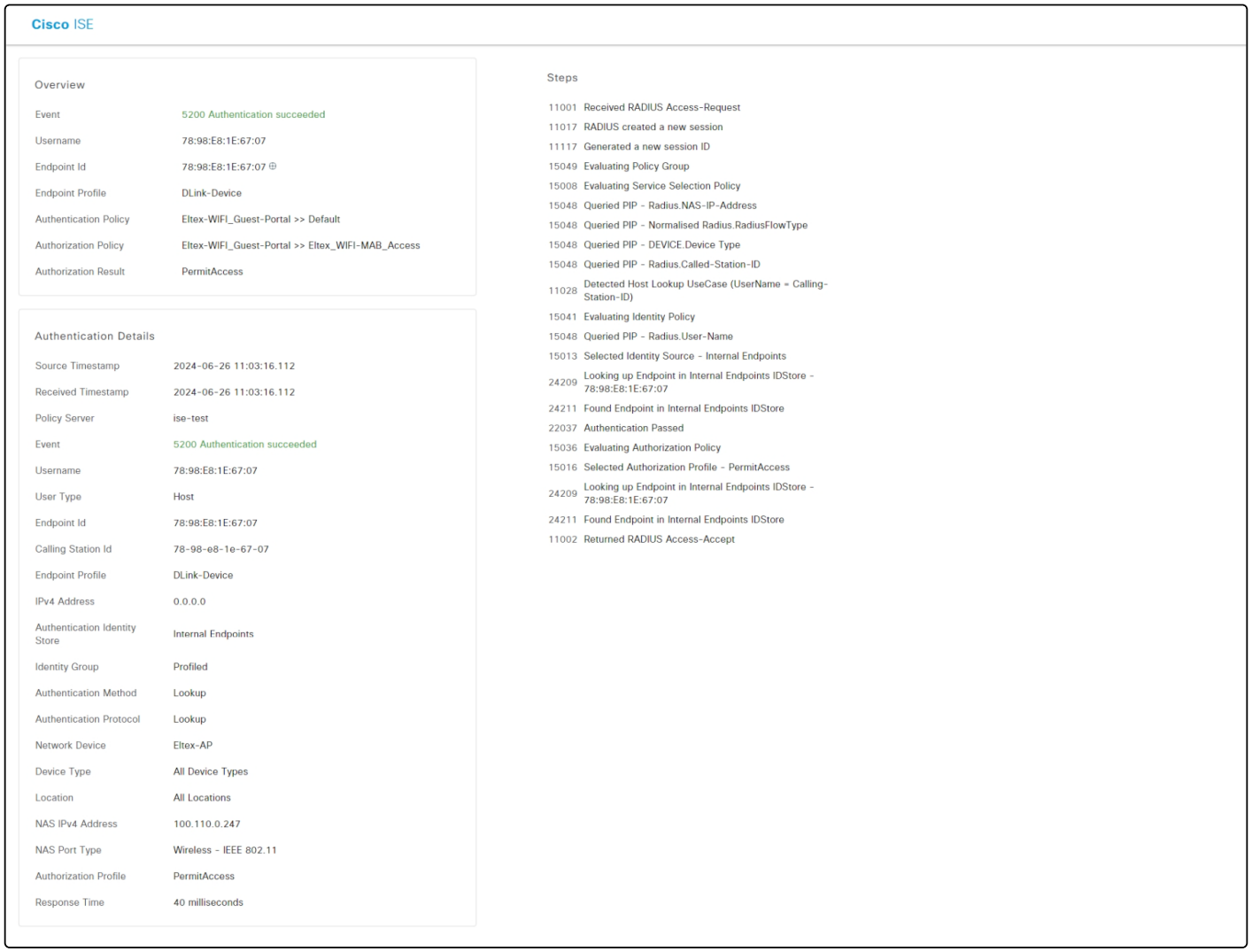
Other Attributes

ConfigVersionId	2163
DestinationPort	1812
Protocol	Radius
NAS-Port	1
Framed-MTU	1500
Acct-Session-Id	5502F7E0-2ACB9095
Connect-Info	CONNECT 0Mbps 802.11a
OriginalUserName	tester
NetworkDeviceProfileId	c9405f99-635e-4f26-a2dc-a76ed3082f4b
IsThirdPartyDeviceFlow	true
AcsSessionID	ise-test/508332223/36973
SelectedAuthenticationIden...	Internal Users
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	WIFI-Guest-Portal-Login_auth
AuthorizationPolicyMatched...	Eltex_WIFI-Login_Access
EndPointMACAddress	78-98-E8-1E-67-07
ISEPolicySetName	Eltex-WIFI_Guest-Portal
IdentitySelectionMatchedRule	WIFI-Guest-Portal-Login_auth
TotalAuthenLatency	61
ClientLatency	0
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled
Network Device Profile	Eltex
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
RADIUS Username	tester
NAS-Identifier	68-13-E2-C2-19-70
Device IP Address	100.110.0.247
CPMSessionID	646e00a1LyhsbvY9V34gwnfTAv6To8G42xavI/OorJtVseOd5FE
Called-Station-ID	68-13-e2-c2-19-70:F.E.-ciscoPortal
CiscoAVPair	AuthenticationIdentityStore=Internal Users, FQSubjectName=9273fe30-8c01-11e6-996c-525400b48521#tester, UniqueSubjectID=c1467bfd8c930e1aae8ac252813099b8db49cd6a

Result

Class	CACS:646e00a1LyhsbvY9V34gwnfTAv6To8G42xavI/OorJtVseOd5FE:ise-test/508332223/36973
LicenseTypes	Essential license consumed.

Запись о том, что клиент успешно прошел MAB-аутентификацию и авторизацию через RADIUS (Cisco ISE занесла MAC клиента в базу EndPoints при аутентификации пользователя на портале).


Cisco ISE
Overview
Event 5200 Authentication succeeded
Username 78:98:E8:1E:67:07
Endpoint Id 78:98:E8:1E:67:07
Endpoint Profile DLink-Device
Authentication Policy Eltex-WIFI_Guest-Portal >> Default
Authorization Policy Eltex-WIFI_Guest-Portal >> Eltex_WIFI-MAB_Access
Authorization Result PermitAccess
Authentication Details
Source Timestamp 2024-06-26 11:03:16.112
Received Timestamp 2024-06-26 11:03:16.112
Policy Server ise-test
Event 5200 Authentication succeeded
Username 78:98:E8:1E:67:07
User Type Host
Endpoint Id 78:98:E8:1E:67:07
Calling Station Id 78-98-e8-1e-67-07
Endpoint Profile DLink-Device
IPv4 Address 0.0.0.0
Authentication Identity Store Internal Endpoints
Identity Group Profiled
Authentication Method Lookup
Authentication Protocol Lookup
Network Device Eltex-AP
Device Type All Device Types
Location All Locations
NAS IPv4 Address 100.110.0.247
NAS Port Type Wireless - IEEE 802.11
Authorization Profile PermitAccess
Response Time 40 milliseconds
Steps
11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11117 Generated a new session ID
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Radius.NAS-IP-Address
15048 Queried PIP - Normalised Radius.RadiusFlowType
15048 Queried PIP - DEVICE.Device Type
15048 Queried PIP - Radius.Called-Station-ID
11028 Detected Host Lookup UseCase (UserName = Calling-Station-ID)
15041 Evaluating Identity Policy
15048 Queried PIP - Radius.User-Name
15013 Selected Identity Source - Internal Endpoints
24209 Looking up Endpoint in Internal Endpoints IDStore - 78:98:E8:1E:67:07
24211 Found Endpoint in Internal Endpoints IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15016 Selected Authorization Profile - PermitAccess
24209 Looking up Endpoint in Internal Endpoints IDStore - 78:98:E8:1E:67:07
24211 Found Endpoint in Internal Endpoints IDStore
11002 Returned RADIUS Access-Accept

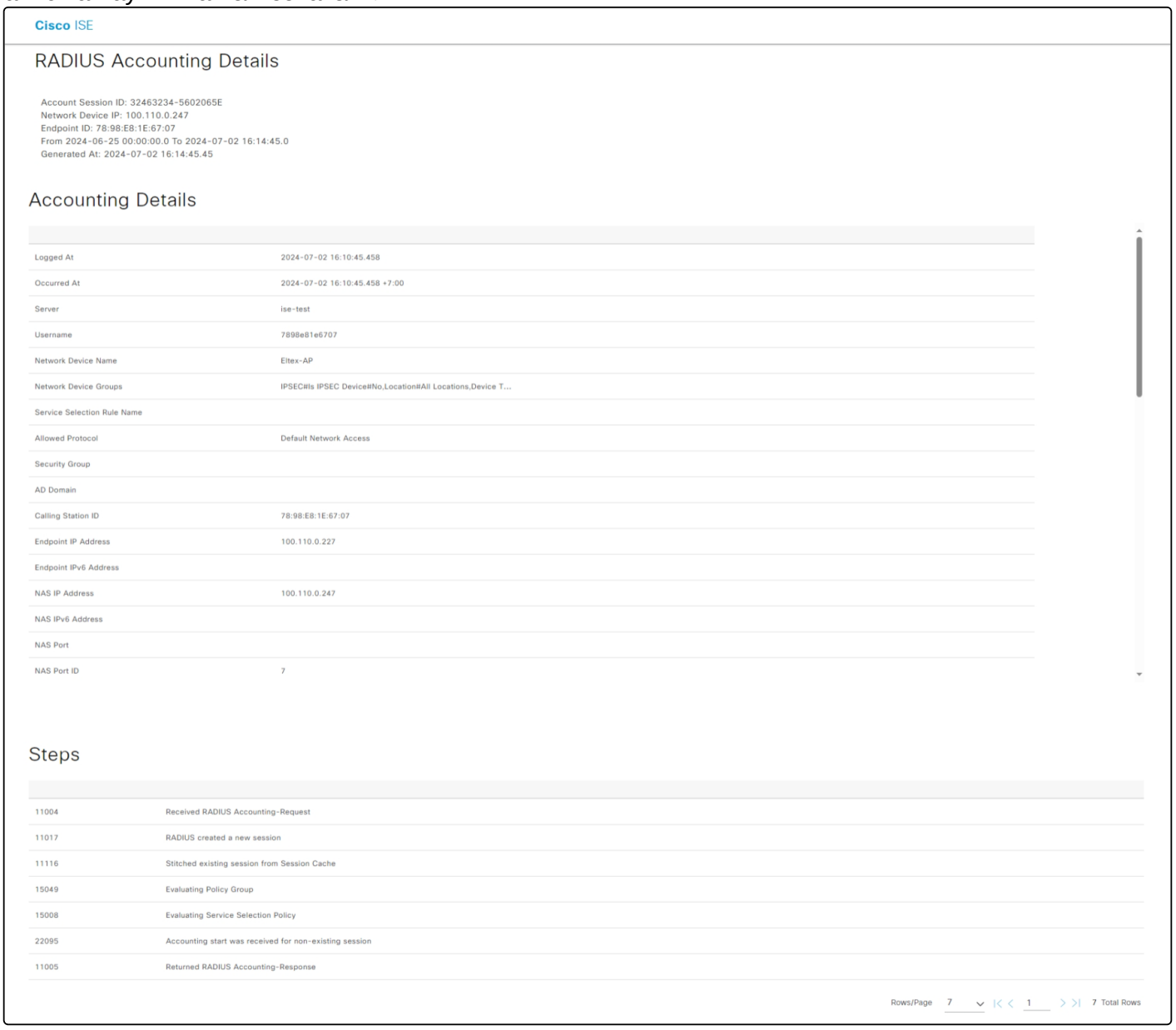
Other Attributes

ConfigVersionId	1022
DestinationPort	1812
Protocol	Radius
NAS-Port	1
Framed-MTU	1500
Acct-Session-Id	68104E6D-7D29B5A6
Connect-Info	CONNECT 0Mbps 802.11a
OriginalUserName	7898e81e6707
NetworkDeviceProfileId	c9405f99-635e-4f26-a2dc-a76ed3082f4b
IsThirdPartyDeviceFlow	true
AcsSessionID	ise-test/508332223/27787
SelectedAuthenticationIden...	Internal Endpoints
AuthenticationStatus	AuthenticationPassed
IdentityPolicyMatchedRule	Default
AuthorizationPolicyMatched...	Eltex_WIFI-MAB_Access
EndPointMACAddress	78-98-E8-1E-67-07
ISEPolicySetName	Eltex-WIFI_Guest-Portal
IdentitySelectionMatchedRule	Default
TotalAuthenLatency	40
ClientLatency	0
DTLSSupport	Unknown
HostIdentityGroup	Endpoint Identity Groups:Profiled
Network Device Profile	Eltex
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	78:98:E8:1E:67:07
NAS-Identifier	68-13-E2-C2-19-70
Device IP Address	100.110.0.247
CPMSessionID	646e00a1xeGwhVnVY9w6deE1KQDIVjVIb1o7_tQDHS03mvJmLDY
Called-Station-ID	68-13-e2-c2-19-70:F.E.-ciscoPortal
CiscoAVPair	AuthenticationIdentityStore=Internal Endpoints
UseCase	Host Lookup

Result

UserName	78:98:E8:1E:67:07
User-Name	78-98-E8-1E-67-07
Class	CACS:646e00a1xeGwhVnVY9w6deE1KQDIVjVIb1o7_tQDHS03mvJmLDY:ise-test/508332223/27787
LicenseTypes	Essential license consumed.

Запись аккаунтинга пользователя:



23.11.2 Авторизация через NeTAMS WNAM

- Описание
- Задача
- Решение
- Лицензирование
- Взаимодействие элементов системы
- Конфигурирование WLC
  - Полная конфигурация WLC
- Конфигурация WNAM
  - Создание сервера
  - Создание площадки
  - Создание группы ваучеров
  - Конфигурирование правил аутентификации
- Отладочная информация Netams WNAM
  - Логирование работы правил авторизации
  - Информация о ваучерах

- Информация о клиентах Wi-Fi
- Расположение логов

Описание

Система Netams WNAM будет рассмотрена для портальной авторизации пользователей Wi-Fi.

> Взаимодействие системы авторизации Netams WNAM с контроллеромы WLC/ESR доступна на WLC/ESR-15/30/3200, vWLC, начиная с версии WNAM 1.6.4010.

В данной статье рассмотрен пример настройки авторизации клиента через гостевой портал путем идентификации по коду ваучера. Другие способы гостевой авторизации выходят за рамки данной статьи, так как взаимодействие между системой WNAM и BRAS WLC не изменяется.

Перед началом построения взаимодействия между Netams WNAM и WLC необходимо настроить и протестировать работу беспроводной сети и контроллера WLC без портальной авторизации и сетевого экрана. Если беспроводная сеть функционирует корректно, можно приступать к настройки портальной авторизации.

В данной статье используется подключение ТД к контроллеру WLC на основе сети L3 с построением Data SoftGRE-туннеля. В статье Настройка WLC детально описана настройка данной схемы подключения.

Рекомендуется ознакомиться с тонкостями настройки BRAS на ESR/WLC с портальной авторизацией на основе SoftWLC в следующих статьях:

- BRAS/BRAS в vrf. L3 WiFi - руководство по настройке с резервированием
- BRAS. L2 WiFi - руководство по настройке и быстрому запуску
- BRAS. Troubleshooting Guide

Задача

Настроить портальную авторизацию через контроллер WLC с порталом WNAM.

- Контроллер WLC имеет адреса:
  - из сети WNAM: 100.110.0.246/23 (Vlan 2);
  - из сети управления ТД: 192.168.1.1/24 (Bridge 1, Vlan 1);
  - из сети клиентов ТД с портальной авторизацией: 192.168.3.1/24 (Bridge 3, Vlan 3).
- Сервер авторизации WNAM имеет адрес: 100.110.1.44/23 (Vlan 2);
- Точка доступа подключена к WLC. Получает адрес контроллера и терминации GRE-туннеля в 43 опции из пула DHCP, настроенного на WLC из сети: 192.168.1.0/24 (Vlan 1);
- Клиенты получают адреса из пула DHCP, настроенного на WLC из сети: 192.168.2.0/24 (Vlan 3).
- Сервис для доступа в Интернет после авторизации на портале имеет имя: INTERNET.

Решение

Настройка будет выполнена на базе заводской конфигурации (Factory).

Шаги выполнения:

1. Конфигурирование WLC:
   a. Конфигурация *object-group* – группы адресов для NAT, неавторизованных пользователей, url-адрес для перенаправления авторизации, адрес WNAM-сервера;
   b. Конфигурация *bridge* – для сетевой связности;
   c. Конфигурация *vlan*;
   d. Конфигурация *ACL* – для ограничения доступа к сети неавторизованных (до авторизации) и авторизованных клиентов (после авторизации);

e. Конфигурация *RADIUS* – для взаимодействия WLC и WNAM;
f. Конфигурация *NAT* – для доступа в интернет Wi-Fi клиентам;
g. Конфигурация *security zone* – для разрешения редиректа запросов неавторизованных клиентов на WNAM;
h. Конфигурация *SSID* – для подключения клиентов;
i. Конфигурация *subscriber-control* – для пересылки неавторизованных клиентов на WNAM.

2. Конфигурирование WNAM:
   a. Создание сервера;
   b. Создание площадки;
   c. Создание группы ваучеров;
   d. Конфигурирование правил аутентификации;
   e. Конфигурирование правил авторизации.

Лицензирование

Для конфигурации взаимодействия **Netams WNAM** и **WLC** необходима лицензия BRAS для WLC.

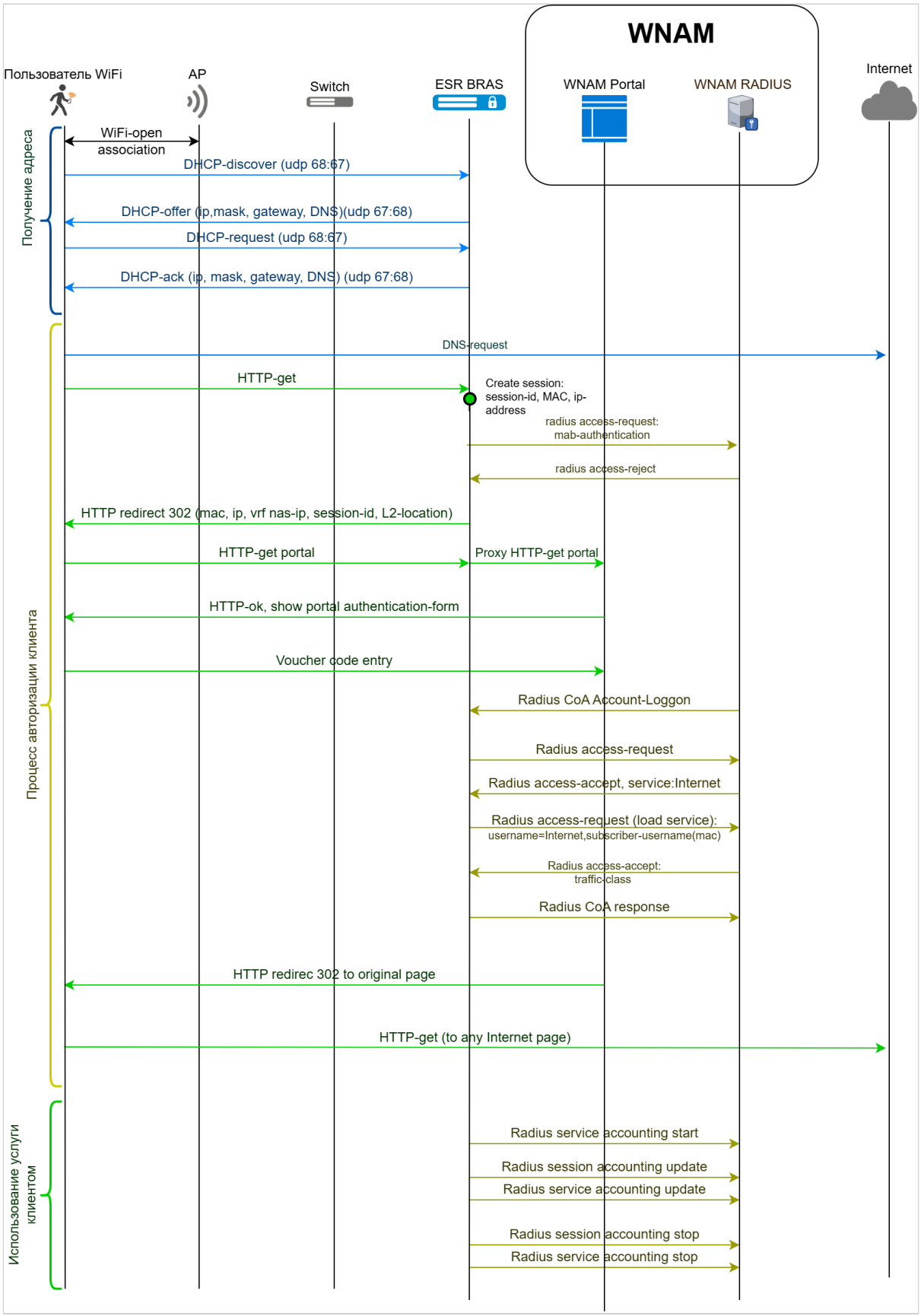
Детальнее о том, как установить и применить лицензию описано в статье Активация функционала по лицензии.

Проверить наличие лицензии можно с помощью команды **show licence**:

show licence

```
wlc# show licence
Feature                          Source     State         Value
Valid from             Expiries
---------------------------------   --------   -----------   ---------------------------------
--------------------   ---------------------
BRAS                             File       Active        true
--                     --
BRAS                             File       Candidate     true
--                     --
WLC                              Boot       Active        true
--                     --
WLC                              Boot       Candidate     true
--                     --
```

Взаимодействие элементов системы



Конфигурирование WLC

1. Конфигурация *object-group*:
   Перейдите в конфигурационный режим:

```
wlc# configure
wlc(config)#
```

   Создайте группу wnam_servers для последующего создания профиля RADIUS:

```
wlc(config)# object-group network wnam_servers
```

   Добавьте адрес WNAM-сервера:

```
wlc(config-object-group-network)#  ip address-range 100.110.1.44
wlc(config-object-group-network)#  exit
```

   Создайте группу *bras_users*:

```
wlc(config)# object-group network bras_users
```

   Добавьте пул адресов клиентов, которые будут попадать в авторизацию через портал (Bridge 1, Vlan 1):

```
wlc(config-object-group-network)# ip address-range 192.168.2.2-192.168.2.254
wlc(config-object-group-network)# exit
```

   Создайте группу *local*:

```
wlc(config)# object-group network local
```

   Добавьте пул адресов из сети клиентов, которые будут получать доступ в интернет через NAT:

```
wlc(config-object-group-network)# ip address-range 192.168.2.1-192.168.2.254
wlc(config-object-group-network)# exit
```

   Создайте группу *defaultService*:

```
wlc(config)# object-group url defaultService
```

   Добавьте url с адресом WNAM-сервера для работы правила фильтрации авторизации пользователей:

```
wlc(config-object-group-url)# http://100.110.1.44
wlc(config-object-group-url)# exit
```

   Создайте группу *redirect*:

```
wlc(config)# object-group service redirect
```

   Добавьте пул портов для прослушивания http/https-трафика:

```
wlc(config-object-group-service)# port-range 3128-3135
```

```
wlc(config-object-group-service)# exit
```

Слушающий порт прокси (HTTP/HTTPS) будет открыт для каждого ядра WLC/ESR. Порты HTTP начинаются с порта 3128.
На WLC-15/30 4 ядра, нужно разрешить порты для HTTP 3128-3131, для HTTPS 3132-3135.
На WLC-3200 24 ядра, нужно разрешить порты для HTTP 3128-3151, для HTTPS 3152-3175.

Полная конфигурация object-group:

```
object-group network wnam_servers
  ip address-range 100.110.1.44
exit
object-group network bras_users
  ip address-range 192.168.2.2-192.168.2.254
exit
object-group network local
  ip address-range 192.168.2.1-192.168.2.254
exit
object-group url defaultService
  url http://100.110.1.44
exit
object-group service redirect
  port-range 3128-3135
exit
```

2. Конфигурация Bridge:
   Конфигурация Bridge для uplink:

```
wlc(config)# bridge 2
```

Пропишите ip-адрес для связности с сервером WNAM:

```
wlc(config-bridge)# ip address 100.110.0.246/23
wlc(config-bridge)# exit
```

Конфигурация *Bridge* для пользователей:

```
wlc(config)# bridge 3
```

Добавьте *location*, по нему сервер WNAM определит площадку для неавторизованных клиентов:

```
wlc(config-bridge)# location data10
wlc(config-bridge)# exit
```

Полная конфигурация *Bridge*:

```
bridge 1
  vlan 1
  description "MGMT-AP"
  security-zone trusted
  ip address 192.168.1.1/24
  no spanning-tree
  enable
exit
bridge 2
  vlan 2
```

```
  description "UPLINK"
  security-zone untrusted
  ip address 100.110.0.246/23
  no spanning-tree
  enable
exit
bridge 3
  description "BRAS-users"
  vlan 3
  mtu 1458
  history statistics
  security-zone users
  ip address 192.168.2.1/24
  no spanning-tree
  location data10
  enable
exit
```

3. Конфигурация *Vlan*:
   Конфигурация клиентского Vlan 3 (Bridge 3):

```
wlc(config)# vlan 3
```

   Добавьте параметр force-up, который переводит Vlan в режим постоянного статуса UP:

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

   Полная конфигурация Vlan:

```
vlan 3
  force-up
exit
```

4. Настройка списков контроля доступа:
   Создайте список контроля доступа для ограничения неавторизованных пользователей в сети. Список разрешает прохождение DNS- и DHCP-трафика:

```
wlc(config-acl)# ip access-list extended BYPASS
```

   Создайте правило с номером 10, это правило отвечает за разрешение получение адреса по протоколу DHCP неавторизованным клиентам:

```
wlc(config-acl)# rule 10
```

   Добавьте действие правила – разрешение:

```
wlc(config-acl-rule)# action permit
```

   Добавьте совпадение по протоколу udp:

```
wlc(config-acl-rule)# match protocol udp
```

   Добавьте совпадение по порту источника:

```
wlc(config-acl-rule)# match source-port 68
```

Добавьте совпадение по порту назначения:

```
wlc(config-acl-rule)# match destination-port 67
```

Включите правило:

```
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
```

Создайте правило под номером 11, оно отвечает за разрешение DNS-запросов неавторизованных клиентов:

```
wlc(config-acl)# rule 11
```

Добавьте действие правило – разрешение:

```
wlc(config-acl-rule)# action permit
```

Добавьте совпадение по протоколу udp:

```
wlc(config-acl-rule)# match protocol udp
```

Добавьте совпадение по порту назначения 53:

```
wlc(config-acl-rule)# match destionation-port 53
```

Включите правило:

```
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# exit
```

Создайте список контроля доступа, который будет применяться после авторизации клиента, он разрешит полный доступ:
Создание списка:

```
wlc(config)# ip access-list extended INTERNET
```

Создайте правило с номером 10, которое разрешает все:

```
wlc(config-acl)# rule 10
```

Добавьте действие правила – разрешение:

```
wlc(config-acl-rule)# action permit
```

Включите правило:

```
wlc(config-acl-rule)# enable
wlc(config-acl-rule)# exit
wlc(config-acl)# exit
```

Полная конфигурация списков контроля доступа:

```
ip access-list extended BYPASS
  rule 10
    action permit
    match protocol udp
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 11
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit
ip access-list extended INTERNET
  rule 10
    action permit
    enable
  exit
exit
```

5. Настройка RADIUS:
   Добавьте RADIUS-сервер с адресом WNAM:

```
wlc(config)# radius-server host 100.110.1.44
```

Укажите ключ для взаимодействия:

```
wlc(config-radius-server)# key ascii-text wnampass
```

Укажите адрес источник (*Bridge 2*):

```
wlc(config-radius-server)# source-address 100.110.0.246
wlc(config-radius-server)# exit
```

Создайте *AAA*-профиль с адресом WNAM-сервера:

```
wlc(config)# aaa radius-profile bras_radius
```

Укажите адрес WNAM-сервера:

```
wlc(config-aaa-radius-profile)# radius-server host 100.110.1.44
wlc(config-aaa-radius-profile)# exit
```

Создайте сервер DAS:

```
wlc(config)# das-server das
```

Укажите ключ:

```
wlc(config-das-server)# key ascii-text wnampass
```

Укажите порт:

```
wlc(config-das-server)# port 3799
```

Добавьте object-group, в которой указан адрес сервера WNAM, запросы с адресов из группы *wnam_servers* поступят в обработку, остальные будут отброшены:

```
wlc(config-das-server)# clients object-group wnam_servers
wlc(config-das-server)# exit
```

Создайте AAA-профиль для DAS-сервера:

```
wlc(config)# aaa das-profile bras_das
```

Укажите имя DAS-сервера, которое создали ранее:

```
wlc(config-aaa-das-server)# das-server das
wlc(config-aaa-das-server)# exit
```

Полная конфигурация RADIUS:

```
radius-server host 100.110.1.44
  key ascii-text wnampass
  source-address 100.110.0.246
exit
aaa radius-profile bras_radius
  radius-server host 100.110.1.44
exit

das-server das
  key ascii-text wnampass
  port 3799
  clients object-group wnam_servers
exit
aaa das-profile bras_das
  das-server das
exit
```

6. Настройка NAT:
   Перейдите в блок конфигурации NAT:

```
wlc(config)# nat source
```

Создайте пул, в котором указывается адрес для подмены:

```
wlc(config-snat)# pool translate
```

Укажите адрес (Bridge 2):

```
wlc(config-snat-pool)# ip address-range 100.110.0.246
wlc(config-snat-pool)# exit
```

Создайте список правил:

```
wlc(config-snat)# ruleset SNAT
```

Укажите внешний интерфейс, в котором будет происходить трансляция адресов:

```
wlc(config-snat-ruleset)# to interface gigabitethernet 1/0/1
```

Создайте правило с номером 1:

```
wlc(config-snat-ruleset)# rule 1
```

Добавьте совпадение по адресу источника, в качестве которого выступает object-group с пулом адресов клиентов:

```
wlc(config-snat-rule)# match source-address object-group local
```

Укажите действие правила – преобразование адресов источника в адрес, указанный в пуле translate:

```
wlc(config-snat-rule)# action source-nat pool translate
```

Включите правило:

```
wlc(config-snat-rule)# enable
wlc(config-snat-rule)# exit
wlc(config-snat-ruleset)# exit
wlc(config-snat)# exit
```

Полная конфигурация NAT:

```
nat source
  pool translate
    ip address-range 100.110.0.246
  exit
  ruleset SNAT
    to interface gigabitethernet 1/0/1
    rule 1
      match source-address object-group local
      action source-nat pool translate
      enable
    exit
  exit
exit
```

7. Конфигурация *security zone-pair*:
Перейдите в блок security zone-pair users self, чтобы открыть http/https-порты в файрволле для клиентов:

```
wlc(config)# security zone-pair users self
```

Добавьте правило с номером 50:

```
wlc(config-security-zone-pair)# rule 50
```

Укажите действие для правила – разрешение:

```
wlc(config-security-zone-pair-rule)# action permit
```

Добавьте совпадение по протоколу tcp:

```
wlc(config-security-zone-pair-rule)# match protocol tcp
```

Добавьте совпадение по пулу портов в object-group:

```
wlc(config-security-zone-pair-rule)# match destionation-port object-group redirect
```

Включите правило:

```
wlc(config-security-zone-pair-rule)# enable
wlc(config-security-zone-pair-rule)# exit
wlc(config-security-zone)# exit
```

Полная конфигурация *security zone-pair*:

```
security zone-pair trusted untrusted
  rule 1
    action permit
    enable
  exit
exit
security zone-pair trusted trusted
  rule 1
    action permit
    enable
  exit
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 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
  rule 50
    action permit
    match protocol tcp
    match destination-port object-group redirect
    enable
  exit
exit
security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit
```

8. Настройка SSID:
   Перейдите в раздел конфигурации WLC

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

Перейдите в конфигурацию SSID:

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

Укажите имя SSID, которое будет вещаться для клиентов:

```
wlc(config-wlc-ssid)# ssid F.E.freeSSID
wlc(config-wlc-ssid)# exit
wlc(config-wlc)# exit
```

Полная конфигурация SSID:

```
wlc
  ssid-profile test-ssid
    description F.E.free
    ssid F.E.freeSSID
    vlan-id 3
    802.11kv
    band 2g
    band 5g
    enable
  exit
exit
```

9. Включение *ssid-profile* в локацию:
   Включите созданный SSID в локацию. ТД получит конфигурацию и начнёт вещать данные SSID. В примере ниже *ssid-profile* включен в локацию *default-location*.

```
ap-location default-location
  ssid-profile test-ssid
exit
```

10. Конфигурация редиректа клиентов:
    Перейдите в блок настроек редиректа:

```
wlc(config)# subscriber-control
```

Добавьте профиль AAA das-сервера:

```
wlc(config-subscriber-control)# aaa das-profile bras_das
```

Добавьте профиль AAA RADIUS для создания сессий:

```
wlc(config-subscriber-control)# aaa sessions-radius-profile bras_radius
```

Добавьте профиль AAA RADIUS для доступа к сервисам:

```
wlc(config-subscriber-control)# aaa services-radius-profile bras_radius
```

Укажите внешний IP WLC (Bridge 2), который будет выступать атрибутом NAS-IP-Address в RADIUS-запросах на WNAM:

```
wlc(config-subscriber-control)# nas-ip-address 100.110.0.246
```

Включите аутентификацию сессий по mac-адресам:

```
wlc(config-subscriber-control)# session mac-authentication
```

Укажите список контроля доступа для неавторизованных клиентов:

```
wlc(config-subscriber-control)# bypass-traffic-acl BYPASS
```

Перейдите в блок конфигурации сервиса:

```
wlc(config-subscriber-control)# default-service
```

Укажите список контроля доступа, который будет применяться для неавторизованных клиентов:

```
wlc(config-subscriber-default-service)# class-map BYPASS
```

Укажите локальный белый список URL, доступ к этим адресам по протоколам HTTP/HTTPS будет работать до авторизации:

```
wlc(config-subscriber-default-service)# filter-name local defaultService
```

Укажите действие сервиса – разрешить:

```
wlc(config-subscriber-default-service)# filter-action permit
```

Укажите url-адрес, куда будут перенаправляться неавторизованные клиенты:

```
wlc(config-subscriber-default-service)# default-action redirect http://100.110.1.44/cp/
eltexwlc
```

Укажите время таймаута сессии:

```
wlc(config-subscriber-default-service)# session-timeout 600
wlc(config-subscriber-default-service)# exit
```

Включите работу редиректа:

```
wlc(config-subscriber-control)# enable
wlc(config-subscriber-control)# exit
```

Полная конфигурация настроек редиректа:

```
subscriber-control
  aaa das-profile bras_das
  aaa sessions-radius-profile bras_radius
  aaa services-radius-profile bras_radius
  nas-ip-address 100.110.0.246
  session mac-authentication
  bypass-traffic-acl BYPASS
  default-service
    class-map BYPASS
    filter-name local defaultService
    filter-action permit
    default-action redirect http://100.110.1.44/cp/eltexwlc
    session-timeout 600
  exit
  enable
exit
```

При конфигурации **default-action redirect** всегда используется шаблон "http://<address WNAM>/cp/eltexwlc", где <address WNAM> сетевой адрес сервера **Netams WNAM**.
В случае указания другого url авторизация работать не будет.

Полная конфигурация WLC

```
#!/usr/bin/clish
#260
#1.26.1
#06/08/2024
#17:35:15
hostname wlc

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 https
  port-range 443
exit
object-group service redirect
  port-range 3128-3131
exit

object-group network wnam_servers
  ip address-range 100.110.1.44
exit
object-group network bras_users
  ip address-range 192.168.2.2-192.168.2.254
exit
object-group network local
  ip address-range 192.168.2.1-192.168.2.254
exit
exit
object-group url defaultService
  url http://100.110.1.44
exit

syslog max-files 3
syslog file-size 512
syslog sequence-numbers
syslog file tmpsys:syslog/default
  severity info
exit

radius-server local
  nas ap
    key ascii-text encrypted testing123
    network 192.168.1.0/24
  exit
  nas local
    key ascii-text encrypted testing123
    network 127.0.0.1/32
  exit
  domain default
    user admin
      password ascii-text encrypted admin
    exit
    user test
      password ascii-text encrypted test
```

```
    exit
  exit
  virtual-server default
    enable
  exit
  enable
exit
username admin
  password encrypted password
exit

radius-server host 100.110.1.44
  key ascii-text encrypted wnampass
  source-address 100.110.0.246
exit
radius-server host 127.0.0.1
  key ascii-text encrypted testing123
exit
aaa radius-profile bras_radius
  radius-server host 100.110.1.44
exit
aaa radius-profile default_radius
  radius-server host 127.0.0.1
exit

das-server das
  key ascii-text encrypted wnampass
  port 3799
  clients object-group wnam_servers
exit
aaa das-profile bras_das
  das-server das
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
security zone dmz
exit

ip access-list extended BYPASS
  rule 10
    action permit
    match protocol udp
```

```
    match source-port 68
    match destination-port 67
    enable
  exit
  rule 11
    action permit
    match protocol udp
    match destination-port 53
    enable
  exit
exit
ip access-list extended INTERNET
  rule 10
    action permit
    enable
  exit
exit

subscriber-control
  aaa das-profile bras_das
  aaa sessions-radius-profile bras_radius
  aaa services-radius-profile bras_radius
  nas-ip-address 100.110.0.246
  session mac-authentication
  bypass-traffic-acl BYPASS
  default-service
    class-map BYPASS
    filter-name local defaultService
    filter-action permit
    default-action redirect http://100.110.1.44/cp/eltexwlc
    session-timeout 600
  exit
  enable
exit

bridge 1
  vlan 1
  description "MGMT-AP"
  security-zone trusted
  ip address 192.168.1.1/24
  no spanning-tree
  enable
exit
bridge 2
  vlan 2
  description "UPLINK"
  security-zone untrusted
  ip address 100.110.0.246/23
  no spanning-tree
  enable
exit
bridge 3
  description "BRAS-users"
  vlan 3
  mtu 1458
  security-zone users
  ip address 192.168.2.1/24
  no spanning-tree
  location data10
  enable
exit
```

```
interface gigabitethernet 1/0/1
  description "UPLINK"
  mode switchport
  switchport access vlan 2
exit
interface gigabitethernet 1/0/2
  description "AP-MGMT"
  mode switchport
exit
interface gigabitethernet 1/0/3
  mode switchport
exit
interface gigabitethernet 1/0/4
  lldp receive
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
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
  rule 10
    action permit
    match protocol tcp
    match destination-port object-group ssh
```

```
    enable
  exit
  rule 20
    action permit
    match protocol tcp
    match destination-port object-group http
    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
  rule 50
    action permit
    match protocol tcp
    match destination-port object-group redirect
    enable
  exit
exit
security zone-pair users untrusted
  rule 1
    action permit
    enable
  exit
exit

security passwords default-expired

nat source
  pool translate
    ip address-range 100.110.0.246
  exit
  ruleset factory
    to zone untrusted
    rule 10
      description "replace 'source ip' by outgoing interface ip address"
      action source-nat interface
      enable
    exit
```

```
  exit
  ruleset SNAT
    to interface gigabitethernet 1/0/1
    rule 1
      match source-address object-group local
      action source-nat pool translate
      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

ip route 0.0.0.0/0 100.110.0.1

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
    ssid-profile default-ssid
  exit
  ssid-profile default-ssid
    description F.E.free
    ssid F.E.freeSSID
    vlan-id 3
    802.11kv
    band 2g
```

```
    band 5g
    enable
  exit
  ap-profile default-ap
    password ascii-text encrypted testing123
    services
      ip ssh server
      ip http server
    exit
  exit
  radius-profile default-radius
    auth-address 192.168.1.1
    auth-password ascii-text encrypted testing123
    domain default
  exit
  ip-pool default-ip-pool
    description default-ip-pool
    ap-location default-location
  exit
  enable
exit

ip ssh server

clock timezone gmt +7

ntp enable
ntp broadcast-client enable
ntp server 194.190.168.1
exit

ip https server
```

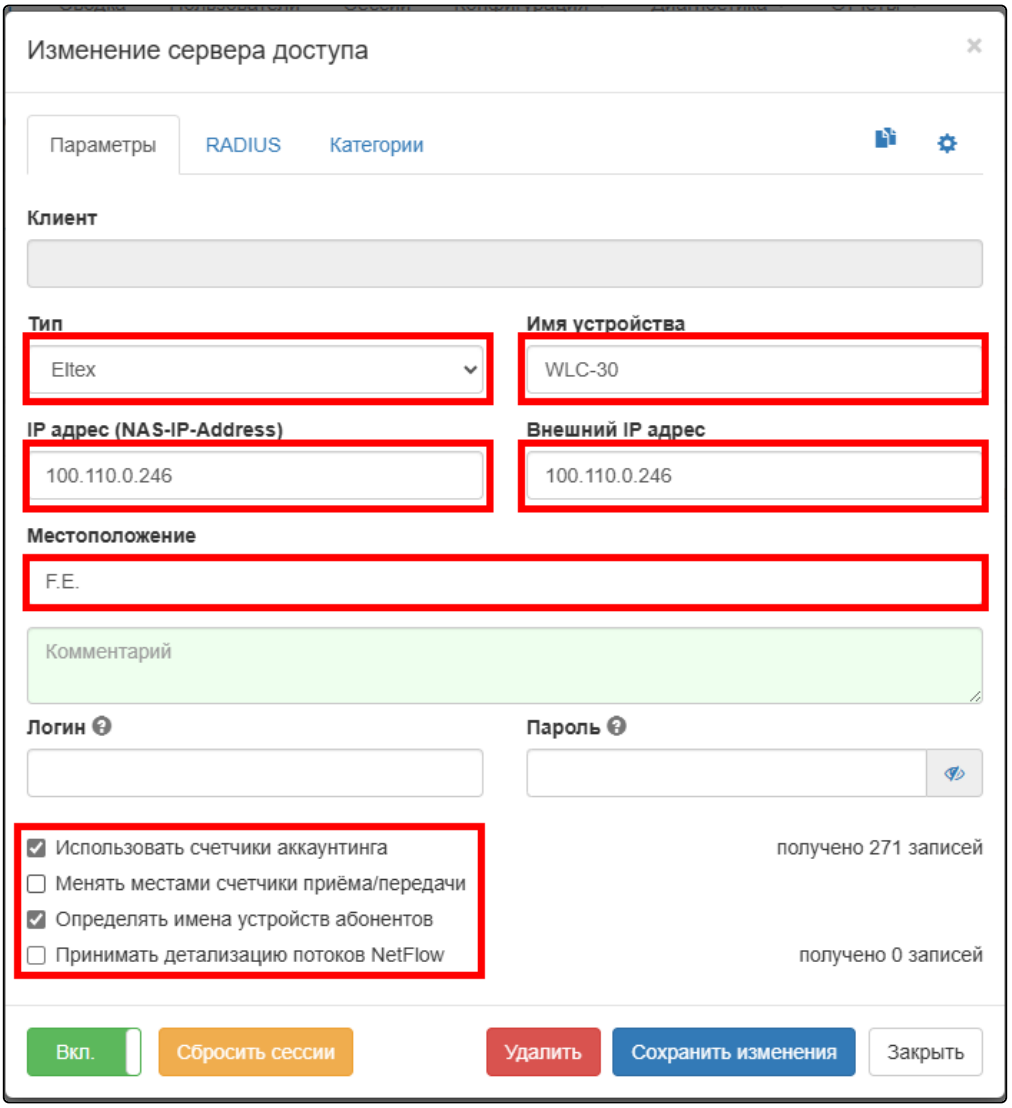
Конфигурация WNAM

Создание сервера

На стороне системы авторизации перейдите: *Конфигурация → Сервера доступа → Создать сервер*.

В закладке *Параметры*:

- Создаётся объект Сервер доступа (тип: Eltex);
- Заполните поля «*IP адрес*» и «*Внешний IP адрес*» (адрес WLC, смотрящий в сторону WNAM);
- «*Имя устройства*» и «*Местоположение*» указывается произвольно.

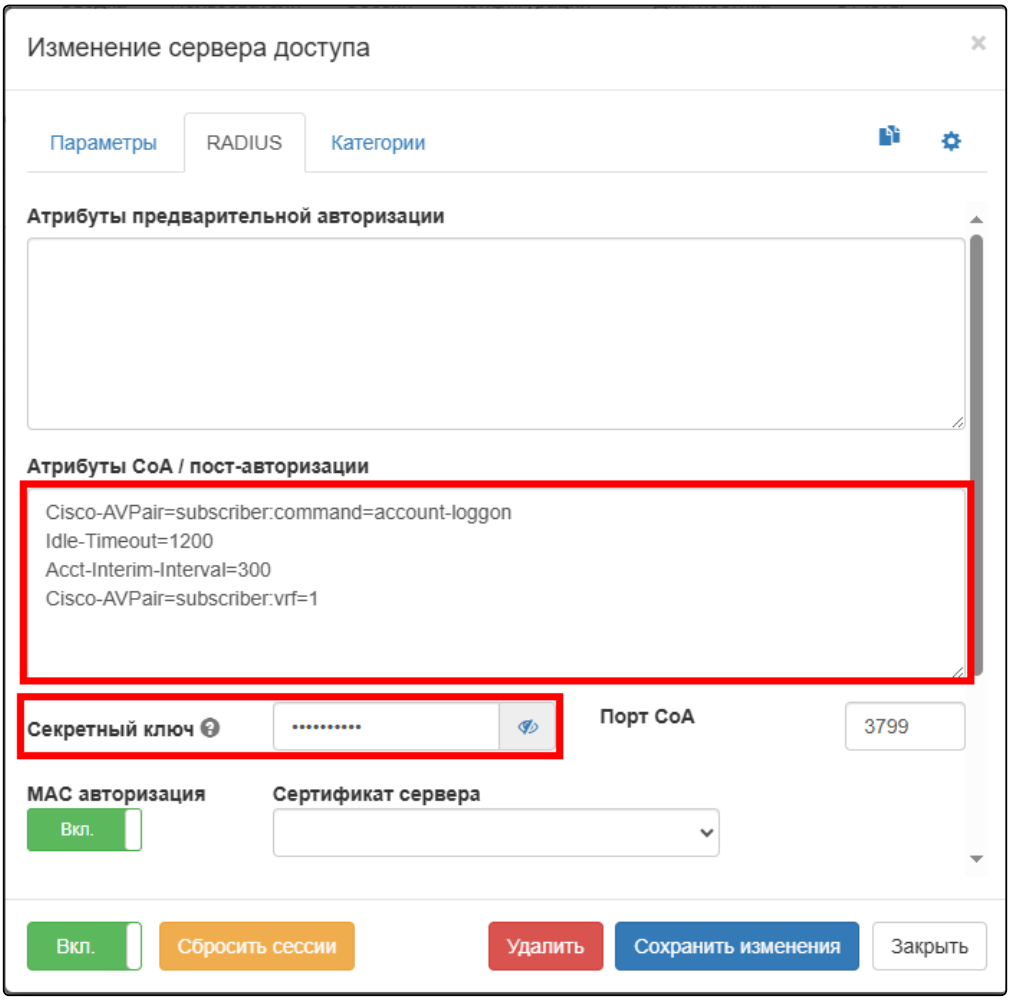


В поле «*Атрибуты CoA / пост-авторизации*» задайте:

```
Cisco-AVPair=subscriber:command=account-loggon
Idle-Timeout=1200
Acct-Interim-Interval=300
Cisco-AVPair=subscriber:vrf=1
```

В поле ввода «*Секретный ключ*» укажите ключ, который указали для *radius-server host 100.110.1.44* в конфигурации WLC:

```
wnampass
```

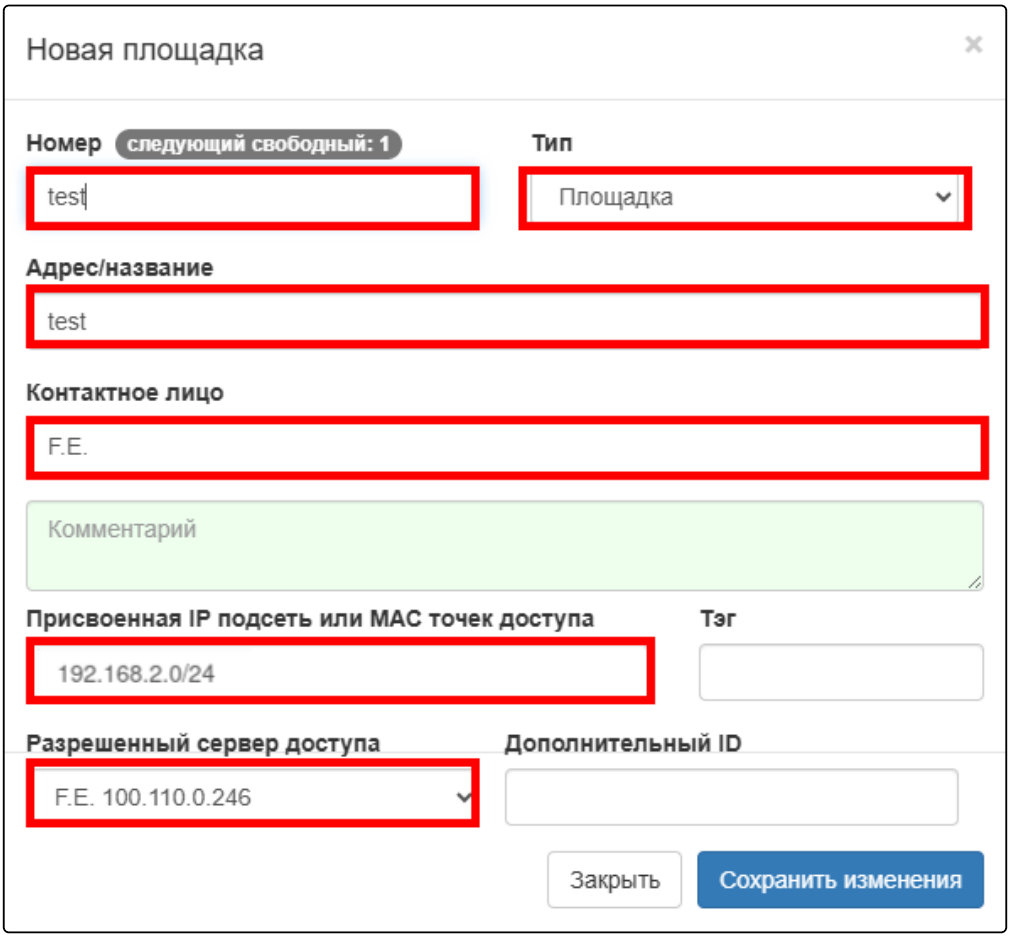


Создание площадки

1. Создайте площадку, к которой будет привязана страница гостевого портала: *Конфигурация → Площадки → Создать площадку*.

В поле *«Тип»* выберите **Площадка**, в поле *«Разрешенный сервер доступа»* выберите созданный ранее сервер. В поле *«Присвоенная IP подсеть или MAC точек доступа»* укажите наш пул IP для пользователей портала (сеть Bridge 3 на WLC).

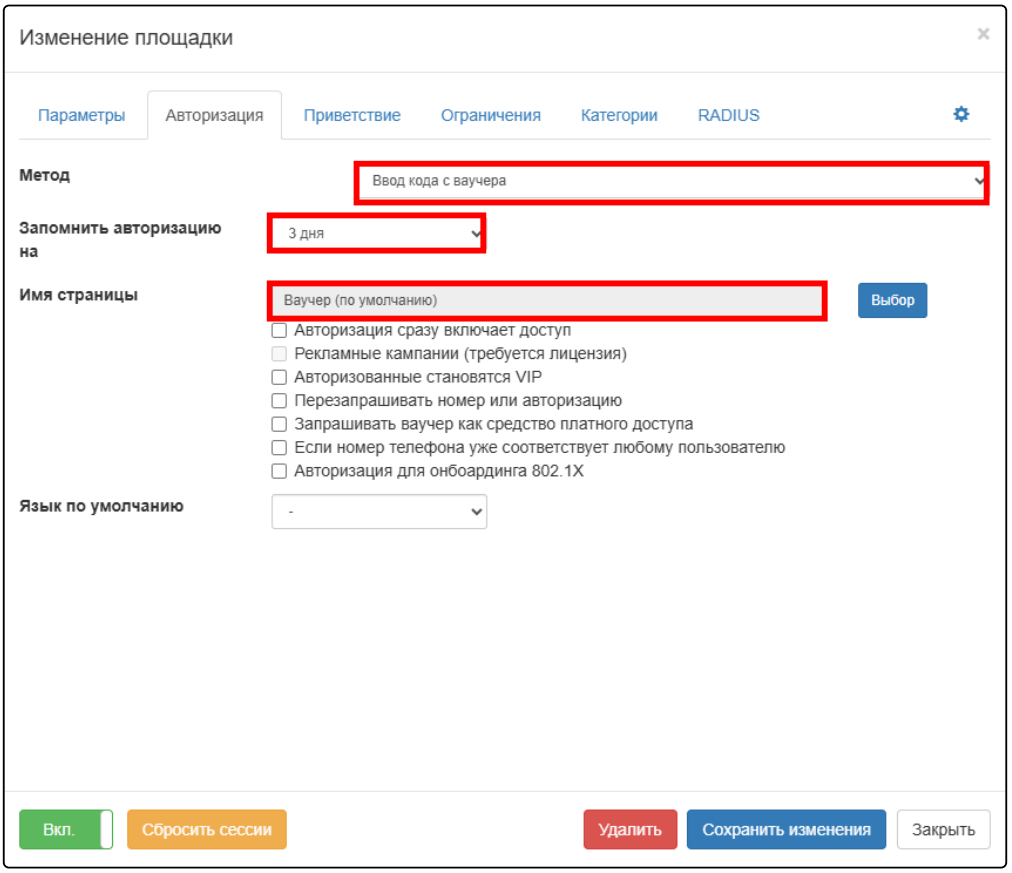
Таким образом через привязку пулов IP можно привязать разные **Площадки** с разными порталами авторизации, трафик клиентов которых терминируется на одном WLC. Разрешенный сервер соответственно на разных площадках будет один и тот же.



2. Выберите созданную площадку.

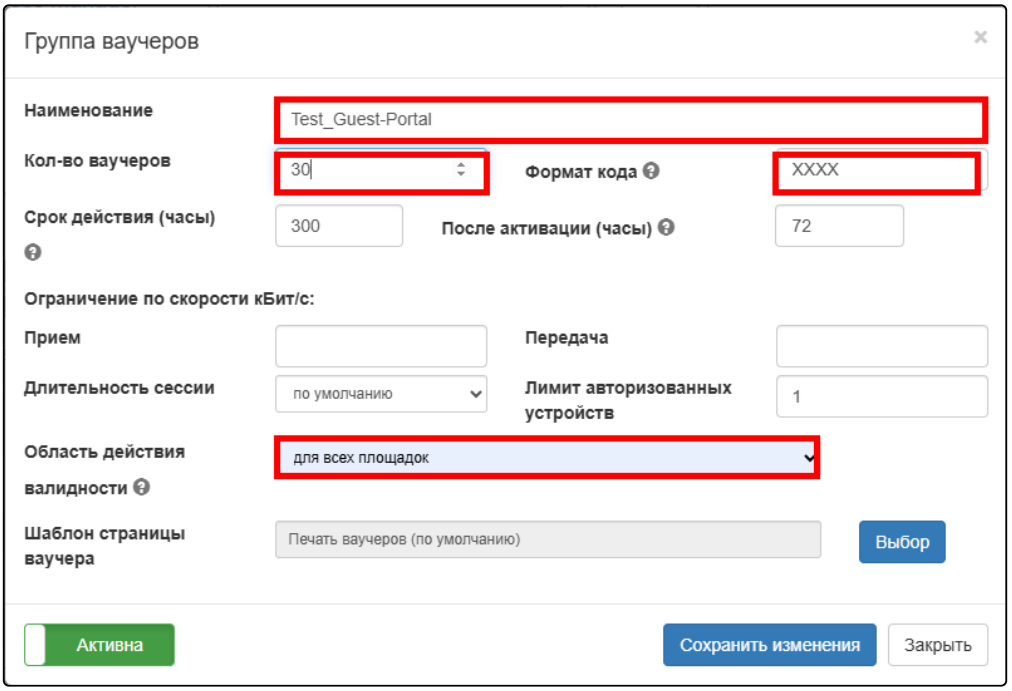
На вкладке Авторизация выберите в поле *«Метод»* − **Ввод кода с ваучера**. Укажите срок валидности ваучера для авторизации. В параметре *«Имя страницы»* выберите **Ваучер (по умолчанию)**. Данных настроек достаточно для работы гостевого портала с авторизацией по коду из Ваучера.

Настройка других способов авторизации выходит за рамки данной статьи.

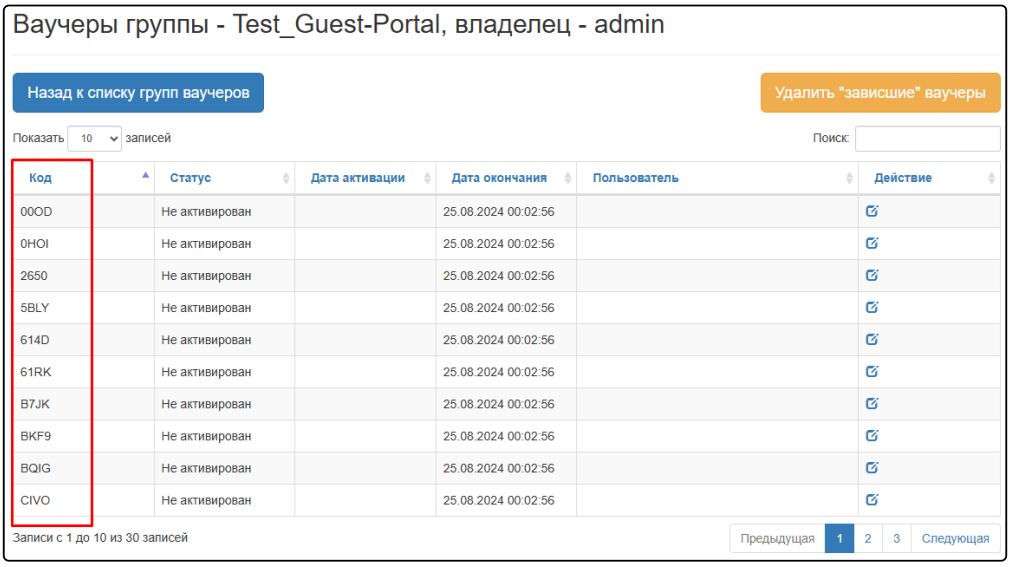


Создание группы ваучеров

1. Перейдите к созданию ваучеров для авторизации: *Конфигурация → Гостевая авторизация → Ваучеры → Создать группу ваучеров*.



В дальнейшем коды данных ваучеров будут использоваться для авторизации клиентов на гостевом портале.



Конфигурирование правил аутентификации

1. Перейдите во вкладку *Конфигурация → Правила аутентификации*.

Создайте новое правило аутентификации и настройте как на скриншоте приведенном ниже. *«Источник запроса»* выберите **Проводной**.

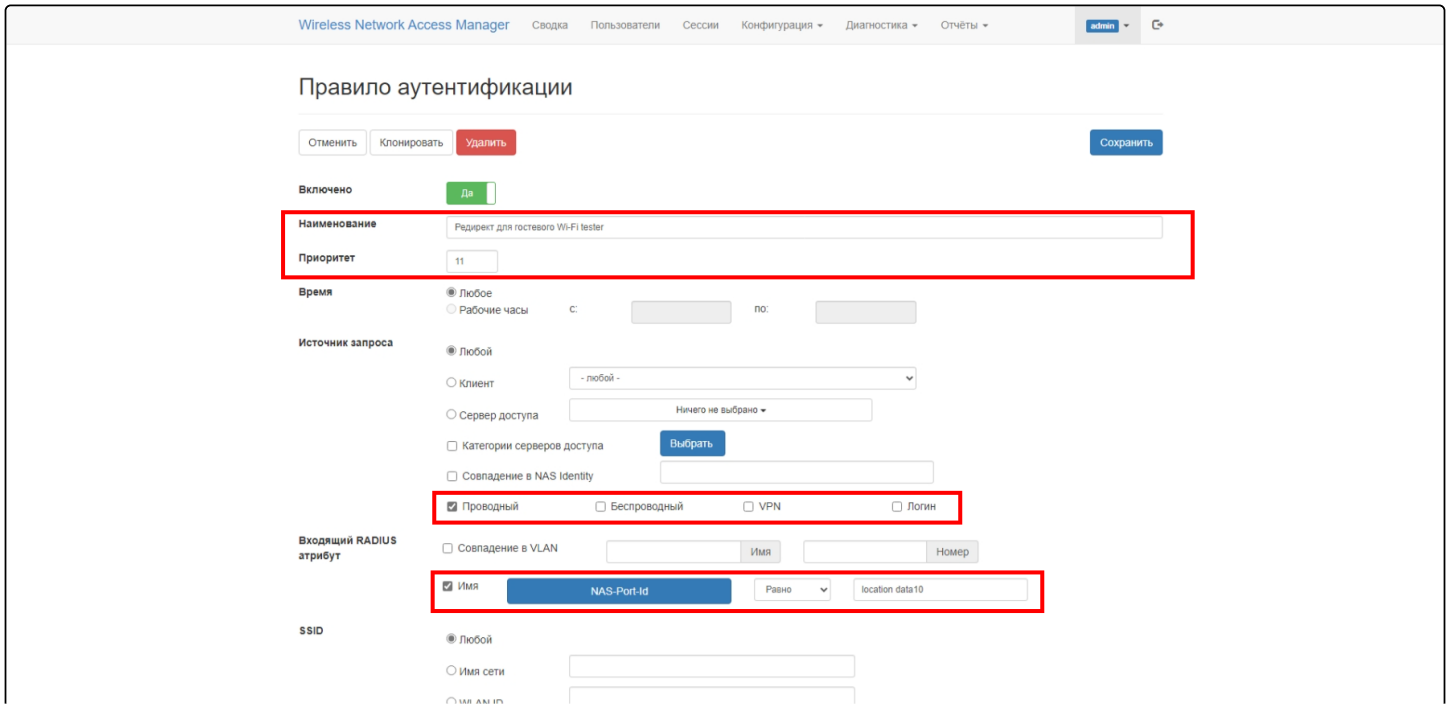
В параметре *«Входящий радиус атрибут»* выберите **NAS-Port-ID**, равным тому **location**, указанный в настройках Bridge 3 на WLC, на которой терминируется клиентский трафик.

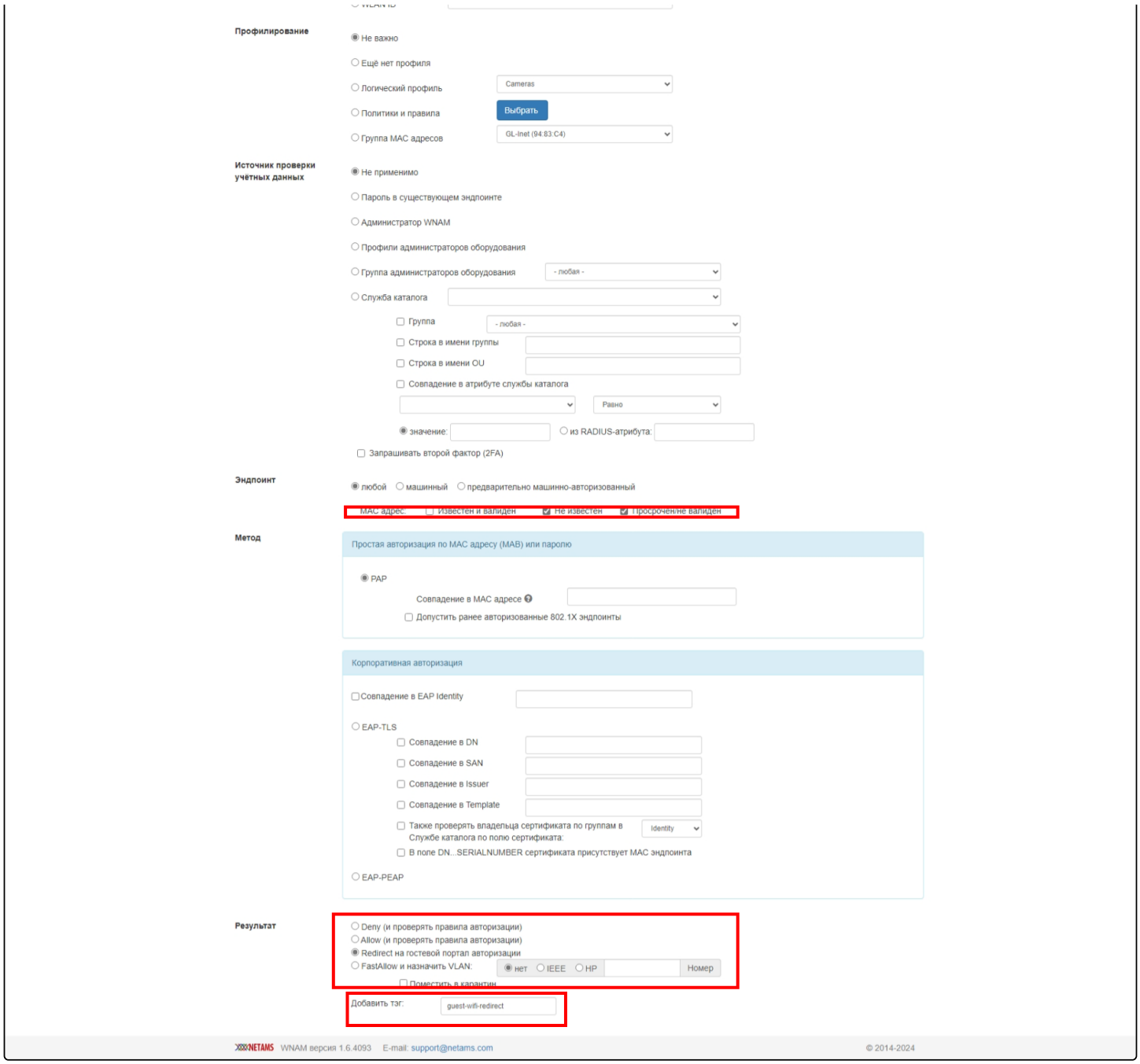
Таким образом свяжите данное правило с SSID с гостевым доступом.

В правило можно добавить дополнительными параметрами при необходимости.

Правило аутентификации привязывается к правилу авторизации при помощи тега. В данном примере указан тег *guest-wifi-redirect*.

Тег должен быть уникальным и должен совпадать с соответствующим правилом авторизации. Если сработало правило аутентификации, далее по данному тегу запускается соответствующее правило авторизации.

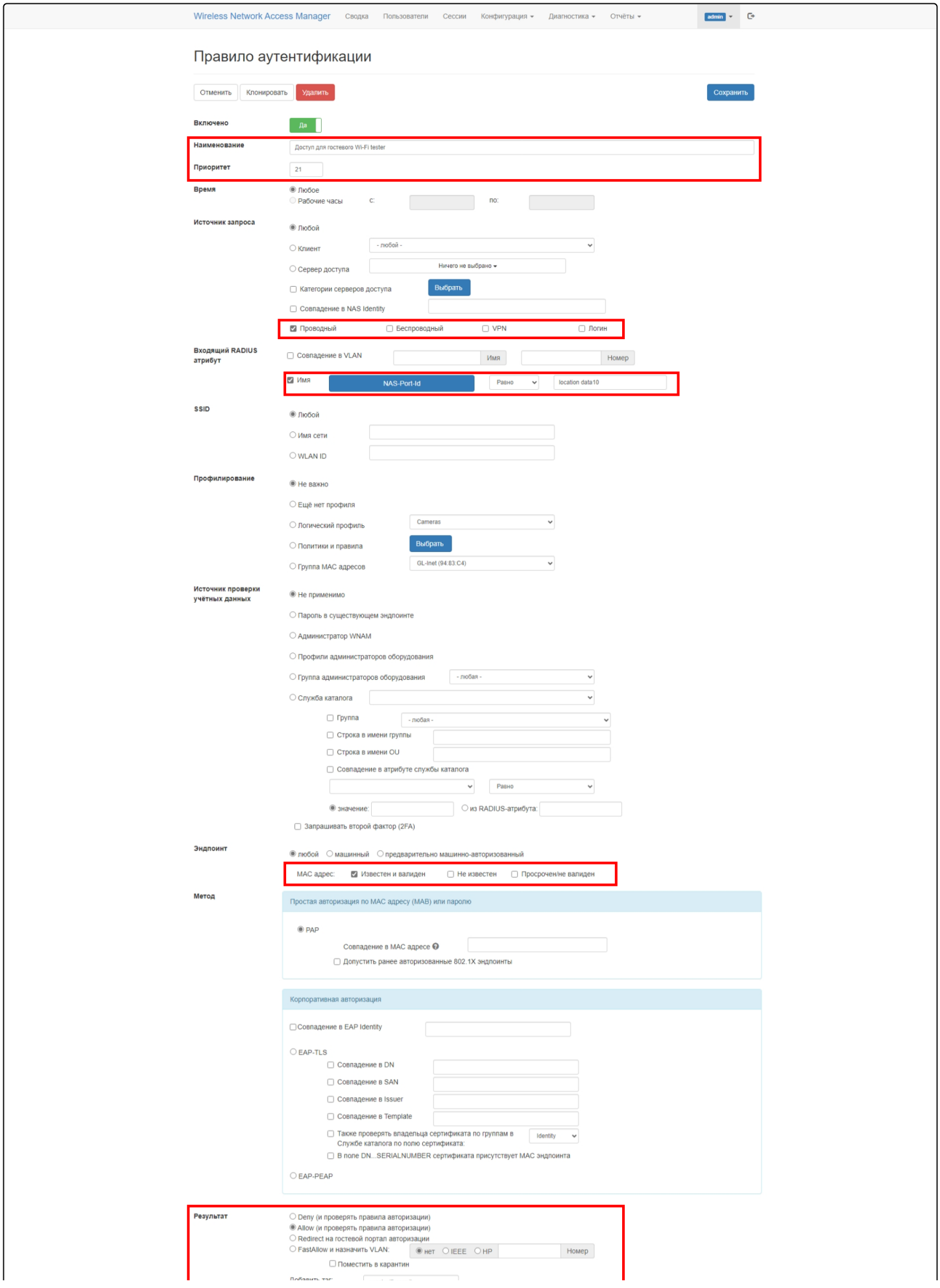




2. Приступите к созданию правила аутентификации для доступа клиента в Internet.

Параметры *«Источник запроса»* и *«Входящий RADIUS атрибут»* настройте так же, как в правиле для редиректа (см. выше).

Необходимо использовать уникальный тег, как в примере выше. В данном примере указан тег *guest-wifi-permit*.


Wireless Network Access Manager
Сводка
Пользователи
Сессии
Конфигурация
Диагностика
Отчёты
admin
Правило аутентификации
Отменить
Клонировать
Удалить
Сохранить
Включено
Да
Наименование
Доступ для гостевого Wi-Fi tester
Приоритет
21
Время
Любое
Рабочие часы
с:
по:
Источник запроса
Любой
Клиент
- любой -
Сервер доступа
Ничего не выбрано
Категории серверов доступа
Выбрать
Совпадение в NAS Identity
Проводный
Беспроводный
VPN
Логин
Входящий RADIUS атрибут
Совпадение в VLAN
Имя
Номер
Имя
NAS-Port-Id
Равно
location data10
SSID
Любой
Имя сети
WLAN ID
Профилирование
Не важно
Ещё нет профиля
Логический профиль
Cameras
Политики и правила
Выбрать
Группа MAC адресов
GL-inet (94:83:C4)
Источник проверки учётных данных
Не применимо
Пароль в существующем эндпоинте
Администратор WNAM
Профили администраторов оборудования
Группа администраторов оборудования
- любая -
Служба каталога
Группа
- любая -
Строка в имени группы
Строка в имени OU
Совпадение в атрибуте службы каталога
Равно
значение:
из RADIUS-атрибута:
Запрашивать второй фактор (2FA)
Эндпоинт
любой
машинный
предварительно машинно-авторизованный
MAC адрес:
Известен и валиден
Не известен
Просрочен/не валиден
Метод
Простая авторизация по MAC адресу (MAB) или паролю
PAP
Совпадение в MAC адресе
Допустить ранее авторизованные 802.1X эндпоинты
Корпоративная авторизация
Совпадение в EAP Identity
EAP-TLS
Совпадение в DN
Совпадение в SAN
Совпадение в Issuer
Совпадение в Template
Также проверять владельца сертификата по группам в Службе каталога по полю сертификата:
Identity
В поле DN...SERIALNUMBER сертификата присутствует MAC эндпоинта
EAP-PEAP
Результат
Deny (и проверять правила авторизации)
Allow (и проверять правила авторизации)
Redirect на гостевой портал авторизации
FastAllow и назначить VLAN:
нет
IEEE
HP
Номер
Поместить в карантин

Конфигурирование правил авторизации

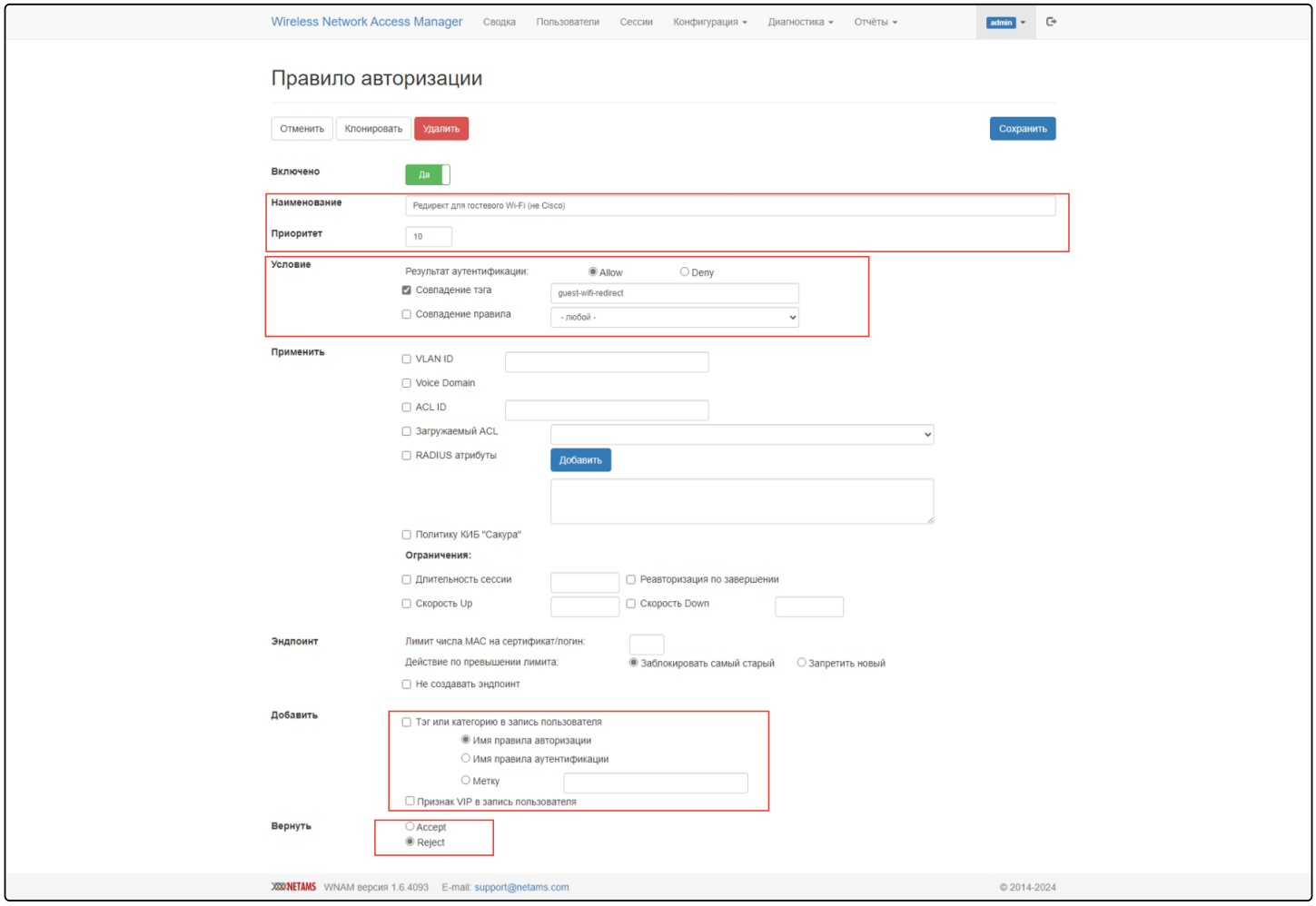
1. Создайте правила авторизации.

Перейдите во вкладку: *Конфигурация → Правила авторизации.*

Первое правило для редиректа на портал приведите к виду как на примере ниже.

В результате должен быть ответ протокола Radius-формата **Access-Reject** от сервиса авторизации системе BRAS на WLC.

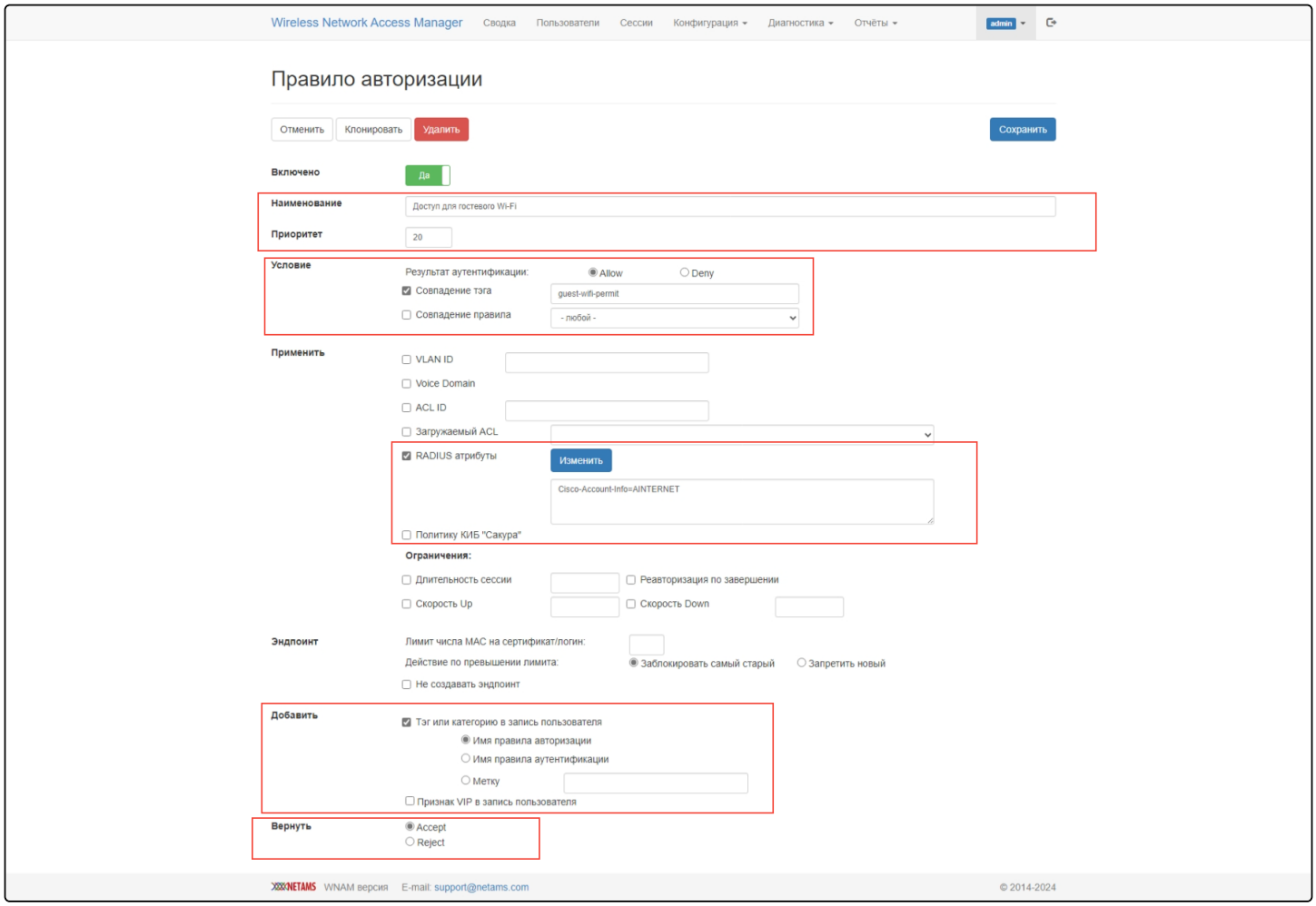
Правило привязывается по совпадению тега, поэтому тег должен быть такой же, как и в правиле аутентификации.



2. Второе правило для предоставления доступа в Internet. В блоке *«Применить»* параметра *«RADIUS-атрибуты»* пропишите атрибут, назначающий сервис доступа с названием INTERNET, который настроен в виде списка контроля доступа на WLC.

```
Cisco-Account-Info=AINTERNET
```

В результате, на данном этапе, должен быть ответ протокола Radius формата **Access-Accept** от сервиса авторизации системе BRAS на WLC. В нем будет содержаться атрибут с указанием наименования сервиса доступного абоненту.



Логика взаимдействия на этапе предоставления доступа в Интернет

Контроллер WLC в ходе авторизации запрашивает параметры сервиса INTERNET в пакете Radius *Access-Request*, а WNAM, в свою очередь, отдаёт их в ответном пакете *Access-Accept*, где в атрибуте *«Cisco-AVPair»*, со значением "subscriber:traffic-class=INTERNET".
Эта последовательность зашита в логику взаимодействия с оборудованием Eltex и не требует дополнительной настройки.

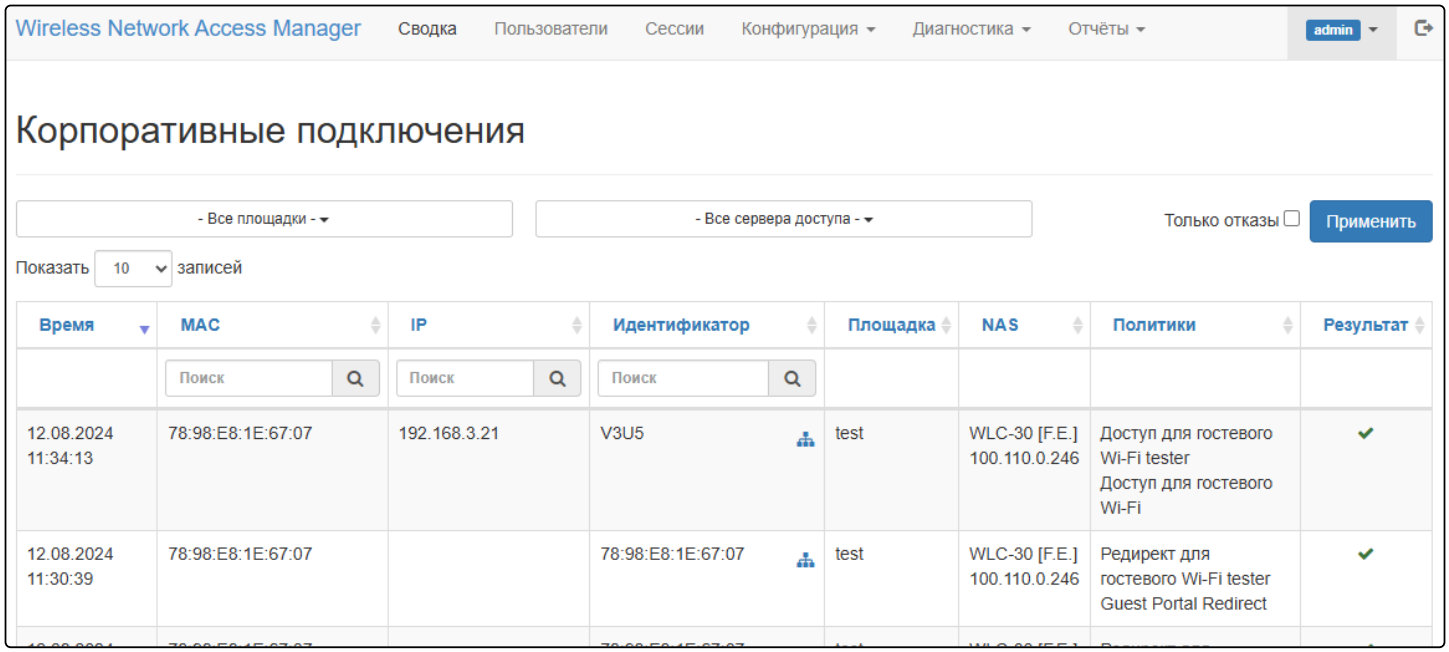
На этом конфигурация сервиса Netams WNAM завершена.

После конфигурирования портала и контроллера WLC при подключения к SSID с названием **F.E.freeSSID** будет регистрация в сети. Клиент попадёт на портал авторизации, где необходимо ввести один из свободных ваучеров. Посмотреть доступные ваучеры можно при переходе на следующую вкладку: *Конфигурация → Гостевая авторизация → Ваучеры*. Выберите созданную группу *Test_Guest-Portal* и введите **Свободный**. После авторизации будет предоставлен доступ в интернет, а введенный ваучер привяжется.

Отладочная информация Netams WNAM

Логирование работы правил авторизации

Для просмотра и мониторинга логов работы правил авторизации перейдите в вкладку *Диагностика → Корпоративные подключения:*



Пример лога гостевого Wi-Fi tester Guest Portal Redirect

```
1: fillFromRadiusAttributes - identity: '78:98:E8:1E:67:07', portType: EthernetMAB
2: fillFromRadiusAttributes - mac: '78:98:E8:1E:67:07'
3: fillFromRadiusAttributes - password: present in request
4: fillFromRadiusAttributes - nas: 'WLC-30 [F.E.]', ip: 100.110.0.246, id:
6614c699fd772e622ebb0689, vendor: ELTEX [enabled]
5: fillFromRadiusAttributes - nas: IP address: 100.110.0.246, identifier: 'null', port:
'location data10'
6: fillFromRadiusAttributes - site: 'test', id: new [enabled]
7: fillFromRadiusAttributes - session id: '30984765436309012 55'
8: radius - received 8 attributes in the request:
    Cisco-AVPair-subscriber:vrf = 1
    User-Name = 78:98:E8:1E:67:07
    Cisco-AVPair-subscriber:CELL = d998075724dc24029b359a8db24682a0
    User-Password = (password length: 8)
    NAS-IP-Address = 100.110.0.246
    Cisco-AVPair-subscriber:l2-interface = softgre 1.4
    Acct-Session-Id = 30984765436309012 55
    NAS-Port-Id = location data10
9: filterForPapMacMethod - checkMABPassword: matched captiveportal_pass for 'Редирект для
гостевого Wi-Fi tester'
10: authentication - a1profiles candidates: 1 with preliminary processing result:
RadiusResponse [state=OK, attributes=[]]
11: authentication - final result: Redirect with policy 'Редирект для гостевого Wi-Fi tester'
 and tag 'guest-wifi-redirect'
12: authorization - guest redirect
13: radius - send RADIUS REJECT, reason: This will instruct Wi-Fi controller to execute
redirect action
```

Пример лога гостевого Wi-Fi tester Доступ для гостевого Wi-Fi

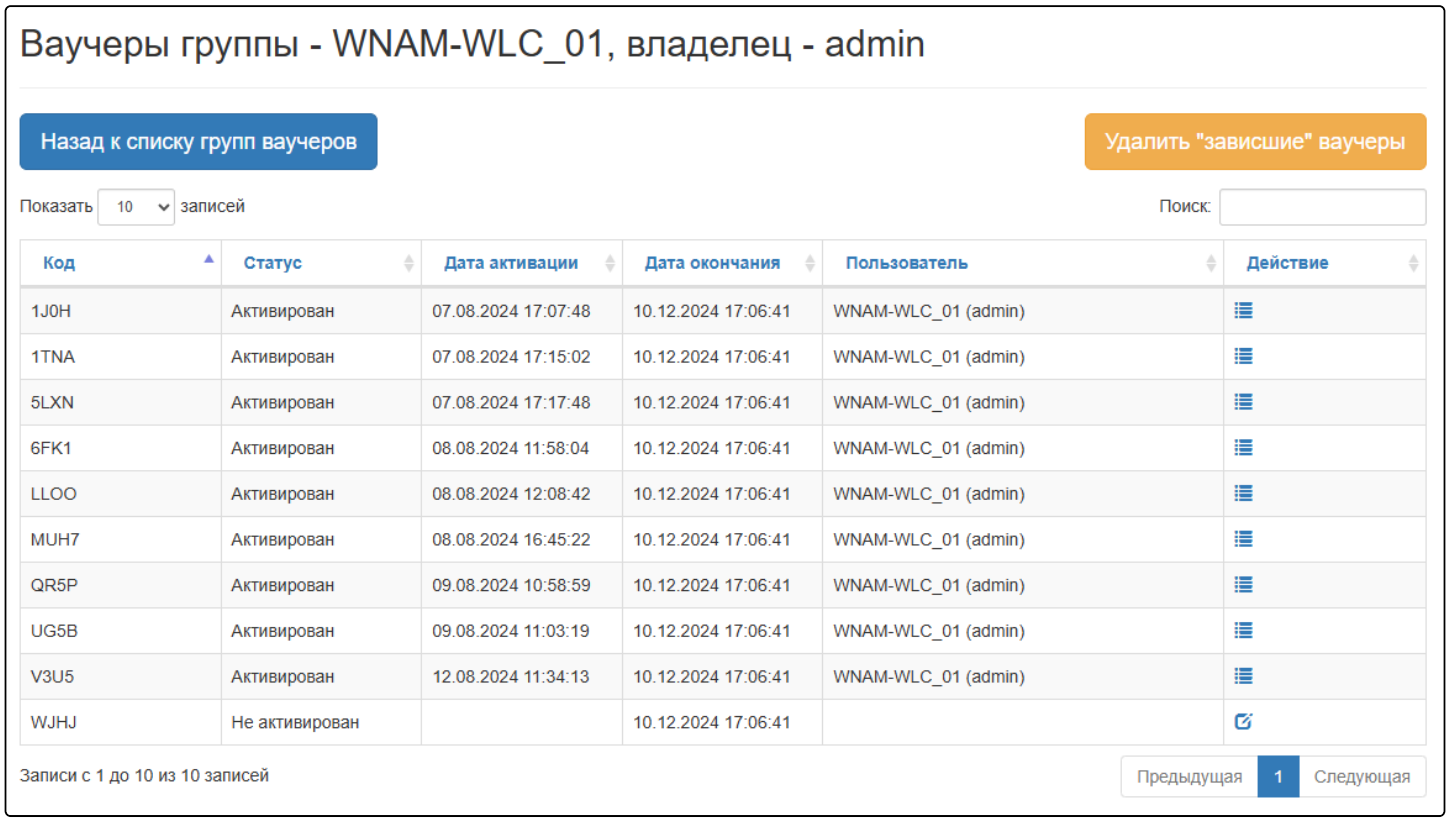
```
1: fillFromRadiusAttributes - identity: '78:98:E8:1E:67:07', portType: EthernetMAB
2: fillFromRadiusAttributes - mac: '78:98:E8:1E:67:07'
3: fillFromRadiusAttributes - password: present in request
4: fillFromRadiusAttributes - nas: 'WLC-30 [F.E.]', ip: 100.110.0.246, id:
6614c699fd772e622ebb0689, vendor: ELTEX [enabled]
```

```
5: fillFromRadiusAttributes - nas: IP address: 100.110.0.246, identifier: 'null', port:
'location data10'
6: fillFromRadiusAttributes - site: 'test', id: new [enabled]
7: fillFromRadiusAttributes - session id: '3098476543630901255'
8: radius - received 8 attributes in the request:
    Cisco-AVPair-subscriber:vrf = 1
    User-Name = 78:98:E8:1E:67:07
    Cisco-AVPair-subscriber:CELL = d998075724dc24029b359a8db24682a0
    User-Password = (password length: 8)
    NAS-IP-Address = 100.110.0.246
    Cisco-AVPair-subscriber:l2-interface = softgre 1.4
    Acct-Session-Id = 3098476543630901255
    NAS-Port-Id = location data10
9: filterForPapMacMethod - checkMABPassword: matched captiveportal_pass for 'Доступ для
гостевого Wi-Fi tester'
10: authentication - a1profiles candidates: 1 with preliminary processing result:
RadiusResponse [state=OK, attributes=[]]
11: authentication - final result: Allow with policy 'Доступ для гостевого Wi-Fi tester' and
tag 'guest-wifi-permit'
12: authorization - a2profiles candidates: 7
13: authorization - final result: Accept with policy 'Доступ для гостевого Wi-Fi'
14: radius - send RADIUS ACCEPT with 1 attributes
15: radius -     attribute: Cisco-Account-Info = AINTERNET
16: addIP - Set IP address 192.168.3.21 on Accounting message (session 3098476543630901255)
```

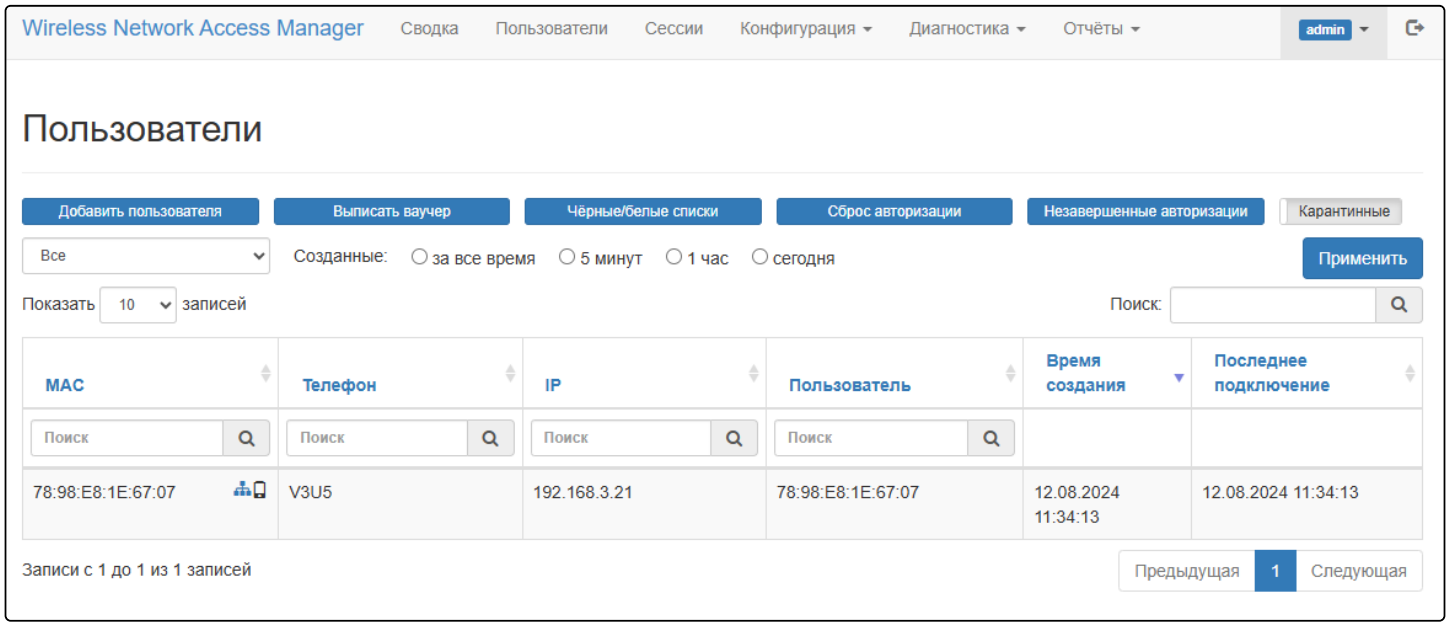
Информация о ваучерах

Информация о статусе ваучеров находится по следующему пути: *Конфигурация → Гостевая авторизация → Ваучеры.*

Выберите нужную группу.



Информация о клиентах Wi-Fi



Активные клиентские подключения к Wi-Fi можно посмотреть на контроллере WLC-командой:

```
wlc# show subscriber-control sessions status
```

Ниже приведен пример вывода активных клиентских сессий на контроллере WLC:

```
wlc# sh subscriber-control sessions status
Session id              User name          IP address         MAC address          Interface
Domain
---------------------   ---------------    ---------------    ------------------
---------------------   ---------------
3098476543630901251     78:98:E8:1E:67:    192.168.3.21       78:98:e8:1e:67:07    softgre 1.4
--
                        07
```

```
wlc# sh subscriber-control services counters session-id 3098476543630901251
Service id              Service name       Recv packets       Recv bytes           Send packets
Send bytes
---------------------   ---------------    --------------     --------------       --------------
--------------
3134505340649865218     A INTERNET         4559               3868861              3842
692224
```

```
wlc# sh wlc clients
MAC User            MAC AP              Hostname AP                          SSID              RSSI
AP-Location         Username
------------------  ------------------  -------------------------------      ---------------
-------   ------------------   ------------------
78:98:e8:1e:67:07   68:13:e2:02:ea:20   WEP-3ax                              F.E.freeSSID      -35
default-location    --
```

Расположение логов

Лог авторизации пользователей находится на сервере WNAM в файле: */home/wnam/logs/wnam.log*

Пример вывода логов авторизации файла /home/wnam/logs/wnam.log

```
11:33:41.702 DEBUG [EltexWlcService.java:196] - CP ELTEX WLC clicked: username=78:98:E8:1E:67:0
7, ip=192.168.3.21, server=100.110.0.246, sessionId=3098476543630901255, dst='http://
www.msftconnecttest.com/redirect'
11:33:41.716 DEBUG [PageGenerator.java:713] - processAuthRequest ELTEXWLC: username=78:98:E8:1E
:67:07, ip=192.168.3.21, server=100.110.0.246, site_id=new, domain_id=3098476543630901255, dst='
http://www.msftconnecttest.com/redirect' adv curr/max=1/1
11:33:41.719 DEBUG [PageGenerator.java:1300] - captive portal redirected to VOUCHER page,
username=78:98:E8:1E:67:07, cust=new, form='6614c99dfd772e622ebb06a7'
11:34:13.380 DEBUG [VoucherHandler.java:52] - postVoucher CODE='V3U5',
FORM=6614c99dfd772e622ebb06a7, MAC=78:98:E8:1E:67:07, IP=192.168.3.21, site_id=new, name=78:98:
E8:1E:67:07
11:34:13.382 DEBUG [VoucherHandler.java:62] - find_voucher: 66b34731933c505a427dad16,
code=V3U5, status=Не активирован
11:34:13.395 DEBUG [VoucherHandler.java:125] - postVoucher OK CODE='V3U5', voucher='Группа:
WNAM-WLC_01, владелец: admin', vg='WNAM-WLC_01'
11:34:13.399 DEBUG [PageGenerator.java:390] - processRedirectRequestCi mac=78:98:E8:1E:67:07,
method=ORIGINAL, formName=, redirectUrl=null, key=b04fb14d-36fb-4c30-a886-bfbab119088c
11:34:13.401 DEBUG [PageGenerator.java:849] - loginAtNasCi ELTEXWLC mac=78:98:E8:1E:67:07, ip=1
92.168.3.21, server=100.110.0.246, dst='http://www.msftconnecttest.com/redirect'
11:34:13.406 DEBUG [EltexWlcService.java:66] - backToEltexWLC login server='100.110.0.246',
user=78:98:E8:1E:67:07, password=password, dst='http://www.msftconnecttest.co...'
11:34:13.407 DEBUG [EltexWlcService.java:85] - open EltexWLC access REQ for IP=192.168.3.21,
MAC=78:98:E8:1E:67:07 at NAS_IP=100.110.0.246
11:34:13.411 DEBUG [WnamRadiusService.java:558] - handleRadiusPacket AUTH as=100.110.0.246,
secret_len=10, attrs=[Vendor-Specific: 0x, User-Name: 78:98:E8:1E:67:07, User-Password:
<stripped out>, NAS-IP-Address: 100.110.0.246, Acct-Session-Id: 3098476543630901255, Vendor-
Specific: 0x, Vendor-Specific: 0x, NAS-Port-Id: location data10]
11:34:13.411 DEBUG [ProfilingService.java:440] - handleMac on MAC: 78:98:E8:1E:67:07 for vendor
D-Link International
11:34:13.412 DEBUG [ProfilingService.java:466] - handleMac on MAC: 78:98:E8:1E:67:07 checks
added: 1, res: [D-Link International]
11:34:13.414 DEBUG [ProfilingService.java:1091] - Endpoint 78:98:E8:1E:67:07 logical profile
set to Home Network Devices
11:34:13.414 DEBUG [ProfilingService.java:1102] - Endpoint 78:98:E8:1E:67:07 policy set
assigned: [DLink-Device]
11:34:13.416 DEBUG [ProfilingService.java:469] - handleMac on MAC: 78:98:E8:1E:67:07 profiled
in 5 ms.
11:34:13.433 DEBUG [WnamRadiusService.java:558] - handleRadiusPacket AUTH as=100.110.0.246,
secret_len=10, attrs=[User-Name: INTERNET, Vendor-Specific: 0x, NAS-IP-Address: 100.110.0.246,
NAS-Port-Id: location data10, User-Password: <stripped out>, Vendor-Specific: 0x, Vendor-
Specific: 0x, Acct-Session-Id: 3134505340649865221, Vendor-Specific: 0x, Vendor-Specific: 0x,
Vendor-Specific: 0x]
11:34:13.434 DEBUG [WnamRadiusService.java:558] - handleRadiusPacket ACCT as=100.110.0.246,
secret_len=10, attrs=[User-Name: 78:98:E8:1E:67:07, Vendor-Specific: 0x, Acct-Session-Id:
3098476543630901255, Acct-Status-Type: Start, Vendor-Specific: 0x, Event-Timestamp: 1723436510,
NAS-Port-Id: location data10, Called-Station-Id: CC-9D-A2-71-94-E0:data10, Vendor-Specific: 0x,
Vendor-Specific: 0x, Vendor-Specific: 0x, NAS-Identifier: F.E.wlc-30, Framed-IP-Address:
192.168.3.21, Calling-Station-Id: 78-98-E8-1E-67-07, NAS-IP-Address: 100.110.0.246]
11:34:13.435 DEBUG [WnamRadiusService.java:558] - handleRadiusPacket ACCT as=100.110.0.246,
secret_len=10, attrs=[User-Name: 78:98:E8:1E:67:07, Vendor-Specific: 0x, Acct-Session-Id:
3098476543630901255, Acct-Status-Type: Interim-Update, Vendor-Specific: 0x, Event-Timestamp:
1723436806, NAS-Port-Id: location data10, Called-Station-Id: CC-9D-A2-71-94-E0:data10, Vendor-
Specific: 0x, Vendor-Specific: 0x, Vendor-Specific: 0x, NAS-Identifier: F.E.wlc-30, Framed-IP-
Address: 192.168.3.21, Calling-Station-Id: 78-98-E8-1E-67-07, Vendor-Specific: 0x, Vendor-
Specific: 0x, Acct-Input-Gigawords: 0, Acct-Input-Octets: 128192, Acct-Output-Gigawords: 0,
Acct-Output-Octets: 149134, Acct-Session-Time: 286, NAS-IP-Address: 100.110.0.246]
11:34:13.436 DEBUG [EltexWlcService.java:176] - sendCoa attrs=8, fail=false, resp=CoA-ACK
```

```
11:34:13.437 DEBUG [EltexWlcService.java:148] - open EltexWLC access SUCCESS for IP=192.168.3.2
1, MAC=78:98:E8:1E:67:07, num_avp=1
11:34:13.440 DEBUG [WnamRadiusService.java:558] - handleRadiusPacket ACCT as=100.110.0.246,
secret_len=10, attrs=[User-Name: INTERNET, Vendor-Specific: 0x, Acct-Session-Id:
3134505340649865221, Vendor-Specific: 0x, Acct-Status-Type: Start, Vendor-Specific: 0x, Event-
Timestamp: 1723436806, NAS-Port-Id: location data10, Called-Station-Id: CC-9D-A2-71-94-
E0:data10, Vendor-Specific: 0x, Vendor-Specific: 0x, Vendor-Specific: 0x, NAS-Identifier:
F.E.wlc-30, Framed-IP-Address: 192.168.3.21, Calling-Station-Id: 78-98-E8-1E-67-07, NAS-IP-
Address: 100.110.0.246]
11:34:13.450 DEBUG [WnamCmdService.java:630] - ACCT Interim-Update new session ID=3098476543630
901255, MAC=78:98:E8:1E:67:07, IP=192.168.3.21, User=78:98:E8:1E:67:07, NAS_IP=100.110.0.246,
site_id=new
11:34:13.450 DEBUG [WnamCmdService.java:630] - ACCT Start new session ID=3098476543630901255,
MAC=78:98:E8:1E:67:07, IP=192.168.3.21, User=78:98:E8:1E:67:07, NAS_IP=100.110.0.246, site_id=n
ew
11:34:13.450 DEBUG [WnamCmdService.java:630] - ACCT Start new session ID=3098476543630901255,
MAC=78:98:E8:1E:67:07, IP=192.168.3.21, User=INTERNET, NAS_IP=100.110.0.246, site_id=new
```

23.11.3 Авторизация через RADIUS

- Алгоритм работы
- Конфигурация WLC
  - Использование сертификатов
  - Полная конфигурация
- Диаграмма подключения

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 проводится MAB-авторизация (MAC Authentication Bypass) на RADIUS-сервере, подставляется MAC-адрес клиента в атрибут User-Name, а в User-Password записывается radius-secret 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.

Клиент обращается на HTTP-ресурс. ТД перехватывается запрос и клиент перенаправляется 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
```

Если URL содержит спецсимволы из зарезервированного набора: **! * ' ( ) ; : @ & = + $, / ? % # [ ]** ,то необходимо использовать двойные кавычки "" при конфигурировании параметра **redirect-url-custom.**

```
wlc
  portal-profile default-portal
    redirect-url-custom "https://100.110.0.161:8443/portal/PortalSetup.action?
portal=10968c1f-36fe-4e5c-96ff-9d74f689b29b?
action_url=<SWITCH_URL>&redirect=<ORIGINAL_URL>&ap_mac=<AP_MAC>"
    age-timeout 10
    verification-mode external-portal
  exit
```

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>&r
edirect=<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>
- <NAS_IP>

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
```

Использование сертификатов

Для повышения безопасности передачи данных между клиентом и ТД необходимо обеспечить шифрование трафика с использованием SSL. Для этого требуется:

- SSL-сертификат (формат PEM);
- Приватный ключ (формат PEM).

На ТД возможно использовать RSA-сертификаты. ECDSA-сертификаты не поддержаны.

Для защиты приватного ключа в схеме с портальной авторизацией рекомендуется использовать пароль.

Стандартный процесс выпуска сертификатов не предусматривает автоматическое шифрование приватного ключа. Однако это можно выполнить вручную с помощью утилиты **OpenSSL**.

Команда для шифрования ключа:

```
openssl rsa -aes256 -in private_key.pem -out private_key_encrypted.pem
```

Параметры:

- `-aes256` – алгоритм шифрования (можно заменить на `-aes128` или `-aes192`);
- `-in private_key.pem` – исходный незашифрованный ключ;
- `-out private_key_encrypted.pem` – зашифрованный ключ.

После выполнения команды OpenSSL запросит пароль, который будет использоваться для защиты ключа.

Этот подход обеспечит дополнительный уровень защиты приватного ключа от несанкционированного доступа.

Данная процедура проводится вне процесса выпуска сертификата и является дополнительной мерой безопасности.

После шифрования ключа его необходимо добавить к сертификату, например через текстовый редактор. Файл сертификата с шифрованным ключом должен иметь вид:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
-----BEGIN ENCRYPTED PRIVATE KEY-----

-----END ENCRYPTED PRIVATE KEY-----
```

Загрузите файл сертификата с шифрованным ключом на контроллер WLC в директорию *crypto:cert/*

Настройте проверку сертификата и включите режим HTTPs:

```
wlc
  ap-profile default-ap
    captive-portal
      ap-ip-alias certificate_alias
      crypto cert certificate_encrypted.pem
      crypto private-key-password ascii-text password
      proxy-https
    exit
```

Перед применением конфигурации произойдёт проверка псевдонима сертификата и пароля шифрованного ключа.

Допустимо использовать сертификат без шифрованного ключа. В таком случае приватный ключ добавляется к сертификату. Настройка **crypto private-key-password** не требуется.

Формат файла для сертификата без шифрованного ключа:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
-----BEGIN PRIVATE KEY-----

-----END PRIVATE KEY-----
```

Конфигурация:

```
wlc
  ap-profile default-ap
    captive-portal
      ap-ip-alias certificate_alias
      crypto cert certificate.pem
      proxy-https
    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
```

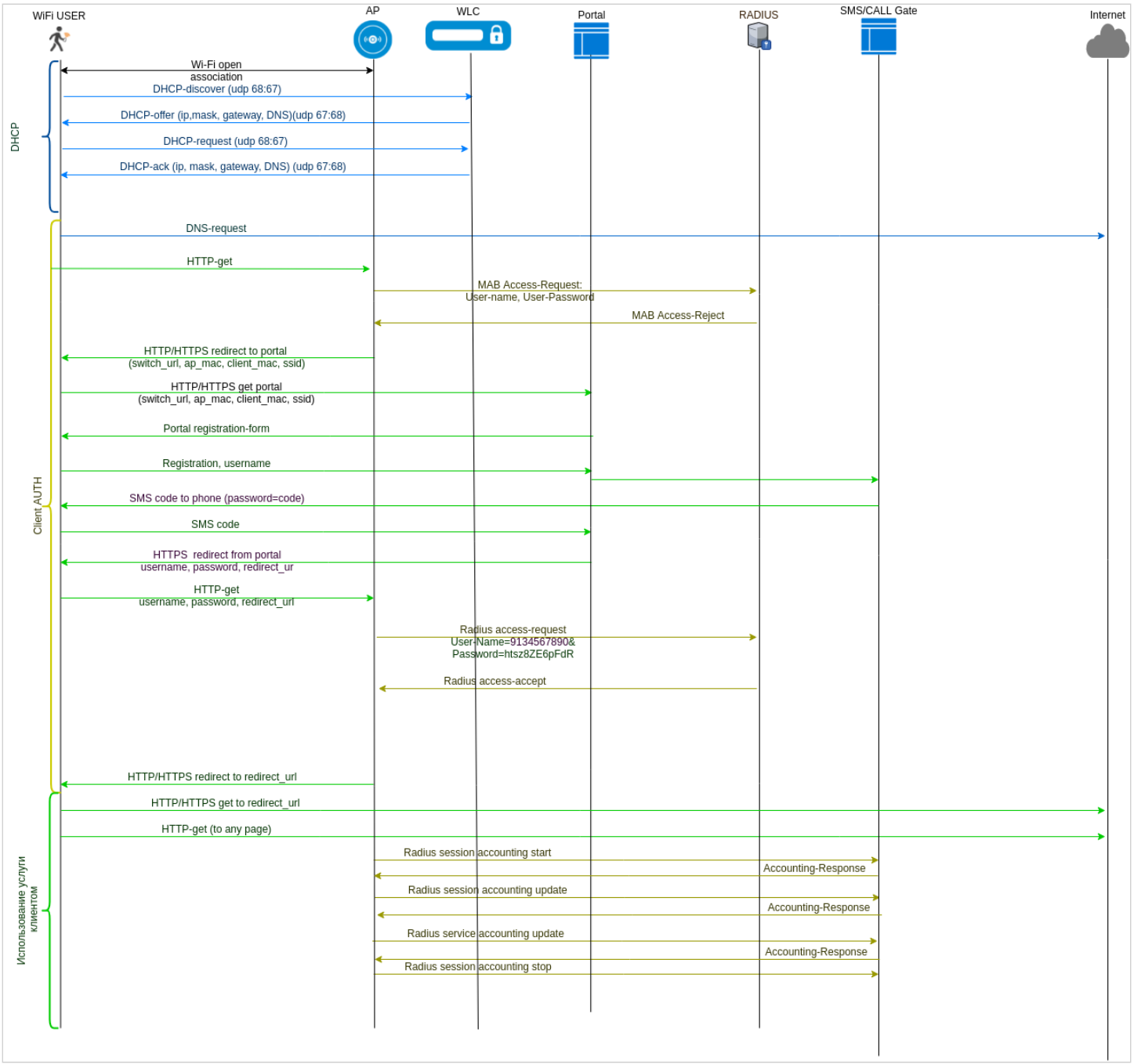
```
    match protocol udp
    match destination-port object-group dns
    enable
  exit
  rule 70
    action permit
    match protocol tcp
    match destination-port object-group netconf
    enable
  exit
  rule 80
    action permit
    match protocol tcp
    match destination-port object-group sa
    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



23.12 Резервирование WLC

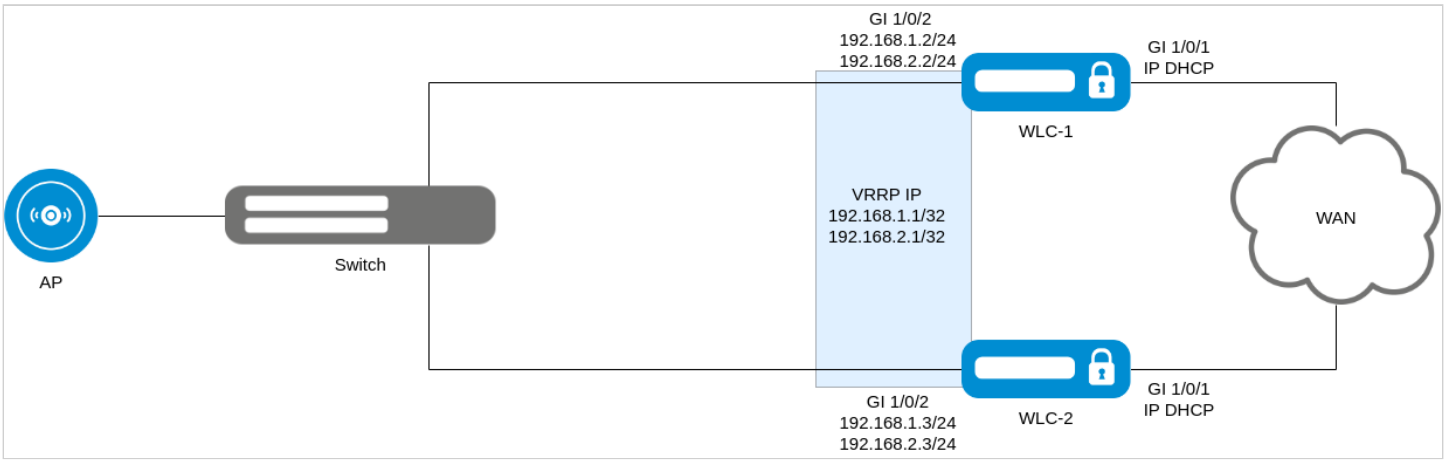
- Описание
- Схема включения
- Задача
- Решение
  - Пример настройки WLC-1
    - Полная конфигурация WLC-1
  - Пример настройки WLC-2
    - Полная конфигурация WLC-2
- Проверка

23.12.1 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.

23.12.2 Схема включения



23.12.3 Задача

Организовать резервирование контроллера WLC.

23.12.4 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 и их ПО в директории system:access-points-firmwares
- 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 клиентских интерфейсах, где включен vrrp, необходимо включить:

```
vrrp timers garp refresh 60
```

Данная команда определяет интервал, по истечении которого будет происходить периодическая отправка Gratuituous ARP-сообщений, пока маршрутизатор находится в состоянии Master. Настройку нужно включать, если клиентский трафик туннелируется.

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
  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
  remote-delete
  enable
exit
```

Настраиваем Softgre-Controller для синхронизации туннелей SoftGRE:

```
softgre-controller
  failover
exit
```

Настраиваем WLC для синхронизации точек доступа и их ПО в директории system:access-points-firmwares

```
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
#270
#1.30.x
#2024-11-22
#05:32:21
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
  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
  remote-delete
  enable
exit
```

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
  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
  remote-delete
  enable
exit
```

Настраиваем Softgre-Controller для синхронизации туннелей SoftGRE:

```
softgre-controller
  failover
exit
```

Настраиваем WLC для синхронизации точек доступа и их ПО в директории system:access-points-firmwares:

```
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
#270
#1.30.x
#2024-11-22
#05:32:21
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
  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
  remote-delete
  enable
exit
```

23.12.5 Проверка

Для проверки синхронизации туннелей, WLC, DHCP можно посмотреть вывод:

```
wlc-30r# show high-availability state
VRRP role:                          Backup
AP Tunnels:
    State:                          Successful synchronization
    Last synchronization:           2024-11-25 16:18:18
DHCP option 82 table:
    State:                          Disabled
    Last state change:              --
DHCP server:
VRF:                                --
    State:                          Successful synchronization
    Last synchronization:           2024-11-25 16:18:33
crypto-sync:
    State:                          Successful synchronization
    Last synchronization:           2024-11-25 16:18:34
Firewall:
    State:                          Disabled
    Last state change:              --
WLC:
    State:                          Successful synchronization
    Last synchronization:           2024-11-25 16:18:34
WEB profiles:
    State:                          Disabled
```

24 Часто задаваемые вопросы

- Ошибка "error - certificate is not yet valid" при comit
- Как снизить MTU на ТД
- Не удалось получить маршруты по BGP и/или OSPF, сконфигурированных в VRF
- Закрываются сессии SSH/Telnet, проходящие через контроллер WLC
- Как полностью очистить конфигурация WLC и как сбросить на заводскую конфигурацию?
- Как привязать subinterface к созданным VLAN?
- Есть ли функционал в контроллерах WLC для анализа трафика?
- Как настроить ip prefix-list 0.0.0.0/0?
- Проблема прохождения асинхронного трафика
- Как можно сохранить локальную копию конфигурации контроллера?

24.1 Ошибка "error - certificate is not yet valid" при comit

```
error - certificate is not yet valid
check radius: got 1 errors during validation
check cert and ca in radius local: certificate does not match ca
```

Если дата и время установлены некорректно, при commit может появиться ошибка **"error - certificate is not yet valid"**. Для решения этой проблемы необходимо установить дату и время через u-boot.

> ⚠ Актуально только для устройств WLC-30 и ESR-30.

Зайдите в загрузчик через консольный интерфейс. В процессе загрузки устройства после появления сообщения:

```
Autobooting in 5 seconds, enter to command line available now
u-boot>
```

Введите слово **stop**.

Далее внесите команды **date reset** для сброса даты и **reset** для перезагрузки устройства.

```
u-boot> date reset
u-boot> reset
```

24.2 Как снизить MTU на ТД

ТД может получить значение MTU через DHCP option 26. Снижение MTU требуется, если ТД работает на канале с заниженным MTU, например через VPN. Значение в option 26 нужно задавать в HEX. Пример настройки MTU 1400 DEC (0578 HEX):

```
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 26 hex-bytes 0578
  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
```

ТД применит новое значение MTU после перезагрузки. Пример команды:

```
reload wlc ap <mac>
```

Для схемы с туннелированием клиентского трафика, нужно настроить в профиле SoftGRE туннеля, аналогичное MTU как на ТД. Пример настройки:

```
tunnel softgre 1
  mode data
  local address 192.168.1.1
  default-profile
  mtu 1400
  enable
exit
```

Туннель SoftGRE применит новое значение MTU после переподнятия. Пример команды для одной ТД и для всех:

```
clear wlc ap <mac>
clear wlc ap
```

⚠ Перезагрузка ТД и переподнятие туннеля вызовет перерыв сервиса у клиентов

24.3 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
```

24.4 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
```

24.5 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
```

24.6 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
```

24.7 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
```

24.8 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
```

24.9 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
```

24.10 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
```

25 Приложение A. Packet Flow

- Порядок обработки входящего/исходящего трафика сетевыми службами контроллерами WLC
- Порядок обработки транзитного трафика сетевыми службами контроллерами WLC

25.1 Порядок обработки входящего/исходящего трафика сетевыми службами контроллерами WLC

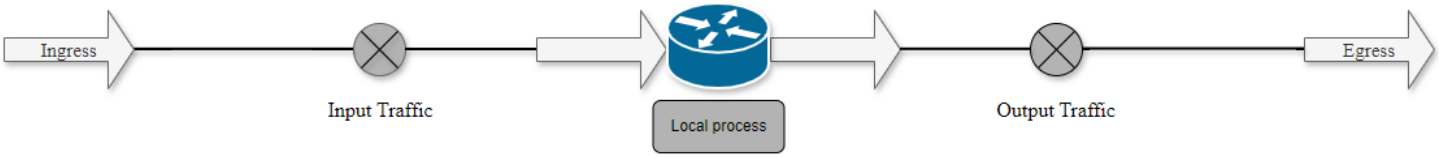


Таблица 25 – Порядок обработки входящего трафика

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.

25.2 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]

Шаг	Описание
11	tcp adjust-mss[1]
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