

Вас приветствует LTE CPE!

Справочник по LTE CPE

Выпуск 01

Дата 2012-09-22

Huawei Technologies Co., Ltd.

Адрес: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Веб-сайт: <http://www.huawei.com>

Эл. почта: mobile@huawei.com

Авторские права © Huawei Technologies Co., Ltd. 2013. Все права защищены.

Ни одна из частей данного документа не может быть воспроизведена или передана по каналам связи в любой форме или любыми средствами без предварительного письменного согласия компании Huawei Technologies Co., Ltd.

Товарные знаки



HUAWEI и другие товарные знаки Huawei являются товарными знаками компании Huawei Technologies Co., Ltd.

Другие товарные знаки и наименования компаний, упомянутые в данном документе, принадлежат исключительно их владельцам.

Примечание

Покупка оборудования, услуг и функций оговаривается в коммерческом контракте между компанией Huawei и заказчиком. Все оборудование или его часть, а также услуги и функции, описанные в данном документе, могут не совпадать с объемом покупки или не соответствовать целям использования. Если иначе не оговорено контрактом, то все утверждения, сведения и рекомендации, приводимые в данном документе, не являются явно выраженной или подразумеваемой гарантией любого вида (истинности или достоверности).

Документ содержит текущую информацию на момент его издания, которая может быть изменена без предварительного уведомления. При подготовке документа были приложены все усилия для обеспечения достоверности информации, но все утверждения, сведения и рекомендации, приводимые в данном документе, не являются явно выраженной или подразумеваемой гарантией (истинности или достоверности).

Содержание

1 Подготовка к работе	6
1.1 Вас приветствует CPE	6
1.2 Требования к компьютеру	6
2 Главная страница.....	7
2.1 Обзор	7
2.1.1 Состояние сети Интернет	7
2.1.2 Использование сети Интернет	7
2.1.3 Состояние сети Wi-Fi	7
2.1.4 Использование сети LAN	8
2.2 О продукте	8
2.2.1 О продукте	8
2.2.2 Список устройств	8
2.3 Обновление	8
2.3.1 Локальное обновление	8
2.3.2 Обновление HTTP	9
3 Интернет.....	10
3.1 Подключение к сети	10
3.1.1 Выбор режима сети	10
3.1.2 Выбор режима подключения	10
3.1.3 Выбор сети для подключения	11
3.1.4 Включение и отключение роуминга данных	11
3.1.5 Выбор профиля APN	12
3.2 Управление APN	12
3.2.1 Создание профиля APN	12
3.2.2 Изменение профиля APN	12
3.2.3 Удаление профиля APN	13
3.3 Управление PIN-кодом	13
3.3.1 Просмотр статуса USIM-карты	13
3.3.2 Включение проверки PIN-кода	13
3.3.3 Отключение проверки PIN-кода	13
3.3.4 Проверка PIN-кода	14
3.3.5 Изменение PIN-кода	14




3.3.6 Установка автоматической проверки PIN-кода.....	14
3.3.7 Проверка PUK-кода.....	15
3.4 Настройка MTU.....	15
3.5 Разблокировка USIM-карты	16
4 LAN.....	17
4.1 Настройки DHCP.....	17
4.1.1 Настройки хоста LAN.....	17
4.1.2 Настройки DHCP	17
4.1.3 Список связанных адресов.....	18
4.2 Статическая маршрутизация	19
4.3 Динамическая маршрутизация.....	20
5 Wi-Fi	21
5.1 Wi-Fi	21
5.1.1 Общие настройки.....	21
5.1.2 Профиль SSID	21
5.2 Управление доступом.....	24
5.2.1 Настройки.....	24
5.2.2 Список доступа Wi-Fi	24
5.3 Настройки WPS	26
5.4 Гостевой доступ Wi-Fi	26
5.5 Дополнительные настройки	27
5.6 WDS.....	28
6 Безопасность.....	30
6.1 Уровень брандмауэра	30
6.2 Фильтрация MAC-адресов	30
6.2.1 Белый список MAC-адресов	30
6.2.2 Черный список MAC-адресов.....	32
6.3 Фильтрация URL-адресов.....	32
6.3.1 Белый список URL-адресов	32
6.3.2 Черный список URL-адресов.....	33
6.4 Фильтрация IP-адресов	33
6.4.1 Белый список IP-адресов.....	33
6.4.2 Черный список IP-адресов	34
6.5 Контроль доступа к услугам.....	34
6.6 ALG.....	35
6.7 Переадресация портов	35
6.8 UPnP	37
6.8.1 UPnP	37
6.9 DMZ.....	37
7 Сервисы	38

7.1 DDNS.....	38
7.2 Сообщения SMS	38
7.2.1 Просмотр сообщений SMS.....	38
7.2.2 Отправка сообщений SMS.....	39
7.2.3 Сохранение сообщений SMS	39
7.2.4 Пересылка сообщений SMS	39
7.2.5 Ответ на сообщения SMS	39
7.2.6 Удаление сообщений SMS.....	40
7.3 Настройки SMS	40
8 Система	41
8.1 Обслуживание.....	41
8.1.1 Перезагрузка.....	41
8.1.2 Сброс.....	41
8.1.3 Загрузка файла конфигурации	41
8.1.4 Выгрузка файла конфигурации	42
8.2 Смена пароля	42
8.3 Дата и время.....	43
8.4 Диагностика	43
8.4.1 Команда Ping.....	44
8.4.2 Команда Traceroute.....	44
8.4.3 Проверка системы.....	44
8.4.4 Проверка статуса беспроводной сети.....	46
8.5 Журнал	46
8.6 Уведомление системы	46
9 Часто задаваемые вопросы.....	48
10 Сокращения	49
11 Уведомление об авторских правах и отказ от гарантий.....	51

1 Подготовка к работе

1.1 Вас приветствует CPE

В данном документе вместо LTE (Long Term Evolution) CPE (customer premises equipment) далее будет использоваться просто CPE. Внимательно ознакомьтесь со следующими символами для безопасной и корректной эксплуатации Вашего CPE:

-  Дополнительная информация по теме
-  Дополнительные методы или ярлыки для действия
-  Потенциальные проблемы или обозначения, на которые необходимо обратить внимание

1.2 Требования к компьютеру

Для обеспечения нормальной работы Ваш компьютер должен соответствовать требованиям CPE.

Пункт	Требование
Процессор	Pentium 500 МГц или выше
Память	ОЗУ 128 МБ или выше
Жесткий диск	50 МБ свободного места
Операционная система	<ul style="list-style-type: none"> • Microsoft: Windows XP, Windows Vista или Windows 7 • Mac: Mac OS X
Разрешение экрана	1024 x 768 пикселей или выше
Браузер	<ul style="list-style-type: none"> • Internet Explorer 6.0 или более поздней версии • Firefox 4.0 или более поздней версии • Opera 11 или более поздней версии • Safari 3 или более поздней версии • Chrome любой версии

2 Главная страница

2.1 Обзор

2.1.1 Состояние сети Интернет

Для просмотра состояния сети Интернет:

1. Выберите **Главная > Обзор**.

Откроется страница **Состояние сети Интернет**.

2. Посмотрите информацию о состоянии сети Интернет, включая **Статус USIM-карты, Режим сети, Статус** и т.д.

----Конец

2.1.2 Использование сети Интернет

Для просмотра данных об использовании ресурсов сети:

1. Выберите **Главная > Обзор**.

Откроется страница **Использование сети Интернет**.

2. Посмотрите данные, включая скорость передачи и приема, объем принимаемого и передаваемого трафика и время, прошедшее с момента подключения.

----Конец

2.1.3 Состояние сети Wi-Fi

Для просмотра состояния сети Wi-Fi:

1. Выберите **Главная > Обзор**.

Откроется страница **Состояние сети Wi-Fi**.

2. Посмотрите информацию о состоянии сети Wi-Fi, включая **SSID, IP-адрес, MAC-адрес, режим рассылки** и режим шифрования беспроводной сети.
3. Посмотрите данные статистики сети Wi-Fi, включая количество принятых и переданных по сети Wi-Fi байтов, пакетов, ошибочных пакетов и отброшенных пакетов.

----Конец

2.1.4 Использование сети LAN

Для просмотра информации о состоянии подключения локальной сети (LAN) выберите **Главная > Обзор**.

Откроется страница **Использование сети LAN**. Посмотрите данные о состоянии сети LAN, включая **IP-адрес**, **MAC-адрес** и **DHCP-сервер**. Также Вы можете посмотреть данные статистики сети LAN, включая количество принятых и переданных по сети LAN байтов, пакетов, ошибочных пакетов и отброшенных пакетов.

2.2 О продукте

2.2.1 О продукте

Для просмотра основной информации о продукте выберите **Главная > О продукте**.

Откроется страница **О продукте**. На данной странице приведена основная информация о CPE, включая модель, серийный номер (SN), международный идентификатор мобильного оборудования (IMEI), версию прошивки и аппаратного обеспечения.

2.2.2 Список устройств

В списке устройств приведена информация об активных устройствах.

Для просмотра списка устройств выберите **Главная > О продукте**.

Откроется страница **Список устройств**. На этой странице Вы можете посмотреть информацию об устройствах, включая **Имя ПК**, **MAC-адрес**, **IP-адрес** и **Время аренды**. **Время аренды** - это оставшийся срок аренды, назначенный динамическим DHCP-сервером. Если устройство имеет привязку к статическому IP-адресу, то параметры **Время аренды** и **Имя ПК** имеют значения "-" и "Неизвестно" соответственно.

2.3 Обновление

С помощью данной функции Вы сможете обновить операционную систему до последней версии. Обновление системы выполнять рекомендуется, потому что в новой версии, как правило, устраняются некоторые ошибки предыдущей версии, что повышает стабильность системы.

2.3.1 Локальное обновление

Перед обновлением сохраните нужную версию ПО на компьютере.

Для выполнения локального обновления:

1. Выберите **Главная > Обновление**.

Откроется страница **Обновление**.

2. Нажмите **Обзор** на вкладке **Локальное обновление**. В появившемся диалоговом окне выберите файл нужной версии ПО.

3. Нажмите **Открыть**. Диалоговое окно закроется. В поле **Файл обновлений** будет отображаться путь и имя файла новой версии ПО.
4. Нажмите **Обновить**. В открывшемся диалоговом окне подтвердите выполнение данной операции.



В процессе обновления не отключайте питание CPE и не отсоединяйте CPE от компьютера.

5. Нажмите **ОК**. Начнется обновление ПО. После обновления будет выполнена автоматическая перезагрузка CPE.

---Конец

2.3.2 Обновление НТТР

Для выполнения обновления НТТР:

1. Выберите **Главная > Обновление**.
Откроется страница **Обновление**.
2. Нажмите **Проверить** для проверки обновлений.

Если...	Тогда...
Обновления найдены.	Перейдите к шагу 3.
Обновления не найдены.	Процедура завершена.

3. Нажмите **Обновить** для загрузки обновлений.
На экране отобразится ход загрузки.
4. После завершения загрузки начнется процесс автоматического обновления.
На экране отобразится ход обновления.
5. После обновления будет выполнена автоматическая перезагрузка CPE.
На экране появится сообщение о том, что обновление завершено.



В процессе обновления не выполняйте никаких операций на CPE.

6. Если произошел сбой обновления, CPE может не включиться. В этом случае попробуйте принудительно восстановить предыдущую версию системы.



Для принудительного восстановления системы нажмите одновременно кнопку WPS и кнопку WLAN, а затем нажмите кнопку питания.

---Конец

3 Интернет

3.1 Подключение к сети

3.1.1 Выбор режима сети

Вы можете выбрать сетевой режим для CPE. Параметру **Режим сети** можно установить следующие значения: **4G/3G Авто**, **4G/3G/2G Авто**, **4G**, **3G** или **2G**.

Для выбора режима сети:

1. Вставьте действующую USIM-карту в CPE.
2. Включите питание CPE и выполните вход на веб-интерфейс в качестве пользователя admin.
3. Выберите **Интернет > Подключение к сети**.

Откроется страница **Подключение к сети**.

4. Установите параметру **Режим сети** одно из следующих значений:

Значение	Описание
4G/3G Авто	CPE автоматически выберет себе рабочий режим в порядке предпочтения 4G и 3G .
4G/3G/2G Авто	CPE автоматически выберет себе рабочий режим в порядке предпочтения 4G, 3G и 2G.
4G	CPE получает доступ только к сетям 4G.
3G	CPE получает доступ только к сетям 3G.
2G	CPE получает доступ только к сетям 2G.

5. Нажмите **Подтвердить**.

---Конец

3.1.2 Выбор режима подключения

Вы можете выбрать режим подключения к сети на странице **Подключение к сети**. **Всегда вкл.** - это постоянное подключение к сети. Если позволяют условия, и установлено значение **Всегда вкл.**, CPE будет автоматически подключаться к сети

Интернет. **Вручную** - это режим ручного подключения и отключения CPE от сети Интернет. **По запросу** – это режим подключения CPE к сети Интернет только после Вашего запроса доступа (например, при использовании поисковой системы). Отключение CPE от сети Интернет происходит после определенного периода бездействия.

Для выбора режима подключения к сети:

1. Выберите **Интернет > Подключение к сети**.
Откроется страница **Подключение к сети**.
2. Установите параметру **Режим подключения** значение **Всегда вкл., Вручную** или **По запросу**.
 - При выборе режима **Вручную** включите опцию **При перезагрузке**, которая позволит CPE сохранять одинаковый статус подключения до и после перезагрузки.
 - При выборе **По запросу** установите **Макс. время простоя**.
3. Нажмите **Подтвердить**.

----Конец

3.1.3 Выбор сети для подключения

Если CPE не подключен к сети, а **Режим подключения** имеет значение **Вручную**, Вы можете самостоятельно выбрать сеть для подключения на странице **Подключение к сети**. Для выбора сети:

1. Установите параметру **Выбор сети** значение **Вручную**.
По умолчанию **Выбор сети** установлен как **Авто**, что позволяет CPE автоматически выбирать сеть.
2. Нажмите **Поиск**.
3. Из списка найденных сетей выберите сеть, к которой хотите подключиться, и нажмите **Регистрация**.
4. Нажмите **Подтвердить**.

---Конец

3.1.4 Включение и отключение роуминга данных

Для включения или отключения параметра **Роуминг**:

1. Выберите **Интернет > Подключение к сети**.
Откроется страница **Подключение к сети**.
2. Установите или уберите флажок в поле **Роуминг**.
3. Нажмите **Подтвердить**.

----Конец

3.1.5 Выбор профиля APN

Профиль APN - это группа параметров, относящихся к имени точки доступа (APN). Для доступа CPE к сети Интернет Вы можете выбрать профиль APN.

Для настройки параметров:

1. Выберите **Интернет > Подключение к сети**.

Откроется страница **Подключение к сети**.

2. Выберите профиль.
3. Нажмите **Подтвердить**.

----Конец

3.2 Управление APN

3.2.1 Создание профиля APN

Для создания профиля APN:

1. Выберите **Интернет > Управление APN**.

Откроется страница **Управление APN**.

2. Нажмите **Добавить**.
3. На появившейся странице задайте параметры **Имя профиля, APN, Логин и Пароль**.
4. Установите параметру **Аутентификация** значение **Отсутствует, PAP, CHAP** или **Авто**.
5. Нажмите **Подтвердить**.

----Конец

3.2.2 Изменение профиля APN

Для изменения профиля APN:

1. Выберите **Интернет > Управление APN**.

Откроется страница **Управление APN**.

2. Выберите **Профиль APN**, параметры которого хотите изменить, и нажмите **Изменить**.
3. На появившейся странице измените значения параметров **Имя профиля, APN, Логин и Пароль**.
4. Установите параметру **Аутентификация** значение **Отсутствует, PAP, CHAP** или **Авто**.
5. Нажмите **Подтвердить**.

----Конец

3.2.3 Удаление профиля APN

Для удаления профиля APN:

1. Выберите **Интернет > Управление APN**.

Откроется страница **Управление APN**.

2. Выберите **Профиль APN**, который хотите удалить, и нажмите **Удалить**.
3. В появившемся диалоговом окне нажмите **ОК**.

----Конец

3.3 Управление PIN-кодом

На странице **Управление PIN-кодом** Вы можете выполнить следующие операции:

- Посмотреть статус USIM-карты.
- Включить или отключить проверку PIN-кода.
- Проверить PIN-код.
- Изменить PIN-код.
- Установить автоматическую проверку PIN-кода.
- Проверить код разблокировки PIN-кода (PUK-код).

3.3.1 Просмотр статуса USIM-карты

Для просмотра статуса USIM-карты:

1. Выберите **Интернет > Управление PIN-кодом**.

Откроется страница **Управление PIN-кодом**.

2. Посмотрите статус USIM-карты в поле **Статус USIM-карты**.

----Конец

3.3.2 Включение проверки PIN-кода

Для включения проверки PIN-кода:

1. Выберите **Интернет > Управление PIN-кодом**.

Откроется страница **Управление PIN-кодом**.

2. Установите флажок в поле **Включить** для функции **Проверка PIN-кода**.
3. Введите PIN-код (от 4 до 8 цифр) в поле **Ввод PIN-кода**.
4. Нажмите **Подтвердить**.

----Конец

3.3.3 Отключение проверки PIN-кода

Для отключения проверки PIN-кода:

1. Выберите **Интернет > Управление PIN-кодом**.
Откроется страница **Управление PIN-кодом**.
 2. Установите флажок в поле **Отключить** для функции **Проверка PIN-кода**.
 3. Введите PIN-код (от 4 до 8 цифр) в поле **Ввод PIN-кода**.
 4. Нажмите **Подтвердить**.
- Конец

3.3.4 Проверка PIN-кода

Если проверка PIN-кода включена, а PIN-код не проверен, рекомендуется выполнить его проверку.

Для проверки PIN-кода:

1. Выберите **Интернет > Управление PIN-кодом**.
Откроется страница **Управление PIN-кодом**.
 2. Введите PIN-код (от 4 до 8 цифр) в поле **Ввод PIN-кода**.
 3. Нажмите **Подтвердить**.
- Конец

3.3.5 Изменение PIN-кода

PIN-код можно изменить, только если включена проверка PIN-кода, и PIN-код проверен.

Для изменения PIN-кода:

1. Выберите **Интернет > Управление PIN-кодом**.
Откроется страница **Управление PIN-кодом**.
 2. Установите флажок в поле **Включить** для функции **Проверка PIN-кода**.
 3. Установите флажок в поле **Включить** для функции **Смена PIN-кода**.
 4. Введите текущий PIN-код (от 4 до 8 цифр) в поле **PIN-код**.
 5. Введите новый PIN-код (от 4 до 8 цифр) в поле **Новый PIN-код**.
 6. Ещё раз введите новый PIN-код в поле **Подтверждение PIN-кода**.
 7. Нажмите **Подтвердить**.
- Конец

3.3.6 Установка автоматической проверки PIN-кода

Вы можете включить или отключить автоматическую проверку PIN-кода. Если автоматическая проверка включена, то после перезапуска CPE будет автоматически проверять PIN-код. Данную функцию можно включить, только если включена проверка PIN-кода, и PIN-код проверен.

Для включения автоматической проверки PIN-кода:

1. Выберите **Интернет > Управление PIN-кодом**.
- Откроется страница **Управление PIN-кодом**.
2. Установите флажок в поле **Включить** для функции **Проверка PIN-кода**.
3. Установите флажок в поле **Включить** для функции **Запоминание PIN-кода**.
4. Нажмите **Подтвердить**.

----Конец

3.3.7 Проверка PUK-кода

Если включена проверка PIN-кода, и PIN-код три раза подряд не прошел проверку, он будет заблокирован. В этом случае необходимо выполнить проверку PUK-кода и изменить PIN-код для его разблокировки.

Для проверки PUK-кода:

1. Выберите **Интернет > Управление PIN-кодом**.
- Откроется страница **Управление PIN-кодом**.
2. Введите PUK-код в поле **PUK-код**.
3. Введите новый PIN-код в поле **Новый PIN-код**.
4. Ещё раз введите новый PIN-код в поле **Подтверждение PIN-кода**.
5. Нажмите **Подтвердить**.

----Конец

3.4 Настройка MTU

Вы можете задать максимальное количество байтов в пакетах, передаваемых через сетевой порт.

Примечание: Слишком большое значение MTU может вызвать сбой сетевого соединения.

Для изменения значения MTU:

1. Выберите **Интернет > MTU для Интернет**.
- Откроется страница **MTU для Интернет**.
2. Введите значение MTU в поле **MTU для Интернет**.
3. Нажмите **Подтвердить**.

----Конец

3.5 Разблокировка USIM-карты

Для получения кода разблокировки обратитесь к провайдеру услуг. После разблокировки USIM-карты произойдет автоматическая перезагрузка CPE.

Примечание: Если безуспешных попыток будет слишком много, USIM-карта заблокируется навсегда.

Для разблокировки USIM-карты:

1. Выберите **Интернет > Блокировка SIM-карты**.
Откроется страница **Блокировка SIM-карты**.
2. Введите код разблокировки в поле **Код разблокировки**.
3. Нажмите **Подтвердить**.
----Конец

4 LAN

4.1 Настройки DHCP

4.1.1 Настройки хоста LAN

Вы можете изменить IP-адрес хоста на любой другой IP-адрес, который легко запомнить. Однако необходимо, чтобы новый IP-адрес был уникальным в Вашей сети. Если Вы измените IP-адрес CPE, то доступ к веб-интерфейсу пользователя будет осуществляться по новому IP-адресу.

Для изменения IP-адреса CPE:

1. Выберите **LAN > Настройки DHCP**.
- Откроется страница **Настройки DHCP**.
2. Установите значение параметра **IP-адрес**.
3. Установите флажок в поле **Включить** для параметра **DHCP-сервер**.
4. Нажмите **Подтвердить**.

----Конец

4.1.2 Настройки DHCP

DHCP позволяет клиентам автоматически получать настройки TCP/IP при запуске сервера.


Вы можете сконфигурировать CPE в качестве DHCP-сервера или отключить функцию DHCP-сервера, когда CPE работает в режиме маршрутизации.

Когда CPE выполняет функции DHCP-сервера, он автоматически предоставляет настройки TCP/IP для клиентов LAN, которые поддерживают возможности DHCP-клиента. Если службы DHCP-сервера отключены, Вам потребуется другой DHCP-сервер в сети LAN, в противном случае Вы должны будете настроить каждый клиент вручную.


Для конфигурирования настроек DHCP:

1. Выберите **LAN > Настройки DHCP**.
- Откроется страница **Настройки DHCP**.
2. Установите флажок в поле **Включить** для параметра **DHCP-сервер**.

3. Установите значение параметра **Начальный IP-адрес**.

 Данный IP-адрес должен отличаться от IP-адреса, установленного на странице **Настройки хоста LAN**, но оба адреса должны принадлежать одному сетевому сегменту.

4. Установите значение параметра **Конечный IP-адрес**.

 Данный IP-адрес должен отличаться от IP-адреса, установленного на странице **Настройки хоста LAN**, но оба адреса должны принадлежать одному сетевому сегменту.

Конечный IP-адрес должен совпадать или превышать начальный IP-адрес.

5. Установите значение параметра **Время аренды**.


 Значение параметра должно быть в интервале от 1 до 10 080 минут.

6. Нажмите **Подтвердить**.

----Конец

4.1.3 Список связанных адресов

Вы можете установить привязку IP-адреса к MAC-адресу устройства. При каждом подключении к DHCP-серверу устройству будет назначаться один и тот же IP-адрес. Например, Вы можете установить привязку IP-адреса к FTP-серверу в сети LAN.

 После изменения настроек нажмите **Подтвердить**, чтобы изменения вступили в силу. Также может потребоваться перезагрузка DHCP-сервера.

Для конфигурирования или просмотра списка связанных адресов:

1. Выберите **LAN > Настройки DHCP**.
2. Нажмите **Ред. список**.

Откроется страница **Привязка адресов**.

----Конец

Для добавления правила MAC/IP:

1. Нажмите **Добавить**.
2. На открывшейся странице установите значения параметров **MAC-адрес** и **IP-адрес**.
3. Нажмите **Подтвердить**.

----Конец

Для изменения правила MAC/IP:

1. Выберите правило, которое хотите изменить, и нажмите **Изменить**.
2. На открывшейся странице установите значения параметров **MAC-адрес** и **IP-адрес**.
3. Нажмите **Подтвердить**.

----Конец

Для удаления правила MAC/IP:

1. Выберите правило, которое хотите удалить, и нажмите **Удалить**.
2. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Для удаления всех правил MAC/IP:

1. Нажмите **Удалить все**.
2. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Чтобы изменения вступили в силу, нажмите **Применить** или **Назад**, а затем на экране **Настройки DHCP** нажмите **Подтвердить**.

4.2 Статическая маршрутизация

Если в сети LAN используется каскадное подключение маршрутизаторов, то добавьте правила статической маршрутизации, чтобы обеспечить доступность устройств, подключенных к маршрутизаторам. Данная функция аналогична динамической маршрутизации. Тем не менее, для неё требуется конфигурирование вручную и постоянная доступность маршрутизатора.

- Если маршрутизатор каскадного соединения имеет постоянный IP-адрес, рекомендуется включить статическую маршрутизацию.
- Если маршрутизатор каскадного соединения имеет переменный IP-адрес, рекомендуется использовать динамическую маршрутизацию.

Для конфигурирования настроек статической маршрутизации:

1. Выберите **LAN > Статическая маршрутизация**.

Откроется страница **Статическая маршрутизация**.

2. Нажмите кнопку **Добавить**, расположенную в правом верхнем углу на странице **Статическая маршрутизация**.
3. Установите значение параметра **IP-адрес назначения**.
4. Установите значение параметра **Маска подсети**.
5. Установите значение параметра **IP-адрес маршр-ра**. Значение данного параметра - это IP-адрес CPE, который используется каскадно-соединенными устройствами для передачи данных. IP-адрес должен быть доступен.
6. Нажмите **Подтвердить**.

----Конец

4.3 Динамическая маршрутизация

Динамическая маршрутизация используется при каскадном подключении маршрутизаторов, соответствующих протоколу RIP, в сети LAN. На данной странице Вы можете включить или отключить RIP, а также задать его версию и режим работы.

Для конфигурирования настроек динамической маршрутизации:

1. Выберите **LAN > Динамическая маршрутизация**.

Откроется страница **Динамическая маршрутизация**.

2. Установите флажок в поле **Включить** для параметра **RIP**.
3. Установите значение параметра **Операция**. Если Вы установите **Активная**, CPE будет активно выполнять изменения маршрутов и уведомлять о них окружающие маршрутизаторы. Если Вы установите **Пассивная**, CPE не будет выполнять изменения маршрутов без соответствующего уведомления.
4. Установите параметру **Версия** значение **RIP v1**, **RIP v2** или **RIP v1/RIP v2**.
5. Нажмите **Подтвердить**.

---Конец

5 Wi-Fi

5.1 Wi-Fi

5.1.1 Общие настройки

Данная функция предназначена для настройки основных параметров Wi-Fi.

Для конфигурирования основных настроек Wi-Fi:

1. Выберите **Wi-Fi > Настройки Wi-Fi**.
Откроется страница **Настройки Wi-Fi**.
2. Установите флажок в поле **Включить** для функции **Wi-Fi**.
3. Установите параметру **Режим** одно из следующих значений:

Значение	Описание
802.11b/g/n	Клиент Wi-Fi может получать доступ к CPE в режиме 802.11b, 802.11g или 802.11n. При подключении клиента к CPE в режиме 802.11n рекомендуется использовать шифрование AES.
802.11b/g	Клиент Wi-Fi может получать доступ к CPE в режиме 802.11b или 802.11g.
802.11b	Клиент Wi-Fi может получать доступ к CPE в режиме 802.11b.
802.11g	Клиент Wi-Fi может получать доступ к CPE в режиме 802.11g.
802.11n	Клиент Wi-Fi может получать доступ к CPE в режиме 802.11n.

4. Нажмите **Подтвердить**.

----Конец

5.1.2 Профиль SSID

Конфигурирование CPE на странице **Профиль SSID** позволит клиенту Wi-Fi подключаться к CPE на основании установленных правил, повышающих безопасность доступа.

Для конфигурирования CPE на странице **Профиль SSID**:

1. Выберите **Wi-Fi > Настройки Wi-Fi**.

Откроется страница **Настройки Wi-Fi**.

2. Установите **SSID**.



SSID может содержать от 1 до 32 символов ASCII.

Клиент Wi-Fi подключается к CPE с помощью найденного SSID.

3. Установите параметр **Макс. количество устройств**.



Данный параметр определяет максимальное количество клиентов Wi-Fi, подключенных к CPE.

Максимум 32 клиента могут подключиться к CPE.

4. Установите флажок в поле **Включить** для параметра **Скрыть рассылку SSID**.

Когда SSID скрыт, клиент не может найти информацию Wi-Fi о CPE.

5. Установите флажок в поле **Включить** для параметра **Изоляция AP**.

Клиенты могут подключаться к CPE, но не могут взаимодействовать друг с другом.

6. Установите значение параметра **Безопасность**.



Если данный параметр имеет значение **Отсутствует (не рекоменд.)**, клиент Wi-Fi напрямую подключается к CPE. Такой способ подключения предоставляет много рисков для безопасности.

Если данный параметр имеет значение **WEP**, клиент Wi-Fi подключается к CPE в режиме веб-шифрования.

Если данный параметр имеет значение **WPA-PSK**, клиент Wi-Fi подключается к CPE в режиме шифрования WPA-PSK.

Если данный параметр имеет значение **WPA2-PSK (рекомендуется)**, клиент Wi-Fi подключается к CPE в режиме шифрования WPA2-PSK. Данный режим рекомендуется из-за высокого уровня безопасности.

Если данный параметр имеет значение **WPA-PSK и WPA2-PSK**, клиент Wi-Fi подключается к CPE в режиме шифрования WPA-PSK или WPA2-PSK.

7. Установите параметру **Режим аутентификации** одно из следующих значений и настройте соответствующие параметры.

Значение	Параметр	Описание
WEP	Режим аутентификации	<ul style="list-style-type: none"> • С общим ключом: При подключении клиента к CPE используется режим аутентификации с общим ключом. • Открытая аутентификация: При подключении клиента к CPE используется режим открытой аутентификации. • Обе: При подключении клиента к CPE используется либо режим открытой аутентификации, либо режим аутентификации с общим ключом.
	Длина пароля	<ul style="list-style-type: none"> • 128 бит: В поля Пароль 1 ~ Пароль 4 можно ввести только 13 символов ASCII или 26 шестнадцатеричных символов. • 64 бита: В поля Пароль 1 ~ Пароль 4 можно ввести только 5 символов ASCII или 10 шестнадцатеричных символов.
	Индекс текущего пароля	Индекс может иметь значение 1, 2, 3 или 4 . После выбора ключевого индекса соответствующий ключ вступит в силу.
WPA-PSK	WPA-PSK	Можно ввести только от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Параметр может иметь значение TKIP+AES, AES или TKIP .
WPA2-PSK (рекомендуется)	WPA-PSK	Можно ввести только от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Параметр может иметь значение TKIP+AES, AES или TKIP .
WPA-PSK и WPA2-PSK	WPA-PSK	Можно ввести только от 8 до 63 символов ASCII или от 8 до 64 шестнадцатеричных символов.
	Шифрование WPA	Параметр может иметь значение TKIP+AES, AES или TKIP .

8. Нажмите **Подтвердить**.---**Конец**

5.2 Управление доступом

5.2.1 Настройки

Данная функция регулирует доступ к CPE. Для каждого SSID можно установить политику ограничения доступа.

Доступ к MAC-адресу каждого SSID можно задать значением **Отключить**, **Черный список** или **Белый список**.

- Если MAC-доступ SSID получил значение **Отключить**, то данный SSID не будет ограничен в доступе.
- Если MAC-доступ SSID получил значение **Черный список**, тогда к SSID смогут подключаться только устройства, которых нет в черном списке.
- Если MAC-доступ SSID получил значение **Белый список**, тогда к SSID смогут подключаться только устройства из белого списка.

Для конфигурирования настроек, связанных с управлением MAC-адресами Wi-Fi:

1. Выберите **Wi-Fi > Управление доступом**.

Откроется страница **Управление доступом**.

2. Установите MAC-доступ SSID.

3. Нажмите **Подтвердить**.

----Конец

5.2.2 Список доступа Wi-Fi

Данная функция позволит установить политики доступа к SSID на основании MAC-адресов. При установке MAC-адреса Вы можете задать соответствующий ему SSID.

Для добавления записи в Список доступа Wi-Fi:

1. Выберите **Wi-Fi > Управление доступом**.

Откроется страница **Управление доступом**.

2. Нажмите **Ред. список**.

Откроется страница **Список доступа Wi-Fi**.

3. Нажмите **Добавить**.

4. Установите значение параметра **MAC-адрес**.

5. Чтобы MAC-адрес вступил в силу для **SSID-1**, установите флажок в поле **Включить** для параметра **SSID-1**.

Для остальных SSID процедура аналогична процедуре для **SSID-1**.

6. Нажмите **Подтвердить**.

----Конец

Для изменения записи в списке доступа Wi-Fi:

1. Выберите **Wi-Fi > Управление доступом**.
Откроется страница **Управление доступом**.
2. Нажмите **Ред. список**.
Откроется страница **Список доступа Wi-Fi**.
3. Выберите запись, которую хотите изменить, и нажмите **Изменить**.
4. На открывшейся странице установите значение параметра **MAC-адрес**.
5. Чтобы MAC-адрес вступил в силу для **SSID-1**, установите флажок в поле **Включить** для параметра **SSID-1**.

Для остальных SSID процедура аналогична процедуре для **SSID-1**.

6. Нажмите **Подтвердить**.

----Конец

Для удаления записи из списка доступа Wi-Fi:

1. Выберите **Wi-Fi > Управление доступом**.
Откроется страница **Управление доступом**.
2. Нажмите **Ред. список**.
3. Откроется страница **Список доступа Wi-Fi**.
4. Выберите запись, которую хотите удалить, и нажмите **Удалить**.
5. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Для удаления всех записей из списка доступа Wi-Fi:

1. Выберите **Wi-Fi > Управление доступом**.
Откроется страница **Управление доступом**.
2. Нажмите **Ред. список**.
Откроется страница **Список доступа Wi-Fi**.
3. Нажмите **Удалить все**.
4. В появившемся диалоговом окне нажмите **ОК**.

----Конец


Чтобы изменения вступили в силу, нажмите **Применить**. Для возврата на предыдущую страницу нажмите **Назад**.

5.3 Настройки WPS

Функция WPS позволяет быстро подключать беспроводных клиентов к сети без специального конфигурирования параметров беспроводной сети типа SSID, режима безопасности и пароля. Добавить беспроводного клиента можно с помощью кнопки WPS или PIN-кода.

Для подключения клиента к сети CPE:

- В режиме PBC нажмите кнопки WPS на CPE и на клиенте.
- В режиме PIN-кода маршрутизатора введите на клиенте PIN-код маршрутизатора.
- В режиме PIN-кода клиента введите на клиенте PIN-код клиента.


 Если включена функция **Скрыть рассылку SSID**, WPS не работает. WPS поддерживает только WPA2-PSK, WPA2-PSK и WPA-PSK и открытую аутентификацию.

Для конфигурирования настроек WPS Wi-Fi:

1. Выберите **Wi-Fi > Настройки WPS**.

Откроется страница **Настройки WPS**.

2. Установите флажок в поле **Включить** для функции **WPS**.
3. Задайте **Режим WPS**.

 Если данный параметр имеет значение **PBC**, то после нажатия кнопки **Подтвердить** нажмите кнопку WPS на CPE, а затем на клиенте. После этого клиент подключится к CPE.

Если данный параметр имеет значение **PIN-код маршрутизатора**, то для подключения к CPE введите на клиенте PIN-код маршрутизатора.

Если данный параметр имеет значение **PIN-код клиента**, введите PIN-код клиента. После ввода PIN-кода нажмите **Подкл. клиента**, чтобы подключить клиент к CPE.

4. Нажмите **Подтвердить**.

----Конец

5.4 Гостевой доступ Wi-Fi

На странице **Список SSID** приводится информация о тех SSID, которые необходимо настроить. Для конфигурирования SSID:

1. Выберите **Wi-Fi > Гостевой доступ Wi-Fi**.

Откроется страница **Список SSID**.

2. Выберите SSID, который хотите настроить, и нажмите **Изменить**.
3. Установите флажок в поле **Включить** для параметра **Статус**.
4. Установите **SSID**.

- ☰ **SSID** может содержать от 1 до 32 символов ASCII.
SSID не может содержать следующие символы: / ' = " \ &

5. Установите параметр **Макс. количество устройств**.

- ☰ Количество подключенных устройств должно быть целым числом в диапазоне от 1 до 32.

6. Установите флажок в поле **Включить** для функции **Скрыть рассылку SSID**.

7. Установите значение параметра **Изоляция AP**.

Если в поле **Включить** установлен флажок, клиенты могут подключаться к CPE, но не могут взаимодействовать друг с другом. Если в поле **Включить** флажок не установлен, клиенты могут подключаться к CPE и могут взаимодействовать друг с другом

8. Установите значение параметра **Безопасность**.

Если параметру **Режим** установлено значение **802.11n** на странице **Настройки Wi-Fi**, тогда для параметра **Безопасность** можно выбрать только **WPA-PSK**, **WPA2-PSK** или соответствующее значение параметра **Режим аутентификации**.

Если параметр **Безопасность** имеет значение **WPA-PSK**, **WPA2-PSK** или **WPA-PSK и WPA2-PSK**, то можно установить значения **WPA-PSK** и **Шифрование WPA**.

- ☰ **WPA-PSK** может содержать от 8 до 63 символов ASCII или 64 шестнадцатеричных символа.

Если параметр **Безопасность** имеет значение **WEP**, задайте параметры **Режим аутентификации**, **Длина пароля** и **Индекс текущего пароля**, а также сконфигурируйте соответствующие ключи.

Если параметр **Длина пароля** имеет значение **128 бит**, **WPA-PSK** может содержать от 8 до 63 символов ASCII или 64 шестнадцатеричных символа.

Если параметр **Длина пароля** имеет значение **64 бита**, 64-битный ключ шифрования может содержать 5 символов ASCII или 10 шестнадцатеричных символов.

9. Нажмите **Подтвердить**.

----Конец

5.5 Дополнительные настройки

Дополнительные настройки влияют на производительность Wi-Fi. Эти настройки помогут Вам получить максимальную скорость и оптимальную производительность доступа.

Для конфигурирования дополнительных настроек:

1. Установите **Канал**.

Авто означает, что выбран канал с наилучшим качеством сигнала.

Значения от 1 до 13 - это номер выбранного канала.

2. Установите параметр **Частота 802.11n**.

Если данному параметру установить значение **20 МГц**, 802.11n будет поддерживать только полосу пропускания 20 МГц.

Если данному параметру установить значение **20/40 МГц**, 802.11n будет поддерживать полосу пропускания 20 МГц и 40 МГц.

Если параметр **Режим** имеет значение **802.11b** или **802.11g**, данный параметр устанавливать не надо.

3. Установите **Скорость**.

Скорость зависит от выбранного режима.

Если параметр **Скорость** имеет значение **Авто**, то клиент Wi-Fi подключается к CPE по каналу с наилучшим качеством сигнала.

Если задана определенная скорость, клиент будет подключаться к CPE на указанной скорости. Если условия канала не соответствуют требованиям, снижается производительность соединения.

4. Установите **Мощность передачи**.

Если параметр имеет значение **100%**, клиент Wi-Fi использует полную мощность при передаче сигналов.

Если параметр имеет значение **80%**, **60%** или **40%**, клиент Wi-Fi использует меньшую мощность при передаче сигналов. В этом случае клиенты Wi-Fi, расположенные далеко от CPE, не смогут подключиться к нему.

5. Установите **WMM**.

WMM (Wi-Fi Multimedia) - это сертификация лаборатории Альянса Wi-Fi на совместимость с устройствами стандарта IEEE 802.11e. Данный режим обеспечивает качественную работу функций в сетях IEEE 802.11. WMM назначает приоритеты трафику по четырем категориям доступа (AC) – голос, видео, "best effort" и фоновый трафик. Тем не менее, WMM не обеспечивает гарантированную пропускную способность. Режим WMM предназначен для качественной работы простых приложений на Wi-Fi-телефонах, например, IP-телефонии (Voice over IP).

6. Нажмите **Подтвердить**.

---Конец

5.6 WDS

В режиме повторителя модуль Wi-Fi CPE поддерживает систему WDS (Wireless Distribution System). Для использования WDS устройствам Wi-Fi необходимо настроить одинаковый радиоканал, режим шифрования, SSID и ключ шифрования. В качестве режима шифрования WDS можно выбрать режим **Открытая аутентификация** или **WPA-PSK и WPA2-PSK**. При выборе режима **Открытая аутентификация** для клиентов Wi-Fi можно установить значение **Отсутствует** или **WEP**. При выборе режима шифрования **WPA-PSK и WPA2-PSK** клиенты Wi-Fi смогут использовать шифрование **WPA/WPA2-PSK**. После включения WDS отключите DHCP на всех CPE, которые не подключены напрямую к порту WAN. Убедитесь, что все CPE используют разные IP-адреса шлюза, которые принадлежат одному сетевому сегменту.

Примечание: Если WDS включена, функция WPS не работает. Если для канала установлено значение **Авто**, перейдите на страницу **Дополнительные настройки**, чтобы указать определенное значение для канала.

Для включения WDS:

1. Выберите **Wi-Fi > WDS**.

Откроется страница **Настройки WDS**.

2. Установите флажок в поле **Включить** для функции **WDS**.
3. Нажмите **Поиск**.

Из результатов поиска выберите SSID сетевого устройства.

4. Установите значение параметра **Безопасность**.



WPA-PSK может содержать от 8 до 63 символов ASCII или 64 шестнадцатеричных символа.

5. Нажмите **Подтвердить**.

---**Конец**

6 Безопасность

6.1 Уровень брандмауэра

На данной странице Вы можете настроить уровень брандмауэра.

Для установки уровня брандмауэра:

1. Выберите **Безопасность > Уровень брандмауэра**.

Откроется страница **Уровень брандмауэра**.

2. Установите **Уровень брандмауэра**.
3. Нажмите **Подтвердить**.

---Конец

Для конфигурирования настроек фильтрации брандмауэра:

1. Выберите **Безопасность > Уровень брандмауэра**.

Откроется страница **Уровень брандмауэра**.

2. Установите параметру **Уровень брандмауэра** значение **Специальный**.
3. Установите параметр **Фильтрация MAC-адресов**.
4. Установите параметр **Фильтрация IP-адресов**.
5. Установите параметр **Фильтрация URL-адресов**.
6. Нажмите **Подтвердить**.

---Конец

6.2 Фильтрация MAC-адресов

На данной странице можно сконфигурировать правила фильтрации MAC-адресов.

6.2.1 Белый список MAC-адресов

Для добавления правила белого списка MAC-адресов:

1. Выберите **Безопасность > Фильтрация MAC-адресов**.
Откроется страница **Фильтрация MAC-адресов**.
2. Установите параметру **Режим MAC-фильтрации** значение **Белый список**.
3. Нажмите **Добавить**.
4. На открывшейся странице установите параметр **MAC**.
5. Нажмите **Подтвердить**.

----**Конец**

Для изменения правила белого списка MAC-адресов:

1. Выберите **Безопасность > Фильтрация MAC-адресов**.
Откроется страница **Фильтрация MAC-адресов**.
2. Установите параметру **Режим MAC-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите изменить, и нажмите **Изменить**.
4. На открывшейся странице установите параметр **MAC**.
5. Нажмите **Подтвердить**.

----**Конец**

Для удаления правила белого списка MAC-адресов:

1. Выберите **Безопасность > Фильтрация MAC-адресов**.
Откроется страница **Фильтрация MAC-адресов**.
2. Установите параметру **Режим MAC-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите удалить, и нажмите **Удалить**.
4. В появившемся диалоговом окне нажмите **ОК**.

----**Конец**

Для удаления всех правил белого списка MAC-адресов:

1. Выберите **Безопасность > Фильтрация MAC-адресов**.
Откроется страница **Фильтрация MAC-адресов**.
2. Установите параметру **Режим MAC-фильтрации** значение **Белый список**.
3. Нажмите **Удалить все**.
4. В появившемся диалоговом окне нажмите **ОК**.

----**Конец**

6.2.2 Черный список MAC-адресов

Выберите **Безопасность > Фильтрация MAC-адресов**. Установите параметру **Режим MAC-фильтрации** значение **Черный список**.

Остальные операции аналогичны операциям с белым списком MAC-адресов.

6.3 Фильтрация URL-адресов

На данной странице можно сконфигурировать правила фильтрации URL-адресов.

6.3.1 Белый список URL-адресов

Для добавления правила белого списка URL-адресов:

1. Выберите **Безопасность > Фильтрация URL-адресов**.

Откроется страница **Фильтрация URL-адресов**.

2. Установите параметру **Режим URL-фильтрации** значение **Белый список**.
3. Нажмите **Добавить**.
4. Установите **URL-адрес**.
5. Нажмите **Подтвердить**.

----Конец

Для изменения правила белого списка URL-адресов:

1. Выберите **Безопасность > Фильтрация URL-адресов**.

Откроется страница **Фильтрация URL-адресов**.

2. Установите параметру **Режим URL-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите изменить, и нажмите **Изменить**.
4. На открывшейся странице установите параметр **URL-адрес**.
5. Нажмите **Подтвердить**.

----Конец

Для удаления правила белого списка URL-адресов:

1. Выберите **Безопасность > Фильтрация URL-адресов**.

Откроется страница **Фильтрация URL-адресов**.

2. Установите параметру **Режим URL-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите удалить, и нажмите **Удалить**.
4. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Для удаления всех правил белого списка URL-адресов:

1. Выберите **Безопасность > Фильтрация URL-адресов**.
Откроется страница **Фильтрация URL-адресов**.
 2. Установите параметру **Режим URL-фильтрации** значение **Белый список**.
 3. Нажмите **Удалить все**.
 4. В появившемся диалоговом окне нажмите **ОК**.
- Конец

6.3.2 Черный список URL-адресов

Выберите **Безопасность > Фильтрация URL-адресов**. Установите параметру **Режим URL-фильтрации** значение **Черный список**.

Остальные операции аналогичны операциям с белым списком URL-адресов.

6.4 Фильтрация IP-адресов

На данной странице можно сконфигурировать правила фильтрации IP-адресов.

6.4.1 Белый список IP-адресов

Для добавления правила белого списка IP-адресов:

1. Выберите **Безопасность > Фильтрация IP-адресов**.
Откроется страница **Фильтрация IP-адресов**.
 2. Установите параметру **Режим IP-фильтрации** значение **Белый список**.
 3. Нажмите **Добавить**.
 4. Установите значение параметра **Услуга**.
 5. Установите **Протокол**.
 6. Установите **Диапазон IP-адресов источника**, т.е. IP-адрес или сегмент IP-адресов, которые будут фильтроваться.
 7. Установите **Диапазон портов источника**, т.е. порт или несколько портов, которые будут фильтроваться.
 8. Установите **Диапазон IP-адресов назнач.**, т.е. IP-адрес или сегмент IP-адресов, которые будут фильтроваться.
 9. Установите **Диапазон портов назнач.**, т.е. порт или несколько портов, которые будут фильтроваться.
 10. Нажмите **Подтвердить**.
- Конец

Для изменения правила белого списка IP-адресов:

1. Выберите **Безопасность > Фильтрация IP-адресов**.
Откроется страница **Фильтрация IP-адресов**.
2. Установите параметру **Режим IP-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите изменить, и нажмите **Изменить**.
4. Внесите изменения.
5. Нажмите **Подтвердить**.

----Конец

Для удаления правила белого списка IP-адресов:

1. Выберите **Безопасность > Фильтрация IP-адресов**.
Откроется страница **Фильтрация IP-адресов**.
2. Установите параметру **Режим IP-фильтрации** значение **Белый список**.
3. Выберите правило, которое хотите удалить, и нажмите **Удалить**.
4. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Для удаления всех правил белого списка IP-адресов:

1. Выберите **Безопасность > Фильтрация IP-адресов**.
Откроется страница **Фильтрация IP-адресов**.
2. Установите параметру **Режим IP-фильтрации** значение **Белый список**.
3. Нажмите **Удалить все**.
4. В появившемся диалоговом окне нажмите **ОК**.

----Конец

6.4.2 Черный список IP-адресов

Выберите **Безопасность > Фильтрация IP-адресов**. Установите параметру **Режим IP-фильтрации** значение **Черный список**.

Остальные операции аналогичны операциям с белым списком IP-адресов.

6.5 Контроль доступа к услугам

Данная функция позволяет регулировать количество пользователей, подключенных к CPE.

В списке контроля доступа приводятся типы услуг, контролируемых CPE. По умолчанию правила контроля доступа не действуют.

Для создания списка контроля доступа:

1. Выберите **Безопасность > Контроль доступа к услугам**.

Откроется страница **Контроль доступа к услугам**.

2. Выберите запись, которую хотите настроить, и нажмите **Изменить**.
3. Установите **Диапазон IP-адресов**.



Если **Источник доступа** имеет значение **LAN**, IP-адрес должен принадлежать к тому же сетевому сегменту, что и IP-адрес, установленный на странице **Настройки хоста LAN**.

Если **Источник доступа** имеет значение **Интернет**, IP-адрес должен принадлежать к сетевому сегменту, отличному от сетевого сегмента IP-адреса на странице **Настройки хоста LAN**.

4. Установите параметр **Статус**.
5. Нажмите **Подтвердить**.

----Конец

6.6 ALG

На данной странице можно включить или отключить функцию ALG SIP.

Для включения ALG SIP:

1. Выберите **Безопасность > ALG**.

Откроется страница **Настройки ALG**.

2. Установите флажок в поле **Включить** для функции **ALG SIP**.
3. Установите **Порт SIP**.



Рекомендуется использовать порт по умолчанию с номером 5060. Если порт по умолчанию не используется, программное обеспечение VoIP недоступно для пользователя.

4. Нажмите **Подтвердить**.

----Конец

6.7 Переадресация портов

Если на CPE включено преобразование сетевых адресов (NAT), то доступ к сети Интернет будет открыт только для IP-адреса на стороне WAN. Если компьютер сети LAN предназначен для работы в сети Интернет (например, выполняет функции FTP-сервера), то переадресация портов необходима, чтобы все обращения к порту внешнего сервера из Интернета перенаправлялись на сервер сети LAN.

Для добавления правила переадресации портов:


1. Выберите **Безопасность > Переадресация портов**.

Откроется страница **Переадресация портов**.

2. Нажмите **Добавить**.
3. Установите **Тип**.
4. Установите **Протокол**.
5. Установите **Удал. хост** (необязательно).
6. Установите **Диапазон удал. портов**.

 Номер порта должен быть от 1 до 65535.

7. Установите **Лок. хост**.

 Данный IP-адрес должен отличаться от IP-адреса CPE, но он должен принадлежать к сетевому сегменту, заданному на странице **Настройки хоста LAN**.

8. Установите **Лок. порт**.

 Номер порта должен быть от 0 до 65535.

9. Установите параметру **Статус** значение **Включено** или **Отключено**.
10. Нажмите **Подтвердить**.

----Конец

Для изменения правила переадресации портов:

1. Выберите **Безопасность > Переадресация портов**.
Откроется страница **Переадресация портов**.
2. Выберите правило, которое хотите изменить, и нажмите **Изменить**.
3. Внесите изменения.
4. Нажмите **Подтвердить**.

----Конец

Для удаления правила переадресации портов:

1. Выберите **Безопасность > Переадресация портов**.
Откроется страница **Переадресация портов**.
2. Выберите правило, которое хотите удалить, и нажмите **Удалить**.
3. В появившемся диалоговом окне нажмите **ОК**.

----Конец

Для удаления всех правил переадресации портов:

1. Выберите **Безопасность > Переадресация портов**.
Откроется страница **Переадресация портов**.

2. Нажмите **Удалить все**.
3. В появившемся диалоговом окне нажмите **ОК**.

----Конец

6.8 UPnP

На данной странице можно включить или отключить функцию UPnP.

6.8.1 UPnP

Для включения UPnP:

1. Выберите **Безопасность > UPnP**.
Откроется страница **UPnP**.
2. Установите флажок в поле **Включить** для параметра **UPnP**.
3. Нажмите **Подтвердить**.

----Конец

6.9 DMZ

Если включить функцию DMZ, пакеты из сети WAN будут отправляться непосредственно на указанный IP-адрес сети LAN, прежде чем их отбросит брандмауэр.

Для включения DMZ:

1. Выберите **Безопасность > DMZ**.
Откроется страница **Настройки DMZ**.
2. Установите флажок в поле **Включить** для функции **DMZ**.
3. Установите **Адрес хоста**.



Данный IP-адрес должен отличаться от IP-адреса, установленного на странице **Настройки хоста LAN**. Тем не менее, оба адреса должны быть в одном сетевом сегменте.

4. Нажмите **Подтвердить**.

----Конец

7 Сервисы

7.1 DDNS

DDNS (Dynamic DNS) является услугой динамического обновления DNS в режиме реального времени, которая предоставляет устройствам доменное имя, изменяющее их местоположение в сети. Для конфигурирования настроек DDNS:

1. Выберите **Сервисы > DDNS**.
Откроется страница **DDNS**.
 2. Для параметра **Провайдер услуг** выберите значение **DynDns.org**.
 3. Установите флажок в поле **Включить** для параметра **DDNS**.
 4. Введите **Имя домена** и **Имя хоста**. Например, если провайдер услуг предоставил доменное имя **test.customtest.dyndns.org**, введите **customtest.dyndns.org** для параметра **Имя домена** и **test** для параметра **Имя хоста**.
 5. Введите **Логин** и **Пароль**.
 6. Нажмите **Подтвердить**.
- Конец

7.2 Сообщения SMS

На этой странице можно просматривать, отправлять и удалять сообщения SMS.

7.2.1 Просмотр сообщений SMS

Вы можете просмотреть свои сообщения в папках Входящие, Черновики и Исходящие.

Для просмотра сообщений:

1. Выберите **Сервисы > Сообщения SMS**.
Откроется страница **Сообщения SMS**.
2. Для просмотра полученных сообщений нажмите **Входящие**.
3. Для просмотра черновых вариантов сообщений нажмите **Черновики**.
4. Для просмотра отправленных сообщений нажмите **Исходящие**.

---Конец

7.2.2 Отправка сообщений SMS

Для отправки сообщения:

1. Выберите **Сервисы > Сообщения SMS**.

Откроется страница **Сообщения SMS**.

2. В поле **Номер телефона** введите номер получателя. Если получателей сообщения несколько, то введите несколько номеров телефонов, разделяя их точкой с запятой (;).
3. В поле **Текст** напишите сообщение.
4. Нажмите **Отправить**.

---Конец

7.2.3 Сохранение сообщений SMS

Для сохранения сообщения:

1. Выберите **Сервисы > Сообщения SMS**.

Откроется страница **Сообщения SMS**.

2. В поле **Номер телефона** введите номер получателя.
3. В поле **Текст** напишите сообщение.
4. Нажмите **Сохранить**.

---Конец

7.2.4 Пересылка сообщений SMS

Для пересылки сообщения:

1. Выберите **Сервисы > Сообщения SMS**.

Откроется страница **Сообщения SMS**.

2. Нажмите **Переслать** справа от сообщения, которое хотите переслать.
3. В поле **Номер телефона** введите номер получателя.
4. Нажмите **Отправить**.

---Конец

7.2.5 Ответ на сообщения SMS

Для ответа на сообщение:

1. Выберите **Сервисы > Сообщения SMS**.

Откроется страница **Сообщения SMS**.

2. Нажмите **Ответить** справа от сообщения, на которое хотите ответить.
3. В поле **Текст** напишите сообщение.

4. Нажмите **Отправить**.

----Конец

7.2.6 Удаление сообщений SMS

Для удаления одного или нескольких сообщений SMS:

1. Выберите **Сервисы > Сообщения SMS**.

Откроется страница **Сообщения SMS**.

2. Нажмите **Удалить** справа от сообщения, которое хотите удалить.
3. Для удаления всех сообщений на странице нажмите **Удалить стр.**.

----Конец

7.3 Настройки SMS

Вы можете настроить адрес центра SMS, включить или отключить SMS-отчеты, а также задать сохранение отправленных сообщений.

1. Выберите **Сервисы > Настройки SMS**.

Откроется страница **Настройки SMS**.

2. В поле **Адрес сервис-центра** введите номер центра SMS.
3. Установите, включить или нет **SMS-отчет**.
4. Установите, нужно ли **Сохранять отпр. сообщения**.



Сообщение, отправленное нескольким получателям, сохранить нельзя.

5. Нажмите **Подтвердить**.

----Конец

8 Система

8.1 Обслуживание

8.1.1 Перегрузка

Данная функция позволяет выполнить перегрузку CPE. Настройки вступают в силу только после перегрузки CPE.

Для перегрузки CPE:

1. Выберите **Система > Обслуживание**.
2. Нажмите **Перезагрузить**.
3. В появившемся диалоговом окне нажмите **ОК**.

После этого произойдет перегрузка CPE.

----**Конец**

8.1.2 Сброс

Данная функция позволяет восстановить заводские настройки CPE.

Для восстановления настроек CPE:

1. Выберите **Система > Обслуживание**.
2. Нажмите **Сброс**.
3. В появившемся диалоговом окне нажмите **ОК**.

После этого заводские настройки CPE будут восстановлены.

----**Конец**

8.1.3 Загрузка файла конфигурации

Для создания резервной копии существующего файла конфигурации Вы можете его загрузить. Для загрузки файла:

1. Выберите **Система > Обслуживание**.

Откроется страница **Обслуживание**.

2. Нажмите **Загрузить** на странице **Обслуживание**.

В появившемся диалоговом окне укажите путь и имя резервируемого файла конфигурации.

3. Нажмите **Сохранить**.

Процедура загрузки может быть разной в зависимости от используемого браузера.

----Конец

8.1.4 Выгрузка файла конфигурации

Вы можете выгрузить зарезервированный файл конфигурации для восстановления CPE.
Для выгрузки файла:

1. Выберите **Система > Обслуживание**.

Откроется страница **Обслуживание**.

2. Нажмите **Обзор** на странице **Обслуживание**. В появившемся диалоговом окне выберите резервный файл конфигурации.

3. Нажмите **Открыть**.

Диалоговое окно закроется. В окне справа от параметра **Файл конфигурации** будет отображаться путь и имя резервного файла конфигурации.

4. Нажмите **Выгрузить**.

5. В появившемся диалоговом окне нажмите **ОК**.

Резервный файл конфигурации будет выгружен. После этого произойдет автоматическая перезагрузка CPE.

----Конец

8.2 Смена пароля

Данная функция позволяет изменить пароль для входа пользователя admin. После смены пароля при следующем входе необходимо ввести уже новый пароль.

Для изменения пароля:

1. Выберите **Система > Смена пароля**.

Откроется страница **Смена пароля**.

2. Введите сначала текущий пароль, потом новый пароль и подтвердите новый пароль.

Новый пароль и **Подтверждение пароля** должны содержать от 6 до 15 символов ASCII.

3. Нажмите **Подтвердить**.

----Конец

8.3 Дата и время

Вы можете установить системное время или синхронизировать системное время со временем сети. Если в поле **Синхр. от сети** установить флажок, CPE будет регулярно синхронизировать свое время со временем сервера. Если включить функцию DST, CPE будет настраивать системное время с учетом перехода на летнее время.

Для установки даты и времени:

1. Выберите **Система > Дата и время**.
- Откроется страница **Настройки**.
2. Выберите **Установка вручную**.
3. Установите **Локальное время** или нажмите **Синхр. с ПК**.
4. Нажмите **Подтвердить**.

----Конец

Для синхронизации времени с сетью:

1. Выберите **Система > Дата и Время**.
- Откроется страница **Настройки**.
2. Нажмите **Синхр. от сети**.
3. Установите **Основной сервер NTP** для синхронизации времени.
4. Установите **Дополнительный сервер NTP** для синхронизации времени.
5. Задайте **Часовой пояс**.

Разные страны и регионы находятся в разных часовых поясах. Вы можете выбрать часовой пояс из выпадающего списка.

6. Установите флажок в поле **Переход на летнее время**.

После включения DST сконфигурируйте время начала и время завершения DST. CPE будет автоматически показывать летнее время в зависимости от часового пояса. При необходимости Вы можете задать **Начало летнего времени**, **Конец летнего времени** и **Сдвиг летнего времени**.

7. Нажмите **Подтвердить**.

----Конец

8.4 Диагностика

При некорректной работе CPE Вы можете воспользоваться средствами диагностики на странице **Диагностика**, чтобы своевременно определить проблему и принять меры по её устранению.

8.4.1 Команда Ping

Если CPE не удается подключиться к сети Интернет, выполните команду **ping** для предварительного определения проблемы. Для этого:

1. Выберите **Система > Диагностика**. На странице **Диагностика** установите параметру **Метод** значение **Ping**.

Откроется страница **Ping**.

2. Введите доменное имя в поле **Целевой IP-адрес или домен**, например www.google.com.
3. Задайте **Размер пакета** и **Таймаут** и установите флажок в поле **Включить** для параметра **Без фрагментации**.
4. Нажмите **Ping**.
5. Дождитесь результатов выполнения команды **ping**.

Результаты будут выведены на экран в окне **Результаты**.

----Конец

8.4.2 Команда Traceroute

Если CPE не удается подключиться к сети Интернет, выполните команду **traceroute** для предварительного определения проблемы. Для этого:

1. Выберите **Система > Диагностика**. На странице **Диагностика** установите параметру **Метод** значение **Traceroute**. Откроется страница **Traceroute**.
2. Введите доменное имя в поле **Целевой IP-адрес или домен**, например www.google.com.
3. Установите параметры **Макс. число переходов** и **Таймаут**.
4. Нажмите **Traceroute**.
5. Дождитесь результатов выполнения команды **traceroute**.

Результаты будут выведены на экран в окне **Результаты**.

----Конец

8.4.3 Проверка системы

При некорректной работе CPE Вы можете воспользоваться средствами системной проверки для определения проблемы. Для этого:

1. Выберите **Система > Диагностика**. На странице **Диагностика** установите параметру **Метод** значение **Проверка системы**.

Откроется страница **Проверка системы**.

2. Нажмите **Проверить**.
3. Дождитесь окончания системной проверки.

На странице будут выведены возможные причины появления проблемы в работе CPE.

4. Нажмите **Экспорт** для экспортирования подробной информации в компьютер. В следующей таблице приведены экспортируемые файлы с описанием.

Имя файла	Описание
check_items.txt	Список элементов веб-интерфейса
operateLog_export.txt	Журнал операций
traceLog_export.txt	Системный журнал
router_ver.txt	Информация о версии маршрутизатора
modem_ver.txt	Информация о версии модема
sysmod.txt	Режим системы
boot.log	Журнал загрузки ОС
curcfg.xml	Файл текущей конфигурации
defaultcfg.xml	Файл конфигурации по умолчанию
arp.txt	Таблица ARP
route.txt	Таблица маршрутизации
ps.txt	Информация о процессах
top.txt	Информация об использовании системных ресурсов
mount.txt	Информация об установке системы
wlctl_status.txt	Информация о запуске Wi-Fi
wlctl_isup.txt	Информация о включении Wi-Fi
wlctl_scanresults.txt	Точки доступа в пределах диапазона
iptables.txt	Правила фильтрации для iptables
iptables_nat.txt	Правила NAT для iptables
eatables.txt	Правила фильтрации для eatables
ifconfig.txt	Информация о сетевом адаптере
brctl.txt	Информация о мостовом соединении
plt.log	Журнал ядра системы
pltcheck.log	Журнал самопроверки системы

5. При необходимости отправьте подробную информацию персоналу по техобслуживанию.

---Конец

8.4.4 Проверка статуса беспроводной сети

На данной странице приводится информация о состоянии беспроводной сети, включающая PLMN, статус обслуживания, RSSI и статус роуминга.

Для просмотра информации о состоянии беспроводной сети:

1. Выберите **Система > Диагностика**.
2. На странице **Метод** установите параметру **Метод** значение **Проверка статуса беспр. сети**.

Откроется страница **Статус беспроводной сети**.

----Конец

8.5 Журнал

В журнале сохраняются записи об операциях пользователя и ключевых рабочих событиях. Для просмотра журнала:

1. Выберите **Система > Журнал**.

Откроется страница **Журнал**.

2. Выберите соответствующий уровень записи из выпадающего списка **Уровень записи**.

Количество записей выбранного уровня будет отображаться справа от списка, а сами записи данного уровня в окне ниже. Вы можете просмотреть до 500 последних записей.

3. Выберите операцию.

- **Сброс**: Удаление всех записей журнала CPE.
- **Экспорт**: Экспортирование всех записей журнала CPE в файл на компьютере.

----Конец

8.6 Уведомление системы

На данной странице можно сконфигурировать методы уведомления о ключевых изменениях в состоянии устройства.

1. Выберите **Система > Уведомление системы**.

Откроется страница **Уведомление системы**.

2. Установите **Периодичность**, **IP-адрес приема всплыв. окон** (необязательно), **Отправка SMS на номер** и **Переадресовывать SMS от** (необязательно).

3. Когда **IP-адрес приема всплыв. окон** не указан, уведомления случайным образом рассылаются подключенным клиентам.

4. Проверка сообщений, переадресация и настройки уведомлений вступают в силу только после включения функции **Отправка SMS на номер**.

5. Настройте уведомление для каждого **События**.

6. Нажмите Подтвердить.

----Конец

9

Часто задаваемые вопросы

Не горит индикатор питания.
<ul style="list-style-type: none">• Убедитесь, что кабель питания подсоединен, и CPE включен.• Убедитесь, что адаптер питания подходит для CPE.
Не удается войти на веб-интерфейс пользователя.
<ul style="list-style-type: none">• Убедитесь, что CPE запущен.• Убедитесь, что сетевой кабель подключен к CPE и компьютеру.• Проверьте, правильно ли задан IP-адрес компьютера. <p>Если проблема остается, обратитесь в местный авторизованный центр провайдера услуг.</p>
CPE не находит беспроводные сети.
<ul style="list-style-type: none">• Проверьте, подключен ли адаптер питания.• Убедитесь, что CPE установлен на открытом пространстве, далеко от препятствий типа бетонных или деревянных стен.• Убедитесь, что CPE находится далеко от бытовых электроприборов, которые генерируют сильные электромагнитные поля, таких как микроволновые печи, холодильники и спутниковые антенны. <p>Если проблема остается, обратитесь в местный авторизованный центр провайдера услуг.</p>
Перегревается адаптер питания CPE.
<ul style="list-style-type: none">• CPE может перегреваться вследствие длительной эксплуатации. Поэтому, отключайте CPE, когда Вы его не используете.• Убедитесь, что CPE хорошо проветривается и защищен от попадания прямых солнечных лучей.
Параметры восстанавливаются в значение по умолчанию.
<ul style="list-style-type: none">• Восстановление значений по умолчанию может происходить при неожиданном отключении CPE в процессе конфигурирования.• После настройки параметров загрузите файл конфигурации для быстрого восстановления нужных настроек CPE.

10 Сокращения

AES	Advanced Encryption Standard - Улучшенный стандарт шифрования
ALG	Application Layer Gateway - Шлюз прикладного уровня
CPE	Customer-Premises Equipment - Оборудование в помещении клиента
DHCP	Dynamic Host Configuration Protocol - Протокол динамической конфигурации узла
DMZ	Demilitarized Zone - Демилитаризованная зона
DNS	Domain Name Server/Domain Name System - Сервер доменных имён/Система доменных имён
DST	Daylight Saving Time - Летнее время
HTTP	Hypertext Transfer Protocol - Протокол передачи гипертекста
IMEI	International Mobile Equipment Identity - Международный идентификатор мобильного оборудования
IP	Internet Protocol - Интернет-протокол
LAN	Local Area Network - Локальная сеть
LTE	Long Term Evolution - Долговременное развитие
MAC	Media Access Control - Управление доступом к среде
NAT	Network Address Translation - Преобразование сетевых адресов
NTP	Network Time Protocol - Протокол сетевого времени
PBC	Push Button Configuration - Конфигурирование нажатием кнопки
PIN	Personal Identification Number - Персональный идентификационный номер
SIP	Session Initiation Protocol - Протокол установления сеанса
SN	Serial Number - Серийный номер
SSID	Service Set Identifier - Идентификатор набора служб
USIM	Universal Subscriber Identity Module - Универсальный идентификационный модуль абонента
WAN	Wide Area Network - Глобальная компьютерная сеть

WEP	Wired Equivalent Privacy - Конфиденциальность на уровне проводных сетей
WLAN	Wireless Local Area Network - Беспроводная локальная сеть
WPA	Wi-Fi Protected Access - Защищенный доступ Wi-Fi
WPA-PSK	Wi-Fi Protected Access-Pre-Shared Key - Защищенный доступ Wi-Fi на основе простого общего пароля
WPS	Wi-Fi Protected Setup - Защищенная установка Wi-Fi

11 Уведомление об авторских правах и отказ от гарантий

Данный продукт включает в себя нижеприведенное программное обеспечение с открытым исходным кодом, защищенное авторскими правами и лицензионными соглашениями третьих сторон.

1. Samba

Авторские права © Andrew Tridgell 1994-2002

GNU General Public License V2.0

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

2. DJV Image and Movie Viewersg

Авторские права © 2004-2009 Darby Johnston

<http://djb.sourceforge.net/legal.html>

BSD License/ Modified BSD License

<http://www.opensource.org/licenses/bsd-license>

3. EasySoap++

Авторские права © 2001 David Crowley; SciTegic, Inc.

GNU Library или "Lesser" General Public License V2.0

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>

4. Open BSD

Авторские права © 1996-2011 OpenBSD

BSD License/ Modified BSD License

<http://www.opensource.org/licenses/bsd-license>

5. m2sc

Авторские права © 2009 Google

<http://code.google.com/p/m2sc/>

GNU General Public License 3.0

<http://www.gnu.org/licenses/gpl.html>

При желании приобрести содержащийся в данном продукте исходный код GPL на CD стоимостью \$20, обращайтесь к нам по адресу mobile@huawei.com.