Руководство пользователя

AC1350 Двухдиапазонный гигабитный Wi-Fi роутер Archer C5 Pro

REV1.0.0 1910020856

Содержание

О руководстве

Данное руководство является дополнением к руководству по быстрой настройке, в котором рассказывается о первичной настройке подключения к интернету, в то время как в данном руководстве подробно описывается каждая функция и способы настройки функций.

При использовании этого руководства необходимо учитывать, что некоторые функции роутера могут немного отличаться в зависимости от аппаратной и программной версии устройства, от региона, в котором используется устройства, а также от используемого языка и интернет-провайдера. Все используемые в данном руководстве снимки экрана, изображения и описания приведены исключительно в демонстрационных целях.

Обозначения

Обозначение	Описание
Подчёркнутый текст	Так выглядят гиперссылки, нажав на которые можно перейти к определённому разделу данного руководства или на сайт.
Текст бирюзового цвета	Так выглядят заголовки руководства, ссылки и пункты меню.
>	Элемент структуры меню. Например, Дополнительные настройки > Беспроводной режим > Статистика означает, что раздел «Статистика» находится во вкладке «Дополнительные настройки» пункта меню «Беспроводной режим».
Примечание	Игнорирование подобного примечания может привести к проблемам.
Совет	Полезная информация по использованию устройства.
Иконки веб-интерфейса	• Изменение параметра. • Удаление параметра. • Включение или выключение параметра. • Подробная информация.

Дополнительная информация

Новые прошивки и другие файлы доступны в Центре загрузок на https://www.tp-link.com/ru/support

Руководство по быстрой настройке доступно в том же разделе, что и это руководство, а также в упаковке роутера.

Характеристики доступны на странице продукта на https://www.tp-link.com/ru

Адрес форума техподдержки: https://community.tp-link.com/ru

Контакты службы техподдержки доступны на https://www.tp-link.com/ru/support

Глава 1

Знакомство с роутером

В данной главе описываются возможности и внешний вид роутера.

1.1. Обзор

Роутеры TP-Link предназначены для домашних и небольших офисных сетей, а также для пользователей, которым нужна повышенная производительность сети. Мощные антенны гарантируют качественное подключение по Wi-Fi на всех устройствах во всём доме, а порты Ethernet обеспечат высокую скорость подключения по кабелю.

Более того, роутеры TP-Link легко настроить благодаря понятному веб-интерфейсу управления.

1.2. Внешний вид

1.2.1. Передняя панель

Ниже дано описание расположенных на передней панели индикаторов роутера (слева направо).

Описание индикаторов

Индикатор	Состоян.	Описание
(Питание)	Горит	Система успешно запущена.
	Мигает	Идёт запуск системы или обновление прошивки роутера. Не отключайте роутер и питание.
	Не горит	Питание отключено.

Индикатор	Состоян.	Описание
(Wi-Fi 2,4 ГГц)	Горит	Включён диапазон Wi-Fi 2,4 ГГц.
	Не горит	Диапазон Wi-Fi 2,4 ГГц отключён.
(Wi-Fi 5 ГГц)	Горит	Включён диапазон Wi-Fi 5 ГГц.
	Не горит	Диапазон Wi-Fi 5 ГГц отключён.
(Ethernet)	Горит	Есть подключение по крайней мере к одному порту Ethernet.
	Не горит	Нет устройств, подключённых к порту Ethernet.
(Интернет)	Горит	Есть доступ в интернет.
	Горит оранжевым	Есть подключение к порту Internet роутера, но нет доступа в интернет.
	Не горит	Нет подключения к порту Internet роутера.
(WPS)	Горит / Не горит	Загорается во время синхронизации WPS и автоматически гаснет примерно через пять минут.
	Мигает	Идёт подключение WPS (может длиться до двух минут).

1.2.2. Задняя панель

Расположенные на задней панели разъёмы, порты и кнопки (слева направо).

Кнопка/Порт	Описание
Разъём Power	Обеспечивает подключение роутера к питанию с помощью адаптера.
Кнопка Power On/Off	Нажмите, чтобы включить или выключить роутер.

Кнопка/Порт	Описание
Кнопка Reset	Нажмите и удерживайте не менее пяти секунд, чтобы восстановить заводские настройки роутера.
Кнопка WPS/Wi-Fi On/Off	Нажмите эту кнопку и тут же нажмите аналогичную кнопку на другом устройстве. Если индикатор WPS перестать мигать и стал гореть, значит подключение WPS успешно выполнено.
	Нажмите и удерживайте не менее пяти секунд, чтобы включить или выключить Wi-Fi на роутере.
Порт Internet	Обеспечивает подключение к модему или к интернет-розетке.
Порты Ethernet (1/2/3/4)	Обеспечивают подключение устройств к роутеру по кабелю Ethernet.
Антенны	Предназначены для передачи данных по Wi-Fi. Максимальная производительность Wi-Fi обеспечивается в вертикальном положении.

Глава 2

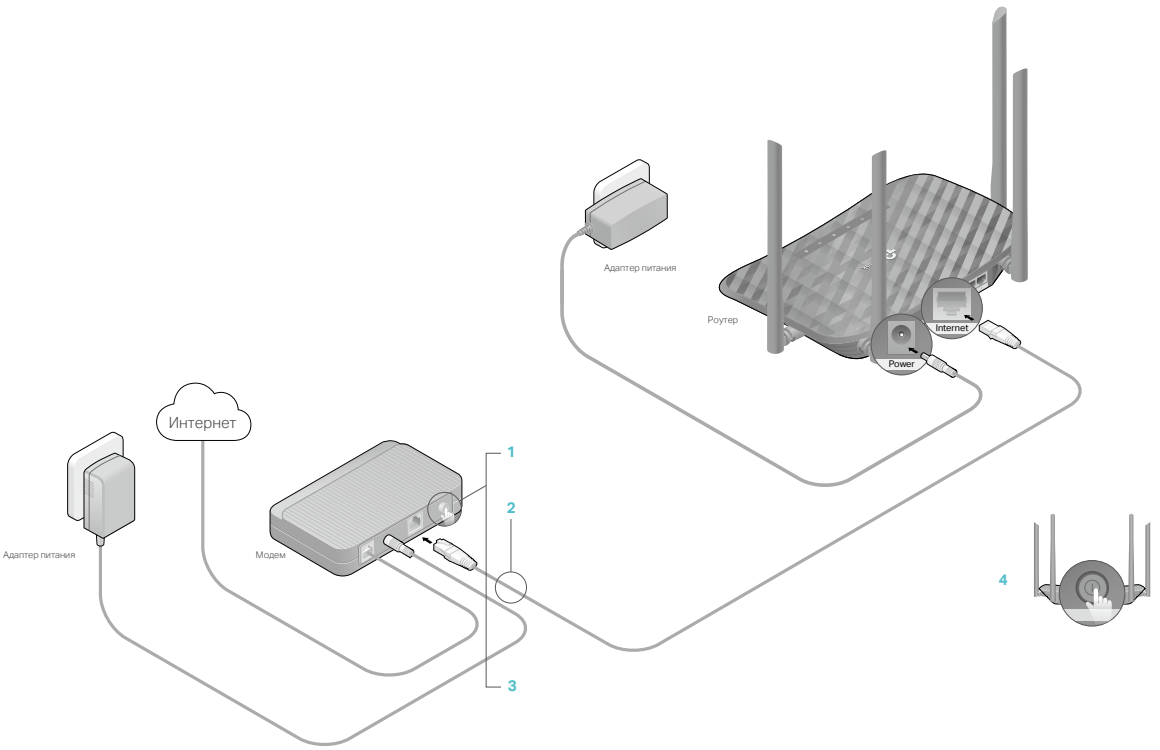
Физическое подключение

2.1. Размещение роутера

- Не размещайте роутер в условиях высокой влажности и температур.
- Размещайте роутер так, чтобы к нему можно подключить другие устройства и чтобы его можно подключить к питанию.
- Спрячьте кабели, чтобы не споткнуться об них.
- Роутер можно размещать на полке или на столе.
- Размещайте роутер как можно дальше от устройств с электромагнитным излучением, в том числе устройств Bluetooth, радиотелефонов и микроволновых печей.

2.2. Подключение роутера

Если используется прямое подключение (без модема), подключите кабель Ethernet к порту Internet роутера и выполните шаги 4 и 5 для завершения физического подключения.



1. Отключите модем и извлеките аккумулятор (если он есть).
2. Подключите модем к порту Internet роутера с помощью кабеля Ethernet.
3. Включите модем и подождите около двух минут, пока завершится перезагрузка.

4. Подключите адаптер питания к роутеру и включите роутер.
5. Если нижеуказанные индикаторы горят, значит физическое подключение выполнено успешно.

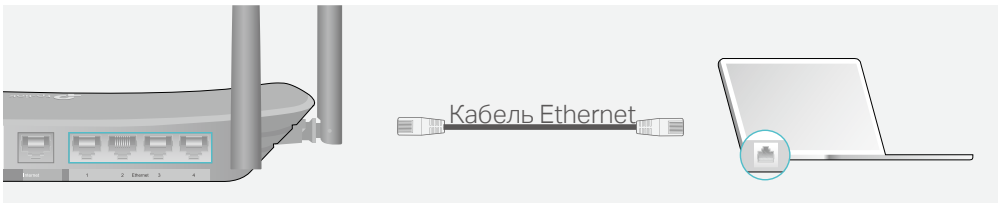
Примечание

Если индикаторы 2,4 ГГц и 5 ГГц не горят, нажмите и удерживайте кнопку WPS/Wi-Fi On/Off на задней панели около трёх секунд, затем отпустите кнопку. Оба индикатора должны загореться.

6. Подключите компьютер к роутеру.

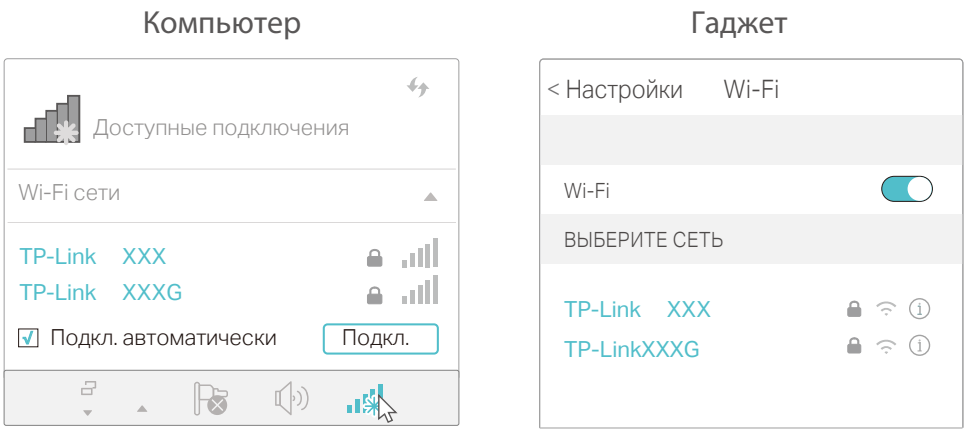
- **Способ 1: по кабелю**

Отключите Wi-Fi на компьютере и подключите устройства по схеме ниже.



- **Способ 2: по Wi-Fi**

1) Найдите имя (SSID) и пароль Wi-Fi, напечатанные на этикетке на нижней панели роутера.
2) Нажмите на компьютере иконку сети или перейдите в настройки Wi-Fi гаджета и выберите SSID роутера, чтобы подключиться к сети.



- **Способ 3: с помощью кнопки WPS**

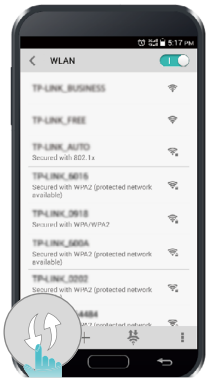
Данным способом к роутеру можно подключить Wi-Fi устройства с поддержкой WPS, включая смартфоны и планшеты на Android и большинство сетевых карт USB.

Примечание

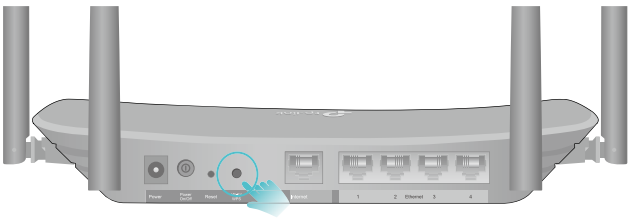
- Функция WPS не поддерживается устройствами iOS.

- WPS нельзя настроить, если на роутере отключён Wi-Fi. Также функция WPS будет отключена, если используется Wi-Fi шифрование WEP.

1) Нажмите иконку WPS на экране устройства (в данном примере используется устройство Android).
2) В течение двух минут нажмите кнопку роутера Reset/WPS.



Рядом

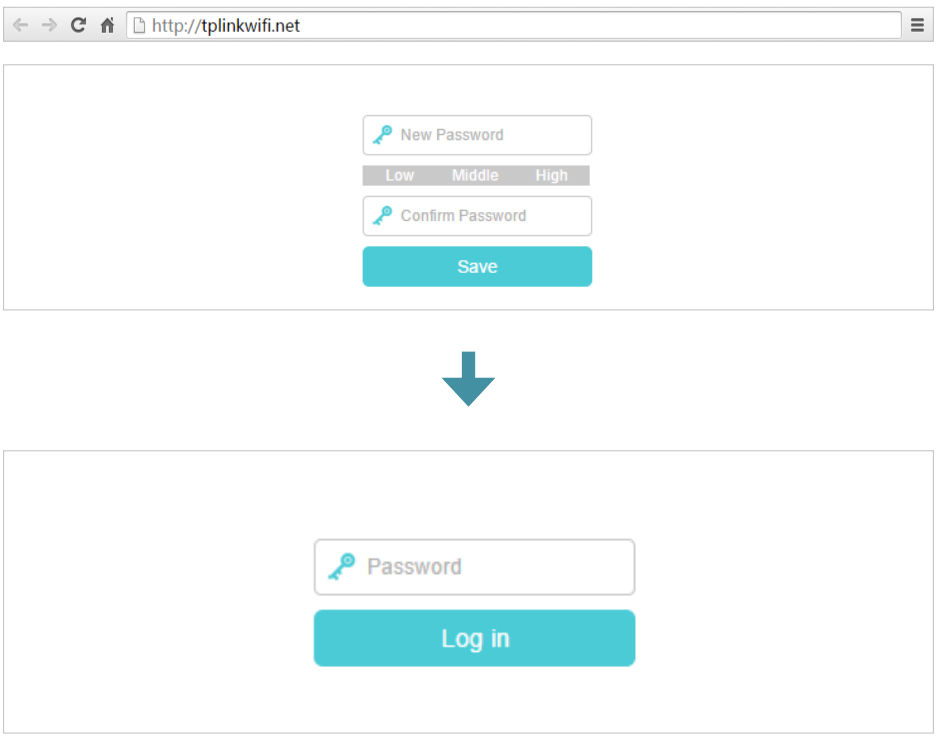


Глава 3

Вход в интерфейс роутера

Веб-интерфейс обеспечивает простую настройку и управление роутером. Веб-интерфейс можно открыть на любом устройстве Windows, macOS или UNIX с помощью браузера, включая Internet Explorer, Mozilla Firefox или Safari.

1. Установите на компьютере автоматическое получение IP-адреса для протокола TCP/IP.
2. Введите в адресной строке браузера http://tplinkwifi.net и создайте пароль для входа, нажмите Сохранить и повторно введите пароль. Затем нажмите Войти для входа в интерфейс роутера.



Примечание

Если окно входя не появляется, воспользуйтесь разделом Часто задаваемые вопросы.

Глава 4

Настройка подключения к интернету

В данной главе описывается процесс подключения роутера к интернету. В роутере есть мастер быстрой настройки, а также параметры многих интернет-провайдеров. Также роутер проверяет успешность выполнения шагов и позволяет создать подключение IPv6, если его поддерживает ваш интернет-провайдер.

4.1. Мастер быстрой настройки

Мастер быстрой настройки поможет без труда настроить роутер.

Совет

Если нужно настроить подключение IPv6, перейдите в раздел Настройка интернет-подключения IPv6.

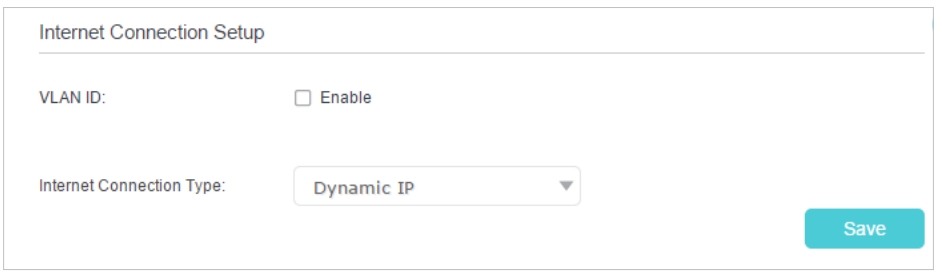
Выполните следующие шаги для настройки роутера.

1. Перейдите на http://tplinkwifi.net и войдите, используя установленный вами пароль роутера.
2. Нажмите Быстрая настройка в верхней части страницы и выполните пошаговые инструкции для подключения роутера к интернету.

4.2. Ручная настройка интернет-подключения

Выполните шаги ниже, чтобы посмотреть или изменить настройки подключения к интернету.

1. Перейдите на http://tplinkwifi.net и войдите, используя установленный вами пароль роутера.
2. Перейдите в раздел Основные настройки > Интернет.
3. Выберите тип интернет-подключения из выпадающего списка.

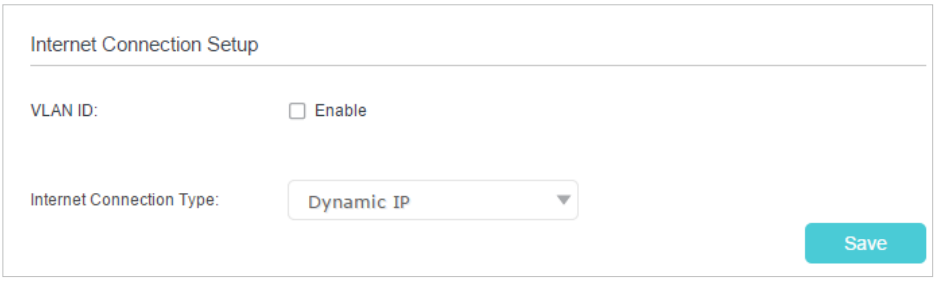


Совет

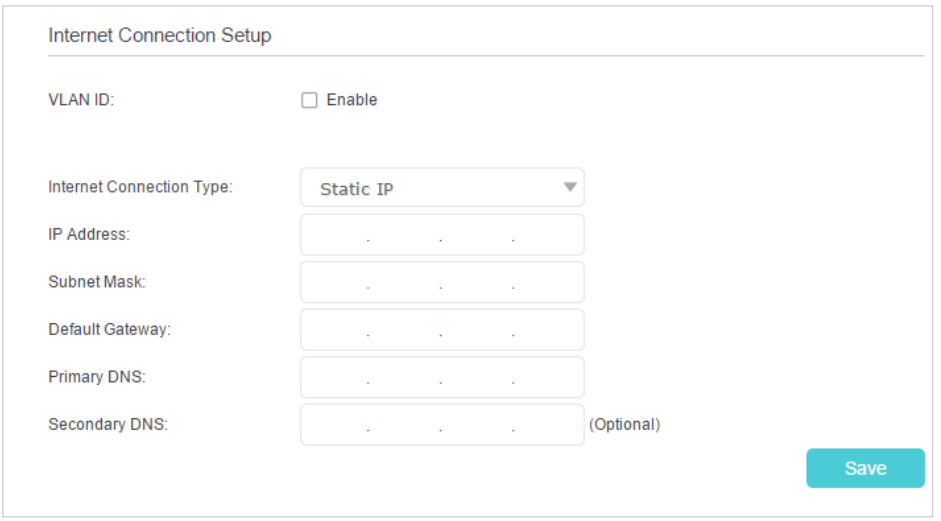
Для каждого типа подключения требуется свой кабель и информация о подключении. Свой тип подключения вы можете определить с помощью указаний в Шаге 4.

4. Выполните указания на странице. Параметры на снимках экрана приведены в качестве примера.

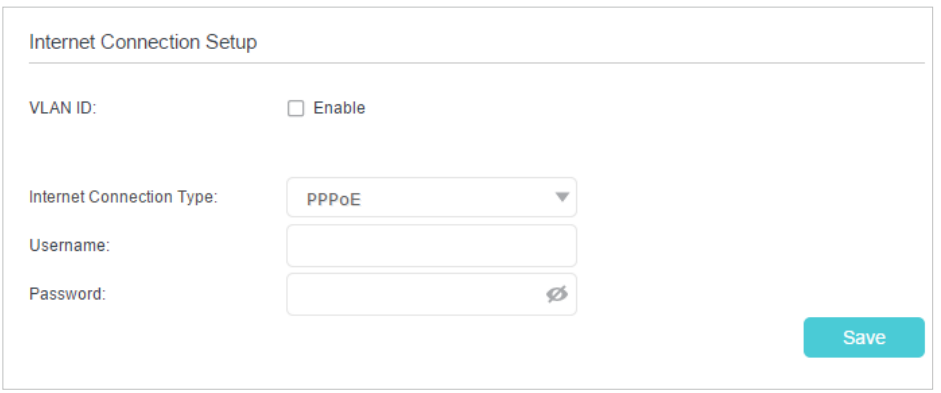
    1) Если выбран Динамический IP-адрес, необходимо указать, нужно ли клонировать MAC-адрес. Этот тип подключения обычно используется для кабельного ТВ или оптического подключения.



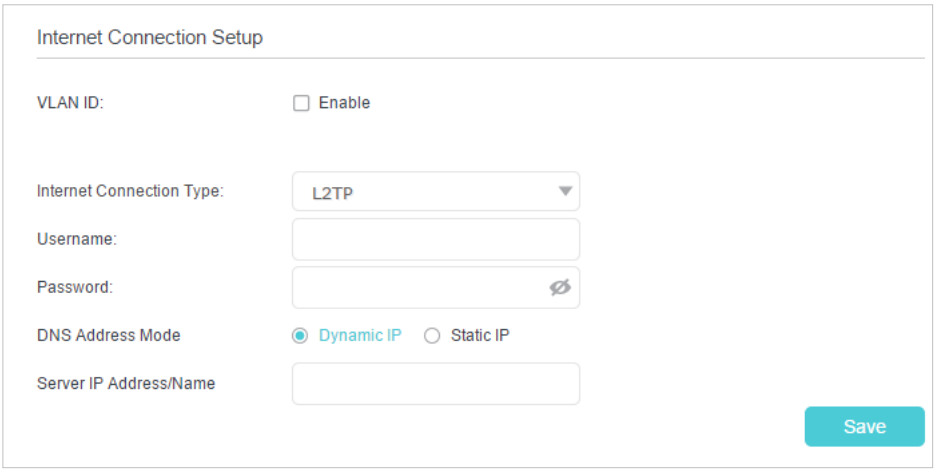
2) Если выбран Статический IP-адрес, необходимо ввести в соответствующие поля предоставленные интернет-провайдером данные.



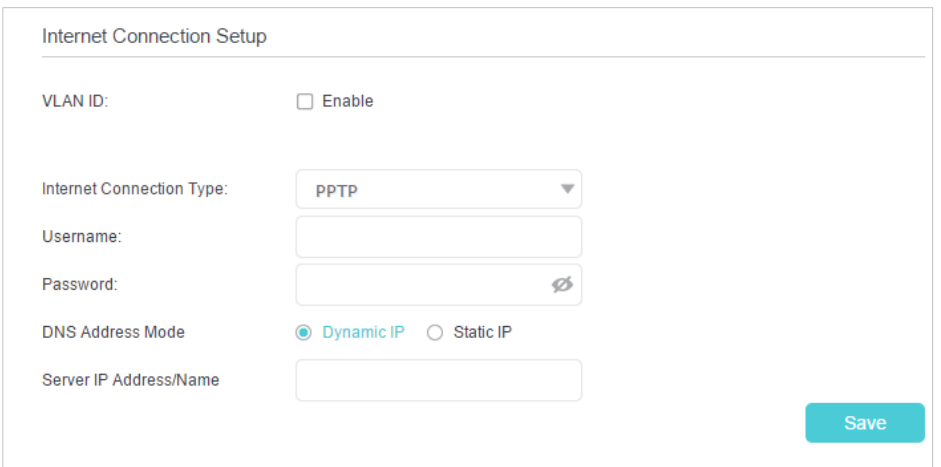
3) Если выбрано подключение PPPoE, введите предоставленные интернет-провайдером Имя пользователя и Пароль. Обычно при подключении PPPoE используется модем.



4) Если выбрано подключение L2TP, введите Имя пользователя и Пароль и выберите Тип адреса DNS согласно указаниям интернет-провайдера — дальнейшие параметры зависят от выбранного типа.



5) Если выбрано подключение PPTP, введите Имя пользователя и Пароль и выберите Тип адреса DNS согласно указаниям интернет-провайдера — дальнейшие параметры зависят от выбранного типа.



5. Нажмите Сохранить, чтобы изменения вступили в силу.

Примечание

На вступление изменённых параметров в силу может потребоваться до двух минут.

Советы

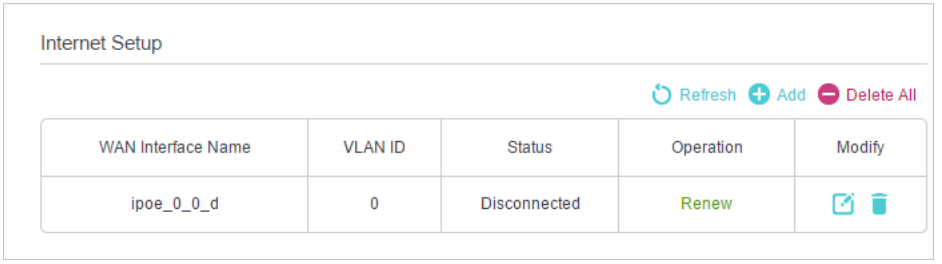
- Состояние интернет-подключения можно проверить в разделе Карта сети в левой части страницы.
- Если используется Динамический IP-адрес и PPPoE, и вам нужно ввести другие параметры, которые не являются обязательными, перейдите в раздел Дополнительные настройки > Сеть > Интернет для завершения настройки.
- Если доступа в интернет по-прежнему нет, воспользуйтесь разделом Часто задаваемые вопросы.

4.3. Настройка интернет-подключения IPv6

Подключение IPv6 можно настроить вручную, если интернет-провайдер предоставляет какой-либо из следующих типов интернет-подключения IPv6: PPPoE, динамический IP-адрес (SLAAC/DHCPv6), статический IP-адрес, туннель 6to4 или Passthrough (мост).

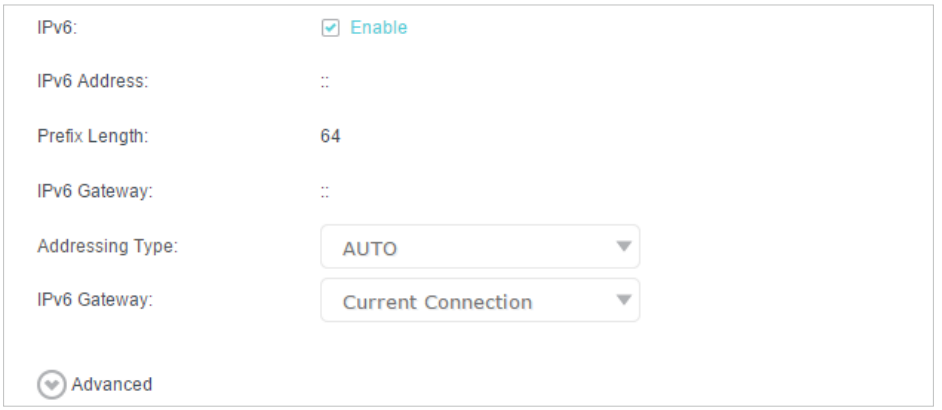
1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.

2. Перейдите в раздел Дополнительные настройки > Сеть > Интернет.



3. Выберите имя интерфейса WAN (в столбце Состояние должно быть написано Подключено) и нажмите иконку .

4. Прокрутите вниз, включите IPv6 и настройте параметры IPv6.



- Тип адресации: уточните у провайдера (DHCPv6 или SLAAC, последний является наиболее распространённым типом адресации).
- Шлюз IPv6: оставьте значение по умолчанию (Текущее подключение).

Примечание: если интернет-провайдер предоставил адрес IPv6, нажмите Дополнительные настройки. Убедитесь, что используется адрес IPv6, предоставленный провайдером, и введите остальные параметры в соответствии с указаниями провайдера.

5. Нажмите Сохранить, чтобы изменения вступили в силу — настройка подключения IPv6 завершена.

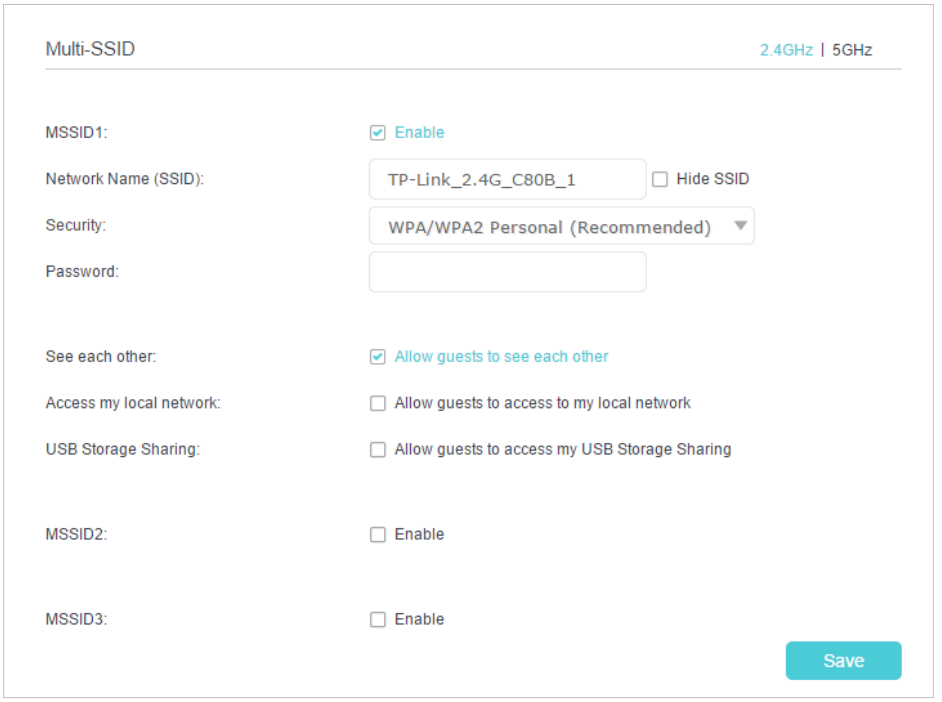
Глава 5

Мульти-SSID

Мульти-SSID позволяет создавать отдельный Wi-Fi доступ для гостей и не раскрывать данные основной сети.

➢ Как создать мульти-SSID

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль роутера.
2. Перейдите в раздел Основные настройки > Multi-SSID или Дополнительные настройки > Беспроводной режим > Multi-SSID.
3. Создайте гостевую сеть и укажите нужные параметры.



1) Нажмите 2,4 ГГц или 5 ГГц для настройки гостевой Wi-Fi сети на диапазоне 2,4 ГГц или 5 ГГц. На каждом диапазоне можно создать не более трёх гостевых сетей.
2) Отметьте окошко Включить, чтобы создать соответствующую сеть.
3) Используйте Имя сети (SSID) по умолчанию или введите собственное (поле чувствительно к регистру). Не отмечайте Скрыть SSID, если не хотите, чтобы при подключении к Wi-Fi гостям нужно было каждый раз вводить его вручную.
4) В выпадающем списке Защита выберите WPA/WPA2 Personal (рекомендуется) и создайте пароль для гостевой сети.

- Видеть друг друга: отметьте окошко Разрешить гостевым пользователям видеть друг друга, если вы хотите разрешить подключённым к гостевой сети Wi-Fi килентам взаимодействовать друг с другом через Ping и т. д.
- Доступ к моей локальной сети: отметьте окошко Разрешить гостевым пользователям доступ к моей локальной сети, если вы хотите разрешить подключённым к гостевой сети Wi-Fi клиентам взаимодействовать с подключёнными к портам LAN роутера или к основной сети устройствами через Ping и т. д.

4. Нажмите Сохранить, чтобы изменения вступили в силу — теперь у гостей будет доступ к вашей гостевой сети.

Совет

Для просмотра информации о гостевой сети перейдите в раздел Дополнительные настройки > Состояние и найдите панель Multi-SSID.

Глава 6

Родительский контроль

Эта функция позволяет блокировать непристойные и вредоносные сайты, а также ограничивать время доступа в интернет.

Хочу

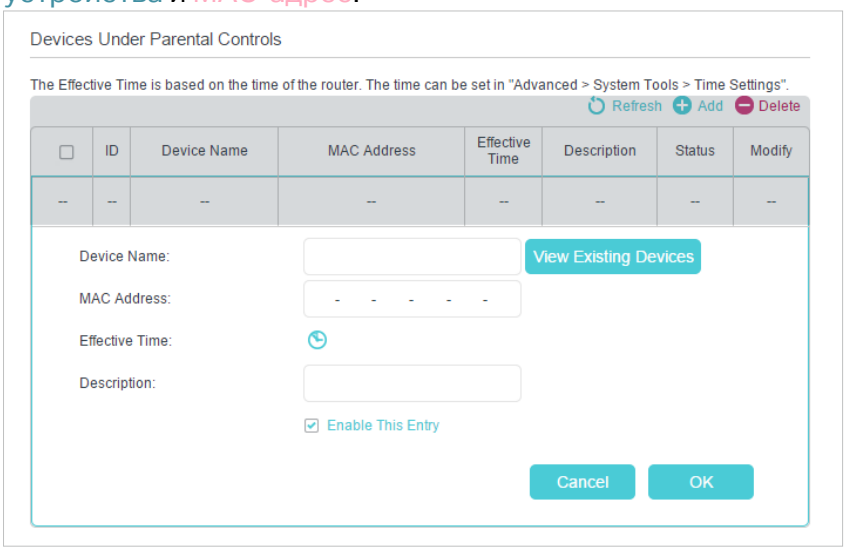
Запретить доступ к некоторым сайтам для детей и других пользователей сети, а также ограничить время доступа в интернет.

Например, нужно, чтобы по будням с 18:00 до 22:00 на устройствах моих детей (например, на компьютере или планшете) был доступ только к сайтам tp-link.com и wikipedia.org.

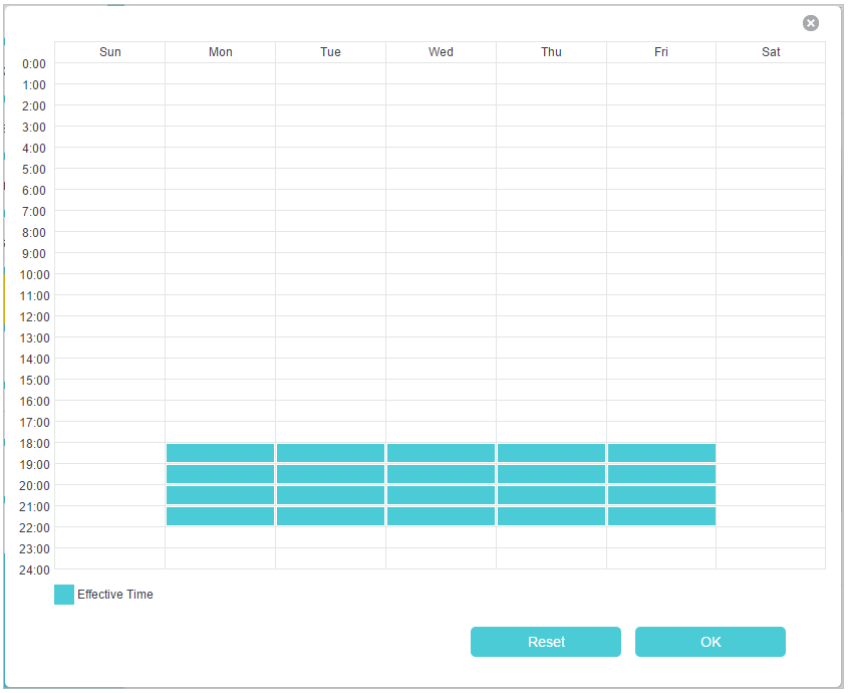
Как это сделать?

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль роутера.
2. Перейдите в раздел Дополнительные настройки > Родительский контроль и включите Родительский контроль.

3. Нажмите Добавить. Затем нажмите Просмотр существующих устройств и выберите нужные подключённые устройства. Либо вручную введите Имя устройства и MAC-адрес.

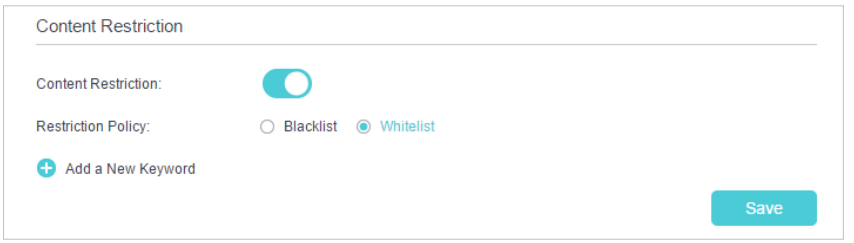


4. Нажмите иконку , чтобы создать Время работы. Перетащите курсор на нужные ячейки и нажмите ОК.



5. Введите Описание для правила, отметьте окошко Включить и нажмите ОК.

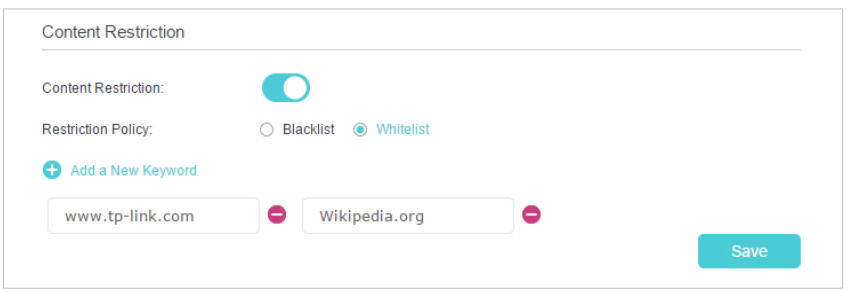
6. Включите Ограничение по названию сайта и выберите Белый список.



Советы

- Чёрный список разрешает доступ ко всем сайтам, кроме указанных.
- Белый список разрешает доступ только к указанным сайтам.

7. Нажмите Добавить новое слово и введите tp-link.com и wikipedia.org и нажмите Сохранить.



8. В чёрный или белый список можно добавить до 32 ключевых слов. Пример:
   - Белый список: введите адрес сайта (например, wikipedia.org), чтобы доступ был только к нему. Если нужно заблокировать доступ ко всем сайтам, не добавляйте в белый список никаких сайтов.
   - Чёрный список: введите адрес сайта (например, wikipedia.org), ключевое слово (например, «wikipedia») или доменное имя (например, .edu или .org), чтобы заблокировать доступ только к соответствующим сайтам.

Готово!

Теперь вы можете контролировать интернет-доступ своих детей.

Глава 7

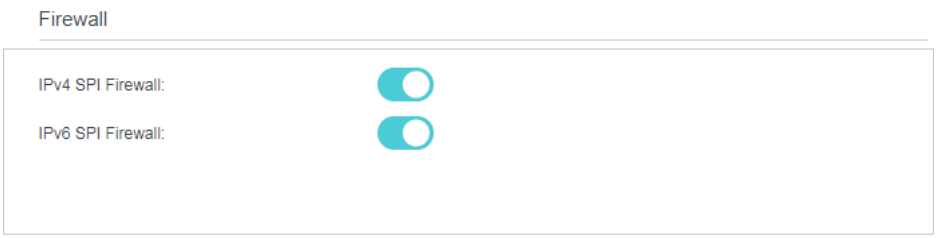
Защита сети

В данной главе рассказывается о том, как защитить домашнюю сеть от несанкционированных пользователей с помощью системы безопасности роутера. Вы можете заблокировать доступ к Wi-Fi сети для конкретных клиентских устройств с помощью фильтрации по MAC-адресу или с помощью контроля доступа, а также защититься от ARP-спуфинга и ARP-атак с помощью привязки IP- и MAC-адресов.

7.1. Межсетевой экран и защита от DoS-атак

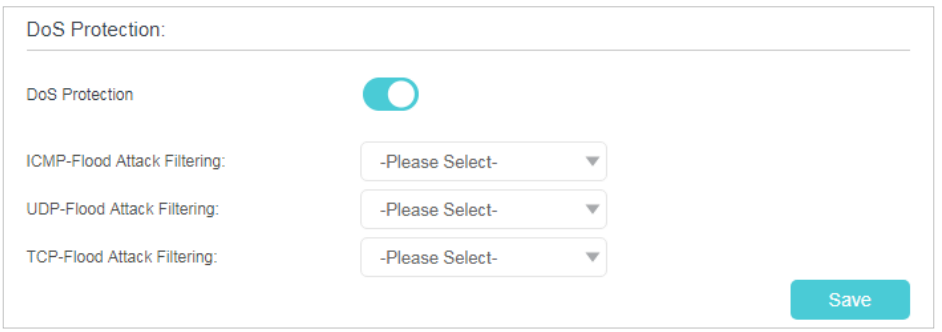
Межсетевой экран SPI и защита от DoS-атак защищают роутер от кибератак.

Межсетевой экран SPI предотвращает кибератаки и проверяет весь проходящий через роутер трафик с помощью протокола. Эта функция включена по умолчанию, рекомендуется не изменять настройки по умолчанию.



Защита от DoS-атак поможет защитить домашнюю сеть от чрезмерного числа запросов, направленных на доведение системы до отказа.

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > Безопасность > Межсетевой экран и защита от DoS-атак.

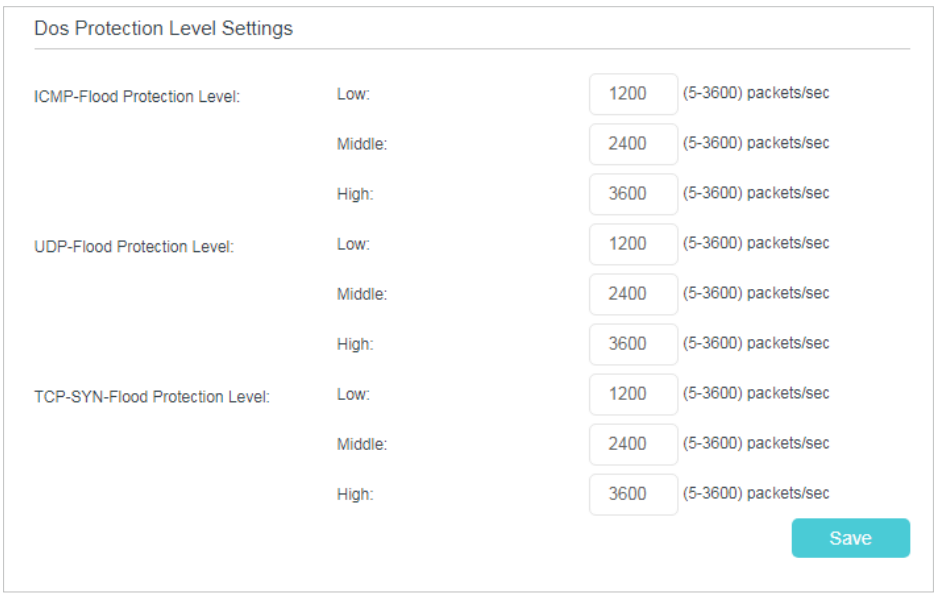


Примечание: Защита от DoS-атак и Статистика трафика должны работать одновременно, для включения статистики трафика перейдите в раздел Дополнительные настройки > Системные инструменты > Статистика трафика.

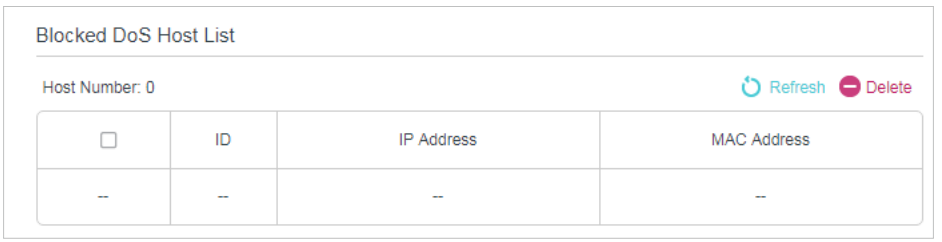
3. Включите Защиту от DoS-атак.
4. Установите уровень защиты (Низкий, Средний или Высокий) для параметров Порог пакетов ICMP-Flood, Порог пакетов UDP-Flood и Порог пакетов TCP-SYN-Flood.
   - Порог пакетов ICMP-Flood — включите для защиты от ICMP-флуда.
   - Порог пакетов UDP-Flood — включите для защиты от UDP-флуда.
   - Порог пакетов TCP-SYN-Flood — включите для защиты от SYN-флуда.
5. Нажмите Сохранить, чтобы изменения вступили в силу.

Советы

1. Уровень защиты основан на количестве пакетов трафика. Их число можно указать в разделе Настройка уровня защиты от DoS-атак.



2. При превышении установленного порогового значения мгновенно сработает защита, и узел-источник будет занесён в Список заблокированных узлов-источников DoS-атак.

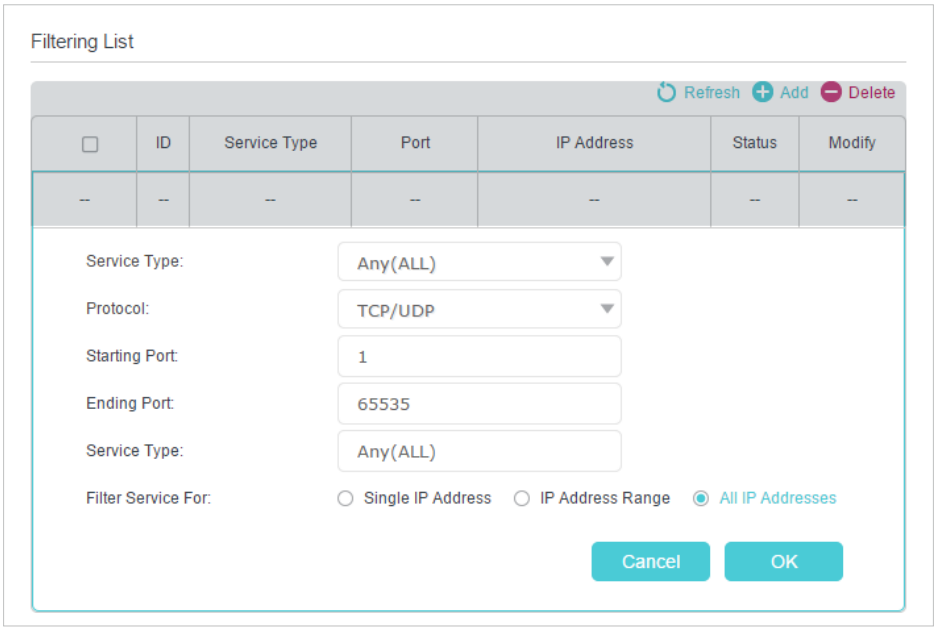


7.2. Фильтрация сервисов

Эта функция позволяет запретить доступ конкретных пользователей к указанным сервисам, а то и вовсе полностью заблокировать доступ в интернет.

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > Защита > Фильтрация сервисов.
3. Включите функцию Фильтрация сервисов.

4. Нажмите Добавить.



5. Выберите Тип сервис из одноимённого выпадающего списка — четыре поля под этим пунктом заполнятся автоматически. Выберите из списка вариант Настроить, если нужного типа сервиса нет в списке, затем введите всю информацию вручную.
6. Укажите IP-адреса, к которым будет применяться правило фильтрации.
7. Нажмите OK, чтобы изменения вступили в силу.

Примечание: если нужно отключить правило, нажмите .

7.3. Контроль доступа

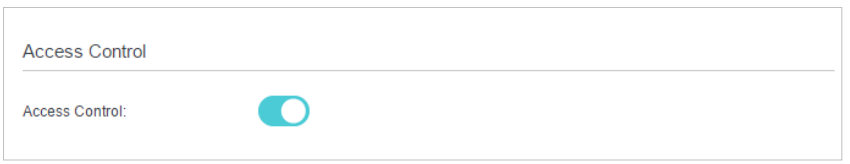
Контроль доступа позволяет запретить доступ к сети (по кабелю и по Wi-Fi) для конкретных клиентских устройств с помощью чёрного или белого списка.

Хочу

Разрешить или запретить доступ к сети для определённых устройств.

Как это сделать?

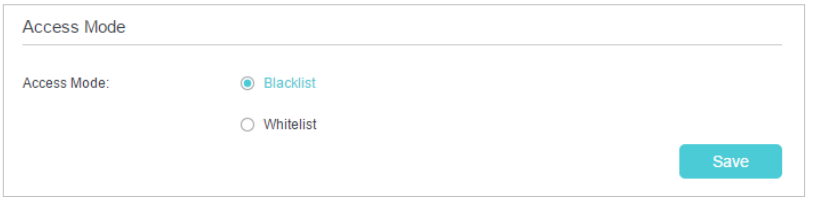
1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, созданный вами для роутера.
2. Перейдите в раздел Дополнительные настройки > Защита > Контроль доступа и включите Контроль доступа.



3. Создайте список запрещённых (рекомендуется) или разрешённых устройств.

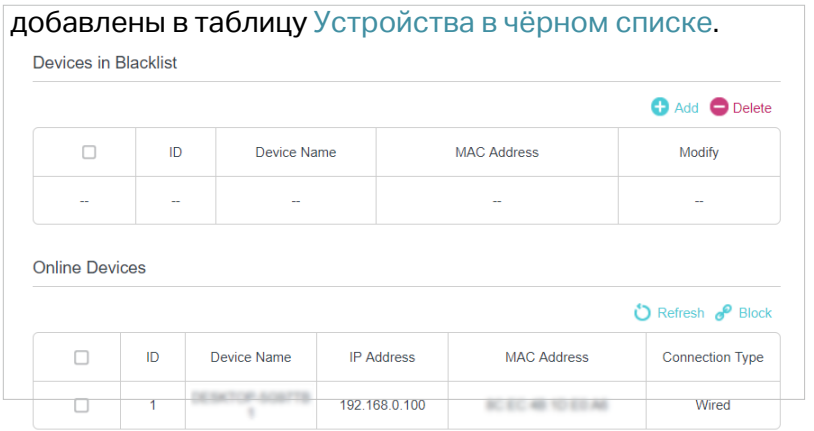
Список запрещённых устройств

1) Выберите Чёрный список и нажмите Сохранить.



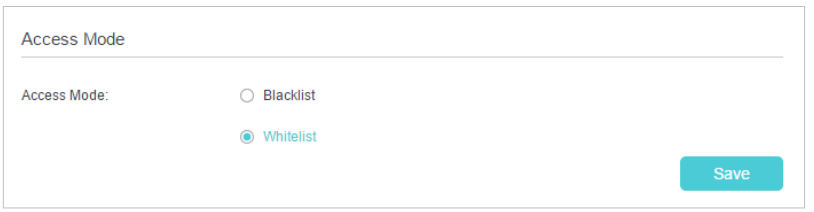
2) Выберите устройства для блокировки в таблице Устройства онлайн (или нажмите Добавить в разделе Устройства в чёрном списке и вручную введите Имя устройства и MAC-адрес).

3) Нажмите Заблокировать над таблицей Устройства онлайн, после чего выбранные устройства будут добавлены в таблицу Устройства в чёрном списке.

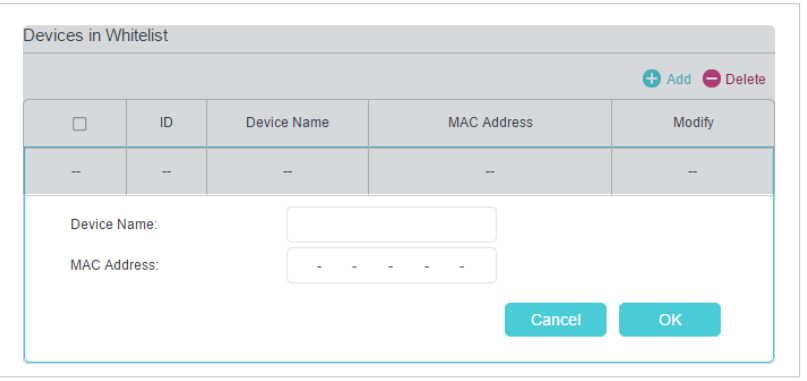


Список разрешённых устройств

1) Выберите Белый список и нажмите Сохранить.



2) Нажмите Добавить в разделе Устройства в белом списке.



3) Введите Имя устройства и MAC-адрес (если нужное устройство подключено к сети, можно скопировать и вставить данные из таблицы Устройства онлайн).

4) Нажмите OK.

Готово! Теперь выбранным устройствам будет разрешён (или запрещён) доступ к сети по кабелю и по Wi-Fi.

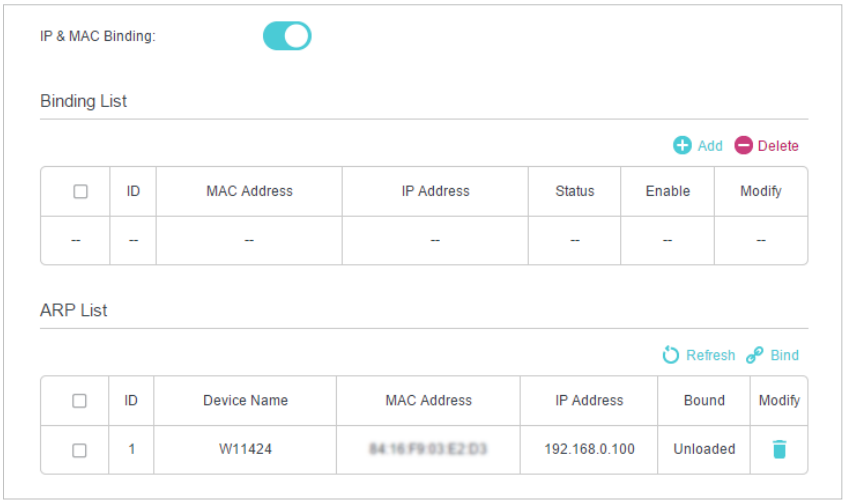
7.4. Привязка IP- и MAC-адресов

Привязка IP- и MAC-адресов (привязка ARP) нужна для привязки IP-адреса сетевого устройства к его MAC-адресу, позволяющей предотвратить ARP-спуфинг и прочие ARP-атаки путём блокировки доступа к сети для устройства с неизвестным MAC-адресом, IP-адрес которого совпадает с таковым в списке привязки.

Я хочу Защититься от ARP-спуфинга и ARP-атак.

Как это сделать?

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > Защита > Привязка IP- и MAC-адресов и включите Привязку IP- и MAC-адресов.



3. Привяжите нужные устройства.

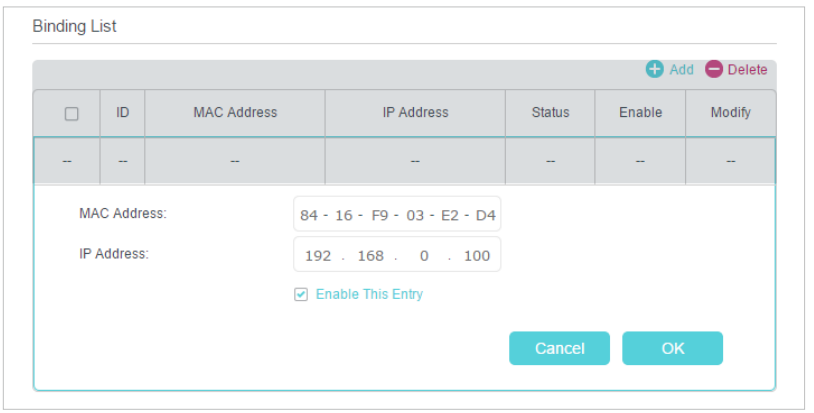
Привязка подключённых устройств

1) Выберите устройства для привязки из Таблицы ARP.

2) Нажмите Связать, чтобы добавить устройство в Таблицу привязки.

Привязка неподключённых устройств

1) Нажмите Добавить.



2) Введите MAC-адрес и IP-адрес, которые надо привязать.

3) Отметьте окошко Включить, чтобы активировать правило, и нажмите OK.

Готово!

Теперь можете не переживать об ARP-спуфинге и об ARP-атаках.

Глава 8

Переадресация NAT

Преобразование сетевых адресов (NAT) позволяет устройствам в локальной сети использовать один публичный IP-адрес для коммуникации с устройствами в интернете — это позволяет защитить локальную сеть за счёт скрытия IP-адресов устройств. Однако, это также создаёт проблему, потому что внешний узел не может поддерживать связь с конкретным устройством в локальной сети. Проброс позволяет решить эту проблему.

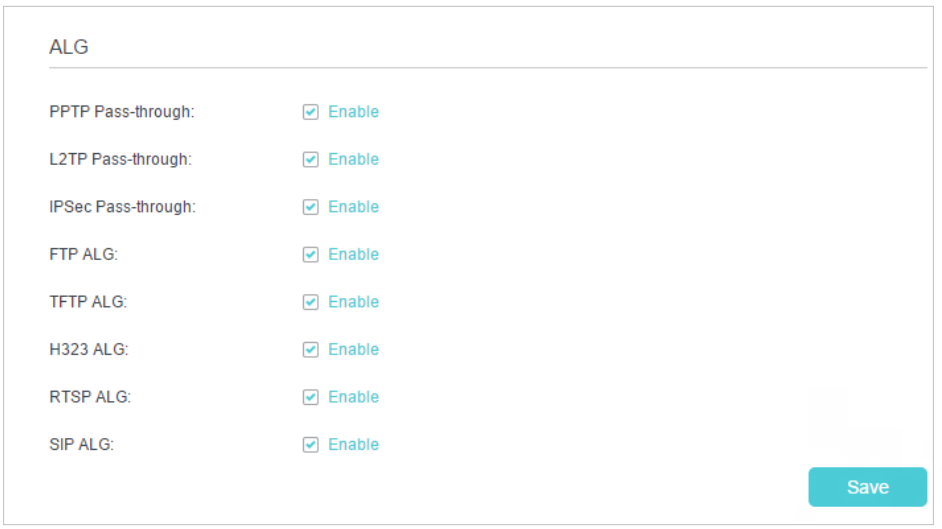
Роутеры TP-Link поддерживают четыре правила проброса. Если используется больше двух правил, приоритет расставляется от высшего к низшему следующим образом: виртуальные серверы, проброс портов, UPnP, DMZ.

- Трансляция адресов и портов с помощью ALG
- Интернет-доступ к локальным ресурсам с помощью виртуальных серверов
- Динамическое открытие портов с помощью запуска портов
- Снятие ограничений портов с приложений с помощью DMZ
- Игры Xbox без задержек благодаря UPnP

8.1. Трансляция адресов и портов с помощью ALG

Шлюз прикладного уровня (ALG) позволяет использовать фильтры преобразования сетевых адресов (NAT) для трансляции адресов и портов для определённых протоколов: FTP, TFTP и т. д. Функцию ALG не рекомендуется отключать.

Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера. Перейдите в раздел Дополнительные настройки > Переадресация NAT > ALG.



- Пропуск трафика PPPoE: позволяет хостам локальной сети самостоятельно устанавливать PPPoE-соединение с внешним сервером через роутер.
- Пропуск трафика PPTP: туннельный протокол типа точка-точка.
- Пропуск трафика L2TP: протокол туннелирования второго уровня.
- Пропуск трафика IPSec: набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP.
- FTP ALG: позволяет клиентам и серверам FTP передавать данные через NAT.
- TFTP ALG: позволяет клиентам и серверам TFTP передавать данные через NAT.
- H323 ALG: позволяет клиентамт Microsoft NetMeeting взаимодействовать через NAT.
- RTSP AI ALG: позволяет клиентам-медиаплеерам взаимодействовать со стриминговыми медиасерверами через NAT.
- SIP ALG: позволяет клиентам взаимодействовать с серверами SIP через NAT.

8.2. Интернет-доступ к локальным ресурсам с помощью виртуальных серверов

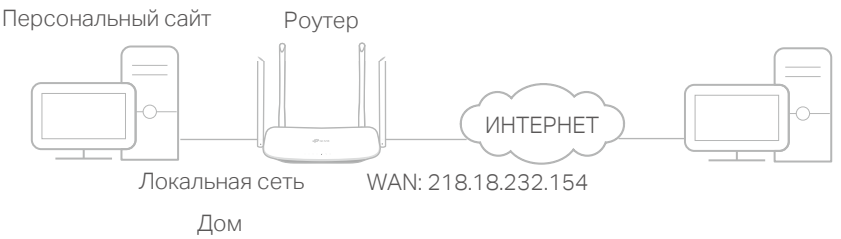
Виртуальные серверы позволяют поделиться по интернету созданным в локальной сети сервером. При этом виртуальные серверы также обеспечивают защиту локальной сети, скрывая от интернета остальные данные.

Виртуальные серверы можно использовать для создания в локальной сети публичных сервисов, например, HTTP, FTP, DNS, POP3/SMTP и Telnet. У каждого сервиса свой порт: у HTTP — порт 80, у FTP — 21, у SMTP — 25, у POP3 — 110. Перед настройкой убедитесь, что используется верный номер порта.

Хочу

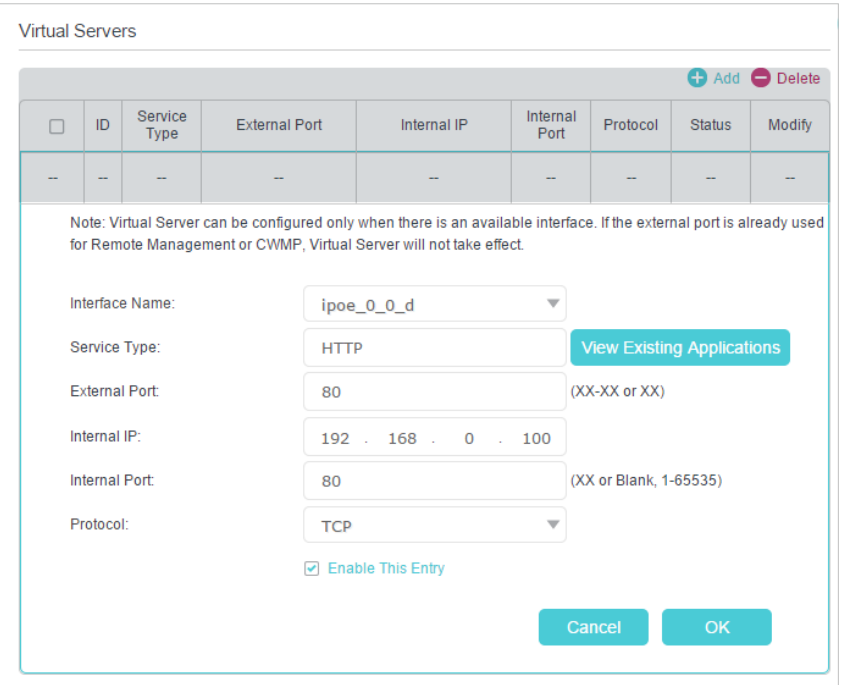
Поделиться с друзьями по интернету созданным в локальной сети персональным сайтом.

Сайт создан на домашнем компьютере (192.168.0.100), который подключён к роутеру (IP-адрес WAN: 218.18.232.154).



Как это сделать?

1. Присвойте компьютеру статический IP-адрес (например, 192.168.0.100).
2. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
3. Перейдите в раздел Дополнительные настройки > Переадресация NAT > Виртуальные серверы.
4. Нажмите Добавить. Нажмите Просмотр приложений и выберите HTTP. Поля Внешний порт, Внутренний порт и Протокол заполнятся автоматически. Введите IP-адрес компьютера (192.168.0.100) в поле Внутренний IP-адрес.
5. Нажмите ОК, чтобы изменения вступили в силу.



Советы

- Если не знаете, какой порт и протокол использовать, оставьте по умолчанию значения полей Внутренний порт и Протокол.
- Если нужного сервиса нет в списке Тип сервиса, введите нужные параметры вручную. Уточните номер порта, используемого для этого сервиса.
- Если нужно использовать несколько сервисов, можно добавить несколько правил виртуальных серверов. При этом значения в поле Внешний порт не должны повторяться.

Готово!

Для посещения сайта надо будет ввести http:// + IP-адрес WAN (в данном случае: http://218.18.232.154).

Советы

- IP-адрес WAN должен быть публичным. Если IP-адрес динамический и он присвоен интернет-провайдером, рекомендуется создать доменное имя, руководствуясь разделом Настройка учётной записи динамического сервиса DNS — тогда для посещения сайта по интернету можно будет ввести адрес http:// + Доменное имя.
- Если значение Внешнего порта по умолчанию изменялось, то для посещения сайта нужно ввести http:// + IP-адрес WAN: + Внешний порт или http:// + Доменное имя: + Внешний порт.

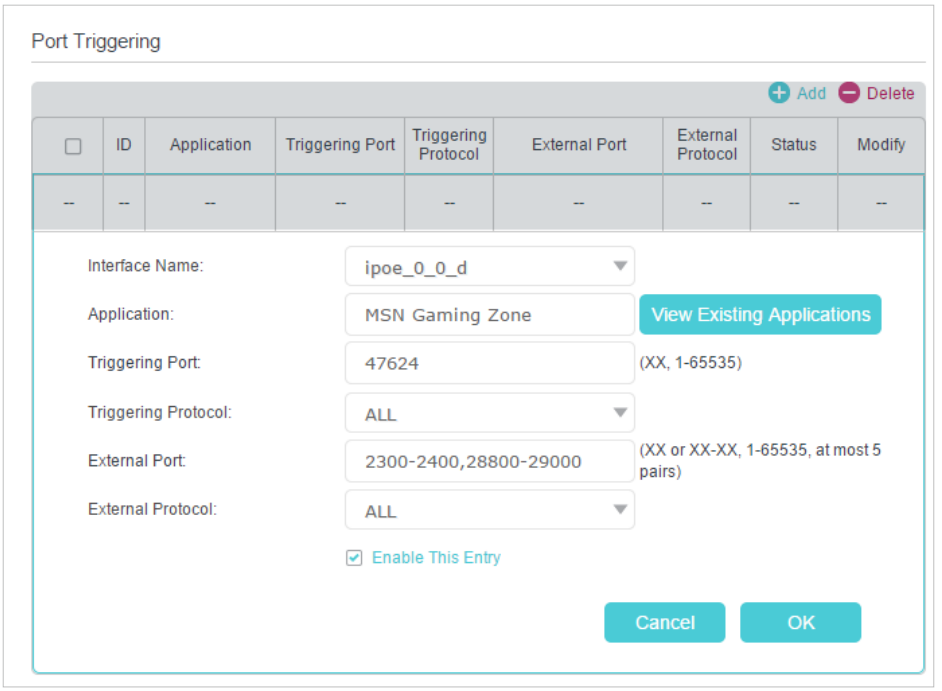
8.3. Динамическое открытие портов с помощью запуска портов

Запуск портов позволяет указать порт запуска и соответствующие внешние порты. Когда узел в локальной сети начинает подключение к порту запуска, все внешние порты будут открываться для последующих подключений. Роутер может записывать IP-адрес узла. Когда данные из интернета возвращаются на внешние порты, роутер может пересылать их на соответствующий узел. Запуск портов обычно используется для онлайн-игр, VoIP-связи и т. д.

Указания по настройке правил запуска портов:

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.

2. Перейдите в раздел Дополнительные настройки > Переадресация NAT > Port Triggering и нажмите Добавить.
3. Нажмите Просмотр приложений и выберите нужное приложение. Поля Триггер порт, Внешний порт и Протокол заполнятся автоматически. В качестве примера ниже рассмотрено приложение MSN Gaming Zone.
4. Нажмите OK.



Советы

- Можно добавить несколько правил запуска портов.
- Значения портов запуска не должны повторяться.
- Если нужного приложения нет в списке после нажатия кнопки Просмотр приложений, введите параметры вручную. Узнайте, какие внешние порты использует приложение, и введите их в поле Внешний порт в нужном формате.

8.4. Снятие ограничений портов с приложений с помощью DMZ

Когда включена функция DMZ, компьютер становится уязвимым к угрозам из интернета, и между внутренними и внешними узлами может создаваться неограниченная по объёму двусторонняя коммуникация. Узел DMZ становится виртуальным сервером, на котором открыты все порты. Фунция DMZ пригодится тем, кто не знает, какие порты открывать для конкретных приложений и устройств, например, для IP-камеры.

Примечание

Когда включена функция DMZ, к узлу DMZ полностью открыт доступ из интернета, что может создать потенциальную угрозу безопасности, поэтому отключайте DMZ, как только эта функция перестала быть нужной.

Хочу

Чтобы в компьютерной онлайн-игре не было ограничений на порты. Например, из-за определённых ограничений портов во время игры онлайн в игру получается войти, но не получается вступить в одну команду с другими игроками. Назначение компьютера в качестве узла DMZ со всеми открытыми портами поможет решить эту проблему.

Как это сделать?

1. Присвойте компьютеру статический IP-адрес (например, 192.168.0.100).
2. Перейдите на http://tplinkwifi.net, и войдите, используя созданный вами пароль для роутера.
3. Перейдите в раздел Дополнительные настройки > Переадресация NAT > DMZ и отметьте окошко Включить DMZ.
4. Введите в поле IP-адрес узла DMZ 192.168.0.100.

5. Нажмите Сохранить.

Готово!

Настройка завершена. Теперь компьютер работает в качестве узла DMZ, и вы сможете играть онлайн вместе с другими игроками.

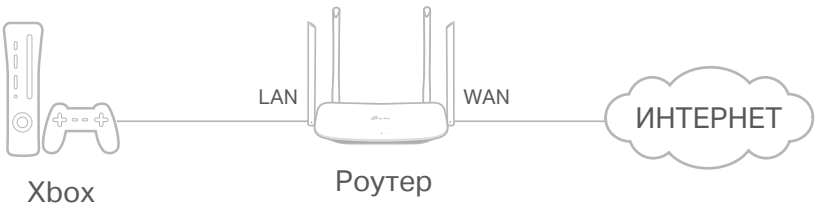
8.5. Игры Xbox без задержек благодаря UPnP

Протокол UPnP (Universal Plug and Play) позволяет приложениям или устройствам-узлам автоматически находить клиентское устройство NAT и отправлять на него запросы на открытие соответствующих портов. Благодаря UPnP приложения и устройства-узлы в локальной сети и в интернете могут свободно взаимодействовать друг с другом, создавая таким образом бесшовную сеть. UPnP может понадобиться для многопользовательских игр, подключений P2P, общения в реальном времени (например, IP-телефония) и т. д.

Советы

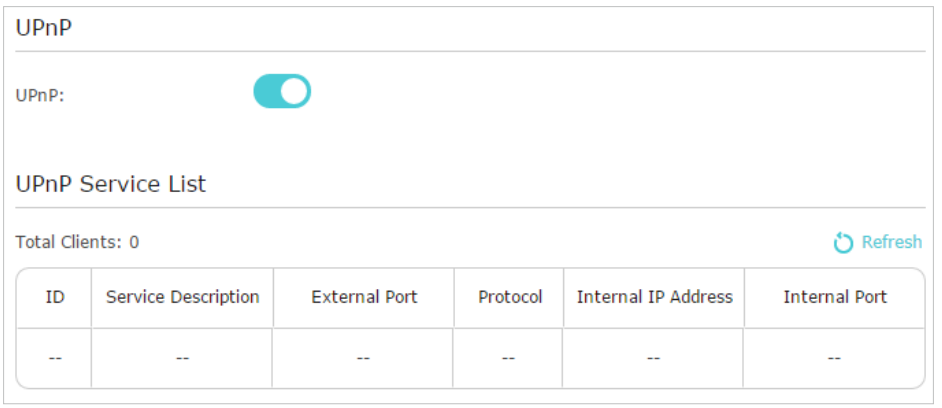
- Функция UPnP включена по умолчанию.
- Для работы этой функции клиентское устройство также должно поддерживать протокол UPnP.
- Функция UPnP должна поддерживаться операционной системой компьютера. На некоторых операционных системах может потребоваться установка компонентов UPnP.

При подключении игровой приставки Xbox к роутеру, UPnP отправит на роутер запрос на открытие соответствующих портов для передачи данных, чтобы в играх не было ни малейших задержек.



При необходимости состояние UPnP можно изменить.

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки >Переадресация NAT > UPnP, чтобы включить или выключить функцию UPnP.



Глава 9

Сервер VPN

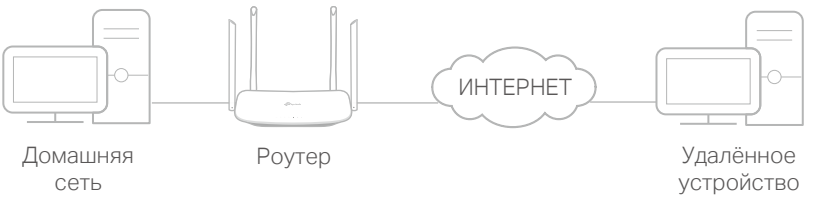
Сервер VPN позволяет получить безопасный доступ к домашней сети вне дома. На данном роутере есть два типа подключения VPN: OpenVPN и PPTP.

OpenVPN чуть сложнее, но гарантирует более высокую безопасность и стабильность. Этот тип подключения подходит для внутренних сетей кампуса или компании.

Подключение PPTP проще и быстрее, совместимо с большинством операционных систем и работает на мобильных устройствах, однако оно не обеспечивает высокий уровень защиты.

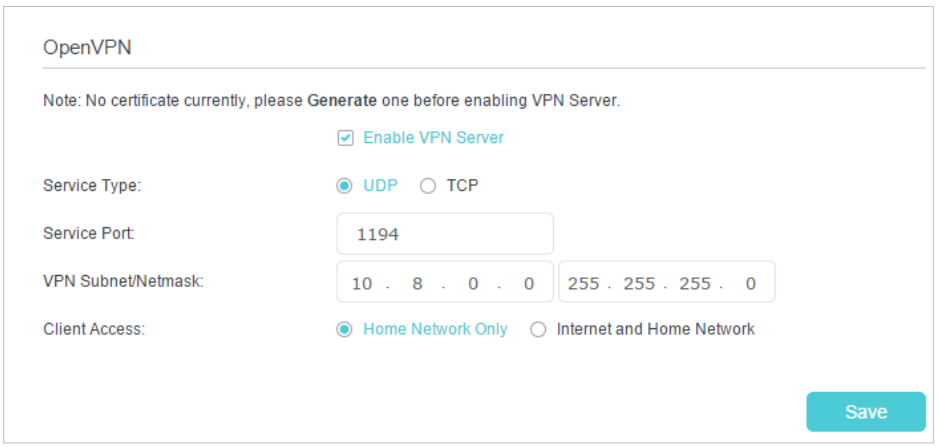
9.1. Доступ к домашней сети через OpenVPN

При подключении OpenVPN домашняя сеть может выступать в качестве сервера, при этом удалённое устройство может получать доступ к серверу через роутер, выступающий в качестве шлюза сервера OpenVPN. Для использования функции VPN необходимо включить сервер OpenVPN на роутере, а также установить и запустить клиентское ПО с VPN на удалённом устройстве. Ниже описан процесс создания подключения OpenVPN.



9.1.1. Шаг 1. Настройка сервера OpenVPN на роутере

1. Перейдите на http://tplinkwifi.net, и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > VPN > OpenVPN и выберите Запустить VPN сервер.

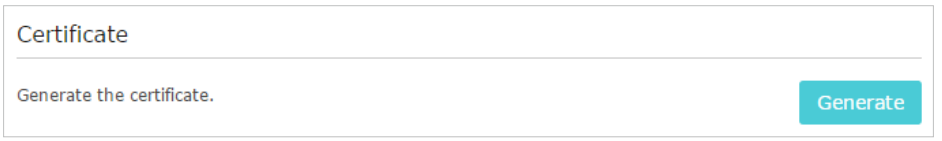


Примечание

- Перед созданием VPN-сервера рекомендуется настроить динамический DNS-сервис или присвоить статический IP-адрес порту WAN роутера и выполнить интернет-синхронизацию системного времени.
- При первой настройке сервера OpenVPN перед созданием VPN-сервера, возможно, понадобится сгенерировать сертификат.

3. Выберите Тип сервиса для сервера OpenVPN — UDP или TCP.
4. Введите число в поле Порт сервиса (от 1024 до 65535) для подключения VPN-устройства.
5. Введите в поля Подсеть/маска подсети VPN диапазон IP-адресов, которые могут быть арендованы устройству сервером OpenVPN.

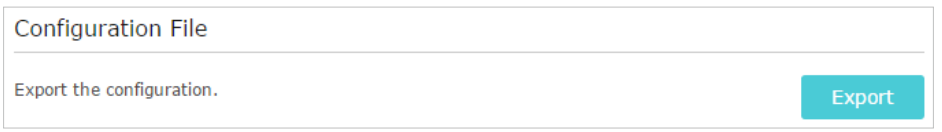
6. В пункте Доступ клиента выберите Только домашняя сеть, если нужно, чтобы у удалённого устройства был доступ только к домашней сети; выберите Интернет и домашняя сеть, если нужно, чтобы у удалённого устройства был доступ в интернет через VPN-сервер.
7. Нажмите Сохранить.
8. Нажмите Генерировать, чтобы создать новый сертификат.



Примечание

Если у вас уже есть сгенерированный сертификат, этот шаг можно пропустить.

9. Нажмите Экспортировать, чтобы сохранить файл с настройками OpenVPN, который будет использоваться удалённым устройством для доступа к роутеру.



9.1.2. Шаг 2. Настройка подключения OpenVPN на удалённом устройстве

1. Перейдите на http://openvpn.net/index.php/download/community-downloads.html, чтобы скачать программу OpenVPN, затем установите её на нужном устройстве.

Примечание

Приложение OpenVPN необходимо установить на каждом устройстве, которое планируется использовать для VPN-подключения. Мобильное приложение доступно на Google Play и в App Store.

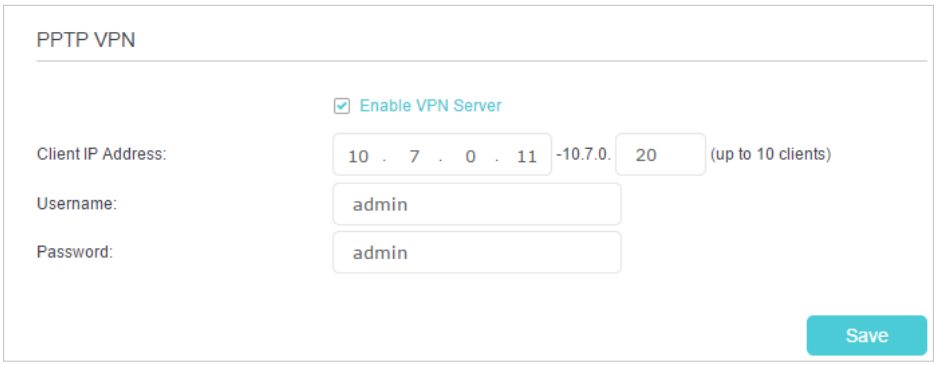
2. После установки скопируйте экспортированный с роутера файл в папку с настройками клиентской утилиты OpenVPN (например, C:\Program Files \OpenVPN\config).
3. Запустите клиентскую утилиту OpenVPN и подключитесь к серверу OpenVPN.

9.2. Доступ к домашней сети через PPTP

VPN-сервер PPTP предназначен для создания подключения VPN на удалённом устройстве. Для использования сервера VPN нужно создать VPN-сервер PPTP на роутере и настроить подключение PPTP на удалённом устройстве. Ниже описаны шаги по настройке VPN-подключения PPTP.

9.2.1. Шаг 1. Настройка VPN-сервера PPTP на роутере

1. Перейдите на http://tplinkwifi.net, и войдите, используя пароль, который вы создали для роутера.
2. Перейдите в раздел Дополнительные настройки > VPN > PPTP VPN и отметьте окошко Запустить VPN сервер.



Примечание

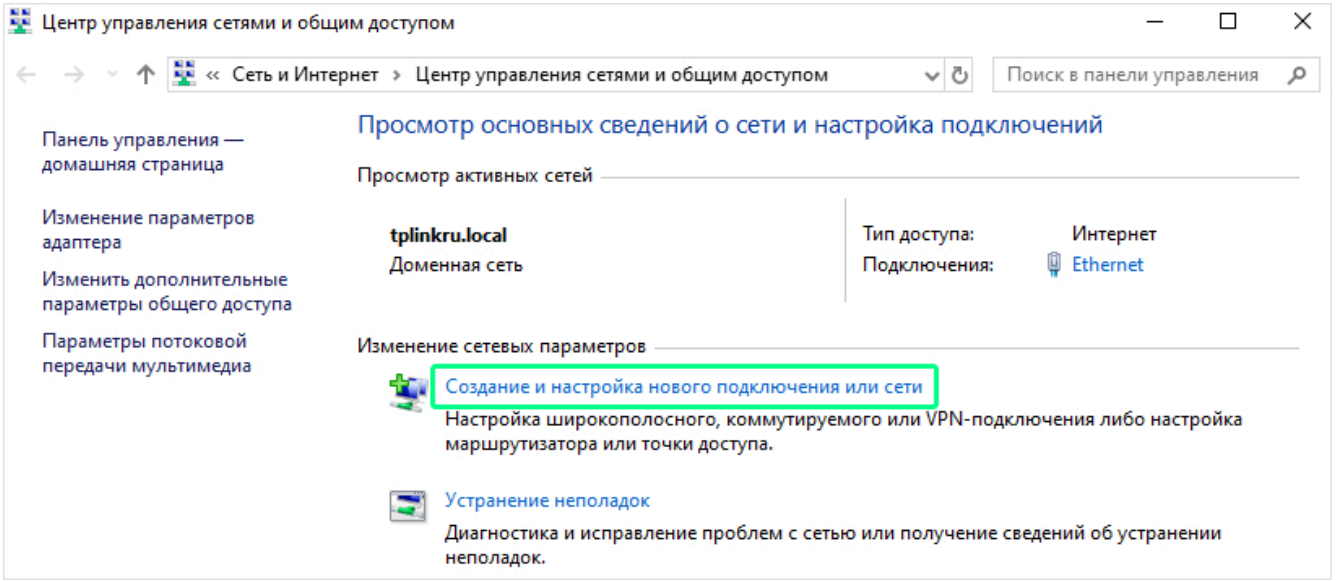
Перед созданием VPN-сервера рекомендуется настроить динамический DNS-сервис или присвоить статический IP-адрес порту WAN роутера и выполнить интернет-синхронизацию системного времени.

3. Введите в поле IP-адрес клиента диапазон IP-адресов (до десяти), которые могут быть арендованы устройствам VPN-сервером PPTP.
4. Введите Имя пользователя и Пароль для аутентификации клиентов на VPN-сервер PPTP.
5. Нажмите Сохранить, чтобы изменения вступили в силу.

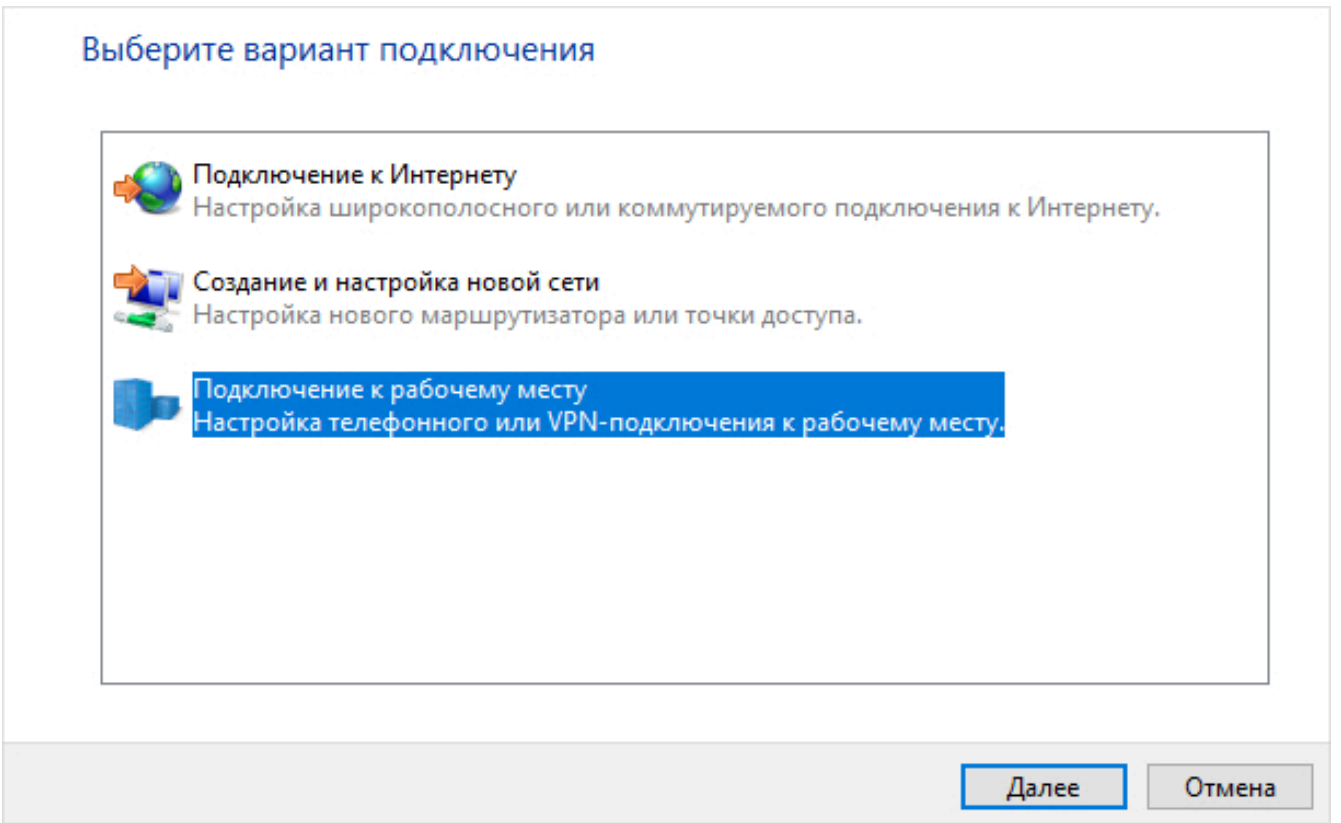
9.2.2. Шаг 2. Настройка VPN-подключения PPTP на удалённом устройстве

Для подключения к серверу PPTP удалённое устройство может использовать как встроенные средства Windows, так и стороннее ПО. В данном руководстве рассматривается настройка на примере встроенных средств Windows.

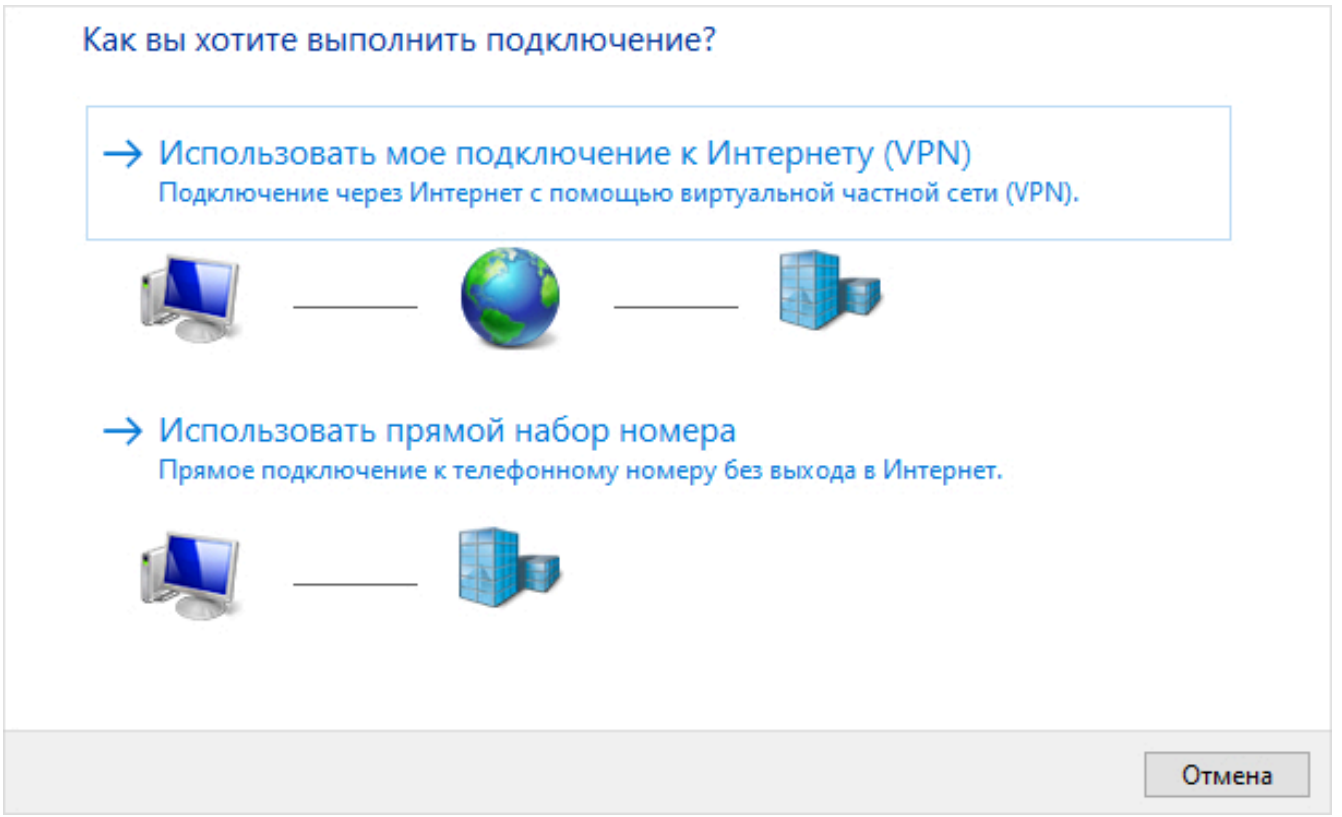
1. Перейдите в раздел Пуск > Параметры > Сеть и Интернет > Центр управления сетями и общим доступом.
2. Выберите Создание и настройка нового подключения или сети.



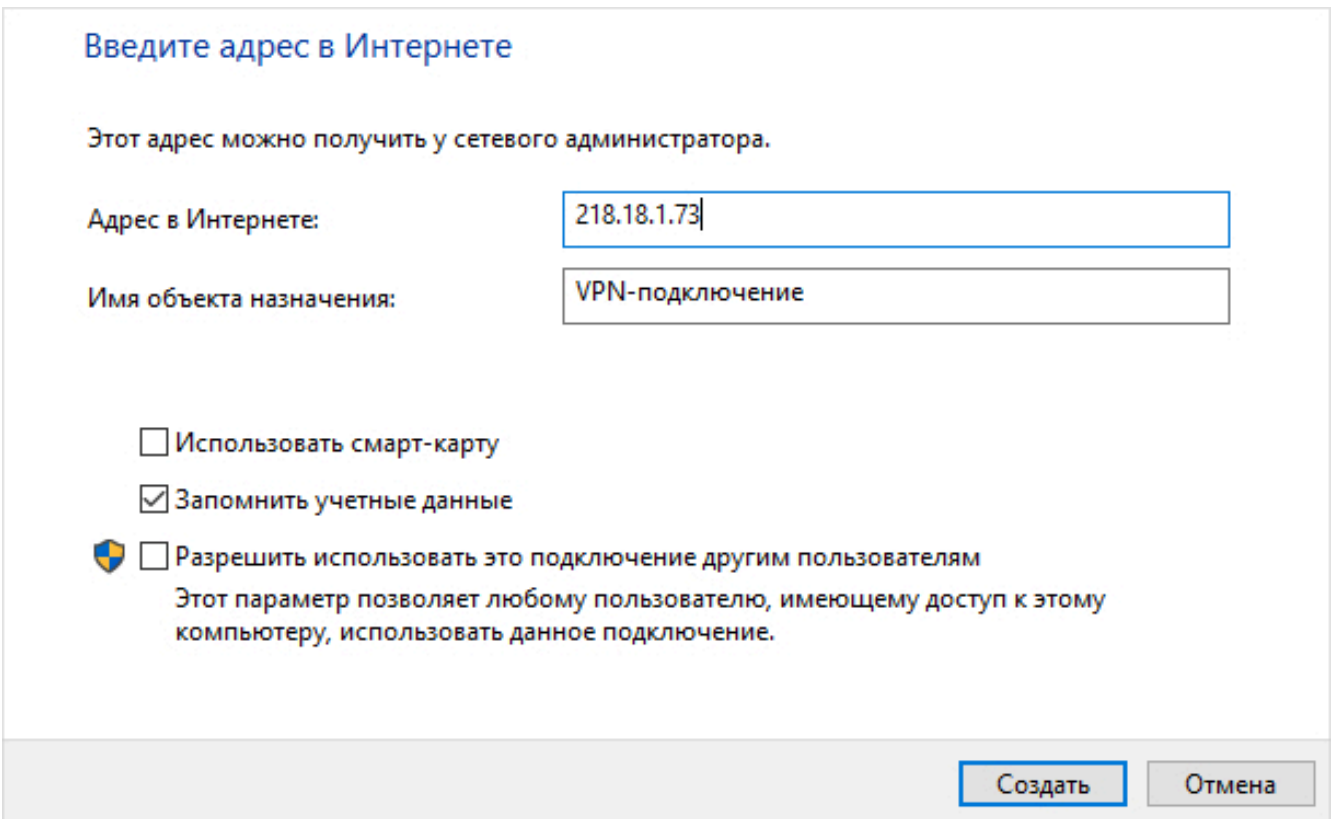
3. Выберите Подключение к рабочему месту и нажмите Далее.



4. Выберите Использовать мое подключение к Интернету (VPN).



5. Введите IP-адрес роутера (например, 218.18.1.73) в поле Адрес в Интернете и нажмите Далее.



6. VPN-подключение PPTP создано.

Глава 10

Настройка параметров сети

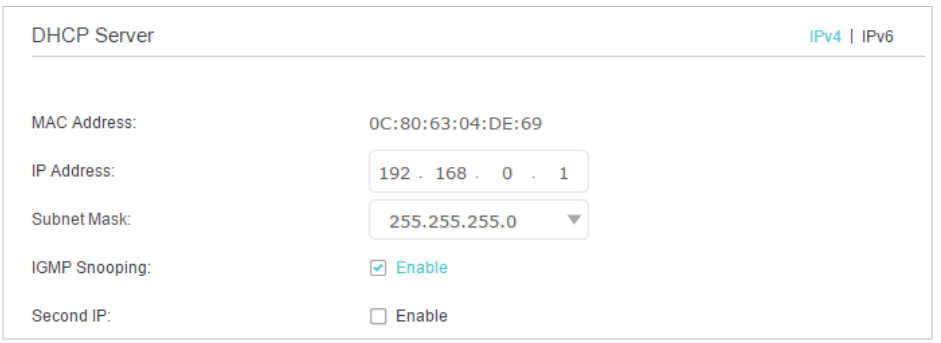
В этой главе рассказывается о настройках сети.

10.1 Изменение настроек сети LAN

10.1.1. Изменение IP-адреса сети LAN

IP-адрес сети LAN роутера по умолчанию (192.168.0.1) можно использовать для входа в веб-интерфейс управления роутера. IP-адрес сети LAN вместе с маской подсети представляют собой подсеть, в которой находятся подключённые устройства. Если IP-адрес конфликтует с другим устройством в локальной сети или если для вашей сети требуется конкретный IP-адрес подсети, его можно изменить:

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > LAN и выберите IPv4.



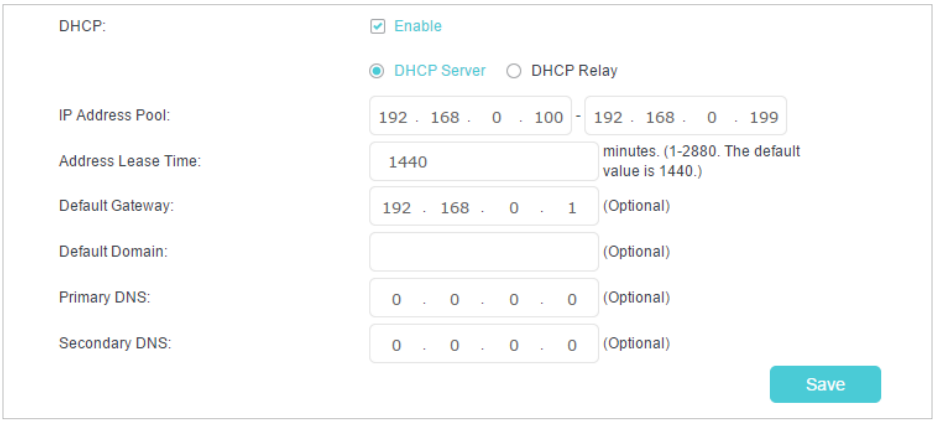
3. Введите новый IP-адрес.
4. Выберите Маску подсети из одноимённого выпадающего списка. IP-адрес сети LAN вместе с маской подсети представляют собой локальную IP-подсеть.
5. Оставьте IGMP Snooping включённым — эта функция прослушивает сетевой трафик IGMP и защищает узлы в локальной сети от получения трафика для многоадресной группы, к которой они не относятся.
6. Можно настроить Вторичный IP-адрес и Маску подсети сети LAN, через которые также будет доступ к веб-интерфейсу управления.
7. Оставьте остальные настройки по умолчанию.
8. Нажмите Сохранить, чтобы изменения вступили в силу.

10.1.2. Использование роутера в качестве сервера DHCP

Роутер можно настроить в качестве сервера DHCP, чтобы он присваивал IP-адреса своим клиентам. Для использования этой функции необходимо указать в настройках всех компьютеров в сети LAN автоматическое получение IP-адреса.

Ниже описан процесс настройки сервера DHCP.

1. Перейдите на http://tplinkwifi.net и войдите, используя созданный вами пароль для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > LAN и выберите IPv4.



3. Включите DHCP и выберите DHCP-сервер.
4. Укажите Пул IP-адресов, при этом начальный и конечный адреса должны быть в одной подсети с IP-адресом LAN. Роутер присвоит клиентам адреса в указанном диапазоне. Диапазон по умолчанию: от 192.168.0.100 до 192.168.0.199.
5. Введите значение в поле Время аренды, под которым подразумевается время, в течение которого клиент DHCP может арендовать свой текущий IP-адрес, присвоенный роутером. После истечения срока действия IP-адреса, пользователю будет автоматически присвоен новый динамический IP-адрес. Значение по умолчанию: 1440 минут.
6. Оставьте остальные настройки по умолчанию и нажмите Сохранить.

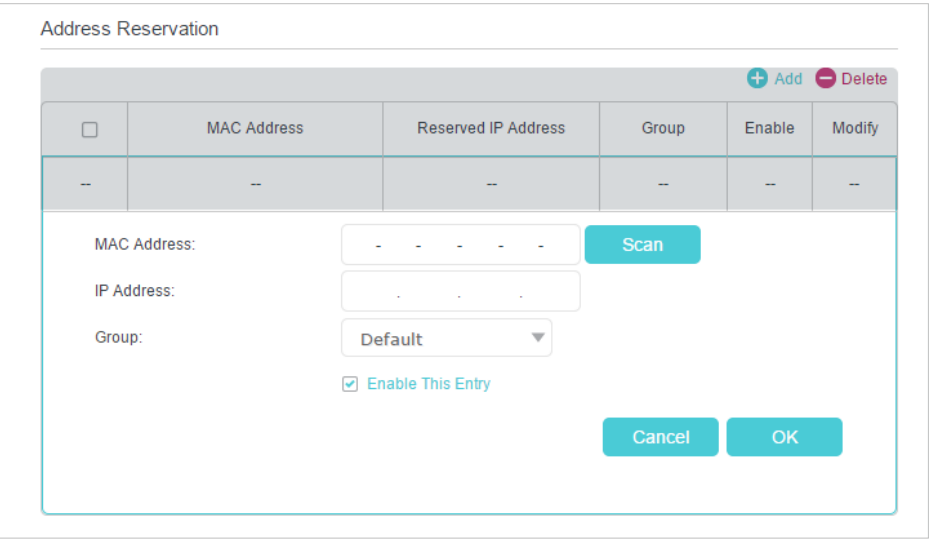
Примечания

1. Роутер можно настроить в качестве DHCP-ретранслятора. DHCP-ретранслятор — это компьютер, передающий DHCP-данные между компьютерами, которые запрашивают IP-адреса, и сервером DHCP, который эти адреса присваивает. Каждый из интерфейсов устройства может быть настроен как DHCP-ретранслятор. Если эта функция включена, DHCP-запросы локальных компьютеров будут направляться на сервер DHCP, работающий в сети WAN.
2. Также с помощью параметр Пул адресов на основе параметров можно присвоить устройствам одного типа IP-адреса в обозначенном диапазоне. Например, чтобы упростить управление сетью, можно присвоить всем камерам IP-адреса в диапазоне от 192.168.1.50 до 192.168.1.80. Включите DHCP и настройте нужные параметры в разделе Дополнительные настройки > Сеть > LAN.

10.1.3. Резервирование IP-адреса LAN

Для клиентов можно резервировать IP-адреса — это значит, что если указать конкретный IP-адрес для устройства в сети LAN, это устройство будет всегда получать один и тот же IP-адрес при каждом подключении к серверу DHCP. Ниже описан процесс настройки резервирования на роутере.

1. Перейдите на http://tplinkwifi.net и выполните вход, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > LAN и выберите IPv4.
3. Прокрутите вниз до таблицы Резервирование адресов и нажмите Добавить, чтобы добавить запись резервирования адреса.



4. Введите MAC-адрес устройства, для которого нужно зарезервировать IP-адрес.
5. Укажите IP-адрес, который нужно зарезервировать.
6. Отметьте Включить эту запись и нажмите Сохранить , чтобы изменения вступили в силу.

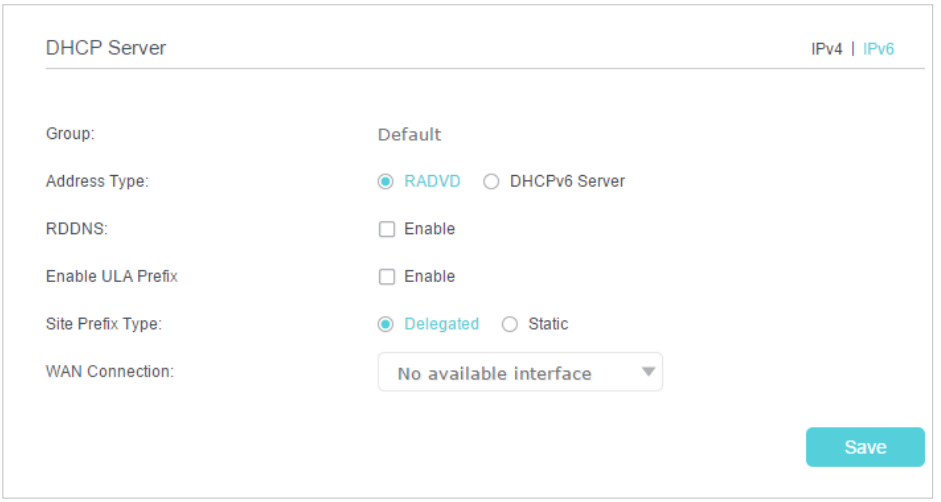
10.2. Настройка параметров IPv6 в сети LAN

На роутере есть два способа присвоения адресов IPv6 в сети LAN:

- Тип адреса RADVD.
- Тип адреса сервера DHCPv6.

10.2.1. Настройка типа адреса RADVD

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > LAN.
3. Перейдите на вкладку IPv6.



1) Выберите тип адреса RADVD, чтобы роутер присваивал узлам префиксы адреса IPv6.

Примечание

Не отмечайте окошки Включить для параметров RDNSS и ULA-префикс, если этого не требует ваш интернет-провайдер. В противном случае может исчезнуть доступ к сети IPv6. Для более подробной информации по RDNSS и ULA-префиксе свяжитесь с нашей службой техподдержки.

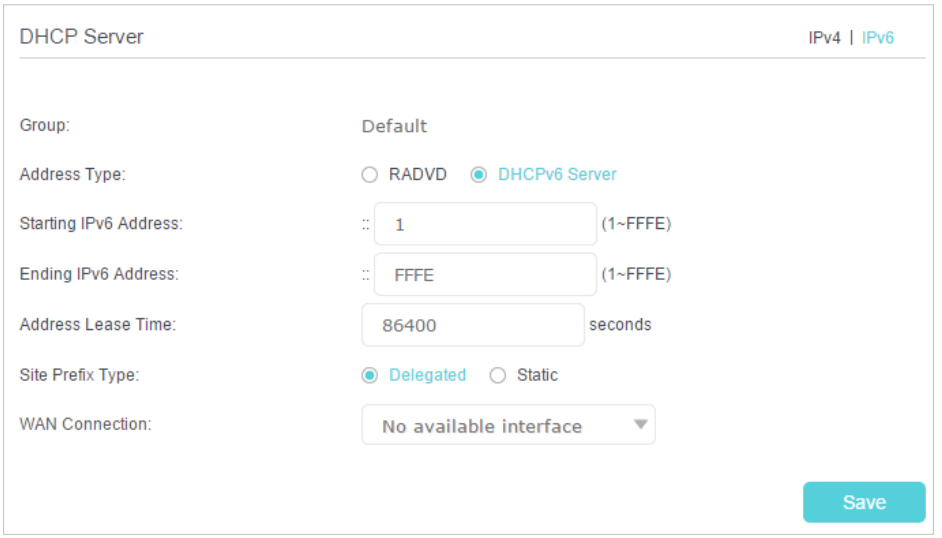
2) Оставьте значение Делегированный для параметра Тип глобального префикса сети. Если интернет-провайдер предоставляет конкретный префикс IPv6, выберите Статический и введите префикс.

3) Оставьте значение по умолчанию для параметра Делегированный префикс подключения WAN.

4. Нажмите Сохранить, чтобы изменения вступили в силу.

10.2.2. Настройка типа адреса сервера DHCPv6

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > LAN.
3. Перейдите на вкладку IPv6.



1) Выберите DHCPv6-сервер у параметра Тип адреса.

2) Введите Начальный IPv6-адрес и Конечный IPv6-адрес. Роутер сгенерирует адреса IPv6 в указанном диапазоне.

3) Оставьте по умолчанию значение параметра Время аренды.

4) Оставьте значение Делегированный для параметра Тип глобального префикса сети. Если интернет-провайдер предоставляет конкретный префикс IPv6, выберите Статический и введите префикс.

5) Оставьте значение по умолчанию для параметра Делегированный префикс подключения WAN.

4. Нажмите Сохранить, чтобы изменения вступили в силу.

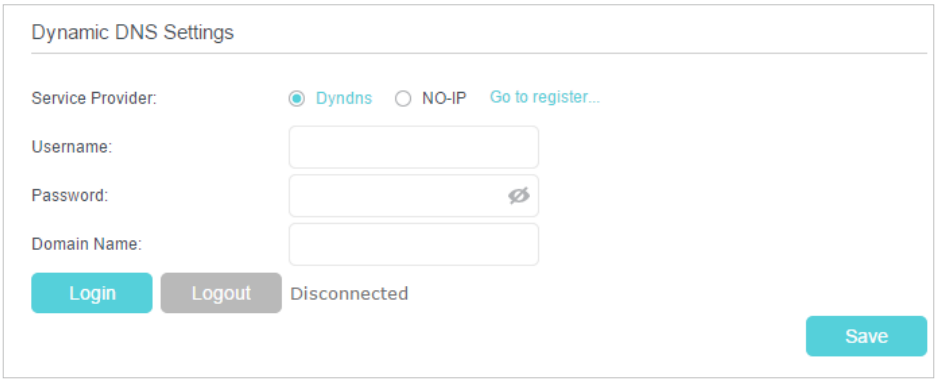
10.3. Настройка динамического DNS

Большинство интернет-провайдеров присваивают роутерам динамический IP-адрес, по которому можно получить удалённый доступ к роутеру. Однако периодически IP-адрес может изменяться. В таком случае можно воспользоваться функцией DDNS, которая позволит вам и вашим близким получать доступ к роутеру и к локальным серверам (FTP, HTTP и т. д.) посредством доменного имени, чтобы не запоминать IP-адрес.

Примечание

DDNS не будет работать, если интернет-провайдер присвоил роутеру частный IP-адрес WAN (например, 192.168.1.x).

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > Динамический DNS.
3. Выберите поставщика услуг DDNS в одноимённом пункте: NO-IP или DynDNS. Если у вас нет учётной записи, необходимо зарегистрироваться, нажав Перейти к регистрации...
4. Введите имя пользователя, пароль и доменное имя своей учётной записи.



5. Нажмите Вход и Сохранить.

Советы

Если нужно войти с другой учётной записи DDNS, нажмите Выйти, затем войдите с другой учётной записи.

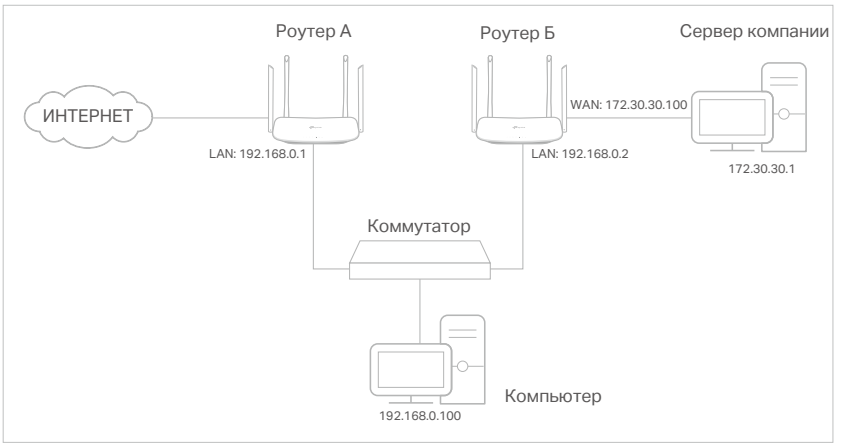
10.4. Создание статической маршрутизации

Статическая маршрутизация настраивается вручную путём добавления записей в соответствующую таблицу. Посредством этих записей роутер передаёт пакеты данных по соответствующему маршруту.

Хочу

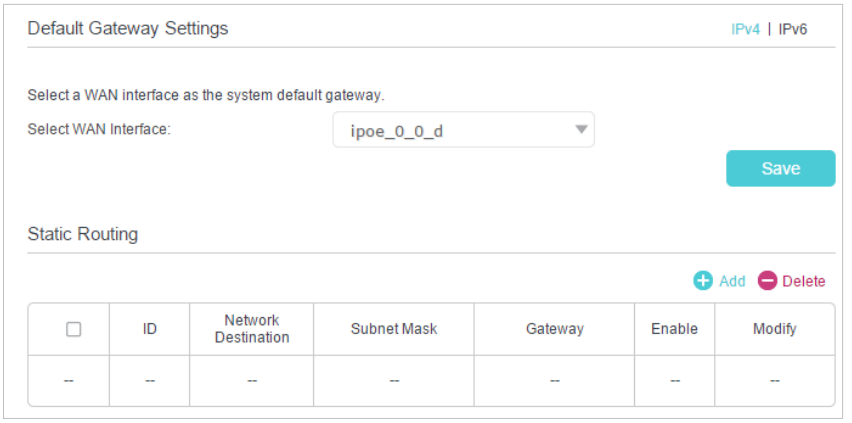
Иметь одновременный доступ к разным сетям и серверам.

Допустим, у вас есть доступ в интернет через домашний Роутер А, но вам также необходим доступ к корпоративной сети. Это можно осуществить с помощью Коммутатора и Роутера Б по схеме ниже. Также для одновременного доступа к интернету и к корпоративной сети необходимо настроить статическую маршрутизацию.

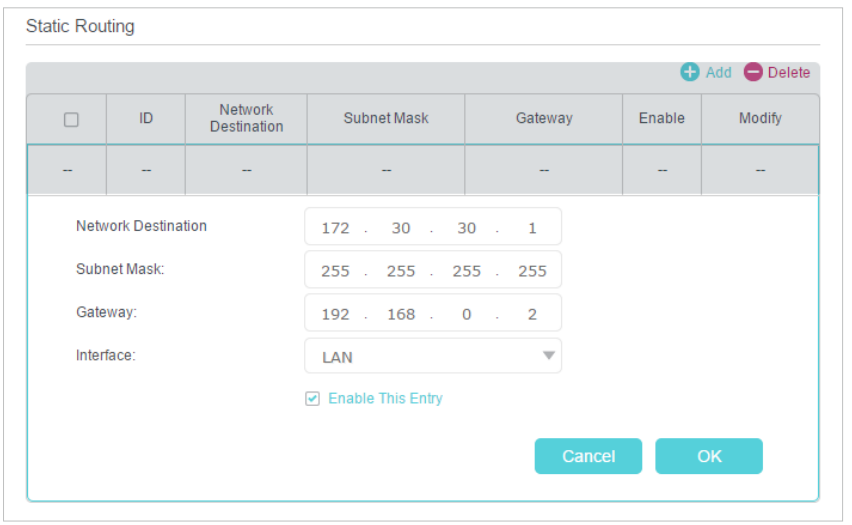


Как это сделать?

1. Создайте для роутеров IP-адреса LAN, чтобы это были два разных IP-адреса в одной подсети. Отключите DHCP на Роутере Б.
2. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для Роутера А.
3. Перейдите в раздел Сеть > Расширенные настройки маршрутизации > Статическая маршрутизация.
4. Выберите текущий интерфейс WAN и нажмите Сохранить.



5. Нажмите Добавить и завершите настройку согласно приведённым ниже указаниям:



IP-адрес назначения: не может быть в одной подсети с IP-адресом WAN или LAN Роутера А. В нашем примере IP-адрес назначения — это IP-адрес корпоративной сети (172.30.30.1).

Маска подсети: если IP-адрес назначения один, введите 255.255.255.255. В противном случае введите маску соответствующей сети. В нашем примере IP-адрес назначения один — 255.255.255.255.

Шлюз: IP-адрес шлюза, на который будут отправляться пакеты данных. Данный IP-адрес должен быть в той же подсети, что и IP-адрес роутера, с которого отправляются данные. В нашем случае пакеты данных будут отправляться на порт LAN Роутера Б, а затем на Сервер, поэтому используется значение 192.168.0.2.

Интерфейс: определяется портом (WAN/LAN), с которого отправляются пакеты данных. В нашем примере данные отправляются на шлюз через порт LAN Роутера А, поэтому выбрано значение LAN.

6. Нажмите OK, чтобы изменения вступили в силу.

Готово!

Откройте браузер на компьютере и введите IP-адрес сервера компании, чтобы подключиться к корпоративной сети.

10.5. Настройка Wi-Fi

10.5.1. Основные настройки

Имя (SSID) и пароль Wi-Fi сети, а также способ шифрования сети роутера предустанавливаются при производстве. Предустановленные SSID и пароль указаны на этикетке роутера. Эти данные можно изменить.

Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.

➢ **Включение и отключение Wi-Fi**

1. Перейдите в раздел Основные настройки > Беспроводной режим.
2. По умолчанию Wi-Fi включён. Если его нужно отключить, уберите галочку в окошках Включить.

➢ **Изменение имени (SSID) и пароля Wi-Fi сети**

1. Перейдите в раздел Основные настройки > Беспроводной режим.
2. Введите новый SSID в поле Имя сети (SSID), введите новый пароль в поле Пароль. Оба поля чувствительны к регистру.

Примечание

При изменении параметров Wi-Fi сети с Wi-Fi устройства, устройство будет отключено от сети после вступления изменений в силу. Запишите новые имя и пароль Wi-Fi сети, чтобы не забыть их.

➢ **Скрытие SSID**

1. Перейдите в раздел Основные настройки > Беспроводной режим.
2. Выберите Скрыть SSID, чтобы имя сети не отображалось в списке доступных Wi-Fi сетей на клиентских устройствах. В таком случае к сети надо будет подключаться вручную.

➢ **Изменение режима или канала**

Перейдите в раздел Дополнительные настройки > Беспроводной режим > Настройки беспроводного режима и выберите 2,4 ГГц или 5 ГГц.

Режим: выберите нужный режим передачи; рекомендуется оставить значение по умолчанию.

- Только 802.11n: для клиентских устройств стандарта 802.11n.
- 802.11g/n смешанный: для клиентских устройств стандартов 802.11g и 802.11n.
- 802.11b/g/n смешанный: для клиентских устройств стандартов 802.11b, 802.11g и 802.11n.

  Примечание: при выборе 802.11n смогут подключаться только устройтва 802.11n. Настоятельно рекомендуется выбрать 802.11b/g/n смешанный, тогда к роутеру смогут подключиться устройства стандартов 802.11b, 802.11g и 802.11n.
- Только 802.11ac: для клиентских устройств стандарта 802.11ac.
- 802.11ac/n смешанный: для клиентских устройств стандартов 802.11ac и 802.11n.
- 802.11a/n/ac смешанный: для клиентских устройств стандартов 802.11a, 802.11n и 802.11ac. Рекомендуется выбрать 11a/n/ac смешанный.

Канал: выберите нужный канал из выпадающего списка. В данном поле указывается рабочая чистота. Не стоит изменять это значение, если нет помех.

Ширина канала: выберите ширину канала из выпадающего списка. По умолчанию установлено значение Авто.

Мощность передатчика: выберите Низкая, Средняя или Высокая. Значение по умолчанию и рекомендуемое значение — Высокая.

➢ **Изменение типа шифрования**

1. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Настройки беспроводного режима.
2. Выберите вкладку 2,4 ГГц или 5 ГГц.
3. Выберите значение из выпадающего списка Защита. Изменять значение по умолчанию рекомендуется только при необходимости. При изменении значения укажите остальные параметры в соответствии с указаниями в разделе помощи.

➢ **Включение Band Steering**

1. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Настройки беспроводного режима.
2. Найдите пункт Band Steering, отметьте окошко Включить и нажмите Сохранить.

10.5.2. Подключение WPS

WPS — это упрощённое быстрое создание защищённого Wi-Fi подключения.

Способ 1: физическая кнопка WPS

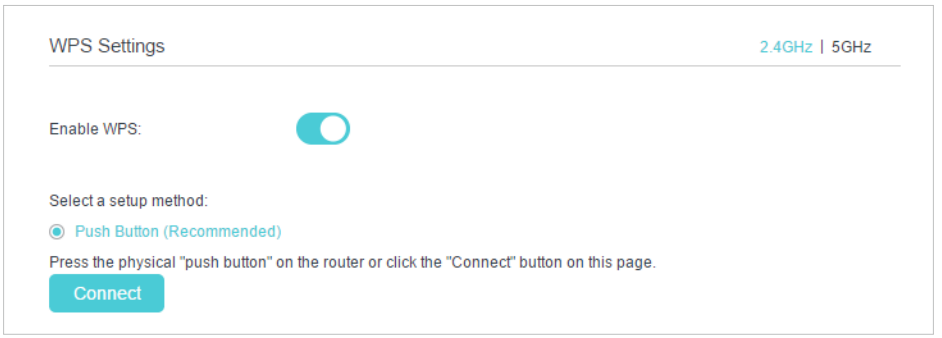
Используйте этот способ, если на клиентском устройстве есть кнопка WPS.

1. Нажмите и удерживайте кнопку WPS роутера в течение 1 секунды.
2. Нажмите кнопку WPS на клиентском устройстве.
3. Во время настройки WPS индикатор WPS будет мигать около двух минут.
4. Если индикатор перестал мигать и стал гореть, значит клиентское устройство успешно подключилось к роутеру.

Способ 2: кнопка WPS в веб-интерфейсе управления

Используйте этот способ, если на клиентском устройстве есть кнопка WPS.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для роутера.
2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > WPS, найдите секцию WPS и выберите диапазон 2,4 ГГц или 5 ГГц.



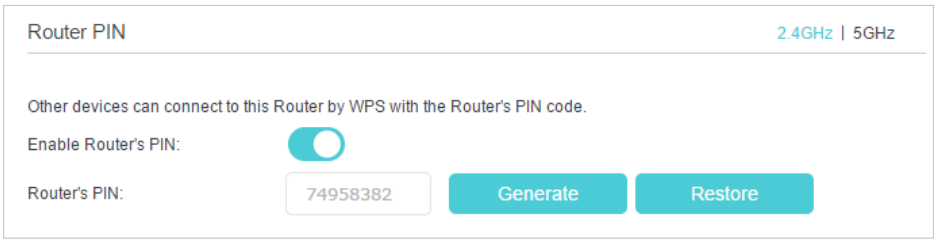
3. Переведите ползунок Включить WPS во включённое положение и нажмите Подключить.
4. Нажмите кнопку WPS на клиентском устройстве.
5. Во время настройки WPS индикатор WPS будет мигать около двух минут.
6. Если индикатор перестал мигать и стал гореть, значит клиентское устройство успешно подключилось к роутеру.

Способ 3: ввод PIN-кода на клиентском устройстве

Используйте этот способ, если клиентское устройство запрашивает PIN-код роутера.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.

2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > WPS, найдите секцию PIN-код маршрутизатора и выберите 2,4 ГГц или 5 ГГц.



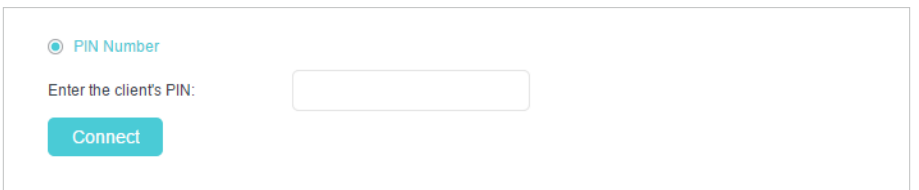
3. Убедитесь, что ползунок PIN-код маршрутизатора переведён во включённое положение и запомните текущий PIN-код роутера. Нажмите Генерировать, если нужен новый PIN-код.
4. Введите PIN-код роутера на клиентском устройстве (PIN-код по умолчанию также указан на этикетке роутера).
5. Во время настройки WPS индикатор WPS будет мигать около двух минут.
6. Если индикатор перестал мигать и стал гореть, значит клиентское устройство успешно подключилось к роутеру.

Примечания

1. При успешном подключении устройства к сети индикатор WPS роутера будет гореть в течение пяти минут.
2. WPS нельзя включить, если на роутере отключён Wi-Fi.

Способ 4: ввод PIN-кода клиентского устройства на роутере

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для роутера.
2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > WPS, найдите секцию WPS и выберите 2,4 ГГц или 5 ГГц.
3. Убедитесь, что ползунок Включить WPS переведён во включённое положение, и выберите PIN-код.



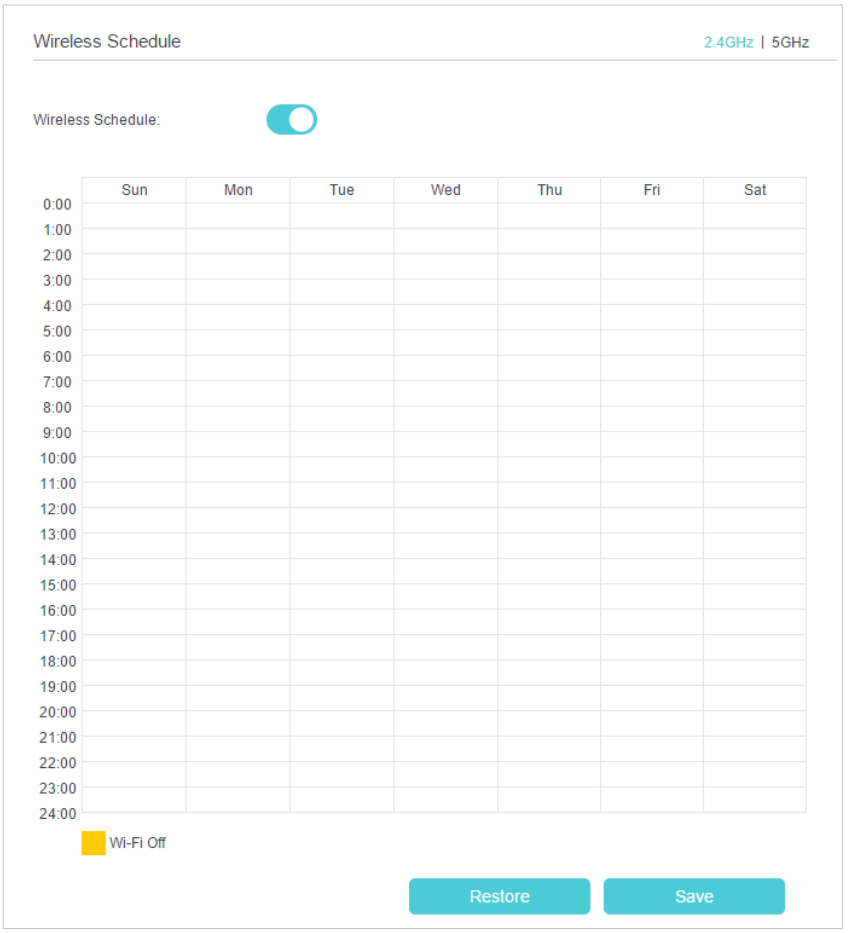
4. Введите клиентский PIN-код и нажмите кнопку Подключить.
5. На экране должно появиться сообщение об успешном подключении.

10.5.3. Wi-Fi по расписанию

Можно установить автоматическое отключение Wi-Fi сети, когда она не нужна.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для роутера.

2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Расписание беспроводного вещания и выберите 2,4 ГГц или 5 ГГц.
3. Переведите ползунок Расписание беспроводного вещания во включённое положение.
4. Удерживайте кнопку мыши и тащите курсор по ячейкам таблицы, чтобы установить время, в течение которого Wi-Fi будет отключён, затем нажмите Сохранить, чтобы изменения вступили в силу.



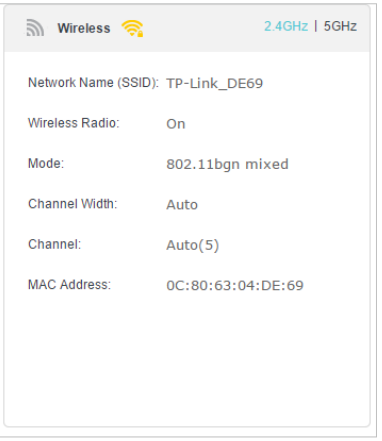
Примечания

1. Перед включением расписания убедитесь, что на роутере установлено правильное время (см. Настройка системного времени).
2. Если расписание установлено лишь для одного диапазона, другой диапазон продолжит работать.
3. При отключении Wi-Fi на одном из диапазонов соответствующий индикатор погаснет.
4. Wi-Fi сеть будет автоматически включена после указанного времени.

10.5.4. Просмотр информации о Wi-Fi сети

➢ Просмотр подробных настроек Wi-Fi

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Состояние. Найдите панель Беспроводной режим.
3. Выберите вкладку 2,4 ГГц или 5 ГГц.



Совет: информация о состоянии Wi-Fi сети также доступна при нажатии иконки роутера в разделе Основные настройки > Карта сети.

➢ **Просмотр подробной информации о подключённых Wi-Fi клиентах**

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Статистика.
3. В этом разделе доступна подробная информация о Wi-Fi клиентах, включая используемый диапазон, шифрование и переданные пакеты.

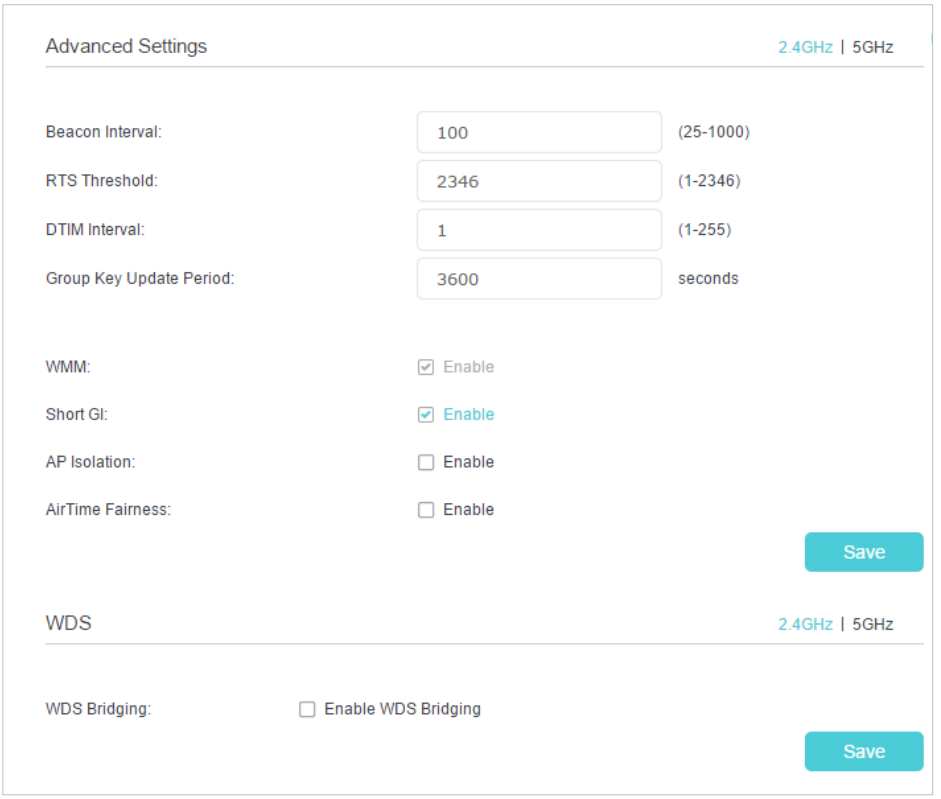
Совет: информация о Wi-Fi клиентах также доступна при нажатии иконок клиентов в разделе Основные настройки > Карта сети.

10.5.5. Дополнительные настройки Wi-Fi

Дополнительные настройки Wi-Fi предназначены для тех, кому недостаточно основных настроек. Если настройки этого раздел вам незнакомы, рекомендуется оставить все значения по умолчанию, в противном случае может ухудшиться производительность сети.

1. Перейдите в раздел http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Дополнительные настройки.

➢ **Изменение дополнительных настроек**



- Интервал маяка: введите время от 25 до 1000 мс, в течение которого будет передаваться импульс, информирующий сеть о том, что роутер по-прежнему активен. Значение по умолчанию: 100 мс.
- Порог RTS: введите значение от 1 до 2346, определяющее размер пактов данных. Значение по умолчанию: 2346. Если размер превышает пороговое значение, роутер отправляет кадры RTS на конкретную приёмную станцию и оговаривает условия отправки кадра данных, в противном случае пакет тут же отправляется.
- Интервал DTIM: введите значение от 1 до 255. Значение 1 означает, что интервал DTIM будет совпадать с интервалом маяка.
- Период обновления группового ключа: введите количество секунд, после которого групповой ключ будет обновляться. По умолчанию указано значение 0 (групповой ключ не обновляется).
- WMM: гарантирует приоритетную передачу пакетов с высоким приоритетом. Этот параметр невозможно отключить для 802.11n или 802.11ac. Настоятельно рекомендуется включить этот параметр.
- Короткий защитный интервал: увеличение пропускной способности за счёт уменьшения защитного интервала. Этот параметр включён по умолчанию.
- Изоляция клиентов: ограничение коммуникации друг с другом между всеми Wi-Fi устройствами в сети. По умолчанию этот параметр отключён.

- Air Time Fairness: предоставление равного эфирного времени для всех подключённых устройств. Эта функция позволит избежать ситуаций, когда одно медленное устройство замедляет работу всей сети.

10.6. Настройка туннеля IPv6

Туннель IPv6 обеспечивает доступ к IPv6 по подключению WAN IPv4 и наоборот.

Туннель IPv6 — это переходный механизм, который обеспечивает узлам IPv6 доступ к IPv4, а также позволяет узлам и сетям IPv6 подключаться друг к другу по инфраструктуре IPv4, пока IPv6 полностью не заменит IPv4. Это временное решение для сетей, в которых нет возможности использовать IPv6 и IPv4 одновременно.

Роутер поддерживает три механизма туннелирования: 6to4, 6rd и DS-Lite. Настройка туннелей 6rd и DS-Lite очень похожа.

10.6.1. Использование туннеля 6to4

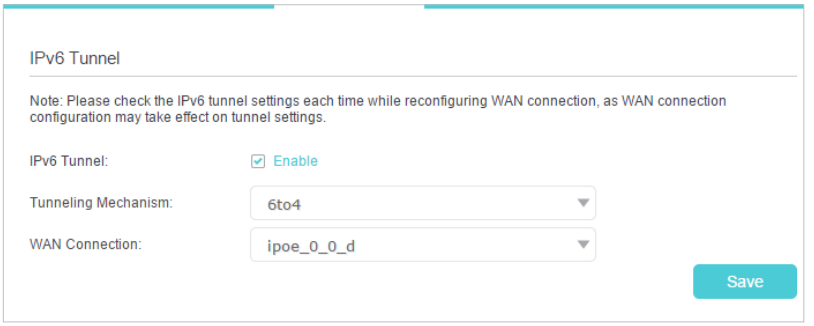
Если в вашей сети есть сервера 6to4, можно использовать этот механизм для доступа к IPv6. Если ваш интернет-провайдер предоставляет только подключение IPv4, то для доступа к сайтам IPv6 можно использовать туннель 6to4.

Хочу

Создать туннель IPv6, даже несмотря на то, что мой интернет-провайдер не предоставляет туннелирование.

Как это сделать?

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > IPv6 Туннель.
3. Включите IPv6 Туннель и выберите механизм туннелирования 6to4, затем выберите подключение WAN из выпадающего списка и нажмите Сохранить.



Примечание

Если в списке нет доступных подключений WAN, убедитесь, что у вас есть подключение к интернету и что подключение не в режиме моста.

Готово! Теперь вы можете посещать сайты IPv6 через туннель 6to4.

Примечание

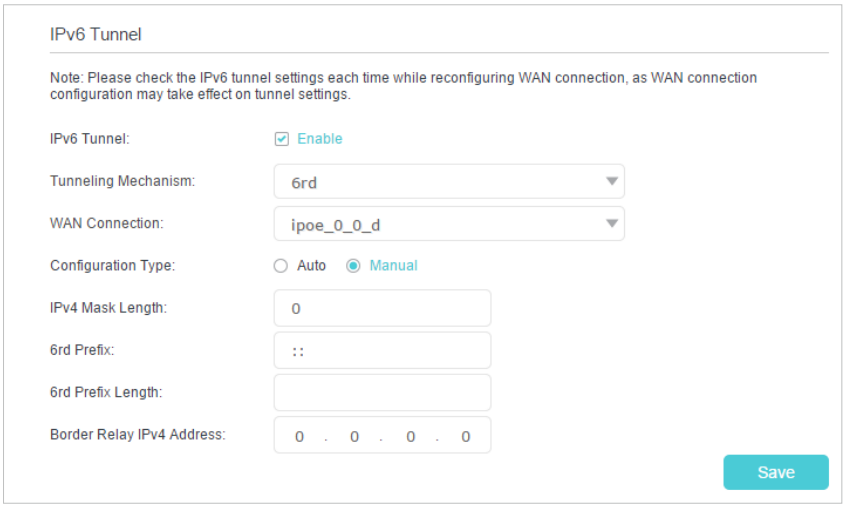
Если доступа к IPv6 по-прежнему нет, возможно, в вашей сети не был найден публичный сервер 6to4. Свяжитесь с интернет-провайдером, чтобы подписаться на сервис IPv6.

10.6.2. Настройка туннеля 6rd путём использования параметров интернет-провайдера

Хочу Создать туннель 6rd, используя параметры провайдера.

Как это сделать?

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Сеть > IPv6 Туннель.
3. Включите IPv6 Туннель и выберите механизм туннелирования 6rd, затем выберите подключение WAN из выпадающего списка и нажмите Сохранить.
4. В зависимости от указаний провайдера, выберите Авто или Вручную. При выборе значения Вручную надо указать дополнительные параметры.
5. Нажмите Сохранить.



Примечание

Если в списке нет доступных подключений WAN, убедитесь, что у вас есть подключение к интернету и что подключение не в режиме моста.

Готово! Теперь вы можете посещать сайты IPv6 через туннель 6rd.

Совет

Настройка туннеля DS-Lite аналогична настройке туннеля 6rd. Если у вас подключение WAN только по IPv6 и вы подписаны на сервис туннелирования DS-Lite, создайте туннель DS-Lite, руководствуясь указаниями выше.

Глава 11

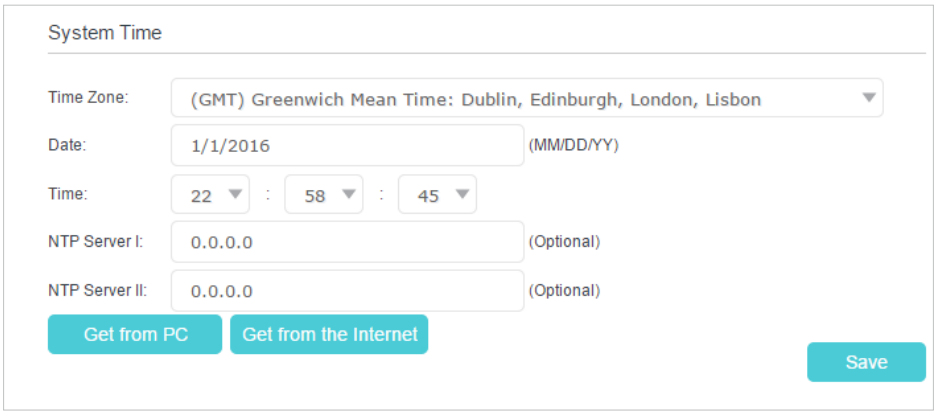
Управление роутером

- Настройка системного времени
- Тестирование сетевого подключения
- Обновление прошивки
- Создание резервной копии и восстановление настроек
- Изменение пароля для входа
- Локальное управление
- Удалённое управление
- Системный журнал
- Настройки CWMP
- Настройки SNMP
- Мониторинг статистики интернет-трафика

11.1. Настройка системного времени

На системное время опираются некоторые функции роутера, например, родительский контроль.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Настройка времени.



3. Выберите один из способов установки системного времени.

   Вручную: выберите свой часовой пояс, введите дату и время.

   Получить с компьютера: нажмите эту кнопку, чтобы использовать время, установленное на компьютере.

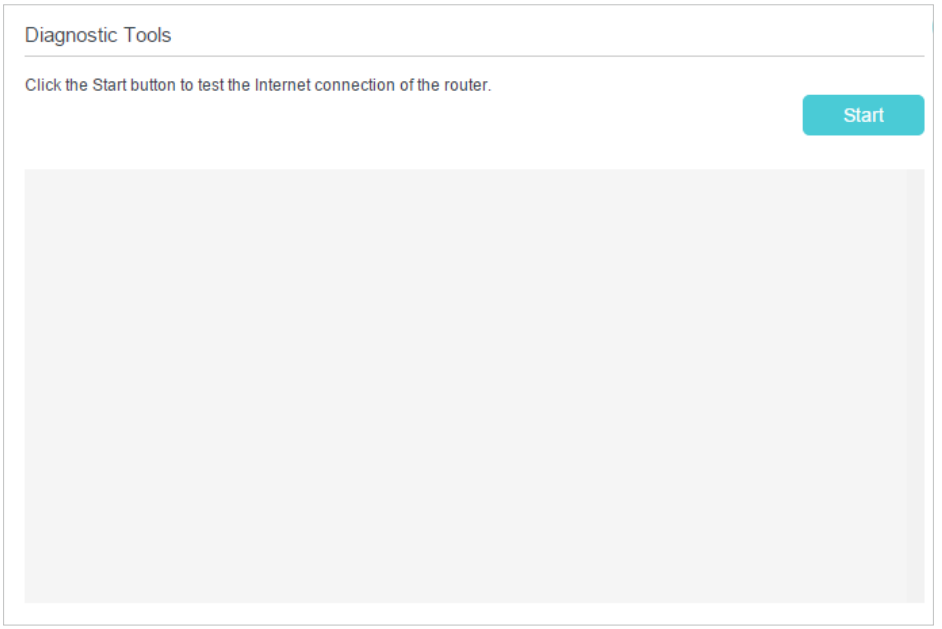
   Получить среднее время по Гринвичу: нажмите эту кнопку, чтобы синхронизировать время с интернетом. Перед выбором этого способа убедитесь, что роутер подключён к интернету.

4. Нажмите Сохранить, чтобы изменения вступили в силу.

11.2. Проверка сетевого подключения

Инструменты диагностики нужны для тестирования подключения к интернету.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Диагностика.



3. Нажмите Начать, чтобы протестировать подключение к интернету. Результаты тестирования появятся в сером окне.

11.3. Обновление прошивки

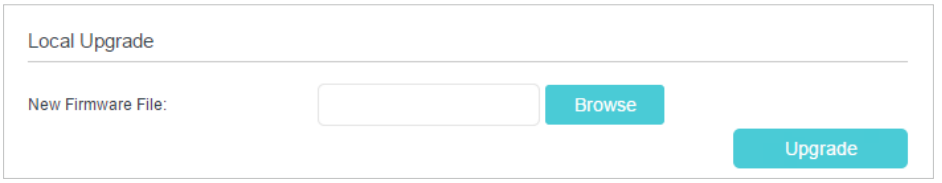
TP-Link стремится постоянно улучшать работу своих устройств. При появлении новой прошивки в веб-интерфейсе управления появится уведомление. Также прошивки можно бесплатно скачать на нашем официальном сайте www.tp-link.com/ru.

Примечания

- Перед обновлением прошивки на всякий случай создайте резервную копию настроек.
- НЕ ОТКЛЮЧАЙТЕ роутер во время обновления прошивки.

Инструкция по обновлению прошивки вручную:

1. Скачайте файл с прошивкой на www.tp-link.com/ru.
2. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
3. Перейдите в раздел Дополнительные настройки > Системные инструменты > Обновление встроенного ПО.
4. Найдите секцию Информация об устройстве. Убедитесь, что версия загруженной прошивки соответствует аппаратной версии устройства.
5. Найдите секцию Локальное обновление. Нажмите Обзор, чтобы найти загруженный файл с прошивкой, и нажмите Обновить.



6. Дождитесь завершения обновления прошивки и перезагрузки роутера — это займёт несколько минут.

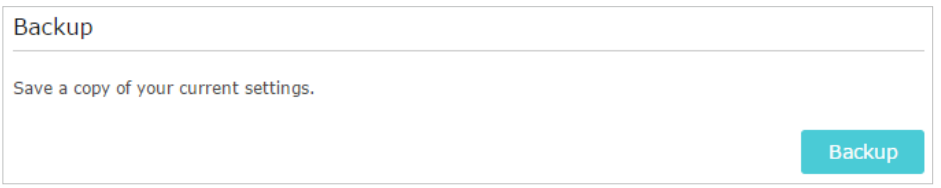
11.4. Создание резервной копии и восстановление настроек

Настройки роутера хранятся в файле на роутере. Файл с настройками можно скопировать на компьютер, чтобы потом при необходимости можно было восстановить настройки роутера. Кроме того, при необходимости можно стереть текущие настройки и восстановить заводские настройки.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Резервная копия и восстановление.

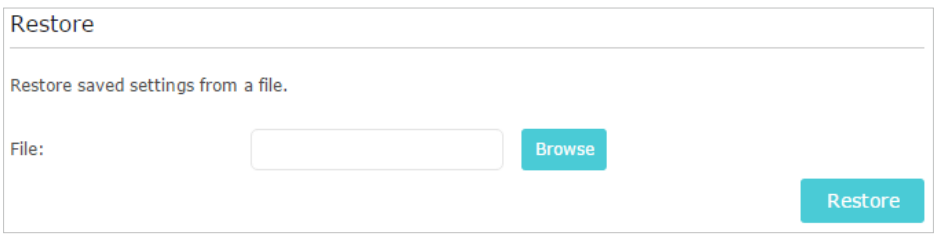
➢ **Создание резервной копии**

Нажмите Резервная копия, чтобы создать копию текущих настроек на компьютер в виде файла с расширением .bin.



➢ **Восстановление настроек**

1. Нажмите Обзор, чтобы найти на компьютере файл с резервной копией настроек, и нажмите Восстановить.

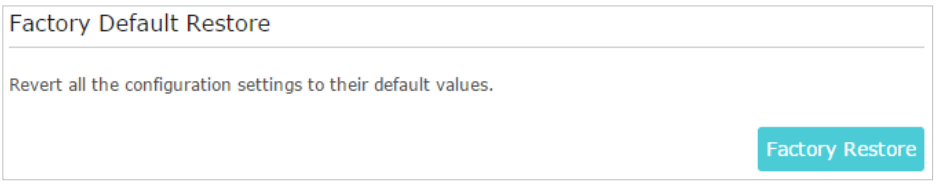


2. Подождите несколько минут, пока завершатся восстановление настроек и перезагрузка роутера.

Примечание: не отключайте роутер во время восстановления настроек.

➢ **Восстановление заводских настроек**

1. Нажмите Восстановить заводские настройки.



2. Подождите несколько минут, пока завершатся восстановление заводских настроек и перезагрузка роутера.

Примечания

- Не отключайте роутер во время восстановления заводских настроек.
- Перед восстановлением заводских настроек настоятельно рекомендуется создать резервную копию текущих настроек роутера.

11.5. Изменение пароля для входа

Пароль для входа в веб-интерфейс управления можно изменить с помощью функции управления учётными записями.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Администратор и найдите секцию Управление учётными записями.

3. Введите старый пароль, затем дважды введите новый (все поля чувствительны к регистру). Нажмите Сохранить.
4. С этого момента используйте для входа новый пароль.

11.6. Локальное управление

Локальное управление позволяет разрешать или запрещать локальным устройствам управлять роутером. По умолчанию роутером могут управлять все подключённые локальные устройства. Также можно выбрать одно устройство для управления роутером и безопасное локальное управление по HTTPS.

Следуйте указаниям ниже, чтобы разрешить локально управлять роутером по HTTPS только выбранному устройству.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Администратор. Найдите секцию Локальное управление.

3. Оставьте по умолчанию значения для параметров Порт для HTTP и Порт для HTTPS. Включите Локальное управление через HTTPS. Введите IP- и MAC-адрес локального устройства, с которого будет выполняться управление роутером.

4. Нажмите Сохранить, чтобы изменения вступили в силу.

Теперь роутером можно управлять как по HTTP (http://tplinkwifi.net), так и по HTTPS (https://tplinkwifi.net).

Примечание: если нужно разрешить управлять роутером всем устройствам, оставьте пустым поле IP-/MAC-адрес.

11.7. Удалённое управление

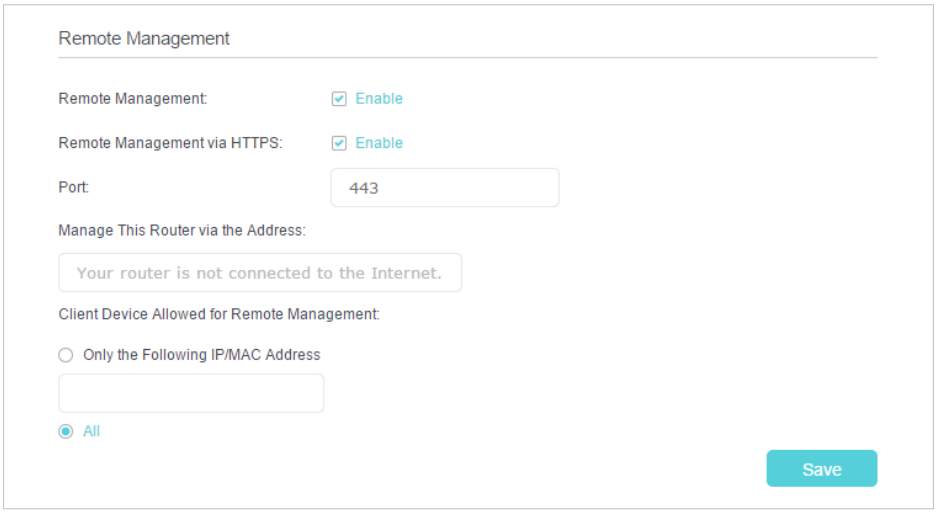
По умолчанию удалённые устройства не могут управлять роутером через интернет. При необходимости можно включить удалённое управление по HTTP и (или) HTTPS (второй вариант безопаснее).

Примечание

Если ваш интернет-провайдер присваивает частные IP-адреса WAN (например, 192.168.x.x или 10.x.x.x), удалённое управление будет недоступно, потому что частные адреса не проходят через интернет.

Выполните указания ниже, чтобы разрешить удалённым устройствам управлять роутером по HTTPS.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Администратор. Найдите секцию Удалённое управление.



3. Включите Удалённое управление и Удалённое управление по HTTPS. Оставьте по умолчанию значение параметра Порт.
4. Укажите клиентское устройство, которому нужно разрешить удалённое управление. Выберите Все, чтобы разрешить всем удалённым устройствам управлять роутером. Если нужно выбрать одно конкретное устройство, выберите Только этот IP- и MAC-адрес и введите IP- и MAC-адрес устройства.
5. Нажмите Сохранить.

Через любое устройство можно выполнить вход в интерфейс роутера по интернету с помощью адреса, отображаемого в поле Управлять роутером через адрес.

Примечания

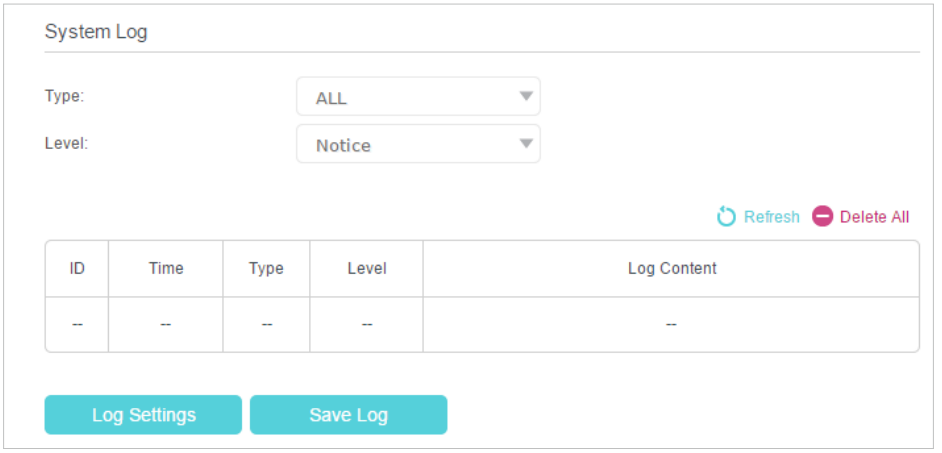
1. Если при удалённом входе в веб-интерфейс управления появилось предупреждение о сертификате, нажмите Доверять (или другой аналогичный вариант). Чтобы это предупреждение больше не появлялось, скачайте и установите сертификат в веб-интерфейсе роутера в разделе Дополнительные настройки > Системные инструменты > Администратор.

2. Обычно у роутеров динамический IP-адрес WAN. Перейдите в раздел Настройка динамического DNS, если нужно войти в веб-интерфейс роутера через доменное имя.

11.8. Системный журнал

Системный журнал помогает лучше понять, что происходит с роутером и где произошёл сбой. Например, при возникновении проблем с работой роутера можно сохранить системный журнал и отправить его сотрудникам службы техподдержки для устранения неполадок.

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Систменый журнал.

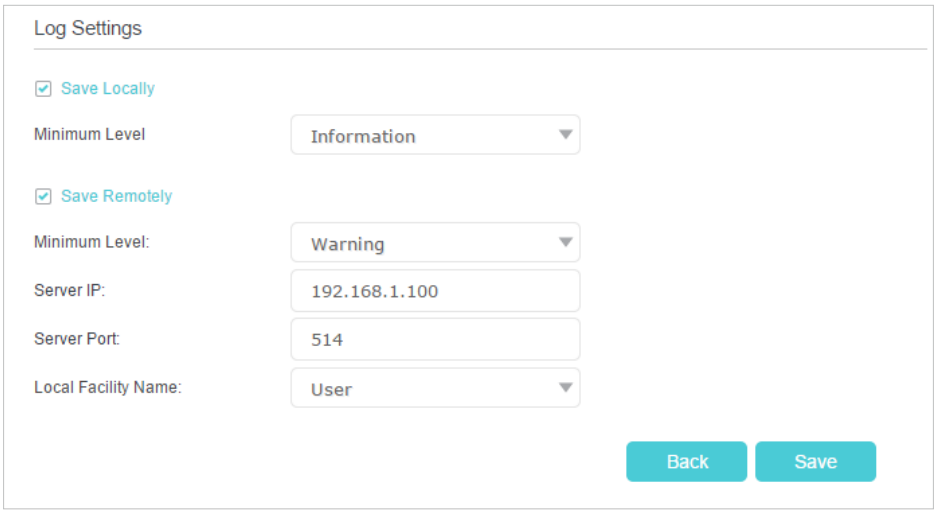


➢ **Просмотр системного журнала**

Можно отфильтровать записи журнала по типу и уровню. Нажмите Обновить, чтобы обновить системный журнал.

➢ **Сохранение системного журнала**

Системный журнал можно сохранить на компьютер или удалённый сервер. Нажмите Сохранить журнал, чтобы сохранить журнал на компьютере в формате txt. Нажмите Настройки журнала чтобы указать путь сохранения.

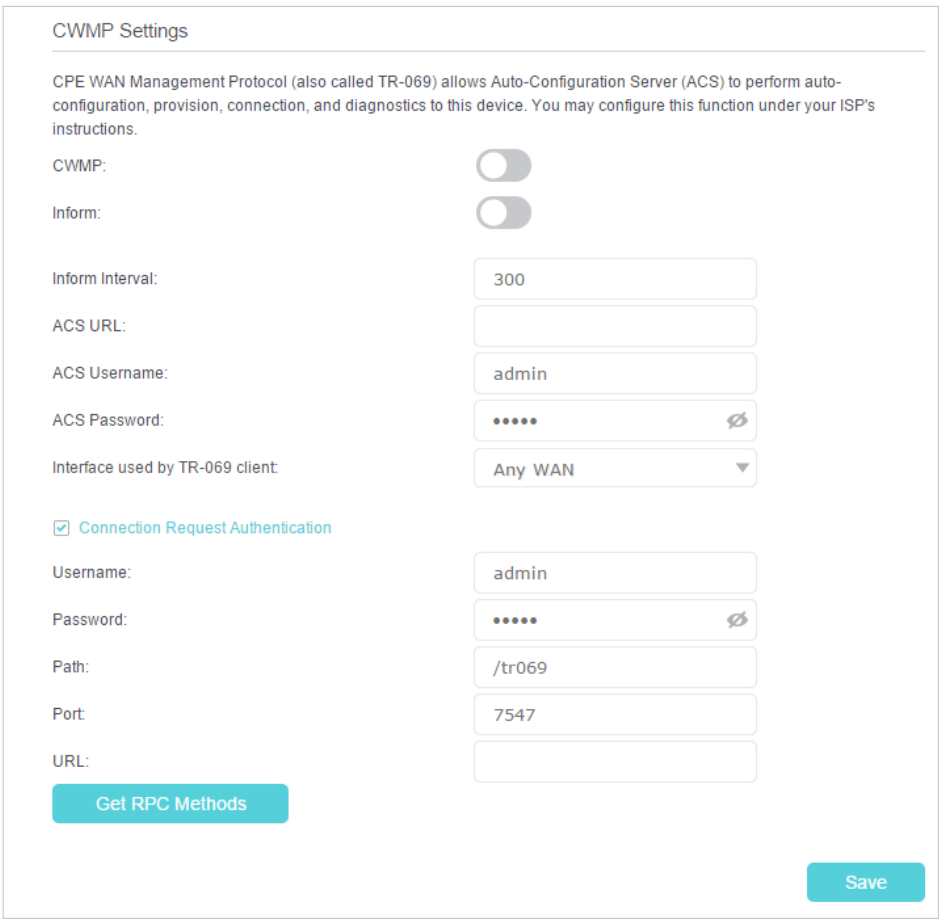


- Сохранить локально: выберите этот пункт, чтобы сохранить системный журнал в локальной памяти роутера, выберите из выпадающего списка минимальный уровень записей системного журнала, которые надо сохранить. Записи журнала будут отображаться в таблице по убыванию в разделе Системный журнал.
- Сохранить удалённо: выберите этот пункт, чтобы отправить системный журнал на удалённый сервер, выберите из выпадающего списка минимальный уровень записей системного журнала, которые надо сохранить, и введите данные удалённого сервера. Если на удалённом сервере есть инструменты для просмотра журналов, то системный журнал можно будет открыть и изучить в реальном времени.

11.9. Настройки CWMP

Роутер поддерживает протокол CWMP (TR-069), позволяющий автоматически собирать данные, выполнять диагностику и настраивать устройства через сервер автоконфигурации (ACS).

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Настройки CWMP.



- CWMP: включение или выключение функции CWMP.
- Уведомление: включение или выключение функции отправки периодических уведомлений на сервер ACS.
- Период уведомления: интервал отправки уведомлений на сервер ACS.
- URL сервера автонастройки: введите предоставленный интернет-провайдером адрес сервера ACS.
- Имя пользователя и пароль сервера автонастройки: введите имя пользователя и пароль для входа на сервер ACS.
- Интерфейс, используемый клиентом TR-069: выберите интерфейс, который будет использоваться клиентом TR-069.

• Аутентификация запроса на соединение: отметьте это окошко, чтобы включить аутентификацию запроса на соединение.

• Имя пользователя и пароль: введите имя пользователя и пароль для авторизации роутера на сервере ACS.

• Путь: укажите путь для подключения к серверу ACS.

• Порт: укажите порт для подключения к серверу ACS.

• URL: укажите URL-адрес для подключения к серверу ACS.

• Простое прохождение UDP через NAT(STUN): отметьте это окошко, чтобы включить STUN для запроса на подключение и установить максимальное и минимальное время жизни (keep alive), адрес сервера и порта.

• Получить метод удалённого вызова процедур: нажмите, чтобы получить способы удалённого вызова процедур.

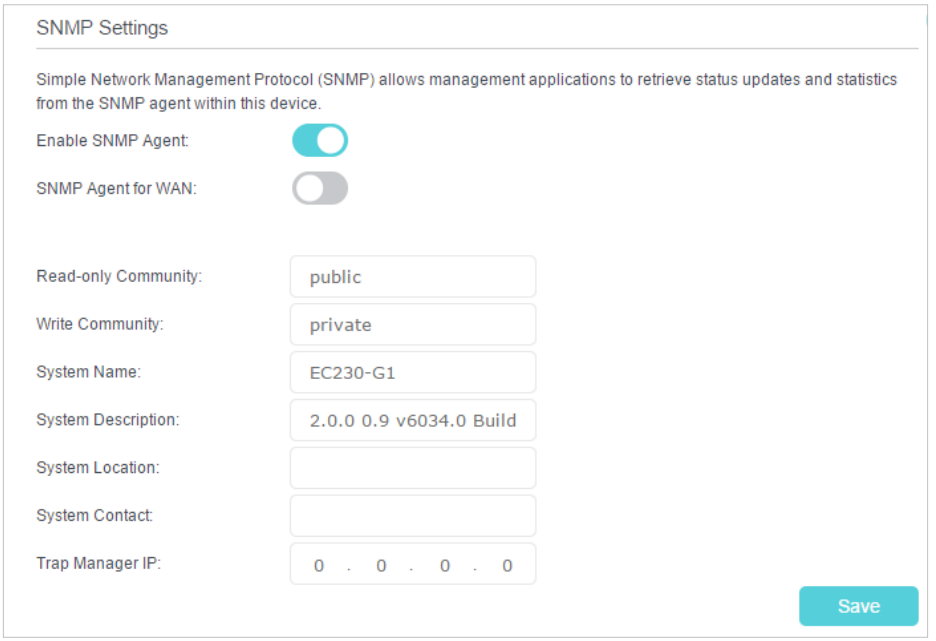
Нажмите Сохранить, чтобы изменения вступили в силу.

11.10. Настройки SNMP

Протокол SNMP широко используется при управлении сетями для мониторинга. SNMP позволяет приложениям управления получать информацию о состоянии и статистику от агента SNMP. Таким образом можно легко искать и изменять информацию в любом узле сети. Также SNMP позволяет быстро выявлять неполадки, проводить диагностику и генерировать отчёты.

Агент SNMP — это приложение роутера, которое получает и обрабатывает SNMP-сообщения, отправляет ответы SNMP-менеджеру и т. д. Таким образом, с помощью SNMP-сообщений можно выполнять мониторинг и управление агентом SNMP.

1. Перейдите http://tplinkwifi.net, и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Настройки SNMP.



• Агент SNMP / Агент SNMP для WAN: встроенный агент SNMP, позволяющий роутеру получать и обрабатывать SNMP-сообщения, отправлять ответы SNMP-менеджеру и т. д.

• Сообщество чтения: название сообщества чтения, защищающего роутер от несанкционированного доступа.

• Сообщество записи: название сообщества записи, защищающего роутер от несанкционированного доступа.

• Имя системы: присвоенное администратором имя управляемого устройства.

• Описание системы: текстовое описание управляемого устройства, включая аппаратную версию устройства.

• Расположение системы: физическое расположение устройства (например: «монтажный шкаф, 3-й этаж»).

• Контакт системы: данные контактного лица, отвечающего за устройство.

• IP-адрес SNMP-менеджера: IP-адрес узла для обработки уведомлений.

Рекомендуется не изменять настройки по умолчанию. Нажмите Сохранить, чтобы изменения вступили в силу.

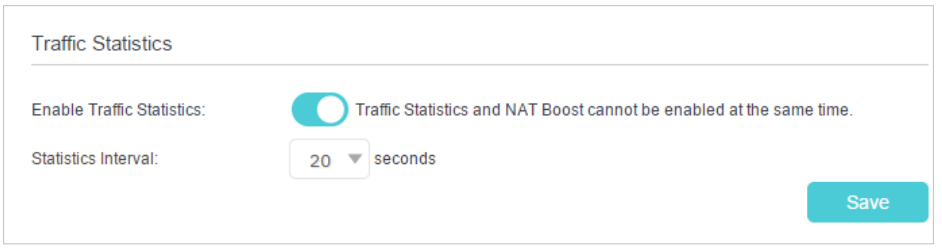
11.11. Мониторинг статистики интернет-трафика

В разделе статистики трафика отображается информация об израсходованном устройствами трафике за последние 10 минут, 24 часа или неделю.

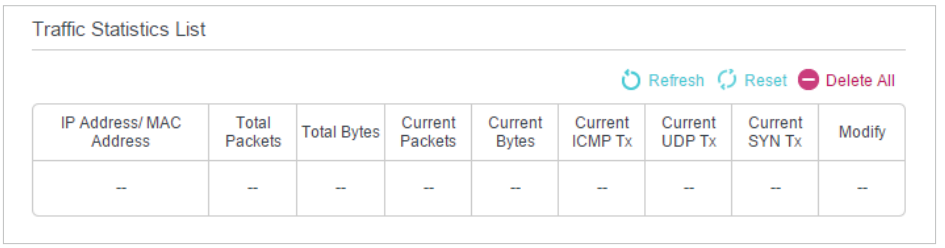
1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.

2. Перейдите в раздел Дополнительные настройки > Системные инструменты > Статистика.

3. Переведите ползунок Включить статистику трафика во включённое положение, чтобы получить возможность просматривать общее число пакетов и байтов, полученных и переданных роутером за указанный Интервал статистики. По умолчанию эта функция отключена.



4. Подробная информация об израсходованном трафике доступна в Таблице статистики трафика.



Часто задаваемые вопросы

B1. Что делать, если я забыл пароль от Wi-Fi сети?

Пароль Wi-Fi сети по умолчанию указан на этикетке роутера. Если же пароль по умолчанию изменялся, то:

1. Подключите роутер к компьютеру по кабелю Ethernet.
2. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
3. Перейдите в раздел Основные настройки > Беспроводной режим, чтобы сбросить пароль Wi-Fi сети.

B2. Что делать, если я забыл пароль от веб-интерфейса?

- Нажмите и удерживайте кнопку Reset не менее пяти секунд, пока все индикаторы роутера на мгновение не загорятся, чтобы восстановить заводские настройки, затем перейдите на http://tplinkwifi.net и создайте новый пароль.

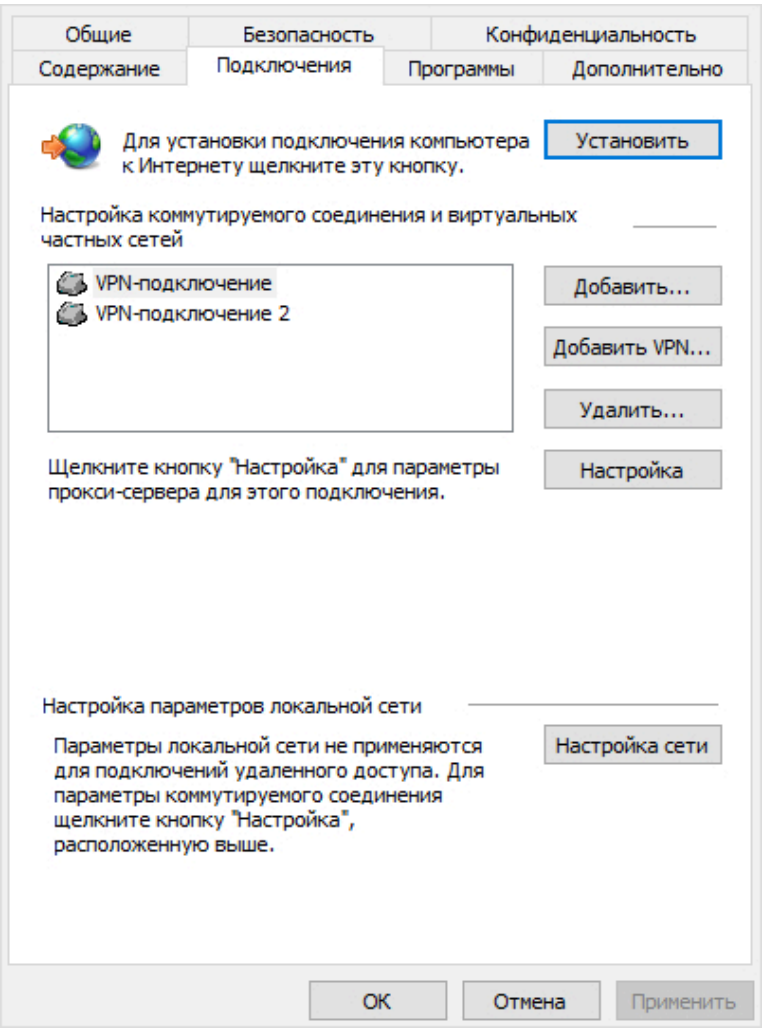
Примечание

- Не забудьте записать новый пароль, чтобы не забыть его. Для доступа в интернет после восстановления заводских настроек роутер надо будет настроить заново.

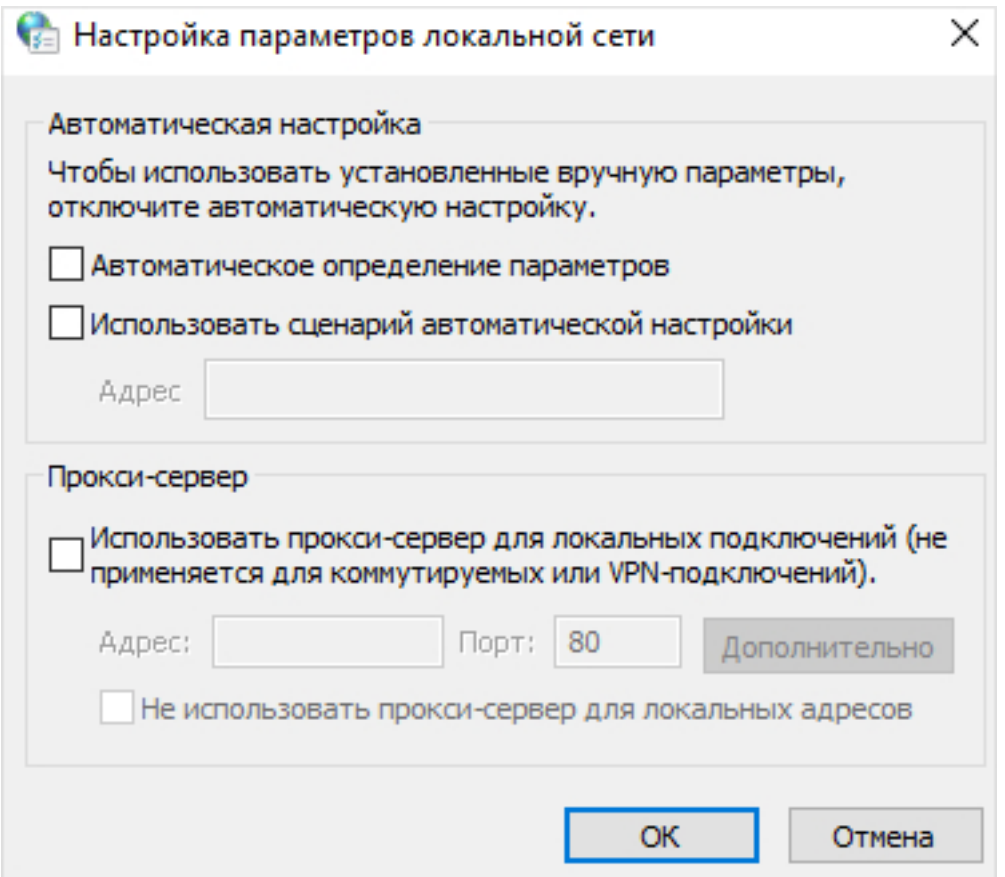
B3. Что делать, если не удаётся войти в веб-интерфейс?

- Убедитесь, что роутер правильно подключён к компьютеру и что горят соответствующие индикаторы.
- Убедитесь, что компьютер автоматически получает IP-адрес и адрес DNS-сервера.
- Убедитесь, что вы верно ввели http://tplinkwifi.net или http://192.168.0.1.
- Проверьте настройки компьютера:

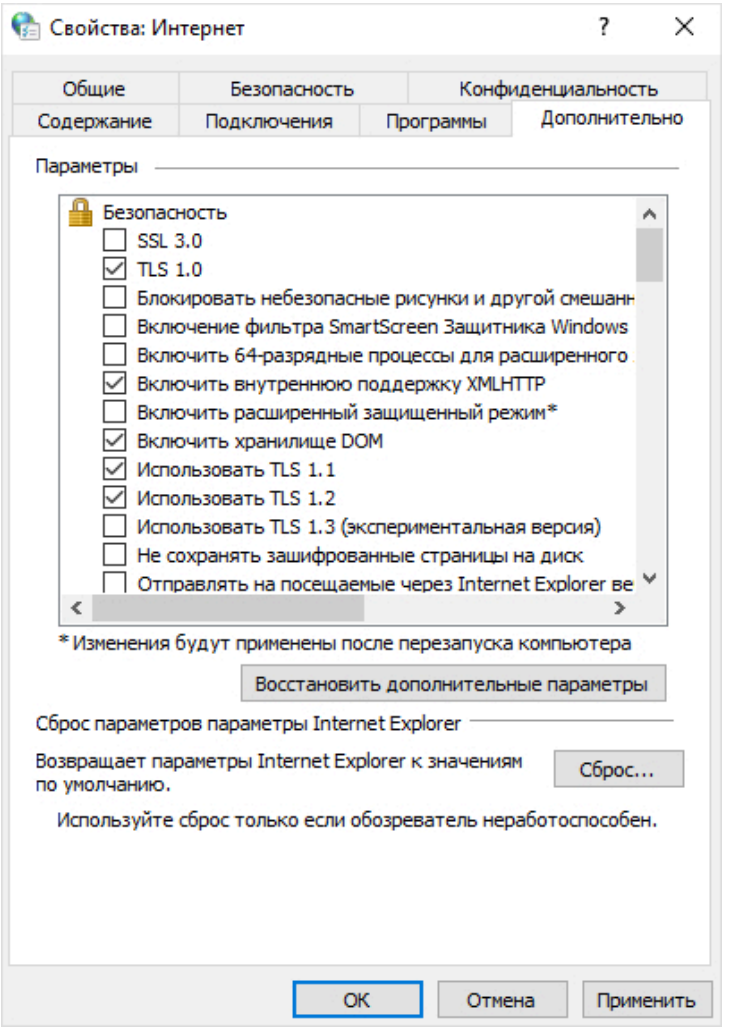
  1) Перейдите в раздел Пуск > Панель управления > Сеть и Интернет и нажмите Просмотр состояние сети и задач.
  2) Нажмите Свойства браузера в нижнем левом углу.
  3) Перейдите на вкладку Подключения.



4) Нажмите Настройка сети, уберите галочки из всех окошек и нажмите OK.



5) Перейдите на вкладку Дополнительно > Восстановить дополнительные параметры, нажмите OK, чтобы сохранить изменения.



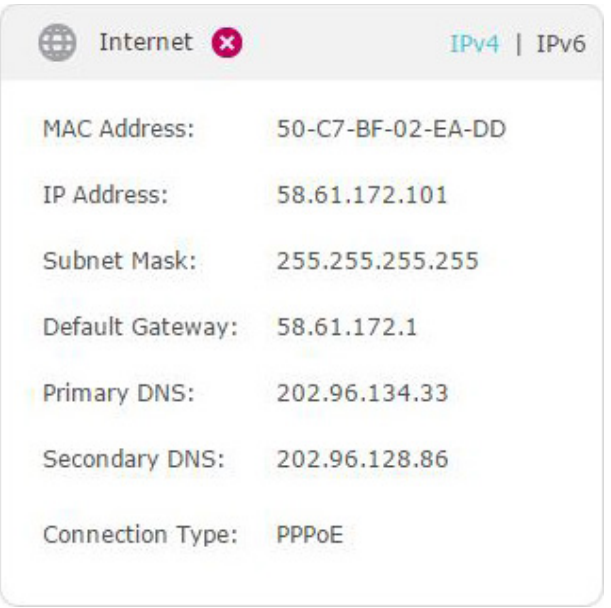
- Попробуйте выполнить вход, используя другой браузер или компьютер.
- Восстановите заводские настройки роутера и повторите попытку. Если войти по-прежнему не получается, свяжитесь с нашей службой техподдержки.

Примечание: для доступа в интернет после восстановления заводских настроек роутер надо будет настроить заново.

B4. Что делать, если после завершения настройки нет доступа в интернет?

1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. Перейдите в раздел Дополнительные настройки > Состояние, чтобы проверить состояние подключения к интернету.

Если IP-адрес действительный (как на снимке экрана ниже), выполните указания ниже.

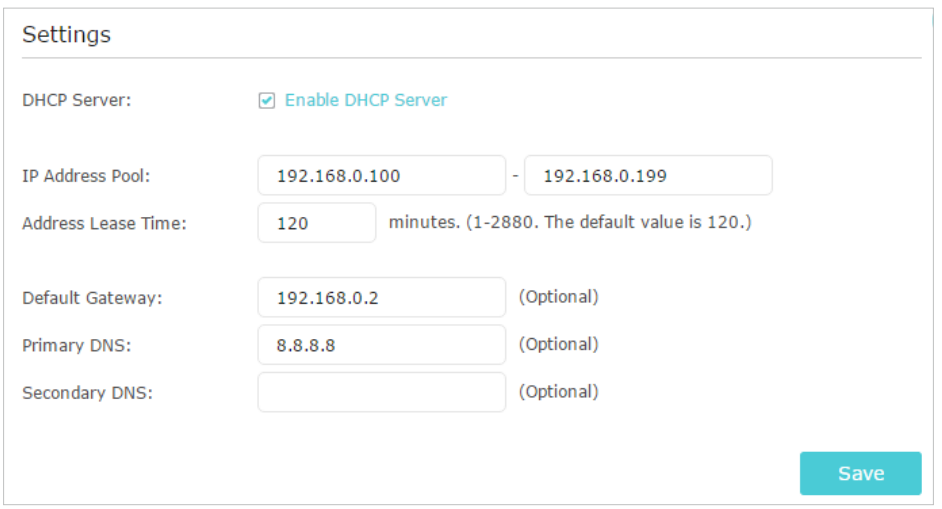


- Возможно, компьютер не распознаёт адреса сервера DNS. Попробуйте настроить сервер DNS вручную.

  1) Перейдите в раздел Дополнительные настройки > Сеть > DHCP-сервер.

  2) Введите 8.8.8.8 в поле Предпочитаемый DNS-сервер и нажмите Сохранить.

  Совет: 8.8.8.8 — это безопасный публичный DNS-сервер от Google.



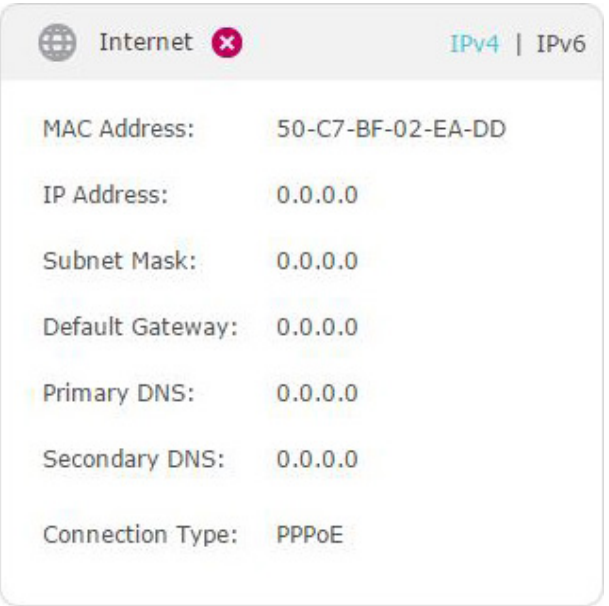
- Перезагрузите модем (если он есть) и роутер.

  1) Отключите на одну минуту модем (если он есть) и роутер.
  2) Включите модем и дождитесь, когда загорится индикатор подключения к интернету.
  3) Включите роутер и подождите пару минут.
  4) Проверьте интернет-подключение.

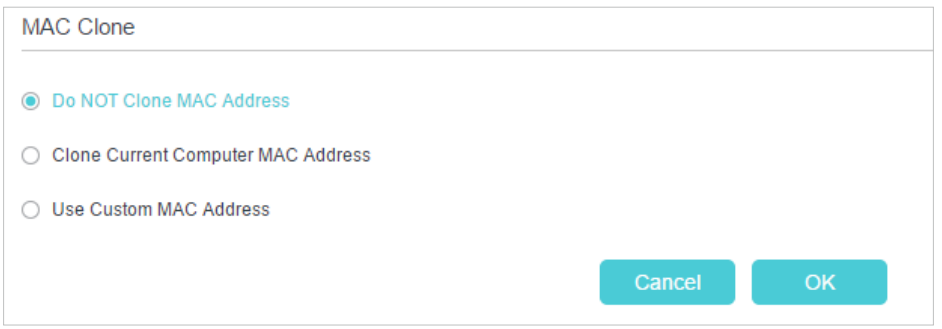
- Восстановите заводские настройки роутера и настройте его заново.

- Обновите прошивку роутера.
- Проверьте настройки TCP/IP устройства, на котором не работает интернет, если все остальные устройства могут подключиться к интернету через роутер.

Если у вас IP-адрес 0.0.0.0 как на изображении ниже, попробуйте выполнить следующие указания:



- Убедитесь в правильности физического подключения между модемом и роутером.
- Выполните клонирование MAC-адреса компьютера.
    1) Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
    2) Перейдите в раздел Дополнительные настройки > Сеть > Интернет и найдите секцию Клонирование MAC-адреса.
    3) Выберите нужную опцию (при выборе опции Использовать заданный MAC-адрес введите нужный адрес) и нажмите OK.



Советы

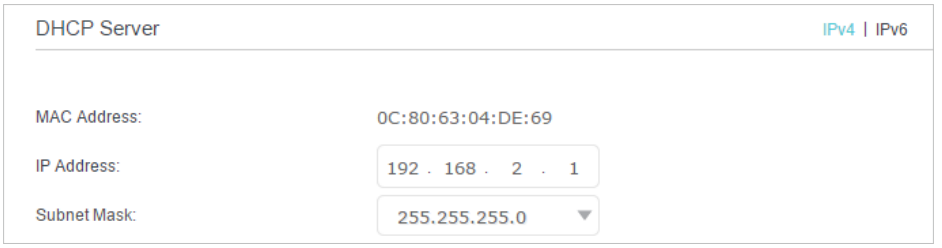
- Некоторые интернет-провайдеры регистрируют MAC-адреса компьютеров своих пользователей при первом интернет-подключении через кабельный модем. При добавлении к сети роутера MAC-адрес изменится, поэтому текущий MAC-адрес необходимо скопировать для роутера.
- При подключении по Wi-Fi и по кабелю MAC-адреса компьютера будут разными.

- Изменение IP-адреса LAN роутера

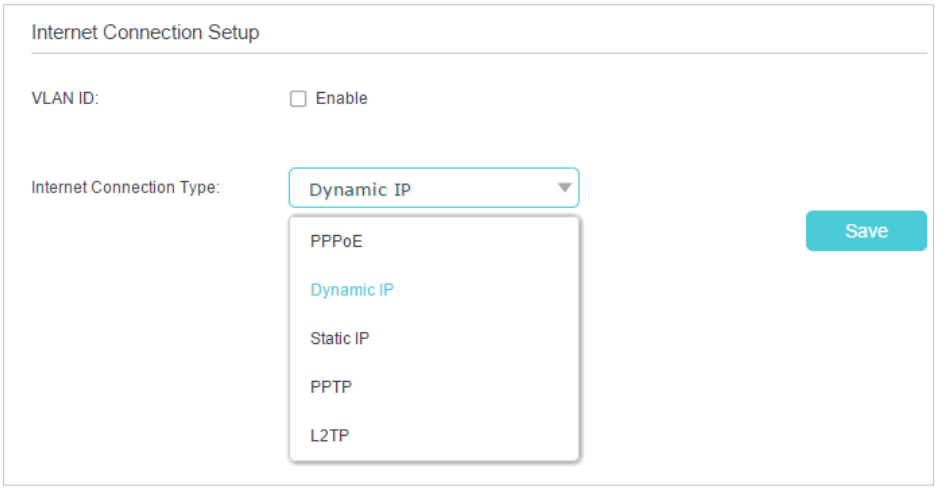
  Примечание

  В большинстве роутеров в качестве IP-адреса LAN по умолчанию используется 192.168.0.1/192.168.1.1, что может создавать конфликт с диапазоном IP-адресов текущего модема или роутера. В таких случаях роутер не может взаимодействовать с модемом и, соответственно, нет доступа в интернет. Для решения этой проблемы необходимо изменить IP-адрес LAN роутера, например, на 192.168.2.1.

  1) Перейдите на http://tplinkwifi.net, и войдите, используя пароль, который вы создавали для роутера.
  2) Перейдите в раздел Дополнительные настройки > Сеть > LAN.
  3) Измените IP-адрес LAN в соответствии с приведённым ниже изображением. В данном примере используется адрес 192.168.2.1.
  4) Нажмите Сохранить.



- Перезагрузите модем (если он есть) и роутер.
  1) Отключите на одну минуту модем (если он есть) и роутер.
  2) Включите модем и дождитесь, когда загорится индикатор подключения к интернету.
  3) Включите роутер и подождите пару минут.
  4) Проверьте интернет-подключение.
- Проверьте тип интернет-подключения.
  1) Уточните у интернет-провайдера свой тип интернет-подключения.
  2) Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
  3) Перейдите в раздел Основные настройки > Интернет.
  4) Выберите свой Тип подключения к Интернет и укажите другие параметры.
  5) Нажмите Сохранить.



6) Снова перезагрузите модем (если он есть) и роутер.

- Обновите прошивку роутера.

Если ничто из указанного выше не помогло, свяжитесь с нашей службой техподдержки.

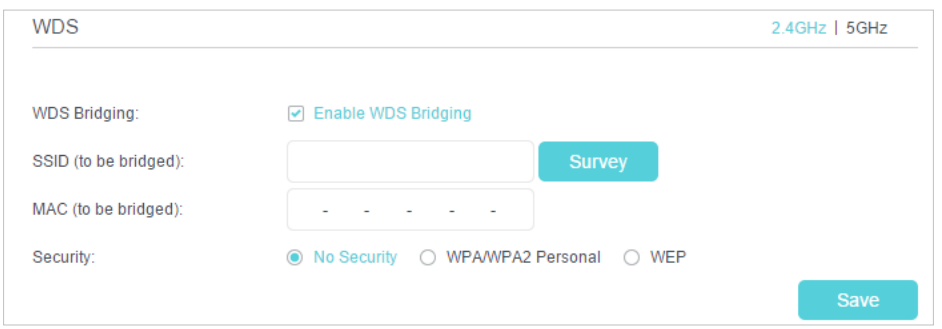
B5. Как использовать мост WDS для расширения Wi-Fi сети?

Если зоны Wi-Fi покрытия основного роутера недостаточно, мост WDS поможет решить эту проблему.

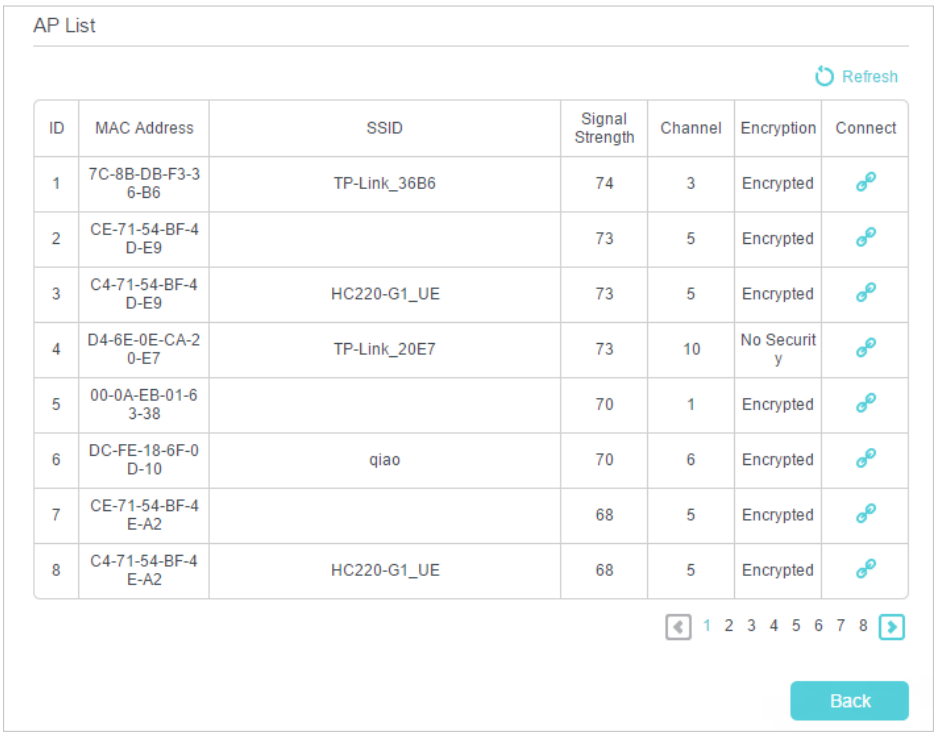
Примечания

- Функция мост WDS настраивается на роутере, который будет расширять Wi-Fi сеть.
- Функция мост WDS может работать на диапазонах 2,4 ГГц и 5 ГГц. В примере используется диапазон 2,4 ГГц.

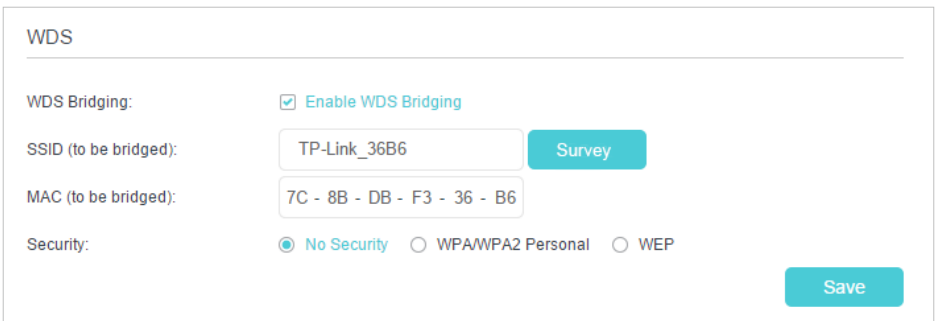
1. Перейдите на http://tplinkwifi.net и войдите, используя пароль, который вы создавали для роутера.
2. IP-адрес LAN дополнительного роутера должен быть в одной подсети с корневым роутером (255.255.255.0). Например, если IP-адрес корневого роутера — 192.168.0.1, то IP-адрес дополнительного роутера может быть в диапазоне от 192.168.0.2 до 192.168.0.254.
3. Перейдите в раздел Дополнительные настройки > Беспроводной режим > Дополнительные настройки. Найдите секцию WDS и отметьте окошко Включить мост WDS.



4. Нажмите Сканировать, чтобы найти все доступные устройства и выбрать сеть.



5. Нажмите иконку подключения — поля SSID, MAC-адрес и Защита заполнятся автоматически.



6. Нажмите Сохранить, чтобы изменения вступили в силу.

7. Перейдите в раздел Дополнительные настройки > Сеть > LAN и отключите параметр DHCP.

Готово! Wi-Fi сеть корневого роутера расширена. Для подключения к расширенной сети используйте имя (SSID) и пароль Wi-Fi сети корневого роутера.

Примечания

- Имя (SSID) и пароль Wi-Fi сети дополнительного роутера могут отличаться от таковых корневого роутера. Изменить SSID и пароль можно в разделе Основные настройки > Беспроводной режим.
- Мост также можно создать вручную: введите имя сети (SSID) и MAC-адрес сети, для которой создаётся мост. Выберите тип защиты и введите сопутствующие параметры, которые должны совпадать с таковыми сети, для которой создаётся мост.

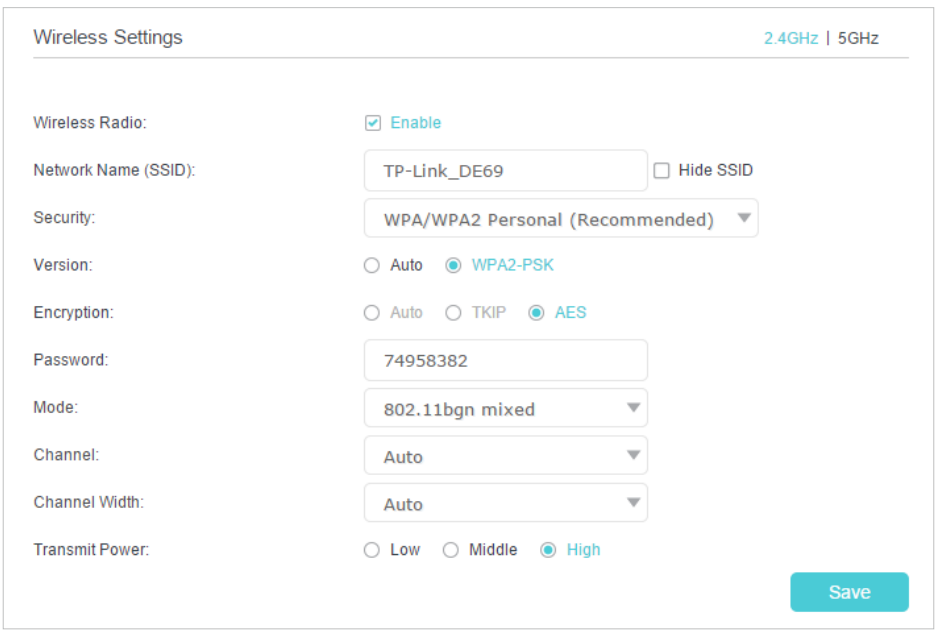
В6. Что делать, если не удаётся найти Wi-Fi сеть или подключиться к ней?

Если не удаётся найти никакую Wi-Fi сеть

Убедитесь, что на клиентском устройстве включён Wi-Fi, и что успешно установлены соответствующие драйвера. Например, если на Windows 7 и более новых версиях Windows появляется сообщение о том, что нет доступных подключений, обычно это связано с тем, что Wi-Fi отключён или что-то мешает его работе. Нажмите Устранить неполадку (или другое аналогичное меню), и вполне возможно, Windows самостоятельно найдёт и устранит неполадку.

Если удаётся найти любую Wi-Fi сеть, кроме своей

- Убедитесь, что горит индикатор WLAN роутера и модема (если он есть).
- Убедитесь, что клиентское устройство находится в радиусе действия роутера, и разместите его ближе к роутеру, если оно слишком далеко.
- Перейдите в раздел Дополнительные настройки > Беспроводной режим > Настройки беспроводного режима и проверьте параметры Wi-Fi. Убедитесь, что имя (SSID) и пароль Wi-Fi сети не скрыты.



Если удаётся найти Wi-Fi сеть, но не удаётся подключиться к ней

- **Проблема с аутентификацией**

  1) Иногда при первом подключении к Wi-Fi сети запрашивается PIN-код (не путать с паролем Wi-Fi и ключом безопасности сети). Обычно PIN-код можно найти только на этикетке роутера.

2) Если не удаётся найти PIN-код или если при его вводе появляется ошибка, можно выбрать опцию подключения с помощью ключа безопсности сети или пароля Wi-Fi.

3) Если по-прежнему появляется ошибка о неверном пароле, перепроверьте пароль роутера.

Примечание: пароль Wi-Fi и ключ безопасности сети чувствительны к регистру.

- **Windows не может подключиться к сети / Подключение к сети выполняется дольше обычного:**
  - Проверьте качество Wi-Fi сигнала — если мощность сигнала низкая, разместите роутер ближе и повторите попытку.
  - Измените Wi-Fi канал роутера на 1-й, 6-й или 11-й, чтобы уменьшить помехи от других сетей.
  - Переустановите или обновите на компьютере драйвер Wi-Fi адаптера.

АВТОРСКИЕ ПРАВА И ТОВАРНЫЕ ЗНАКИ

tp-link является зарегистрированным товарным знаком TP-Link Technologies Co., Ltd. Прочие бренды и наименования продуктов являются товарными знаками или зарегистрированными знаками соответствующих правообладателей.

Заявление о соответствии требованиям Федерального агентства США по связи (FCC)

Продукт: AC1350 Двухдиапазонный гигабитный Wi-Fi роутер

Модель: Archer C5 Pro

Название	Модель
АДАПТЕР ПИТАНИЯ	AMS159A-1201000FU

Ответственная сторона

Компания TP-Link USA Corporation, осуществляющая деятельность под наименованием TP-Link North America, Inc.

Адрес: 145 South State College Blvd. Suite 400, Brea, CA 92821

Сайт: http://www.tp-link.com/us/

Телефон: +1 626 333 0234

Факс: +1 909 527 6803

Электронная почта: sales.usa@tp-link.com

В результате проверки данного оборудования показано его соответствие ограничениям для цифрового устройства класса B согласно спецификациям части 15 правил Федерального агентства США по связи (FCC). Данные ограничения предназначены для обеспечения надлежащей защиты от вредных помех в жилых помещениях. Данное оборудование генерирует, использует и может излучать радиочастотную энергию. Неправильная установка или нарушение инструкций по использованию может привести к возникновению помех при приёме радиосигнала. Однако нет гарантии, что помехи не возникнут в определённом месте установки. Если данное оборудование производит помехи для приёма теле- или радиосигнала (чтобы точно определить это, выключите и включите данное оборудование), то пользователь должен попытаться устранить помехи одним или несколькими описанными ниже методами.

- Перенаправить или переместить принимающую антенну
- Увеличить расстояние между приёмником и данным оборудованием.
- Подключить данное оборудование к розетке или контуру электросети, к которым не подключён приёмник.
- Обратиться за помощью к производителю приёмника или к специалисту по телерадиотехнике.

Данное устройство соответствует требованиям части 15 правил Федерального агентства США по связи (FCC). Использование устройства определяется следующими двумя условиями: (1) это устройство не является источником вредных радиопомех и (2) это устройство должно выдерживать все полученные радиопомехи, в том числе те, которые могут привести к сбоям в его работе.

Изменения или модификации данного продукта, не одобренные ответственной стороной, могут привести к нарушению правил электромагнитной совместимости и совместимости с беспроводными сетями, из-за чего вам может быть запрещено пользоваться данным продуктом.

Воздействие радиочастотной энергии

Излучаемая выходная мощность устройства не превышает ограничений Федерального агентства США по связи (FCC) и Министерства промышленности Канады (IC) по радиочастотному воздействию. При эксплуатации устройство должно находиться на расстоянии не менее 20 см от тела человека.

Устройство разрешено использовать только в помещении.

Маркировка CE

CE

Это цифровое устройство класса B. В домашних условиях данное устройство может создавать радиопомехи — в этом случае пользователю может понадобиться принять соответствующие меры.

ДИАПАЗОН РАБОЧИХ ЧАСТОТ

2400–2483,5 МГц (20 дБм)

5150–5250 МГц (23 дБм)

Декларация о соответствии ЕС

Настоящим компания TP-Link заявляет, что устройство соответствует обязательным требованиям и прочим соответствующим положениям директив 2014/53/EU, 2009/125/EC и 2011/65/EU.

Оригинал декларации о соответствии ЕС можно найти на http://tp-link.com/ru/ce

Воздействие радиочастотной энергии

Данное устройство соответствует требованиям ЕС (2014/53/EU Статья 3.1a) по ограничению воздействия электромагнитных полей на население в целях защиты здоровья.

При эксплуатации устройство должно находиться на расстоянии не менее 20 см от тела человека.

Устройство разрешено использовать только в помещении.

Декларация о соответствии требованиям (Канада)

Данное устройство соответствует стандартам спецификации радиооборудования Канады, не требующим лицензирования. Эксплуатация возможна при соблюдении следующих двух условий:

1. Устройство не должно создавать вредных помех.
2. Устройство должно принимать любые помехи, включая помехи, которые могут приводить к сбоям в работе устройства.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. l'appareil ne doit pas produire de brouillage;
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement

Внимание!

1. Устройства диапазона 5150–5350 МГц следует использовать только в помещениях, чтобы снизить возможный уровень вредных помех в мобильных спутниковых системах, работающих на том же канале.

2. Для устройств со съёмными антеннами: максимально допустимое усиление антенн в диапазоне 5725–5850 МГц должно быть в рамках ограничений ЭИИМ.

Высокомощные радары являются основными пользователями (имеют приоритет) диапазонов 5250–5350 МГц и 5650–5850 МГц; эти радары могут становиться причиной помех и (или) повреждений устройств LE-LAN.

Avertissement:

1. Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
2. Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Воздействие радиочастотной энергии

Излучаемая выходная мощность устройства не превышает ограничений Министерства промышленности Канады (IC) по радиочастотному воздействию. При эксплуатации устройство должно находиться на расстоянии не менее 20 см от тела человека.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Заявление для Министерства промышленности Канады

CAN ICES-3 (B)/NMB-3(B)

Заявление для Южной Кореи

당해 무선설비는 운용중 전파혼신 가능성이 있음.

Уведомление NCC

注意！

依據 低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性或功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通行；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信規定作業之無線電信。低功率射頻電機需忍受合法通信或工業、科學以及醫療用電波輻射性電機設備之干擾。

Уведомление BSMI (только для Тайваня)

安全諮詢及注意事項

- 請使用原裝電源供應器或只能按照本產品注明的電源類型使用本產品。
- 清潔本產品之前請先拔掉電源線。請勿使用液體、噴霧清潔劑或濕布進行清潔。
- 注意防潮，請勿將水或其他液體潑灑到本產品上。
- 插槽與開口供通風使用，以確保本產品的操作可靠並防止過熱，請勿堵塞或覆蓋開口。
- 請勿將本產品置放於靠近熱源的地方。除非有正常的通風，否則不可放在密閉位置中。
- 請不要私自打開機殼，不要嘗試自行維修本產品，請由授權的專業人士進行此項工作。

限用物質含有情況標示聲明書

產品元件名稱	限用物質及其化學符號					
	鉛 Pb	鎘 Cd	汞 Hg	六價鉻 CrVI	多溴聯苯 PBB	多溴二苯醚 PBDE
PCB	○	○	○	○	○	○
外殼	○	○	○	○	○	○
電源適配器	-	○	○	○	○	○

備考1. 超出0.1 wt %” 及 “超出0.01 wt %” 系指限用物質之百分比含量超出百分比含量基準值。

備考2. “○”系指該項限用物質之百分比含量未超出百分比含量基準值。

備考3. “ - “ 系指該項限用物質為排除項目。

Продукт сертифіковано згідно с правилами системи УкрСЕПРО на відповідність вимогам нормативних документів та вимогам, що передбачені чинними законодавчими актами України.

EAC

Руководство по безопасному использованию

- Избегайте контакта устройства с водой и огнём, а также использования устройства в условиях высокой влажности и высоких температур.
- Не пытайтесь самостоятельно разбирать, ремонтировать или модифицировать устройство.
- Не используйте повреждённый USB-кабель для зарядки устройства.
- Используйте только рекомендуемые зарядные устройства.
- Не используйте устройство там, где запрещено использование Wi-Fi устройств.
- Адаптер должен быть установлен в легкодоступном месте недалеко от оборудования.
- Используйте только адаптеры питания от производителя в оригинальной упаковке. Если у вас есть вопросы, обязательно свяжитесь с нами.

Ознакомьтесь с руководством по безопасности и следуйте ему при использовании устройства. Мы не можем гарантировать отсутствие несчастных случаев или ущерба при неправильном использовании устройства. Бережно обращайтесь с данным продуктом и используйте его на свой риск.

Устройство можно использовать в следующих европейских странах:

AT	BE	BG	CH	CY	CZ	DE	DK
EE	EL	ES	FI	FR	HR	HU	IE
IS	IT	LI	LT	LU	LV	MT	NL
NO	PL	PT	RO	SE	SI	SK	UK

Расшифровка символов на товарной этикетке

Символ	Расшифровка
⎓	Постоянный ток
	Использование только в помещении
	ПЕРЕРАБОТКА Данный продукт содержит символ раздельного сбора отходов электрического и электронного оборудования (WEEE). Это означает, что данный продукт должен быть переработан или разобран согласно европейской директиве 2012/19/EU для минимизации воздействия на окружающую среду. При покупке нового электрического или электронного оборудования пользователь вправе отдать данный продукт соответствующей перерабатывающей организации или ритейлеру.