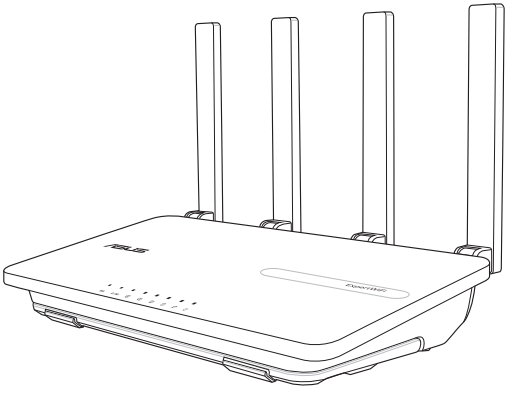
Руководство пользователя

ASUS ExpertWiFi EBR63

Двухдиапазонный беспроводной роутер Wireless-AX3000

Модель: EBR63



IN SEARCH OF INCREDIBLE

R22960
Первое издание
Декабрь 2023

Оглавление

Оглавление

Оглавление

1 Знакомство с устройством

1.1 Приветствие!

Благодарим вас за приобретение беспроводного роутера!

Ультратонкий и стильный роутер поддерживает частоты 2,4ГГц и 5ГГц, для обеспечения высокой скорости передачи данных, SMB , UPnP AV, FTP сервера для круглосуточного доступа к файлам, одновременную работу до 300,000 сессий; а также технологию ASUS Green Network, обеспечивающую энергосбережение до 70% энергосбережение до 70%.

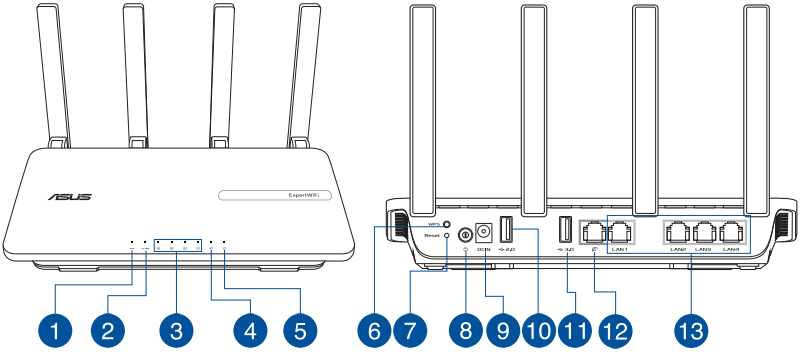
1.2 Комплект поставки

- ☑ Роутер ExpertWiFi EBR63
- ☑ Блок питания
- ☑ Гарантийный талон
- ☑ Сетевой кабель (RJ-45)
- ☑ Краткое руководство

ПРИМЕЧАНИЯ:

- Если какие-либо элементы комплекта поставки отсутствуют или повреждены, обратитесь в службу техподдержки ASUS. Номера телефонов горячей линии службы технической поддержки смотрите в конце этого руководства.
- Сохраните оригинальную упаковку на случай, если в будущем потребуется гарантийное обслуживание, например ремонт или замена.

1.3 Данный беспроводной роутер



1 **Индикатор 5 ГГц**
Выключен: Нет сигнала 5 ГГц.
Включен: Беспроводная система готова.
Мигает: Передача данных через беспроводное подключение.

2 **Индикатор 2,4 ГГц**
Выключен: Нет сигнала 2,4 ГГц.
Включен: Беспроводная система готова.
Мигает: Передача данных через беспроводное подключение.

3 **Индикаторы портов LAN 1 ~ 4**
Выключен: Нет питания или физического соединения.
Включен: Имеется физическое соединение с локальной сетью (LAN).

4 **Индикатор WAN (Internet)**
Красный: Нет IP или физического соединения.
Включен: Имеется физическое соединение с глобальной сетью (WAN).

5 **Индикатор питания**
Выключен: Нет питания.
Включен: устройство готово.
Медленно мигает: Режим восстановления

6 **Кнопка WPS**
Эта кнопка запускает мастер WPS.

7 **Кнопка сброса**
Эта кнопка предназначена для сброса системы к настройкам по умолчанию.

8 **Кнопка питания**
Нажмите эту кнопку включения/отключения системы.

9	**Разъем питания (DCIN)** Подключение блока питания.
10	**Разъем USB 2.0** Подключение устройств USB 2.0, например жесткого диска USB или USB флэш-диска.
11	**Разъем USB 3.2 Gen 1x1** Подключение устройств USB 3.2 Gen 1x1, например жесткого диска USB или USB флэш-диска.
12	**Порт WAN (Internet)** Подключение сетевого кабеля для установки WAN подключения.
13	**Порты LAN 1 ~ 4** Подключение сетевых устройств.

ПРИМЕЧАНИЯ:

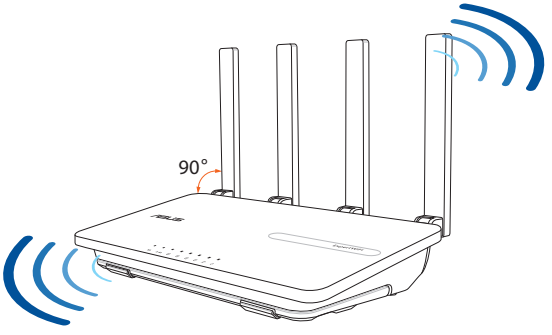
- Используйте только блок питания, поставляемый с устройством. При использовании других блоков питания устройство может быть повреждено.
- **Спецификация:**

Блок питания	Выходное напряжение 12 В с максимальным током 2 А		
Температура при работе	0~40°C	при хранении	0~70°C
Влажность при работе	50~90%	при хранении	20~90%

1.4 Размещение роутера

Для улучшения беспроводной связи между беспроводным роутером и сетевыми устройствами, подключенными к нему, выполните следующее:

- Поместите беспроводной роутер в центре беспроводной сети для максимального покрытия.
- Поместите устройство подальше от металлических преград и прямых солнечных лучей.
- Для предотвращения помех поместите устройство подальше от устройств стандарта 802.11 или устройств, работающих на частоте 2.4 или 5ГГц, устройств Bluetooth, беспроводных телефонов, трансформаторов, мощных двигателей, флюоресцентных ламп, микроволновых лучей, холодильников и другого промышленного оборудования.
- Используйте последнюю прошивку. Для получения подробной информации о наличии свежей прошивки посетите сайт ASUS http://www.asus.com.
- Для обеспечения оптимального сигнала, расположите четыре съемные антенны, как показано на рисунке ниже.



1.5 Системные требования

Для настройки сети необходим компьютер, соответствующий следующим требованиям:

- Сетевой порт RJ-45 (10Base-T/100Base-TX/1000BaseTX)
- Беспроводной интерфейс IEEE 802.11a/b/g/n/ac/ax
- Установленный протокол TCP/IP
- Браузер, например Internet Explorer, Firefox, Safari или Google Chrome

---

ПРИМЕЧАНИЯ:

- Если компьютер не имеет встроенных беспроводных сетевых адаптеров, для подключения к сети вы можете установить в компьютер беспроводной адаптер IEEE 802.11a/b/g/n/ac/ax.
- Беспроводной роутер одновременно поддерживает работу на частотах 2,4 ГГц и 5 ГГц. Это позволяет выполнять интернет-серфинг и работать с электронной почтой, используя частоту 2,4 ГГц и одновременно смотреть потоковое видео высокой четкости, или слушать музыку, используя диапазон 5 ГГц.
- Некоторые устройства IEEE 802.11n, которые вы хотите подключить к сети могут не поддерживать частоту 5 ГГц. Обратитесь к спецификации устройства.
- Длина Ethernet кабеля, используемого для подключения сетевых устройств не должна превышать 100 метров.

1.6 Настройка роутера

ОСТОРОЖНО!

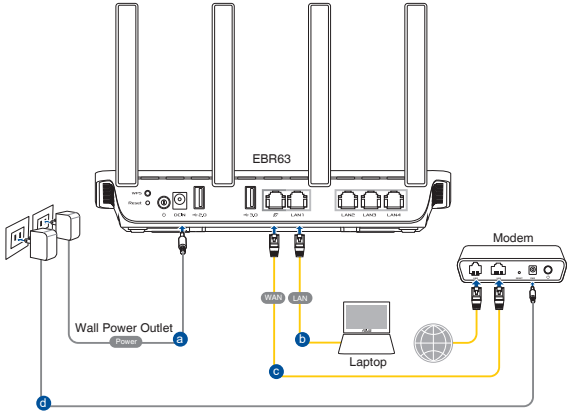
- Во избежание возможных помех с беспроводной связью, при настройке беспроводного роутера используйте проводное соединение.
- Перед настройкой беспроводного роутера, выполните следующие действия:
  - При замене существующего роутера, отключите его от сети.
  - Отключите провода/кабели от модема. Если на модеме есть аккумулятор, отключите его.
  - Перезагрузите модем и компьютер (рекомендуется).

ВНИМАНИЕ!

- Шнур питания должен быть подключен к розетке с заземлением. Подключайте устройство к ближайшей, легкодоступной розетке.
- Если устройство неисправно, не пытайтесь исправить его самостоятельно. Эти ограничения рассчитаны на обеспечение защиты в разумных пределах от вредоносных воздействий при установке в жилом помещении.
- Не пользуйтесь поврежденными сетевыми шнурами, аксессуарами и периферийными устройствами.
- Не устанавливайте это оборудование на высоту более 2 метров.
- Рекомендуется использовать продукт при температуре от 0°C до 40°C.

1.6.1 Проводное подключение

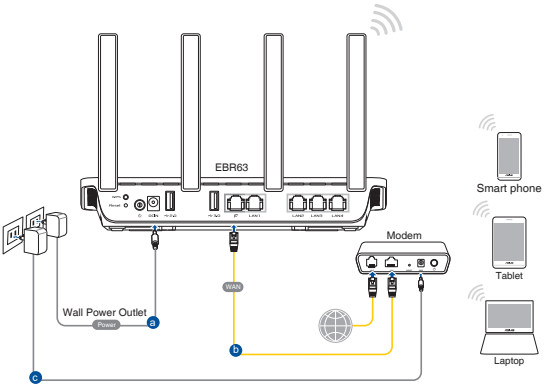
ПРИМЕЧАНИЕ:Для проводного подключения можно использовать любой (прямой или перекрестный) кабель.



Для настройки беспроводного роутера через проводное подключение:

1. Подключите блок питания роутера к разъему DCIN и к розетке.
2. С помощью поставляемого сетевого кабеля подключите компьютер к LAN порту роутера.
3 С помощью другого сетевого кабеля, подключите модем к WAN порту беспроводного роутера.
4. Подключите блок питания модема к разъему DCIN и к розетке.

1.6.2 Беспроводное подключение



Для настройки беспроводного роутера через беспроводное подключение:

1. Подключите блок питания роутера к разъему DCIN и к розетке.
2 Подключите сетевой кабель провайдера или от модема к WAN порту роутера.
3. Подключите блок питания модема к разъему DCIN и к розетке.
4. Установите в компьютер сетевой адаптер IEEE 802.11a/b/g/n/ac/ax.

ПРИМЕЧАНИЕ: Подробную информацию о подключении к беспроводной сети смотрите в руководстве пользователя для WLAN адаптера.

2 Начало работы

2.1 Вход в веб-интерфейс

Данный беспроводной роутер имеет интуитивно понятный графический интерфейс пользователя (GUI), что позволяет легко сконфигурировать его функции через браузер, например Microsoft Edge, Safari или Google Chrome.

ПРИМЕЧАНИЕ: Функции могут изменяться в зависимости от версии прошивки.

Беспроводное подключение к сети:

1. Для просмотра доступных беспроводных сетей щелкните по иконке сети в области уведомлений.
2. Выберите беспроводную сеть EBR63, затем нажмите **Подключиться**.
3. Введите сетевой ключ, указанный на этикетке устройства и нажмите **OK**.
4. Дождитесь подключения компьютера к беспроводной сети. Иконка отображает состояние подключения и мощность сигнала проводного или беспроводного подключения.

Проводное подключение к сети:

Для входа в веб-интерфейс:

1. В браузере введите http://expertwifi.net.
2. Следуйте инструкциям по настройке.

2.2 Автоопределение WAN

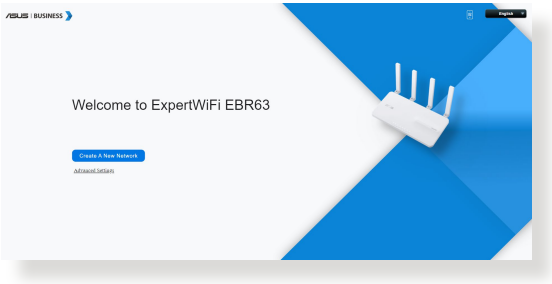
Функция быстрой настройки интернета (QIS) поможет вам быстро настроить подключение к Интернет.

ПРИМЕЧАНИЕ: При первом подключении к Интернет нажмите на роутере кнопку сброса для сброса роутера к заводским настройкам по умолчанию.

Автоопределение WAN:

1. Войдите в веб-интерфейс.

   Роутер автоматически определяет тип подключения к провайдеру.

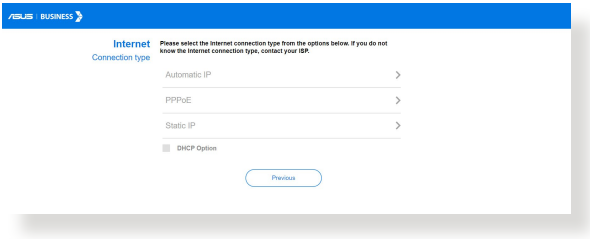


Примечания:

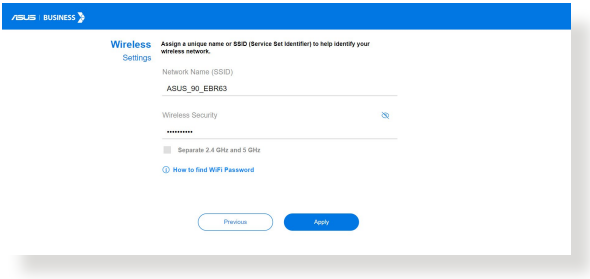
- Подробную информации об изменении имени пользователя и пароля смотрите в разделе **3.2.2 Система**.
- Имя пользователя и пароль отличается от имени сети (SSID) и ключа безопасности. Имя пользователя и пароль позволяют войти в веб-интерфейс роутера для конфигурации параметров беспроводного роутера. Имя сети (SSID) и ключ безопасности позволяют беспроводным устройствам подключаться к беспроводной сети.

2. Выберите тип подключения подключения к провайдеру, например **Автоматический IP (DHCP)**, **PPPoE** или **Статический IP**. Введите необходимую информацию для вашего типа подключения.

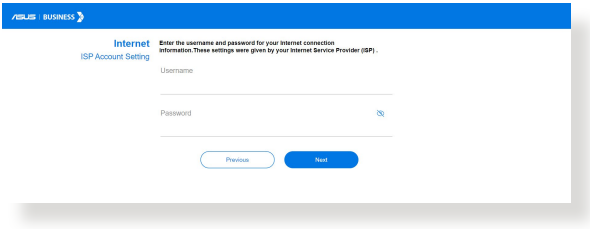
ОСТОРОЖНО! Необходимую информацию о вашем подключении к интернету узнайте у вашего провайдера.



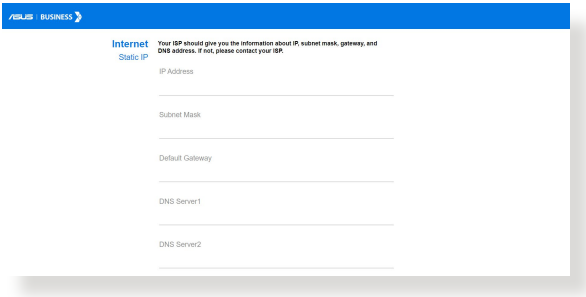
для автоматического IP (DHCP)



для PPPoE



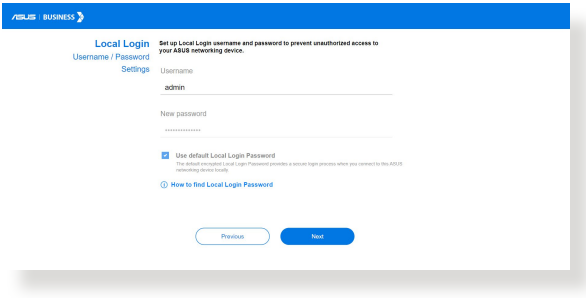
Для статического IP

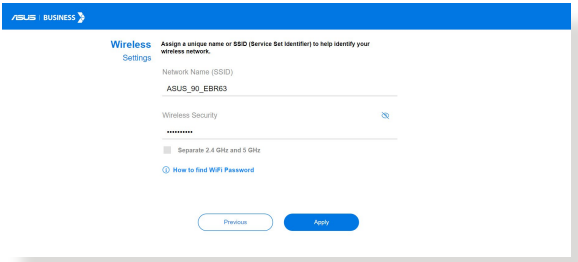


Примечания:

- Автоматическое определение типа подключения имеет место при первой настройке роутера или после сброса роутера к настройкам по умолчанию.
- Если QIS не может определить тип подключения к Интернет, нажмите **Skip to manual settings** и вручную сконфигурируйте тип подключения.

3. Введите имя пользователя, пароль или сохраните их для следующего входа. Сконфигурируйте параметры беспроводной сети. Когда закончите, нажмите **Применить**.





ПРИМЕЧАНИЕ: Если требуется назначить разные SSID для беспроводной сети 2,4 ГГц и 5 ГГц, установите флажок **Отдельные 2,4 ГГц и 5 ГГц**.

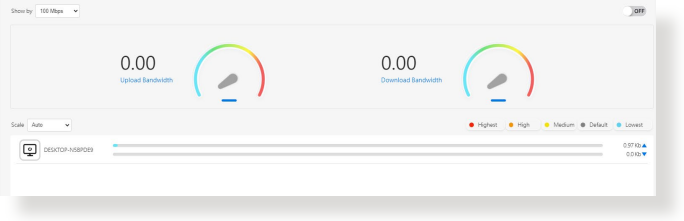
3 Настройка EBR63

3.1 Адаптивная QoS

3.1.1 Монитор пропускной способности

Монитор полосы пропускания позволяет отслеживать общее использование полосы пропускания, а также исходящий и входящий трафик для каждого клиента.

Для использования монитора полосы пропускания перейдите в **Settings** > **Adaptive QoS** > **Bandwidth Monitor**.

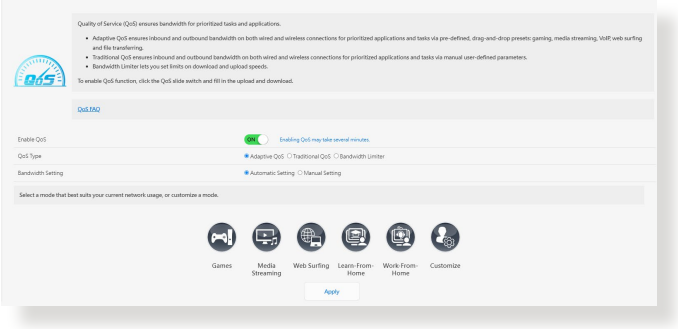


ПРИМЕЧАНИЕ: Для получения подробной информации посетите https://www.asus.com/ru/support/faq/1008717.

3.1.2 QoS

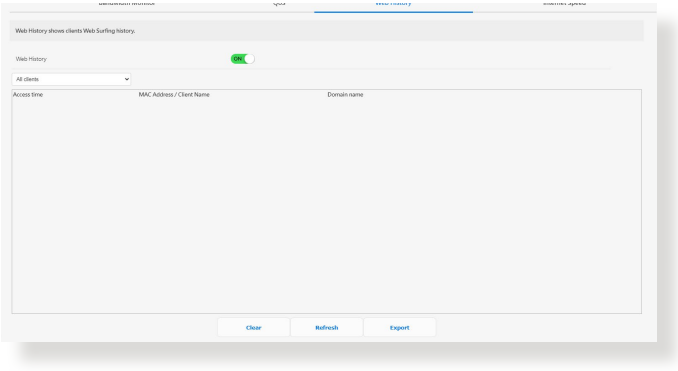
Технология QoS (Quality of Service) гарантирует высокую пропускную способность для приоритетных задач и приложений.

1. **Адаптивная QoS** гарантирует входящую и исходящую пропускную способность для приложений и задач с высоким приоритетом для проводных и беспроводных подключений с помощью предварительных настроек: игры, потоковое видео и аудио, VoIP, веб-серфинг и передача файлов.
2. **Традиционная QoS** оптимизирует входящий и исходящий трафик проводных и беспроводных подключений и устанавливает приоритет приложений и задач.
3. **Ограничитель скорости** позволяет устанавливать ограничения на скорость загрузки и скачивания.



3.1.3 Веб история

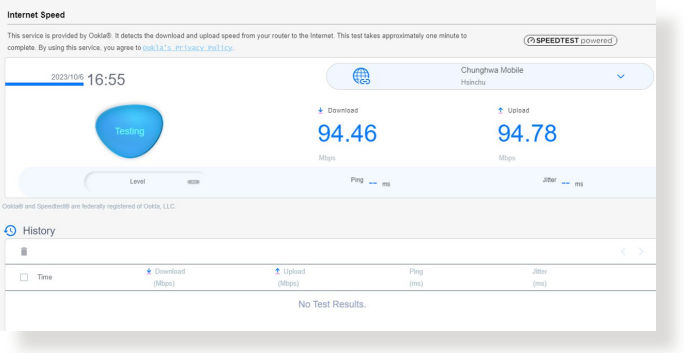
На странице **Веб история** отображается история просмотров веб-страниц клиентами.



3.1.4 Скорость интернета

Эта услуга предоставляется компанией Ookla. Эта функция определяет входную и выходную скорости подключения роутера к интернету.

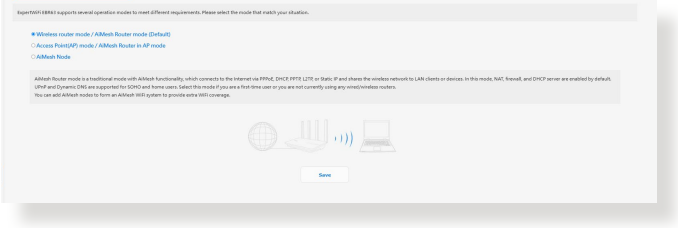
Нажмите **GO** для определения скорости подключения к интернету, что занимает около минуты.



3.2 Администрирование

3.2.1 Режим работы

На странице режим работы можно выбрать наиболее подходящий режим.



Для настройки режима работы:

1. В меню навигации выберите **Настройки** > **Администрирование** > **Режим работы**.
2. Выберите любой из следующих режимов:
   - **Режим беспроводного роутера (по умолчанию)**: В режиме беспроводного роутера, роутер подключается к интернету и предоставляет доступ к интернету для устройств в локальной сети.
   - **Режим точки доступа**: В этом режиме роутер создает новую беспроводную сеть.
3. Нажмите **Сохранить**.

ПРИМЕЧАНИЕ: При изменении режима роутер перезагрузится.

3.2.2 Система

На странице **Система** можно сконфигурировать параметры беспроводного роутера.

Для настройки параметров системы:

1. В меню навигации выберите **Настройки** > **Администрирование** > **Система**.
2. Можно сконфигурировать следующие параметры:
   - **Изменение пароля роутера**: Можно изменить имя пользователя и пароль беспроводного роутера, введя новые.
   - **Настройка USB**: Можно включить режим гибернации жесткого диска и изменить режим USB.
   - **Поведение кнопки WPS**: Физическая кнопка WPS используется для активации WPS.
   - **Часовой пояс**: Выберите часовой пояс для вашей сети.
   - **NTP-сервер**: Для синхронизации времени роутер может подключаться к серверу NTP (Network Time Protocol).
   - **Сетевой мониторинг**: Можно включить DNS-запрос для проверки соответствия имени хоста и IP-адреса или включить Ping для проверки целевого адреса.
   - **Автоматический выход**: Можно задать время для автоматического выхода.
   - **Включить уведомление об отключении WAN-интерфейса:** Эта функция позволяет браузеру отображать страницу с предупреждением, когда роутер отключен от Интернета. Когда отключено, страница с предупреждением не появится.
   - **Включить Telnet**: Нажмите **Да** для включения службы Telnet. Выберите **Нет** для отключения Telnet.
   - **Метод аутентификации**: Можно выбрать HTTP, HTTPS или оба протокола для безопасного доступа к роутеру.
   - **Включить планировщик перезагрузки:** Когда включено, можно задать время и дату перезагрузки.
   - **Включить веб-доступ из WAN**: Выберите **Да** для разрешения доступа к веб-интерфейсу роутера из Интернет. Выберите **No** для предотвращения доступа.
   - **Включить ограничение доступа**: Выберите **Да**, если нуж-

но задать IP-адреса устройств, которым разрешен доступ к веб-интерфейсу роутера из WAN/LAN.

- **Служба**: Эта функция позволяет настроить Telnet / SSH порт / Разрешить ввод пароля / ключа авторизации / тайм-аут простоя.

3. Нажмите **Применить**.

3.2.3 Обновление прошивки

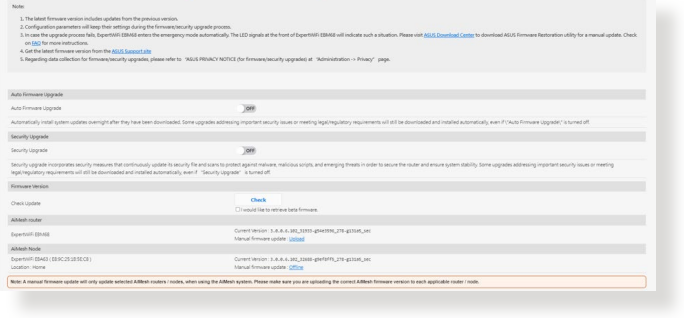
ПРИМЕЧАНИЕ: Скачайте последнюю версию прошивки с сайта ASUS http://www.asus.com.

Для обновления прошивки:

1. В меню навигации выберите **Настройки** > **Администрирование** > **Обновление прошивки**.
2. В поле **Новая прошивка** нажмите **Обзор** для нахождения прошивки.
3. Нажмите **Загрузить**.

Примечания:

- После завершения обновления дождитесь перезагрузки системы.
- При ошибке во время обновления беспроводной роутер переходит в аварийный режим и индикатор питания на передней панели медленно мигает. Подробную информацию о восстановлении системы смотрите в разделе **4.2 Восстановление прошивки**.

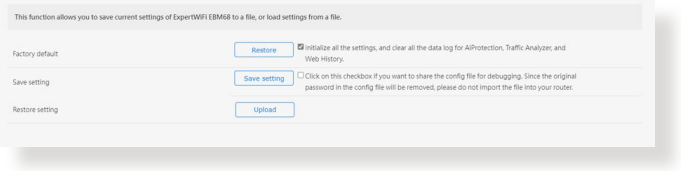


3.2.4 Восстановить/сохранить/загрузить настройки

Для восстановления/сохранения/сброса параметров:

1. В меню навигации выберите **Настройки** > **Администрирование** > **Восстановить/Сохранить/Загрузить настройки**.
2. Выберите задачу:
   - **Заводские настройки**: Инициализируйте все настройки и очистите все журналы для AiProtection, Анализатора трафика и Веб-истории.
   - **Сопри хранении настроек**: Позволяет поделиться конфигурационным файлов в целях отладки. Поскольку исходный пароль в конфигурационном файле будет удален, не импортируйте этот файл в роутер.
   - **Восстановление настроек**: Загрузка ранее сохраненных настроек в роутер.

ОСТОРОЖНО!В случае возникновения проблем, загрузите последнюю версию прошивки и сконфигурируйте новые параметры. Не сбрасывайте роутер к настройкам по умолчанию.



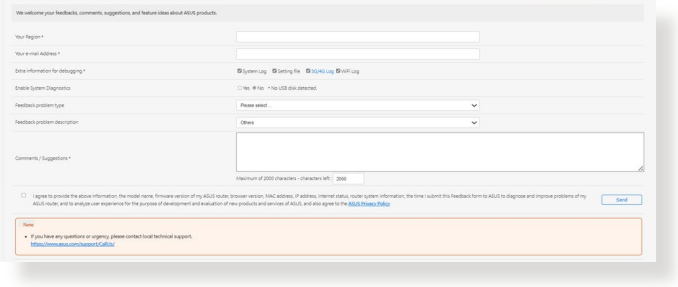
3.2.5 Обратная связь

Для использования обратной связи:

1. В меню навигации выберите **Настройки** > **Администрирование** > **Обратная связь**.
2. Введите свой регион, адрес электронной почты, дополнительную информацию для отладки, комментарии и предложения и отправьте.

ОСТОРОЖНО!

- Подробно прокомментируйте свою ситуацию для получения быстрого ответа.
- Согласитесь с Политикой конфиденциальности ASUS.



3.2.6 Приватность

1. Для привязки учетной записи, DDNS и удаленного подключения (приложение ASUS Router/приложение Lyra/AiCloud/AiDisk):

Обратите внимание, что ваша информация, включая модель продукта, версию микропрограммы, состояние Интернета, IP-адрес, MAC-адрес и имя DDNS, будет собрана ASUS с помощью вышеуказанных функций.

Если требуется отключить обмен информацией с ASUS с помощью вышеуказанных функций, нажмите **Изъять** ниже. Тем не менее, имейте в виду, что эти функции могут не работать при отключении обмена информацией с ASUS.

ОСТОРОЖНО!

- После нажатия **Изъять** будут внесены указанные ниже изменения
  - Используемое в данный момент имя DDNS, не будет храниться в вашем роутере.
  - Приложения ASUS Router, Lyra, AiCloud, AiDisk можно использовать только в том случае, если устройство находится в одной локальной сети с роутером.

---

2. Уведомление о конфиденциальности ASUS (для обновления прошивки и безопасности):

Обратите внимание, что ваша информация будет собираться роутером ASUS в целях обновления прошивки и безопасности. Если требуется отключить обмен информацией с ASUS с помощью вышеуказанных функций, нажмите <Изъять> ниже.

ОСТОРОЖНО!Нажатие **Изъять** может привести к невозможности обновления прошивки до последней версии и обновления защитных механизмов на роутере. Однако в целях безопасности и обеспечения соответствия законодательству, обновления, связанные с безопасностью или законодательными/нормативными требованиями, будут скачиваться и устанавливаться автоматически.

3.3 AiMesh

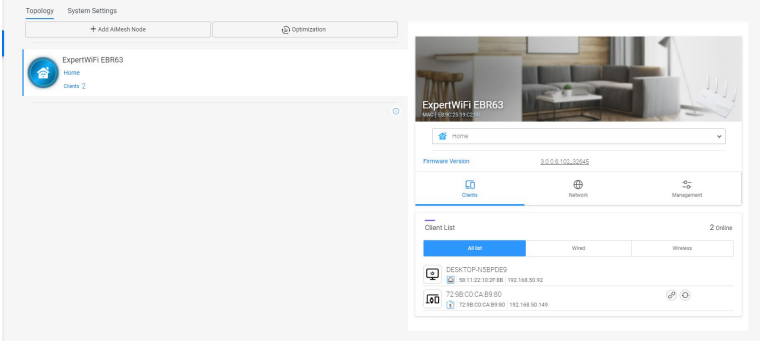
3.3.1 Настройка параметров беспроводной сети

Для защиты беспроводной сети от несанкционированного доступа, необходимо настроить параметры безопасности.

Для настройки параметров беспроводной сети:

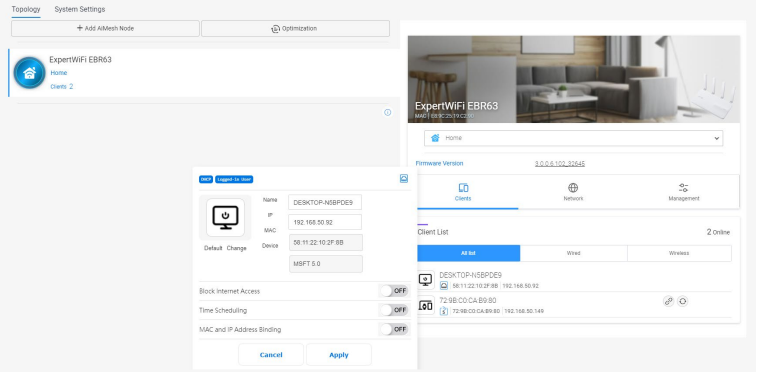
1. В меню навигации выберите **AiMesh** > **Топология**.
2. Можно сконфигурировать проводное и беспроводное подключение, состояние сети и состояние подсветки.

ПРИМЕЧАНИЕ: Можно настроить параметры безопасности для диапазонов 2,4 ГГц и 5 ГГц.



3. Перейдите в **AiMesh** > **Настройки системы** для включения или отключения режима транзитного соединения Ethernet, настройки черного списка роуминга, сброса настроек системы или перезагрузки.

3.3.2 Управление сетевыми клиентами

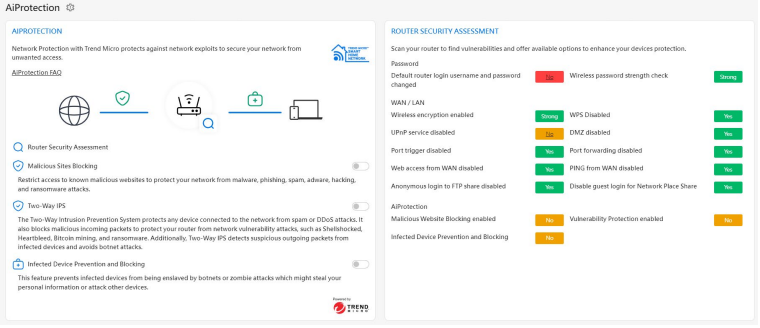


Для управления сетевыми клиентами:

1. В меню навигации выберите **AiMesh** > **Топология**.
2. Выберите иконку **Клиенты** для отображения информации о сетевом клиенте, например имя, MAC-адрес и IP-адрес.
3. Можно заблокировать подключение клиента к вашей сети, включить доступ по расписанию или включить привязку к MAC и IP.
4. Когда закончите, нажмите **Применить**.

3.4 AiProtection

AiProtection обеспечивает мониторинг в режиме реального времени для обнаружения вредоносного программного обеспечения. Также возможна фильтрация нежелательных сайтов и приложений и установка времени доступа к интернету.

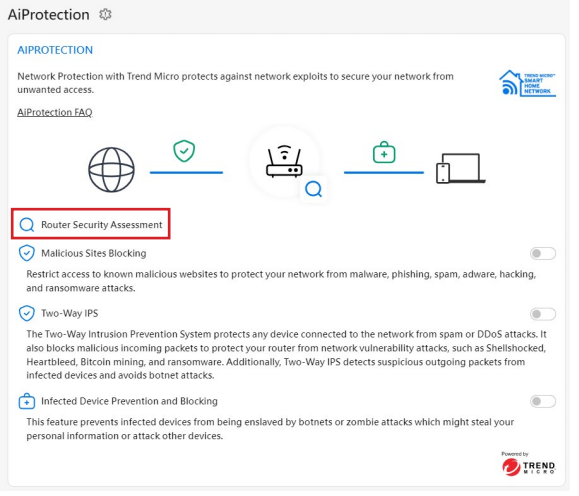


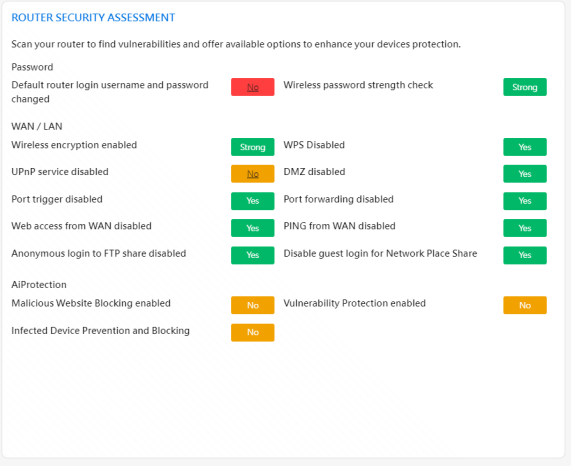
3.4.1 Сетевая защита

Сетевая защита обеспечивает защиту сети от несанкционированного доступа.

Для оценки безопасности роутера:

1. В меню навигации выберите **AiProtection**.
2. Нажмите **Оценка безопасности роутера** для отображения результатов оценки безопасности.





ОСТОРОЖНО!Элементы, помеченные как **Yes** на странице **Оценка безопасности роутера** считаются безопасными. Элементы, помеченные как **No** рекомендуется сконфигурировать соответствующим образом.

3. (На странице **Оценка безопасности роутера** вручную сконфигурируйте элементы, помеченные как **No** (опционально). Для этого:

   a. Щелкните по элементу.

ПРИМЕЧАНИЕ:При щелчке по элементу откроется страница его настроек.

b. На странице настроек безопасности элемента внесите необходимые изменения и нажмите **Применить**.

c. Вернитесь на страницу **Оценка безопасности роутера** и нажмите **Закрыть** для закрытия страницы.

4. Для конфигурации настроек безопасности автоматически нажмите **Защитить роутер**.
5. При появлении подтверждения нажмите **OK**.

Для включения защиты сети:

1. В меню навигации выберите **AiProtection**.
2. Выберите тип защиты, который вы хотите реализовать, и включите его. Можно выбрать между **Блокировка вредоносных сайтов**, **Двусторонняя IPS** и **Профилактика и блокировка зараженных устройств**.

   Блокировка вредоносных сайтов

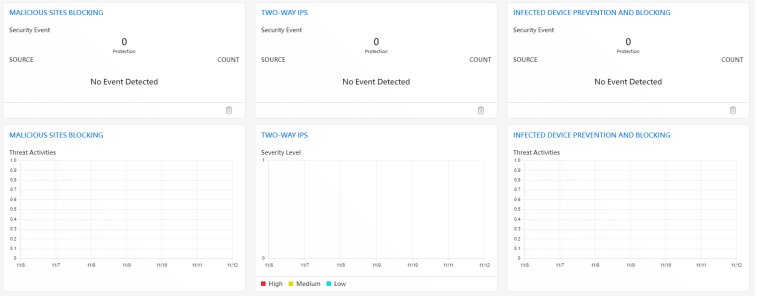
   Эта функция блокирует вредоносные сайты для защиты вашего сетевого устройства от вредоносных программ, фишинга, спама, рекламы, хакеров или вымогателей.

   Двусторонняя IPS

   Двусторонняя IPS (система предотвращения атак) защищает подключенные устройства от спама или DDoS-атак. Она также блокирует вредоносные входящие пакеты для защиты вашего роутера от сетевых атак, например Shellshocked, Heartbleed, Bitcoin mining и вымогателей. Также выполняется обнаружение подозрительных исходящих пакетов для поиска зараженных устройств и предотвращение порабощения их бот-сетями.

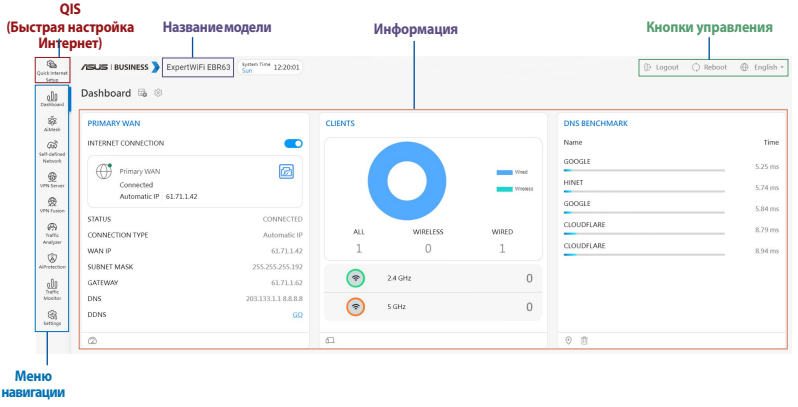
   Профилактика и блокировка зараженных устройств

   Эта функция предотвращает порабощение зараженных устройств бот-сетями или зомби-атаками, которые могут украсть личную информацию или атаковать другие устройства.
3. Согласитесь с **Лицензионным соглашением Trend Micro**.


MALICIOUS SITES BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
TWO-WAY IPS
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
INFECTED DEVICE PREVENTION AND BLOCKING
Security Event
0
Protection
SOURCE
COUNT
No Event Detected
MALICIOUS SITES BLOCKING
Threat Activities
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
11/6
11/7
11/8
11/9
11/10
11/11
11/12
TWO-WAY IPS
Severity Level
1
0
11/6
11/7
11/8
11/9
11/10
11/11
11/12
High
Medium
Low
INFECTED DEVICE PREVENTION AND BLOCKING
Threat Activities
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
11/6
11/7
11/8
11/9
11/10
11/11
11/12

3.5 Информационная панель

Информационная панель позволяет управлять вашей сетью, например, подключением к Интернету, подключением клиентов, тестом DNS, состоянием системы, портами Ethernet и монитором трафика.



3.6 Контроль доступа к устройствам

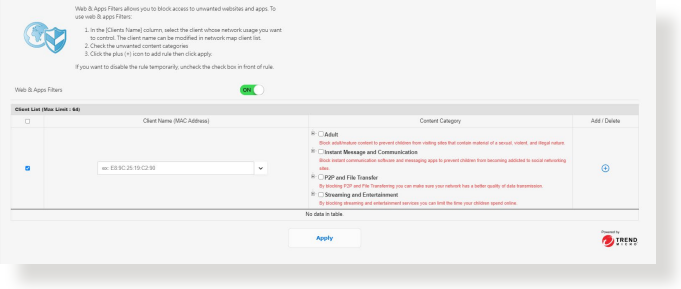
3.6.1 Фильтры для веб и приложений

Фильтры для веб и приложений позволяют блокировать доступ к нежелательным сайтам и приложениям.

Для использования фильтров для веб и приложений:

1. В меню навигации выберите **Настройки** > **Контроль доступа к устройствам** > **Фильтры для веб и приложений**.
2. Для включения фильтров передвиньте ползунок **Фильтры для веб и приложений** в положение **ON**.
3. В столбце **Client Name** выберите клиента, чей сетевой доступ нужно контролировать. Имя клиента можно изменить в сети карте списке клиентов.
4. Пометьте нежелательное содержимое.
5. Нажмите ⊕ для добавления правила и нажмите **Применить**.

Если нужно временно отключить правило, снимите флажок.

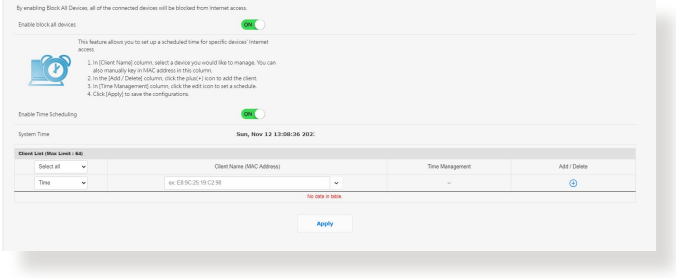


3.6.2 Расписание

Расписание позволяет задать время для доступа в Интернет для конкретных устройств.

Для использования расписания:

1. В меню навигации выберите **Настройки** > **Контроль доступа к устройству** > **Расписание**.
2. Для включения расписания сдвиньте ползунок **Включить расписание** в положение **ON**.
3. В столбце **Имя клиента** введите или выберите имя клиента из выпадающего списка.
4. Нажмите ⊕ для добавления клиентского профиля.
5. Нажмите **Применить** для сохранения настроек.



3.7 Брандмауэр

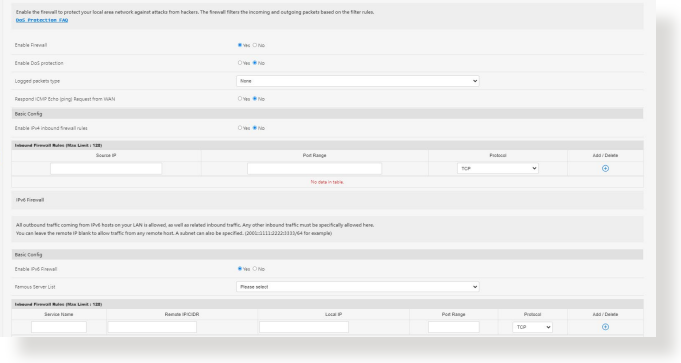
3.7.1 Общие

Роутер может функционировать в качестве аппаратного брандмауэра.

ПРИМЕЧАНИЕ: Брандмауэр включен по умолчанию.

Для настройки параметров брандмауэра:

1. В меню навигации выберите **Настройки** > **Брандмауэр** > **Общие**.
2. В поле **Включить брандмауэр** выберите **Да**.
3. В поле **Включить защиту от DoS** выберите **Да** для защиты вашей сети от DoS (отказ в обслуживании) атак. Это может повлиять на производительность роутера.
4. Можно также отслеживать пакеты между LAN и WAN. В поле Тип регистрируемых пакетов выберите **Отброшенные**, **Принятые** или **Оба**.
5. Нажмите **Применить**.



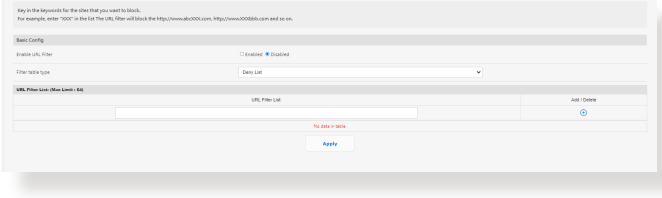
3.7.2 Фильтр URL

Можно запретить доступ к определенным URL-адресам, добавив их в фильтр.

ПРИМЕЧАНИЕ: Фильтр URL функционирует на основе запроса DNS. Если сетевой клиент уже посещал сайт, например http://www.abcxxx.com, то сайт заблокирован не будет (DNS-кэш сохраняет ранее посещенные сайты). Для решения этой проблемы очистите DNS-кэш перед установкой фильтра URL.

Для настройки фильтра URL:

1. В меню навигации выберите **Настройки** > **Брандмауэр** > **Фильтр URL**.
2. В поле **Включить URL фильтр** выберите **Включить**.
3. Введите URL и нажмите ⊕.
4. Нажмите **Применить**.



3.7.3 Фильтр ключевых слов

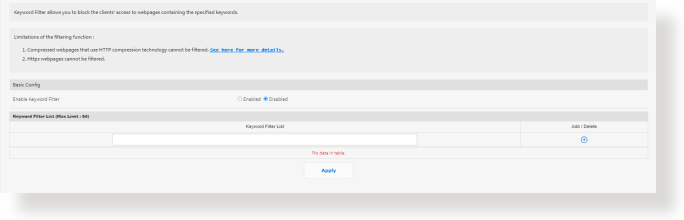
Фильтр ключевых слов блокирует доступ к страницам, содержащим заданные ключевые слова.

Для настройки фильтра ключевых слов:

1. В меню навигации выберите **Настройки** > **Брандмауэр** > **Фильтр ключевых слов**.
2. В поле **Включить фильтр ключевых слов** выберите **Включить**.
3. Введите слово или фразу и нажмите ⊕.
4. Нажмите **Применить**.

ПРИМЕЧАНИЯ:

- Фильтр ключевых слов функционирует на основе запроса DNS. Если сетевой клиент уже посещал сайт, например http://www.abcxxx.com, то сайт заблокирован не будет (DNS-кэш сохраняет ранее посещенные сайты). Для решения этой проблемы очистите DNS-кэш перед установкой фильтра ключевых слов.
- Сжатые веб-страницы не могут быть отфильтрованы. Страницы, загружаемые по протоколу HTTPS, не могут быть заблокированы.

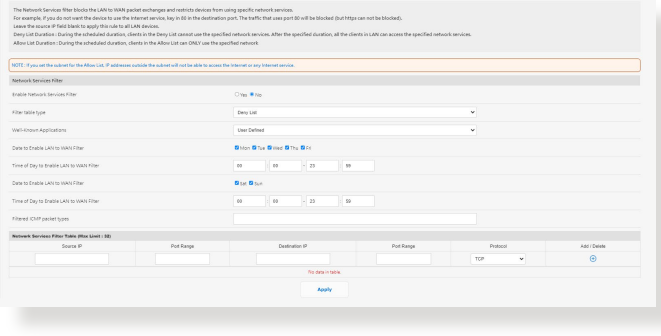


3.7.4 Фильтр сетевых служб

Фильтр сетевых служб позволяет ограничить доступ к конкретным веб-службам, например Telnet или FTP.

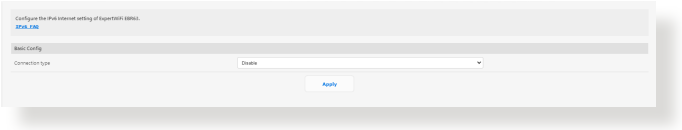
Для настройки фильтра сетевых служб:

1. В меню навигации выберите **Настройки** > **Брандмауэр** > **Фильтр сетевых служб**.
2. В поле **Включить фильтр сетевых служб** выберите **Да**.
3. Выберите режим фильтра. **Черный список** блокирует указанные сетевые службы. **Белый список** разрешает доступ только к указанным сетевым службам.
4. Укажите день и время работы фильтра.
5. Введите исходный IP-адрес, целевой IP-адрес, диапазон портов и протокол. Нажмите ⊕.
6. Нажмите **Применить**.



3.8 IPv6

Данный роутер поддерживает адресацию IPv6, поддерживающую большее количество IP-адресов. Информацию о поддержке IPv6 можно узнать у вашего провайдера.



Для настройки IPv6:

1. В меню навигации выберите **Настройки** > **IPv6**.
2. Выберите **Тип подключения**. Параметры отличаются в зависимости от типа выбранного подключения.
3. Введите параметры IPv6 и DNS.
4. Нажмите **Применить**.

ПРИМЕЧАНИЯ:

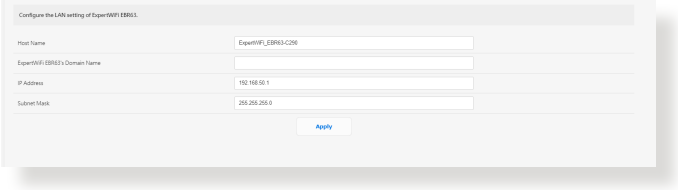
- Конкретную информацию по IPv6 можно узнать у вашего провайдера.
- Для получения подробной информации посетите https://www.asus.com/ru/support/FAQ/113990.

3.9 Локальная сеть

3.9.1 LAN IP

На экране LAN IP можно изменить настройки LAN IP роутера.

ПРИМЕЧАНИЕ: Любые изменения LAN IP повлияют на настройки DHCP.

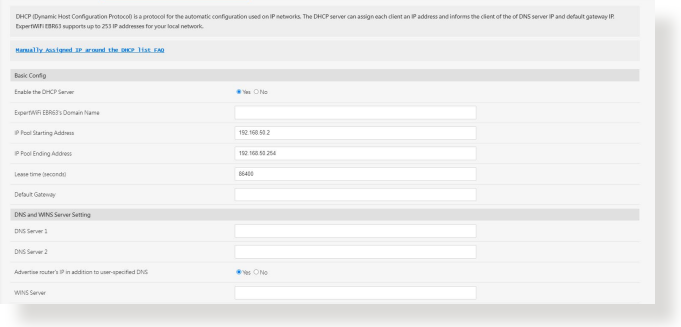


Для изменения параметров LAN IP:

1. В меню навигации выберите **Настройки** > **LAN** > **LAN IP**.
2. Измените **IP-адрес** и **маску подсети**.
3. Когда закончите, нажмите **Применить**.

3.9.2 DHCP-сервер

DHCP (Dynamic Host Configuration Protocol) это протокол для автоматической конфигурации, используемый в сетях IP. Сервер DHCP может назначать каждому клиенту адрес IP и сообщает клиенту о IP DNS-сервера и шлюза по умолчанию.



Для конфигурации DHCP сервера:

1. В меню навигации выберите **Настройки** > **LAN** > **DHCP-сервер**.
2. В поле **Включить DHCP сервер** выберите **Да**.
3. В поле **Имя домена** введите доменное имя для беспроводного роутера.
4. В поле **Начальный адрес пула** введите начальный IP-адрес.
5. В поле **Конечный адрес пула** введите конечный IP-адрес.
6. В поле **Время аренды** введите время аренды IP-адреса. По истечении времени, DHCP сервер назначит новый IP-адрес.

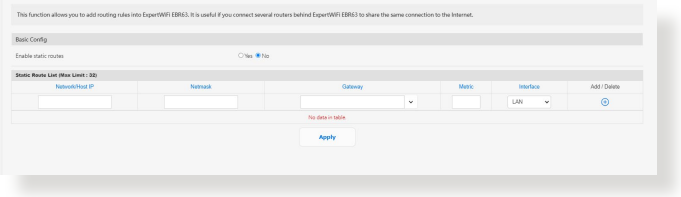
ПРИМЕЧАНИЯ:

- Рекомендуется использовать IP-адрес в формате: 192.168.1.xxx (где xxx может быть любым числом в диапазоне от 2 до 254).
- Начальный IP-адрес пула не должен быть больше конечного IP-адреса.

7. Если необходимо, введите IP-адреса DNS и WINS серверов в разделе **Настройка DNS и WINS сервера**.
8. Роутер также позволяет назначить IP-адреса сетевым клиентам вручную. В поле **Включить назначение вручную** выберите **Да** для назначения IP-адреса для указанного MAC-адреса в сети. До 32 MAC-адресов можно добавить в список DHCP вручную.

3.9.3 Маршрут

Эта функция позволяет добавить правила маршрутизации в роутер. Эта функция полезна при подключении нескольких роутеров за EBR63 для совместного использования одного подключения к Интернету.

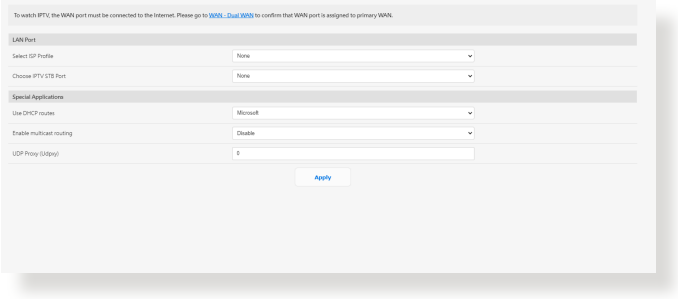


Для конфигурации таблицы маршрутизации:

1. В меню навигации выберите **Настройки** > **LAN** > **Маршрут**.
2. В поле **Включить статические маршруты** выберите **Да**.
3. В **Списке статических маршрутов** введите информацию о маршруте. Нажмите ⊕ или ⊖ для добавления или удаления устройства из списка.
4. Нажмите **Применить**.

3.9.4 IPTV

Беспроводной роутер поддерживает подключение к службе IPTV по локальной сети или через провайдера. На вкладке IPTV можно сконфигурировать параметры IPTV, VoIP, групповой рассылки и UDP. Подробную информацию можно получить у вашего провайдера.

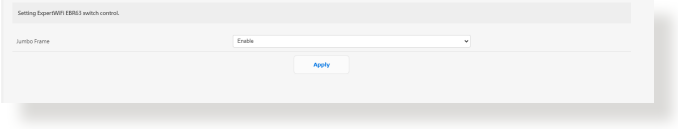


3.9.5 Коммутация

Позволяет настроить в роутере функцию коммутации. Можно объединить два порта LAN со скоростью 1 Гбит/с для увеличения скорости проводного соединения до 2 Гбит/с, что позволит повысить пропускную способность при подключении к NAS или другим сетевым устройствам.

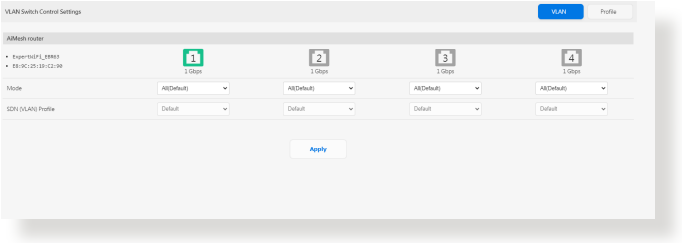
Примечания:

- Для использования протокола управления агрегацией каналов (LACP) устройства должны поддерживать стандарт IEEE 802.3ad.
- Функция агрегации позволяет объединить порты LAN3 и LAN2.



3.9.6 VLAN

VLAN (виртуальная локальная сеть) - это логическая сеть, созданная внутри более крупной физической сети. VLAN позволяют сегментировать сеть на более мелкие виртуальные подсети, которые можно использовать для изоляции трафика и повышения производительности сети.



Для настройки VLAN:

1. В меню навигации выберите **Настройки** > **LAN** > **VLAN**.
2. Для создания профиля VLAN выберите вкладку **Профиль**, затем ⊕. Можно назначить собственный идентификатор VLAN.
3. **Изоляция портов** ограничивает права доступа разных устройств в одной VLAN. Теперь вы создаете сеть "только VLAN", что означает сеть с VID, но без DHCP.
4. Выберите вкладку **VLAN** для выбора порта с определенным профилем и режимом (**Trunk** / **Access**).

ПРИМЕЧАНИЕ: Можно выбрать один из следующих режимов:

Все (по умолчанию) разрешает доступ ко всем тегированным и нетегированным пакетам.

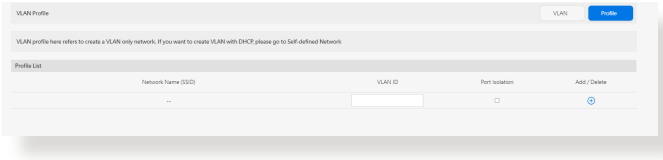
Режим **Доступ** обеспечивает доступ к выбранному SDN (VLAN). Можно выбрать профили, созданные с помощью Guest Network pro или VLAN.

Режим **Trunk**:

- **Разрешить все тегированные:** разрешает доступ только к тегированным пакетам.

- **С выбранным SDN(VLAN):** Разрешает доступ только к выбранным SDN или VLAN.

5. Когда закончите, нажмите **Применить**.



ПРИМЕЧАНИЕ: Для получения дополнительной информации посетите https://www.asus.com/ru/support/FAQ/1049415/.

3.10 Сетевые утилиты

Для использования сетевых утилит в меню навигации выберите **Настройки** > **Сетевые утилиты**.

3.10.1 Сетевая проверка

Отправка пакетов ICMP ECHO_REQUEST на сетевой хост.

3.10.2 Netstat

Отображение сведений о сети.

3.10.3 Пробуждение по сети

Функция WOL (Wake-On-LAN) позволяет разбудить компьютер с любого устройства в сети..

3.10.4 Правило Smart Connect

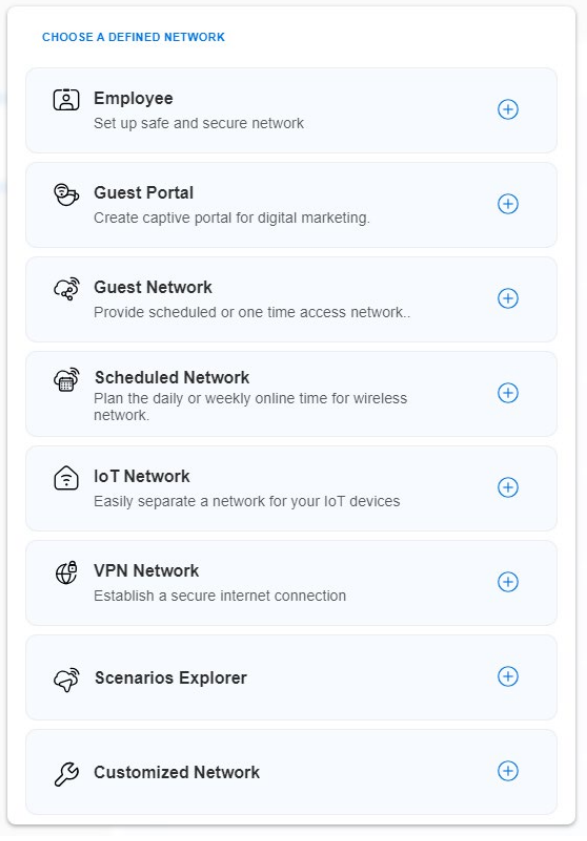
Настройка информации, связанной со Smart Connect.

3.11 Автономная сеть

Автономная сеть (SDN) предоставляет до пяти SSID для разделения и приоритезации устройств для различных целей и сетевых альтернатив, создавая сегменты сети для сотрудников, гостевых порталов, гостевых сетей, сетей по расписанию, сетей IoT и сетей VPN.

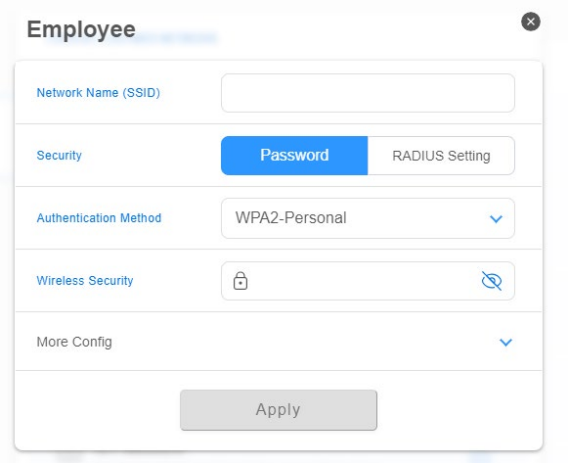
Для создания автономной сети:

1. В меню навигации выберите **Автономная сеть** .
2. Выберите определенную сеть, соответствующую вашему конкретному сценарию.



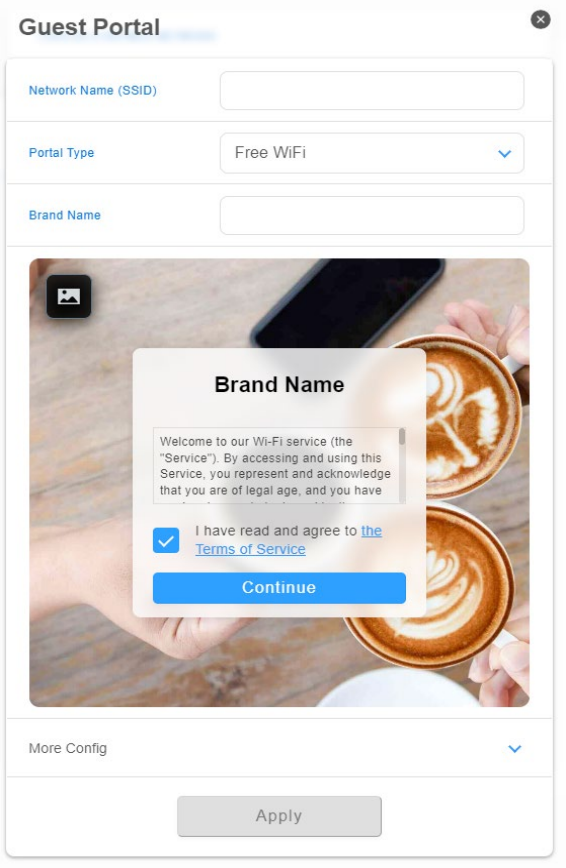
3.11.1 Сотрудники

Позволяет настроить уровень доступа для различных целей для повышения безопасности сети. Рекомендуется для офисов, где назначают разрешения различным отделам.



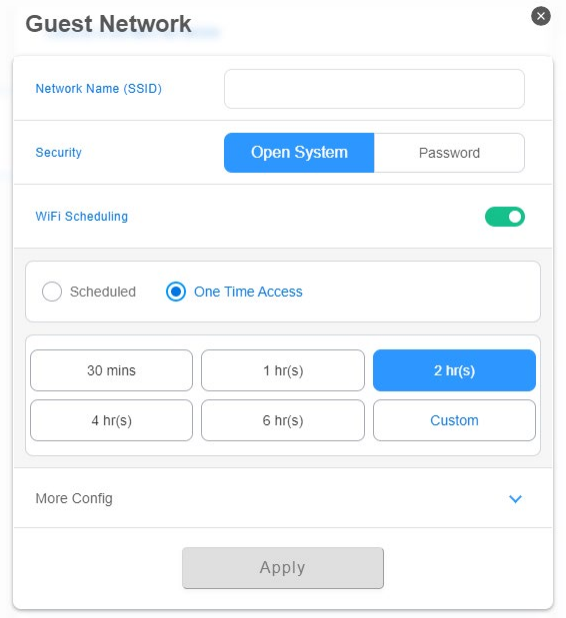
3.11.2 Гостевой портал

Позволяет создать гостевой портал для цифрового маркетинга. Рекомендуется для использования в ресторанах, отелях или мобильных закусочных.



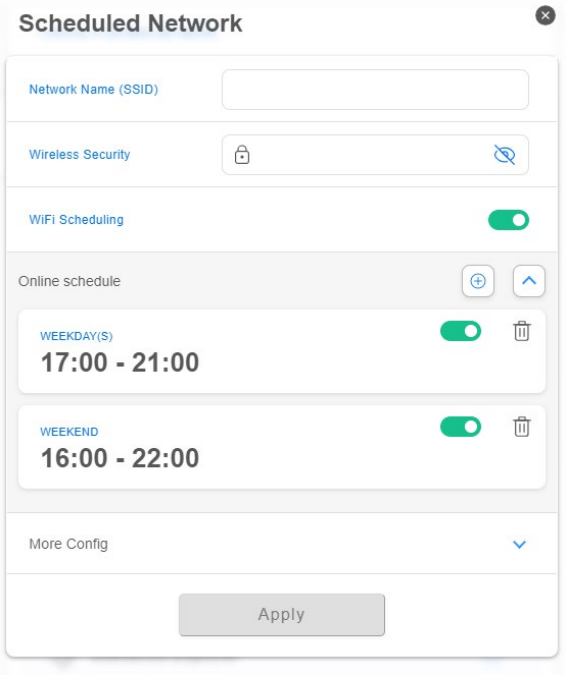
3.11.3 Гостевая сеть

Предоставляет временным посетителям разовый доступ к сети или по расписанию. Рекомендуется для использования в торговых центрах, спортивных залах или для посетителей.



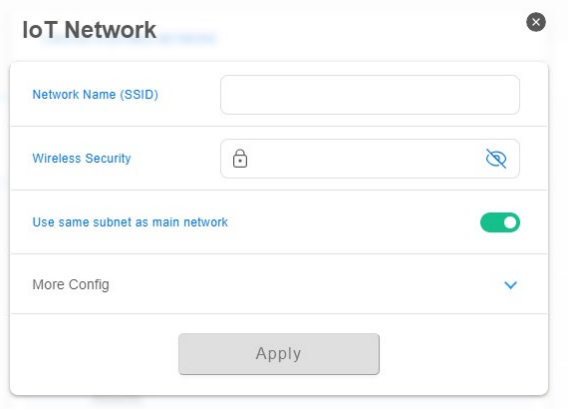
3.11.4 Сеть по расписанию

Планируемое ежедневное или еженедельное время подключения к беспроводной сети. Рекомендуется для дистанционного обучения, использования в классе или для детей.



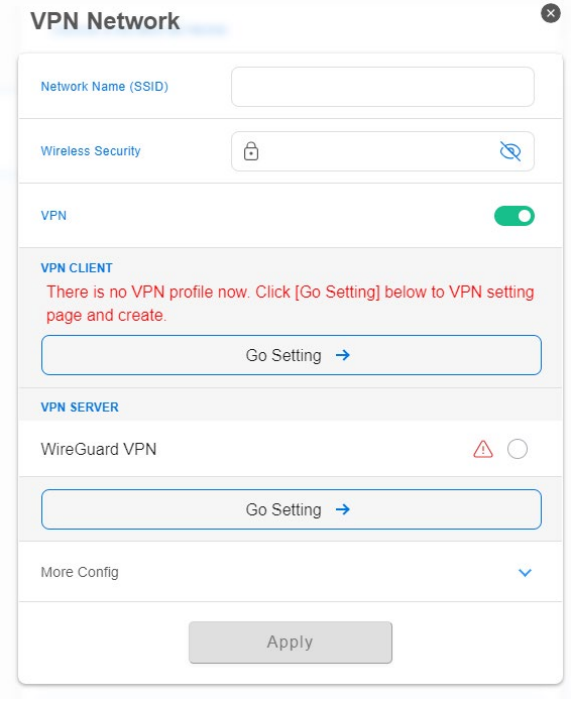
3.11.5 Сеть IoT

Позволяет легко настроить отдельную сеть для IoT-устройств. Рекомендуется для использования с устройствами наблюдения, голосовыми помощниками, освещением, дверными камерами, умными замками и датчиками.



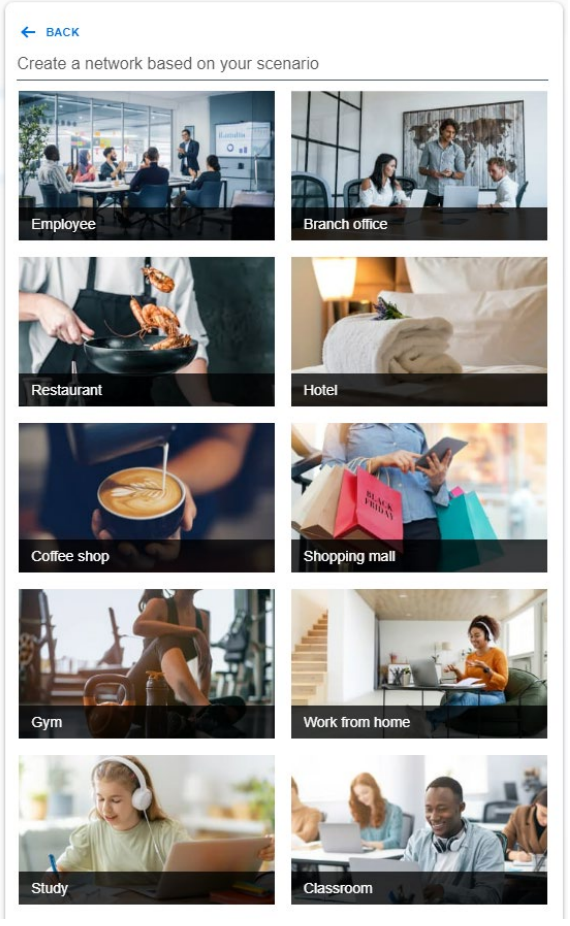
3.11.6 Сеть VPN

Помогает установить безопасное интернет-соединение с помощью VPN. Рекомендуется для работы на дому или в филиале.



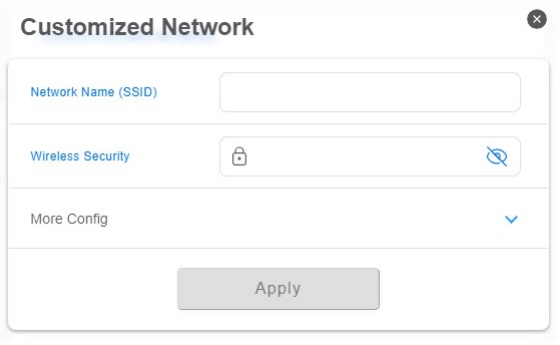
3.11.7 Обозреватель сценариев

Если вы не знаете, какую сеть создать, можно выбрать сектор, соответствующий вашей принадлежности для создания сети.



3.11.8 Настраиваемая сеть

Позволяет выбрать вариант персонализированной сети.



3.12 Системный журнал

Системный журнал содержит записанную сетевую активность.

ПРИМЕЧАНИЕ: Системный журнал очищается при перезагрузке или выключении роутера.

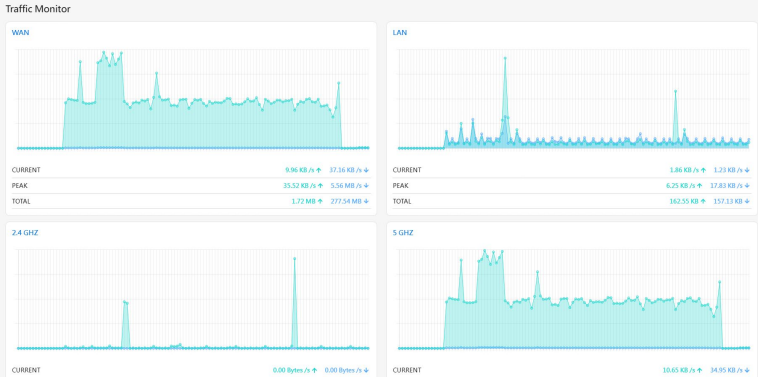
Для просмотра системного журнала:

1. В меню навигации выберите **Настройки** > **Системный журнал**.
2. Сетевую активность можно посмотреть на любой из этих вкладок:
   - Общий журнал
   - Аренда адресов DHCP
   - Журнал беспроводной сети
   - Переадресация портов
   - Таблица маршрутизации
   - IPv6
   - Подключения

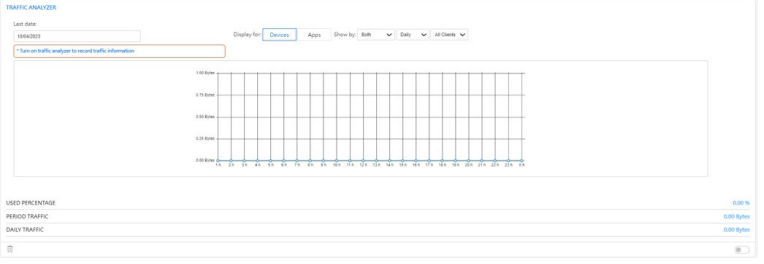
3.13 Мониторинг трафика

3.13.1 Мониторинг трафика

Функция мониторинга трафика позволяет оценить объем трафика, а также скорость подключения к Интернет, проводного и беспроводного подключений. Функция позволяет ежедневно контролировать сетевой трафик. Также имеется возможность отобразить трафик в течение последних 24 часов.



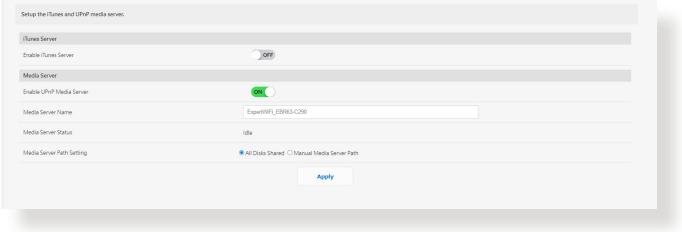
3.13.2 Анализатор трафика



3.14 USB-приложение

3.14.1 Медиасервер

Медиасервер позволяет настроить iTunes и UPnP-сервер.



Для открытия страницы настроек медиасервера перейдите **Настройки** > **USB-приложение** > **Медиасервер**.

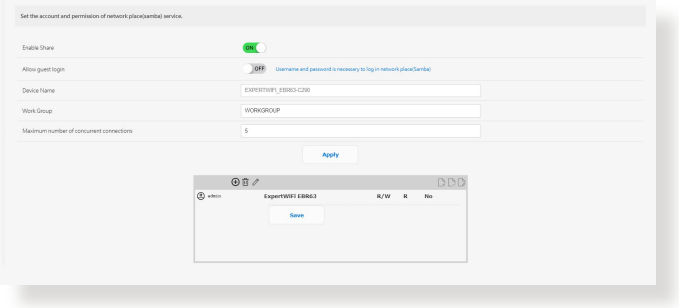
Ознакомьтесь с описанием полей:

- **Включить iTunes сервер**: Выберите ВКЛ/ОТКЛ для включения/отключения iTunes сервера.
- **Включите UPnP медиасервер** Выберите ВКЛ/ОТКЛ для включения/отключения UPnP медиасервера.
- **Имя медиасервера**: Введите имя медиасервера.
- **Настройки медиасервера**: Выберите **Общий доступ ко всем дискам** или **Настройка медиасервера вручную**.

Когда закончите, нажмите **Применить**.

3.14.2 Сетевое окружении (Samba)

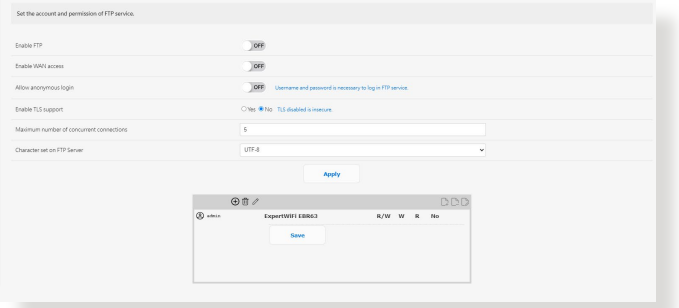
Сетевое окружение (Samba) обеспечивает доступ к сетевому диску из локальной сети. Сетевое окружение (Samba) также позволяет создать учетные записи и назначить им разрешения.



В меню навигации выберите **Настройки** > **USB-приложение** > **Сетевое окружение (Samba)**.

3.14.3 FTP сервер

FTP сервер позволяет настроить учетные записи и разрешения для службы FTP.



Для использования FTP сервера, перейдите в **Настройки** > **USB-приложение** > **FTP сервер**.

3.14.4 Сервер печати

3.14.4.1 Общий принтер ASUS EZ

Утилита ASUS EZ Printing позволяет к USB порту роутера подключить USB принтер и настроить сервер печати. Это позволяет сетевым клиентам печатать файлы и сканировать документы.

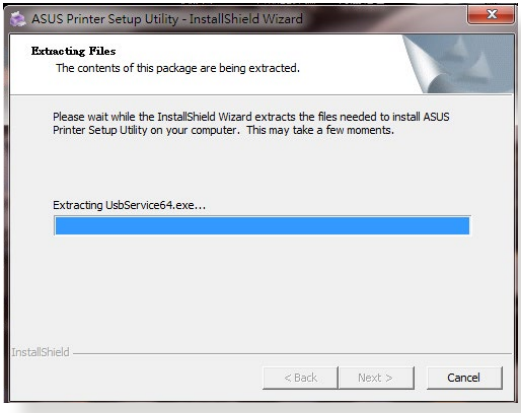
ПРИМЕЧАНИЕ: Функция сервер печати поддерживается в Windows 10/11.

Для установки утилиты EZ Printer sharing:

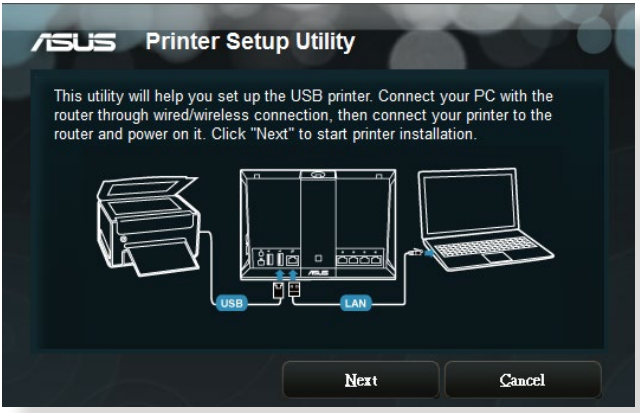
1. В меню навигации выберите **Настройки** > **USB-приложение** > **Сервер печати**.
2. Нажмите **Скачать сейчас** для загрузки утилиты сетевого принтера.

ПРИМЕЧАНИЕ: Утилита сетевого принтера поддерживается только в Windows 10/11. Для установки утилиты на Mac OS, выберите **Используйте протокол LPR для общей печати**.

3. Разархивируйте скачанный файл и нажмите иконку принтера для запуска программы установки утилиты для сетевого принтера.

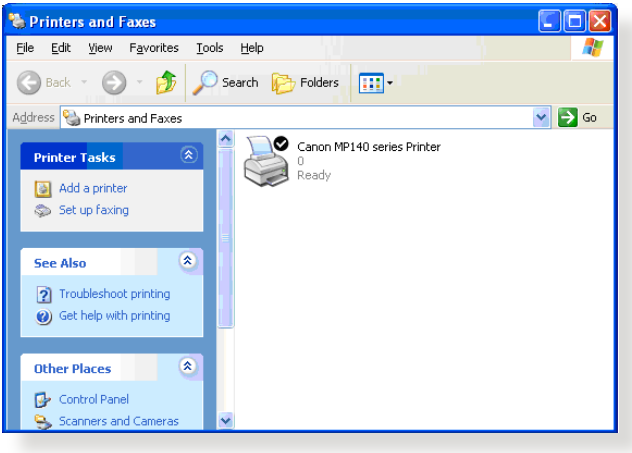


4. Следуйте инструкциям на экране для настройки оборудования, затем нажмите **Next**.



5. Подождите несколько минут до завершения начальной настройки. Нажмите **Далее**.
6. Нажмите **Готово** для завершения установки.
7. Следуйте инструкциям ОС Windows для установки драйвера принтера.

8. После завершения установки драйвера для принтера сетевые клиенты могут использовать принтер.

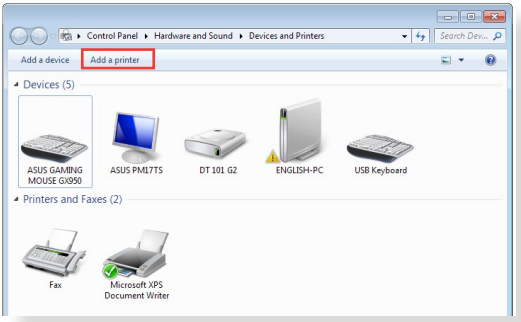


3.14.4.2 Использование LPR для совместного использования принтера

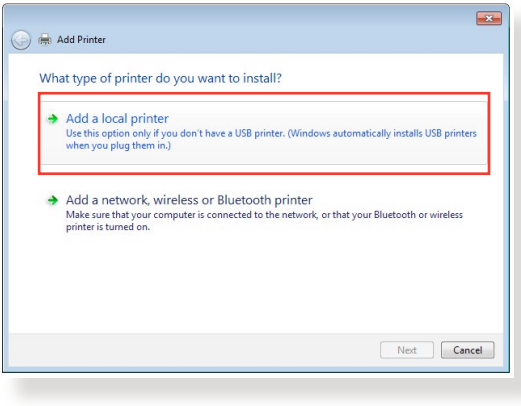
С помощью LPR/LPD (Line Printer Remote/Line Printer Daemon) можно совместно использовать принтер с компьютерами с ОС Windows и MAC..

Для совместного использования принтера LPR:

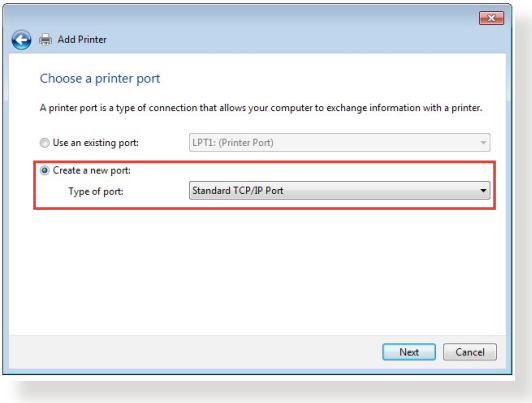
1. Для запуска **Мастера установки принтера** нажмите **Пуск** > **Устройства и принтеры** > **Мастер установки**.



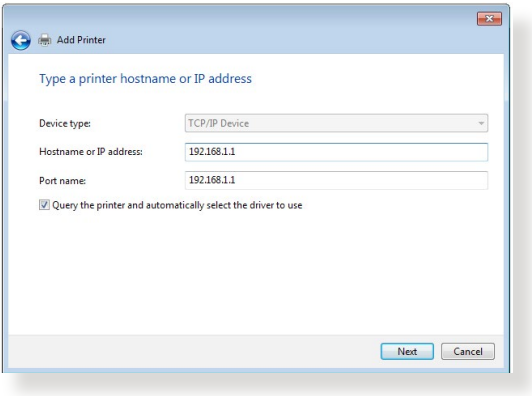
2. Выберите **Добавить локальный принтер**, затем нажмите **Далее**.



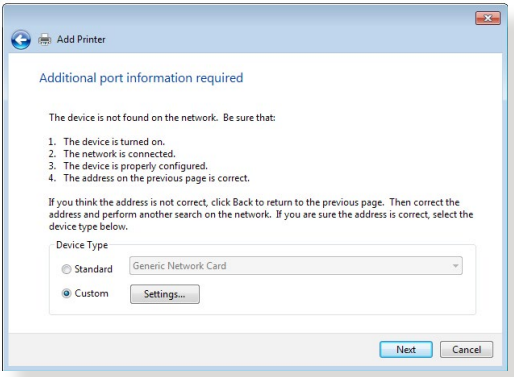
3. Выберите **Создать новый порт**, затем установите **Тип порта** в значение **Стандартный порт TCP/IP**. Нажмите **Новый порт**.



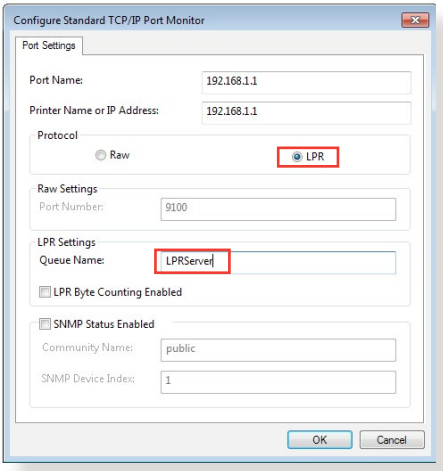
4. В поле **Имя хоста или IP-адрес** введите IP-адрес беспроводного роутера и нажмите **Далее**.



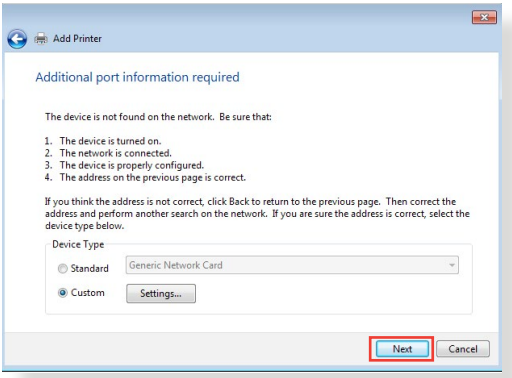
5. Выберите **Пользовательский**, затем нажмите **Настройки**.



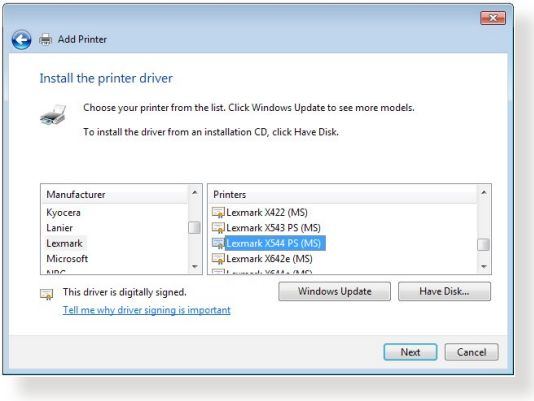
6. Установите **Протокол** в **LPR**. В поле **Имя очереди** введите **LPRServer**, затем нажмите **OK** для продолжения.



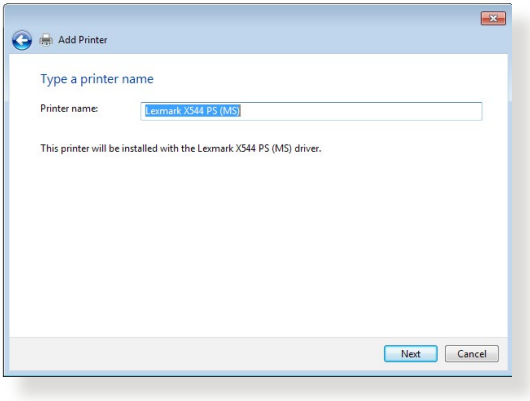
7. Нажмите **Далее** для завершения настройки порта TCP/IP.



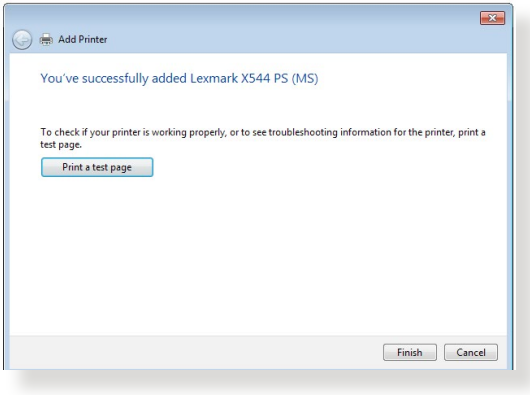
8. Установите драйвер принтера из списка. Если принтер отсутствует в списке, нажмите **Have Disk** для установки драйвера принтера вручную.



9. Нажмите **Далее** для принятия имени принтера по умолчанию.



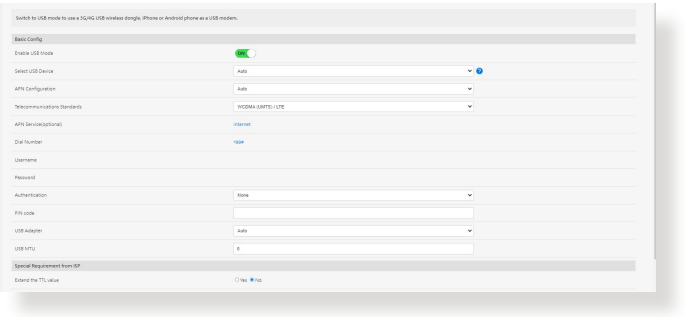
10. Нажмите **Готово** для завершения установки.



3.14.5 USB-модем

Переключитесь в режим USB для использования в качестве модема беспроводный 3G/4G USB адаптер или телефон Android.

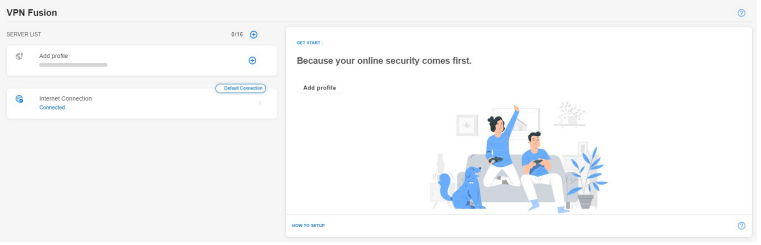
Для использования USB-модема, перейдите в **Настройки** > **USB-приложение** > **USB-модем**.



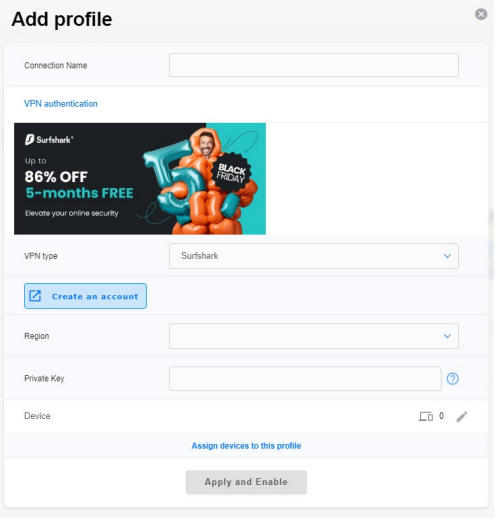
3.15 VPN Fusion

3.15.1 Создание VPN fusion

VPN Fusion позволяет одновременно подключаться к нескольким VPN-серверам и назначать их для сетевых клиентов.

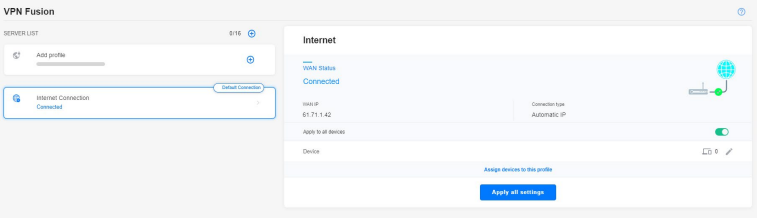


1. В меню навигации выберите **VPN Fusion**.
2. Нажмите ⊕ в поле **Добавить профиль** для настройки нового туннеля VPN.
3. Завершите настройку VPN, включая имя подключения, тип VPN, регион, закрытый ключ и устройство.
4. Нажмите **Применить и включить**.



3.15.2 Подключение к интернету

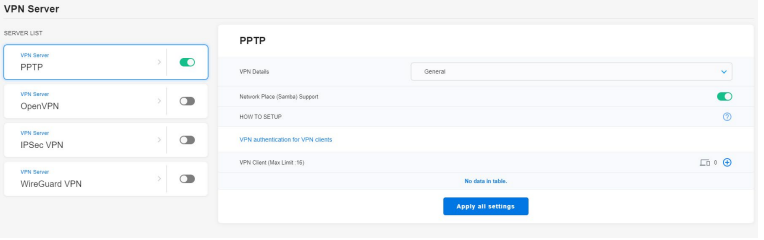
Позволяет управлять состоянием глобальной сети подключенных устройств.



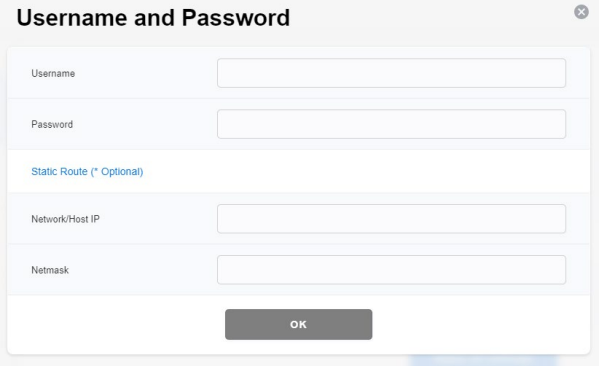
3.16 VPN-сервер

3.16.1 PPTP

1. В меню навигации выберите **VPN-сервер** > **PPTP** и переместите ползунок вправо (по умолчанию он отключен).
2. В поле **VPN-клиент (Максимум: 16)** нажмите ⊕ для добавления учетной записи.



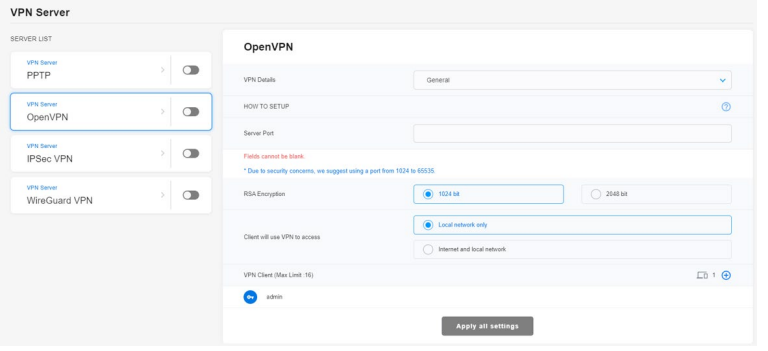
3. Введите «[Имя пользователя]» и «[Пароль]» и нажмите **OK**.



ПРИМЕЧАНИЕ: *[Имя пользователя]* и *[Пароль]* не могут быть изменены позже. Для получения дополнительной информации посетите https://www.asus.com/ru/support/FAQ/114892/.

3.16.2 OpenVPN

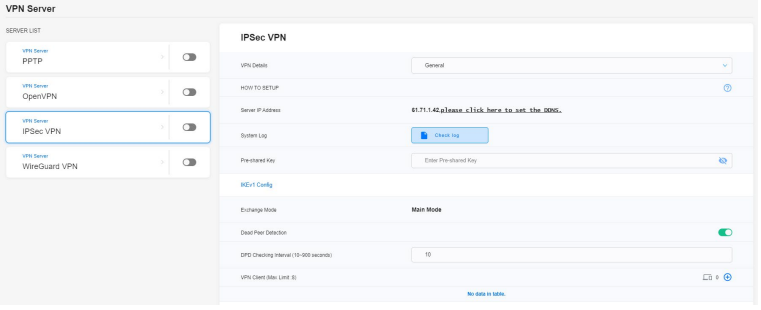
1. В меню навигации выберите **VPN-сервер** > **OpenVPN** и переместите ползунок вправо (по умолчанию он отключен).
2. В поле **Сведения о VPN** сконфигурируйте общие настройки.
3. Введите имя пользователя и пароль в пустой столбец.
4. В поле **VPN-клиент (Максимум: 16)** нажмите ⊕ для добавления учетной записи.
5. Пароль автоматически скрывается. Нажмите **Сохранить все настройки**.



ПРИМЕЧАНИЕ: Для получения дополнительной информации посетите https://www.asus.com/ru/support/FAQ/1008713/.

3.16.3 IPSec VPN

1. В меню навигации выберите **VPN-сервер** > **IPSec VPN** и переместите ползунок вправо (по умолчанию он отключен).
2. Введите ключ в поле **Pre-shared Key**.
3. В поле **VPN-клиент (Максимум: 8)** нажмите ⊕ для добавления учетной записи.
5. Введите *[Имя пользователя]* и *[Пароль]* и нажмите **Сохранить все настройки**.

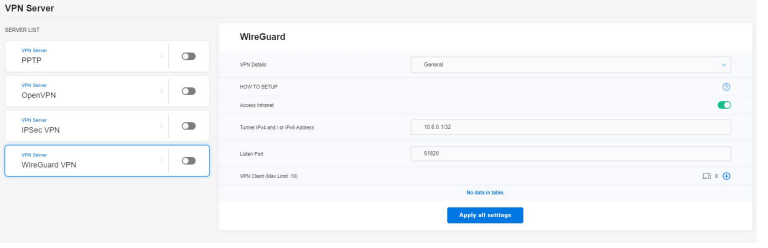


ПРИМЕЧАНИЕ: *[Имя пользователя]* и *[Пароль]* не могут быть изменены позже. Для получения дополнительной информации посетите https://www.asus.com/ru/support/FAQ/1044190/.

3.16.4 WireGuard VPN

1. В меню навигации выберите **VPN-сервер** > **WireGuard VPN**.
2. В поле **VPN-клиент (Максимум: 10)** нажмите ⊕ для добавления учетной записи. Для обычных устройств, таких как ноутбуки или смартфоны, нажмите **Применить**.
3. Нажмите **Сохранить все настройки** для включения WireGuard VPN.
4. Нажмите ··· для получения дополнительной информации.

ПРИМЕЧАНИЕ: В случает использования смартфона для подключения к WireGuard VPN скачайте приложение WireGuard из Google Play или App Store и отсканируйте код в приложении для загрузки конфигурационного файла.

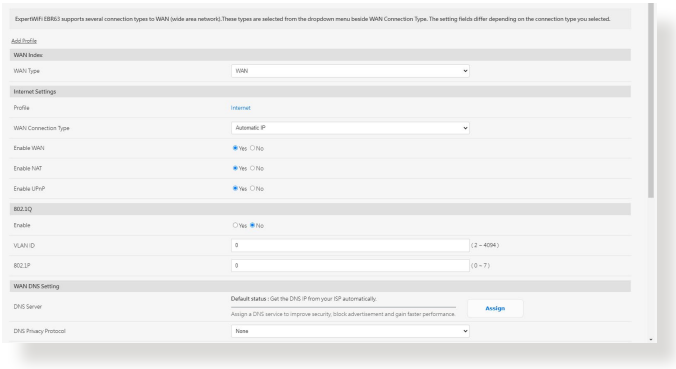


ПРИМЕЧАНИЕ: Для получения дополнительной информации посетите https://www.asus.com/ru/support/FAQ/1048280/.

3.17 WAN

3.17.1 Подключение к интернету

На странице подключение к интернету можно сконфигурировать параметры WAN подключения.



Для конфигурации параметров WAN:

1. В меню навигации выберите **Настройки** > **WAN** > **Подключение к интернету**.
2. Сконфигурируйте нижеследующие параметры. Когда закончите, нажмите **Применить**.
   - **Тип WAN-подключения**: Выберите тип вашего провайдера. Возможные варианты: автоматический IP, PPPoE, PPTP, L2TP или статический IP. Если вы не знаете тип подключения к интернету, проконсультируйтесь с вашим провайдером.
   - **Включить WAN**: Выберите **Да** для включения доступа к интернету. Выберите **Нет** для отключения доступа к интернету.
   - **Включить функцию трансляции сетевых адресов (NAT)**: NAT (трансляция сетевых адресов) представляет собой систему, в которой один публичный IP (WAN IP) используется для предоставления доступа в Интернет для сетевых клиентов с локальным IP-адресом. Локальный IP-адрес каждого сетевого клиента сохраняется в таблице NAT и используется для маршрутизации входящих пакетов данных.

- **Включить UPnP**: UPnP (Universal Plug и Play) позволяет использовать несколько устройств (роутеры, телевизоры, стереосистемы, игровые приставки, сотовые телефоны), которые будут управляться через IP-сети с или без централизованного управления через шлюз. UPnP соединяет компьютеры любых типов, обеспечивая единую сеть для удаленной конфигурации и передачи данных. Новое сетевое устройство обнаруживается автоматически с помощью UPnP. После подключения к сети, устройства можно дистанционно сконфигурировать для поддержки P2P-приложений, интерактивных игр, видеоконференций и веб- или прокси-серверов. В отличие от перенаправления портов, которое требует ручной настройки, UPnP автоматически настраивает роутер для принятия входящих соединений и передает запросы к определенному компьютеру в локальной сети.
- **Подключение к DNS серверу**: Позволяет роутеру автоматически получить IP-адрес DNS сервера от провайдера. DNS - это хост в интернете, который транслирует имена Интернет в IP-адреса.
- **Аутентификация**: Этот пункт может указываться некоторыми поставщиками услуг Интернета. Уточните у вашего провайдера и заполните в случае необходимости.
- **Имя хоста**: Это поле позволяет указать имя хоста для роутера. Обычно, это специальное требование от провайдера. Введите имя хоста здесь, если ваш провайдер назначил его для вашего компьютера.
- **MAC-адрес**: MAC (Media Access Control) адрес уникальный идентификатор для сетевого устройства. Некоторые провайдеры контролируют MAC-адреса устройств, подключенных к их оборудованию и могут запретить подключение устройства с незнакомым MAC-адресом. Во избежание проблем с подключением из-за незарегистрированного MAC-адреса возможны следующие действия:
  - Обратитесь к вашему провайдеру и попросите обновить MAC адрес.
  - Склонируйте или измените MAC-адрес роутера в соответствии с MAC адресом оригинального устройства..

3.17.2 Двойной WAN

Функция Dual WAN позволяет выбрать два подключения к интернету для роутера, первичный WAN и вторичный WAN.

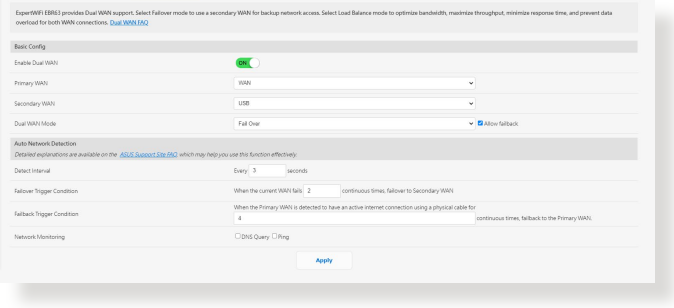
Для конфигурации Dual WAN:

1. В меню навигации выберите **Настройки** > **WAN** > **Dual WAN**.
2. В поле **Включить двойной WAN** нажмите **ВКЛ**.
3. Выберите свои **Первичный WAN** и **Вторичный WAN**. Доступны опции WAN, USB, Ethernet LAN и 2.5G WAN.
4. Выберите **Отказоустойчивость** или **Балансировка нагрузки**.

   Отказоустойчивость: Использование вторичного WAN в качестве резервного.

   Балансировка нагрузки: Оптимизации пропускной способности, уменьшение времени отклика и предотвращение перегрузки обоих WAN.
5. Нажмите **Применить**.

ПРИМЕЧАНИЕ: Подробное объяснение можно найти в FAQ на сайте ASUS https://www.asus.com/ru/support/FAQ/1011719.

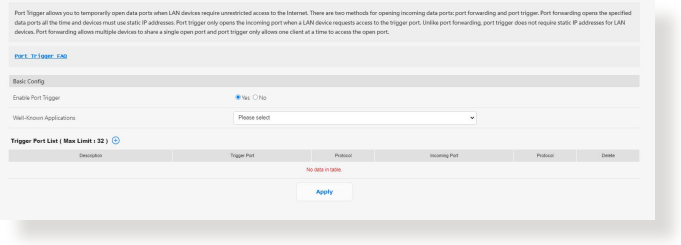


3.17.3 Переключение портов

Port Trigger позволяет временно включать порты, когда устройствам локальной сети требуется неограниченный доступ к Интернету. Существует два метода открытия портов входящих данных: переадресация портов и переключение портов.

- Переадресация портов позволяет постоянно использовать указанные порты и устройства должны использовать статические IP-адреса.
- Переключение портов включает входящий порт только тогда, когда устройство локальной сети запрашивает доступ к переключаемому порту.

В отличие от переадресации портов, переключение порта не требует статических IP-адресов для устройств локальной сети. Переадресация портов позволяет нескольким устройствам совместно использовать один открытый порт, а переключение портов позволяет только одному клиенту одновременно получать доступ к открытому порту.



Для настройки переключения портов:

1. В меню навигации выберите **Настройки** > **WAN** > **Переключение портов**.
2. Сконфигурируйте нижеследующие параметры. Когда закончите, нажмите **Применить**.
   - **Включить переключение портов**: Выберите **Да** для включения переключения портов.
   - **Известные приложения**: Выберите популярные игры и веб-службы для добавления их в список переключения

портов.

- **Описание**: Введите имя или описание службы.
- **Переключаемый порт**: Укажите переключаемый порт для приложения.
- **Протокол**: Выберите протокол TCP или UDP.
- **Входящий порт**: Укажите входящий порт для приема пакетов из интернета.

ПРИМЕЧАНИЯ:

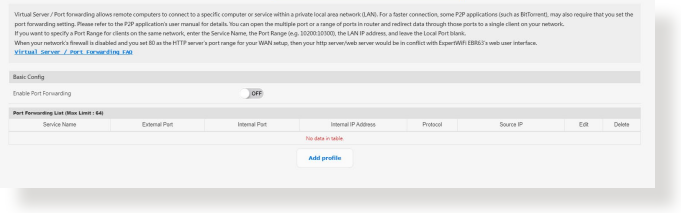
- При подключении к серверу IRC, клиентский компьютер создает исходящее соединение с использованием переключаемых портов в диапазоне 66660-7000. Сервер IRC реагирует путем проверки имени пользователя и создания нового соединения с клиентским ПК, используя входящий порт.
- Если переключение портов отключено, роутер обрывает соединение поскольку не может определить компьютер, запрашивавший доступ к IRC. Когда переключение портов включено роутер назначает входящий порт для получения входящих пакетов. Этот входящий порт закрывается через определенный период времени, поскольку роутер не уверен, что приложение все еще активно.
- Переключения портов может быть использовано только для одного сетевого клиента одновременно.
- Невозможно использовать приложение, использующее переключение портов на нескольких клиентах одновременно. При открытии одного порта несколькими клиентами, запросы с внешнего порта будут направлены клиенту, использующему данный порт последним.
- Для получения подробной информации посетите https://www.asus.com/ru/support/FAQ/114110.

3.17.4 Виртуальный сервер/Переадресация портов

Виртуальный сервер/Переадресация портов позволяет удаленным компьютерам подключаться к определенному компьютеру или службе в локальной сети (LAN). Для более быстрого соединения некоторые P2P-приложения (например, BitTorrent) также могут потребовать настройки переадресации портов. Подробную информацию можно найти в руководстве пользователя приложения P2P. Можно включить несколько портов или диапазон портов на роутере и перенаправлять данные через эти порты на один клиент в вашей сети.

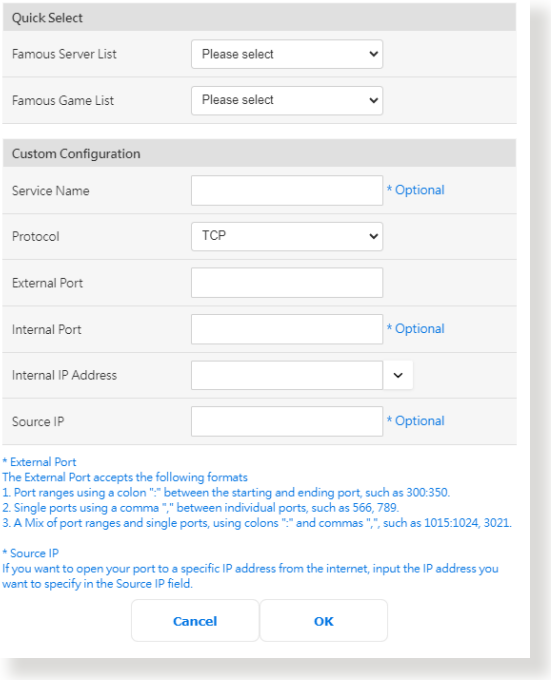
Если нужно задать диапазон портов для переадресации портов для сетевых клиентов, введите имя службы, диапазон портов (например, 10200:10300), IP-адрес и оставьте поле локальный порт пустым.

ПРИМЕЧАНИЕ: Когда выключена переадресация портов, роутер блокирует входящий трафик из Интернет кроме ответов на исходящие запросы из локальной сети. У сетевого клиента нет прямого доступа к интернету и наоборот.



Для настройки переадресации портов:

1. В меню навигации выберите **Настройки** > **WAN** > **Виртуальный сервер/Переадресация портов**.
2. Переместите переключатель в положение **ВКЛ** для включения переадресации портов, затем нажмите **Добавить профиль**. После настройки следующих параметров нажмите **ОК**.



- **Список известных серверов**: Укажите тип службы, к которой требуется доступ.
- **Список известных игр**: Этот пункт содержит список портов, необходимых для правильной работы популярных онлайн игр.
- **Имя службы**: Введите имя службы.
- **Протокол**: Выберите протокол. Если вы не уверены, выберите **BOTH**.
- **Внешний порт**: Принимаются следующие форматы:
  1) Диапазон портов с использованием двоеточия ":" между начальным и конечным портами, например 300:350
  2) Отдельные порты с запятой "," между ними, например 566, 789
  3) Комбинация диапазонов портов и отдельных портов с использованием двоеточия ":" и запятой ",", например, 1015:1024, 3021.
- **Внутренний порт**: Введите порт для пересылки пакетов. Оставь-

те это поле пустым, если хотите перенаправить входящие пакеты на диапазон портов.

- **Внутренний IP-адрес**: Введите IP-адрес клиента в локальной сети.
- **Исходный IP**: Если нужно открыть порт для определенного IP-адреса из Интернет, введите IP-адрес в это поле.

ПРИМЕЧАНИЕ: Для корректной переадресации используйте для локального клиента статический IP-адрес. Подробную информацию смотрите в разделе **3.9 LAN**.

Для проверки правильной настройки переадресации портов:

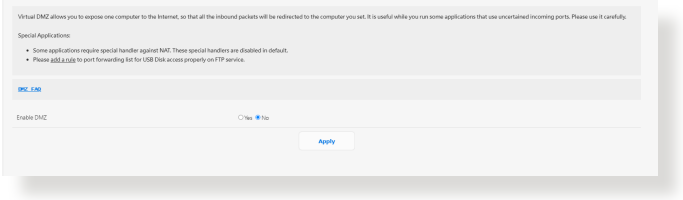
- Убедитесь, что ваш сервер работает.
- вам понадобится клиент, находящийся за пределами вашей локальной сети, но имеющий доступ к Интернет (называемый "Интернет-клиент"). Этот клиент не должен быть подключен к роутеру.
- В интернет-клиенте для доступа к серверу используйте WAN IP роутера. Если переадресация портов работает правильно, вы получите доступ к серверу.

Различия между переключением портов и перенаправлением портов:

- Переключение портов будет работать даже без настройки LAN IP-адреса. В отличие от перенаправления портов, которое требует статический LAN IP-адрес, переключение портов обеспечивает динамическое перенаправление портов с помощью маршрутизатора. Диапазоны портов настроены на прием входящих соединений в течение ограниченного периода времени. Переключение портов позволяет нескольким компьютерам запускать приложения, которые обычно требуют перенаправления портов вручную для каждого компьютера в сети.
- Переключение портов является более безопасным, чем перенаправление портов, поскольку входящие порты открыты не все время. Они открыты только когда приложение совершает исходящее соединение через переключаемый порт.

3.17.5 DMZ

Virtual DMZ позволяет отобразить в Интернете один компьютер, так что все входящие пакеты будут перенаправляться на выбранный компьютер. Эта функция полезна при работе с некоторыми приложениями, использующими неопределенные входящие порты. Используйте это осторожно.



Для настройки DMZ:

1. В меню навигации выберите **Настройки** > **WAN** > **DMZ**.
2. Сконфигурируйте параметры ниже. Когда закончите, нажмите **Применить**.
   - **IP-адрес видимой станции:** Введите LAN IP-адрес клиента, который будет использоваться для DMZ. Убедитесь, что сервер использует статический IP-адрес.

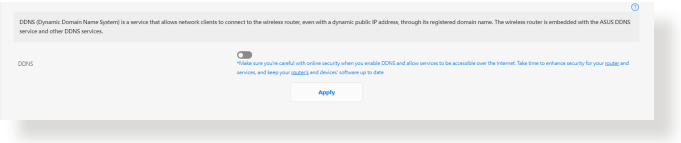
Для удаления DMZ:

1. Удалите LAN IP-адрес из поля **IP-адрес видимой станции**.
2. Когда закончите, нажмите **Применить**.

ПРИМЕЧАНИЕ: Для получения подробной информации посетите https://www.asus.com/ru/support/FAQ/1011723.

3.17.6 DDNS

DDNS (Dynamic Domain Name System) - служба, позволяющая сетевым клиентам подключаться к беспроводному роутеру, даже с динамическим внешним IP адресом, через зарегистрированное доменное имя. Роутер оснащен службой ASUS DDNS и другими службами DDNS.



Для настройки DDNS:

1. В меню навигации выберите **Настройки** > **WAN** > **DDNS**.
2. Сконфигурируйте нижеследующие параметры. Когда закончите, нажмите **Применить**.
   - **Включить DDNS клиент?**: Включение функции DDNS для возможности доступа к роутеру через доменное имя, а не через WAN IP.
   - **Сервер и имя хоста**: Выберите ASUS DDNS или другой DDNS. При использовании ASUS DDNS введите имя хоста в формате xxx.asuscomm.com (где xxx имя хоста).
   - При использовании другого DDNS выберите бесплатную пробную версию и зарегистрируйтесь на сайте. Введите имя пользователя или адрес электронной почты и пароль или DDNS ключ.
   - **Включить шаблон**: Включите шаблон, если он требуется для службы DDNS.

Примечания:

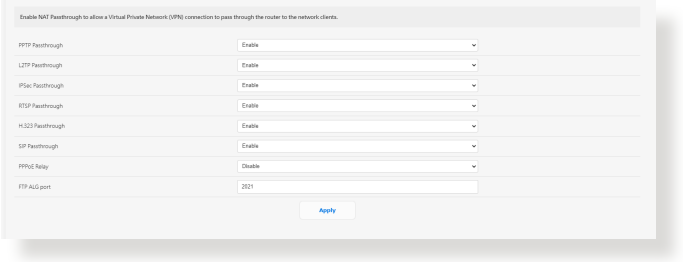
Служба DDNS сервис не будет работать при следующих условиях:

- Когда в беспроводной роутер использует приватный WAN IP адрес (192.168.x.x, 10.x.x.x или 172.16.x.x), как показано желтым текстом.
- Роутер может быть подключен к сети, которая использует несколько таблиц NAT.

3.17.7 NAT Passthrough

Включите NAT Passthrough для разрешения пакетам VPN проходить через роутер к сетевым клиентам.

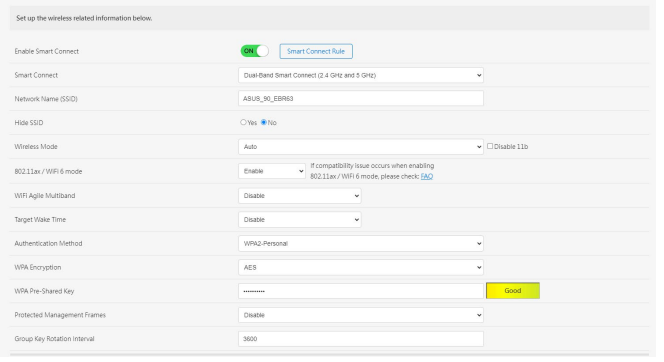
Для настройки NAT Passthrough перейдите в **Настройки** > **WAN** > **NAT Passthrough**. Когда закончите, нажмите **Применить**.



3.18 Беспроводная связь

3.18.1 Общие

На странице Общие можно сконфигурировать основные параметры беспроводной сети.



Для конфигурации основных параметры беспроводной сети:

1. В меню навигации выберите **Настройки** > **Wireless** > **Общие**.
2. Выберите 2,4 или 5 ГГц в качестве диапазона частот для беспроводной сети.
3. Для идентификации вашей беспроводной сети назначьте сетевое имя или SSID (Идентификатор беспроводной сети). Беспроводный устройства могут подключиться к беспроводной сети через назначенный SSID. SSID на информационном баннере обновляются при сохранении настроек.

ПРИМЕЧАНИЕ: Можно назначить уникальные SSID для частотных диапазонов 2,4 ГГц и 5 ГГц.

---

4. В поле **Скрыть SSID** выберите **Да** для предотвращения обнаружения SSID другими беспроводными устройствами. Когда эта функция включена, для доступа к беспроводной сети необходимо ввести SSID вручную.
5. Выберите беспроводной режим, определяющий тип беспроводных устройств, которые могут подключиться к роутеру:
   - **Авто**: Выберите **Авто** для разрешения подключения к роутеру устройств 802.11ax, 802.11ac, 802.11n, 802.11g и 802.11b.

6. Выберите ширину канала для обеспечения высокой скорости передачи данных:

   2,4 ГГц: Выберите частоту 40 МГц или 20 МГц в качестве пропускной способности беспроводной сети.

   5 ГГц: Выберите частоту 160 МГц, 80 МГц, 40 МГц и 20 МГц в качестве пропускной способности беспроводной сети.

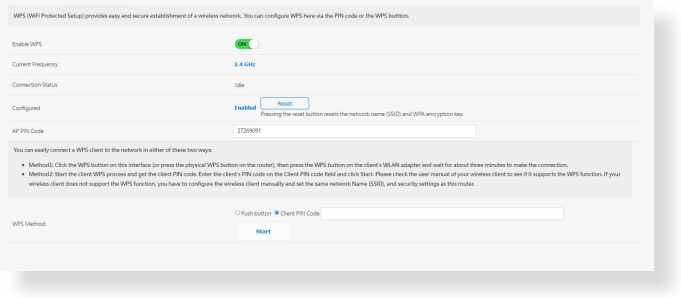
7. Выберите рабочий канал для беспроводного роутера. Выберите **Авто** для автоматического выбора канала с наименьшим количеством помех.

8. Выберите метод аутентификации:
   - **Open System**: Эта опция не обеспечивает безопасности.
   - **WPA/WPA2/WPA3-Personal**: Эта опция обеспечивает высокий уровень безопасности. Можно использовать WPA (с TKIP) или WPA2 (с AES). При выборе этой опции вы должны использовать шифрование TKIP + AES и ввести ключевую фразу WPA (сетевой ключ).
   - **WPA/WPA2/WPA3-Enterprise**: Эта опция обеспечивает очень высокий уровень безопасности. Она работает с интегрированным EAP-сервером или внешним RADIUS-сервером...

3.18.2 WPS

WPS (Wi-Fi Protected Setup) - стандарт беспроводной безопасности, позволяющий быстро подключать устройства к беспроводной сети. Функцию WPS можно сконфигурировать с помощью ПИН-кода или кнопки WPS.

ПРИМЕЧАНИЕ: Убедитесь, что устройства поддерживают WPS.



Для включения WPS в беспроводной сети:

1. В меню навигации выберите **Настройки** > **Wireless** > **WPS**.
2. В поле **Включить WPS** переместите ползунок в положение **ON**.
3. По умолчанию WPS использует 2,4 ГГц. Если нужно изменить частоту на 5 ГГц, в поле **Включить WPS** переместите ползунок в положение **OFF**, в поле **Текущая частота** щелкните **Переключить частоту**, затем в поле **Включить WPS** переместите ползунок в положение **ON** еще раз.

ПРИМЕЧАНИЕ: WPS поддерживает методы аутентификации Open system, WPA-Personal и WPA2-Personal. WPS не поддерживает Shared Key, WPA-Enterprise, WPA2-Enterprise и Radius.

3. В поле **Метод WPS** выберите **Кнопка Push** или **ПИН-код клиента**. При выборе **Кнопка** перейдите к шагу 4. При выборе **ПИН-код клиента** перейдите к шагу 5.
4. Для настройки WPS с помощью кнопки на роутере, выполните следующие действия:

a. Нажмите **Пуск** или нажмите кнопку WPS на задней панели роутера.

b. Нажмите кнопку WPS на роутере. Обычно помечено логотипом WPS.

ПРИМЕЧАНИЕ: Расположение кнопки WPS смотрите в документации беспроводного устройства.

c. Роутер начнет поиск доступных устройств. Если роутер не найдет ни одного устройства, он переключится в режим ожидания.

5. Для настройки WPS с помощью ПИН-кода клиента выполните следующие действия:

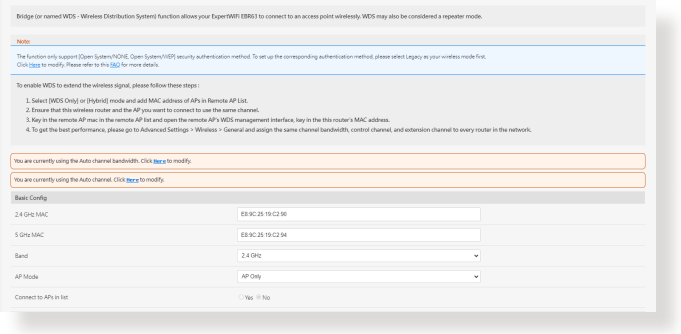
   a. Найдите WPS ПИН-код в руководстве пользователя беспроводного устройства или на самом устройстве.

   b. Введите ПИН-код клиента в текстовое поле.

   c. Нажмите **Пуск** для переключения роутера в режим поиска WPS. Индикаторы роутера быстро мигают до завершения настройки WPS.

3.18.3 WDS (мост)

Мост или WDS (Wireless Distribution System) позволяет использовать роутер для соединения беспроводных устройств по радиоканалу для увеличения зоны покрытия беспроводной сети. Он может также рассматриваться в качестве беспроводного повторителя.

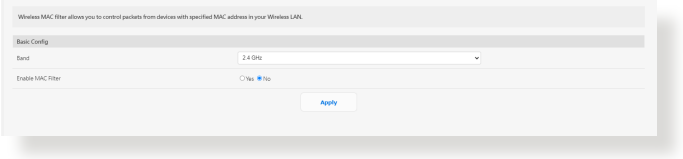


Для настройки беспроводного моста:

1. В меню навигации выберите **Настройки** > **Wireless** > **WDS**.
2. Выберите режим **WDS Only** или **Hybrid** и добавьте MAC-адреса точек доступа в **Список удаленных AP (макс.: 4)**.
3. Убедитесь, что этот роутер и точка доступа, к которой нужно подключиться, используют один канал.
4. Введите MAC-адрес удаленной точки доступа в список. В интерфейс управления WDS удаленной точки доступа введите MAC адрес этого роутера.
5. Для получения максимальной производительности перейдите в **Настройки** > **Беспроводная связь** > **Общие** и назначьте одинаковую полосу пропускания для управляющего и дополнительного каналов для каждого роутера в сети.

3.18.4 Фильтр MAC адресов беспроводной сети

Фильтр MAC адресов беспроводной сети позволяет контролировать пакеты с указанными MAC-адресами в беспроводной сети.

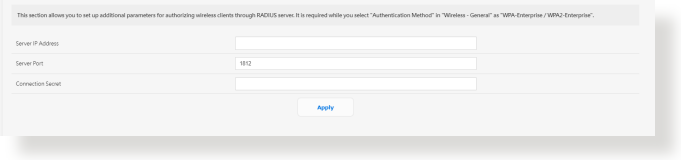


Для настройки фильтра MAC адресов беспроводной сети:

1. В меню навигации выберите **Настройки** > **Беспроводная связь** > **Фильтр MAC-адресов беспроводной сети**.
2. В поле **Включить MAC фильтр** выберите **Да**.
3. В поле **Режим фильтра MAC-адресов** выберите **Принять** или **Отклонить**.
   - Выберите **Принять** для разрешения доступа к беспроводной сети устройствам из списка MAC-фильтра.
   - Выберите **Отклонить** для запрещения доступа к беспроводной сети устройствам из списка MAC-фильтра.
4. В списке MAC-фильтра, нажмите ⊕ и введите MAC-адрес беспроводного устройства.
5. Нажмите **Применить**.

3.18.5 Настройка RADIUS

RADIUS (Служба удаленной аутентификации пользователей) позволяет настраивать дополнительные параметры для авторизации беспроводных клиентов через сервер RADIUS. Это требуется при выборе параметра **WPA-Enterprise / WPA2-Enterprise** в качестве метода аутентификации.



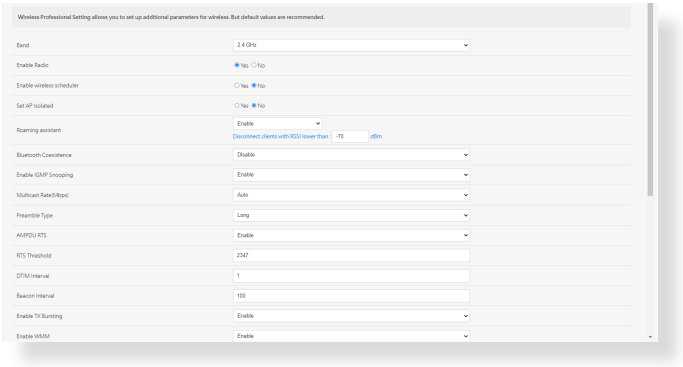
Для настройки параметров RADIUS:

1. Убедитесь, что режим аутентификации беспроводного роутера установлен в значение WPA-Enterprise или WPA2-Enterprise.
2. В меню навигации выберите **Настройки** > **Беспроводная связь** > **Настройка RADIUS**.
3. Выберите диапазон частот.
4. В поле **IP-адрес сервера** введите IP-адрес сервера RADIUS.
5. В поле **Ключ соединения** назначьте пароль для доступа к серверу RADIUS.
6. Нажмите **Применить**.

3.18.6 Профессиональный

Профессиональная настройка позволяет настраивать дополнительные параметры беспроводной сети.

ПРИМЕЧАНИЕ: Мы рекомендуем использовать значения по умолчанию.



На экране **Профессиональный** можно сконфигурировать следующее:

- **Диапазон**: Выберите диапазон, настройки которого нужно изменить.
- **Включить радиомодуль**: Выберите **Да** для включения радиомодуля. Выберите **Нет** для отключения радиомодуля.
- **Включить беспроводный планировщик**: Можно выбрать использование 12-часового или 24-часового формата. Цвет в таблице означает Разрешить или Запретить. Нажмите каждую ячейку для изменения настройки времени в будние дни, затем нажмите **OK**.

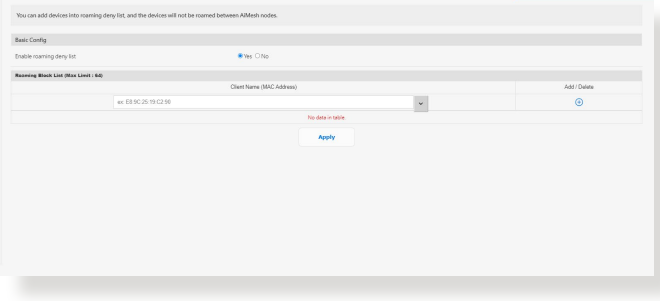
- **Изолировать точку доступа**: Изолирование точки доступа запрещает беспроводным устройствам в сети подключаться друг к другу. Эта функция полезна когда к вашей сети подключается много гостей. Выберите **Да** для включения этой функции или **Нет** для отключения.
- **Помощник при роуминге**: При использовании нескольких точек доступа или беспроводных повторителей иногда не клиенты могут автоматически подключиться к точке доступа с лучшим сигналом, поскольку они все еще подключены к основному беспроводному роутеру. Включение этой опции позволит клиенту отключиться от основного беспроводного роутера, если мощность сигнала ниже определенного порога и подключиться к точке доступа с более сильным сигналом.
- **Включить IGMP Snooping**: Включение этой функции позволяет отслеживать сетевой трафик IGMP для оптимизации многоадресного трафика.
- **Скорость многоадресной передачи (Мбит/с)**: Скорость многоадресной передачи или нажмите **Отключить** для отключения многоадресной передачи.
- **Тип преамбулы**: Тип преамбулы определяет продолжительность времени, которое требуется роутеру для CRC (Cyclic Redundancy Check). CRC - это метод обнаружения ошибок во время передачи данных. Выберите **Короткая** для беспроводной сети с большим трафиком. Выберите **Длинная** для беспроводной сети со старыми беспроводными устройствами.
- **AMPDU RTS**: Включение этой функции позволяет создать группу кадров перед их передачей и использовать RTS для каждого AMPDU для связи между устройствами 802.11g и 802.11bNone.
- **Порог RTS**: Для беспроводных сетей с большим трафиком и большим количеством беспроводных устройств выберите низкий порог RTS.
- **Интервал DTIM**: Интервал DTIM (Delivery Traffic Indication Message) или Data Beacon Rate - это интервал времени перед отправкой сигнала беспроводному устройству в спящем режиме, указывая, что пакет данных ожидает доставки. Значение по умолчанию: три миллисекунды.
- **Сигнальный интервал**: Сигнальный интервал - это период

времени между DTIM-пакетами. Значение по умолчанию: 100 миллисекунд... Для нестабильного беспроводного подключения или для роуминга устройств рекомендуется низкое значение.

- **Включить TX Bursting**: TX Bursting улучшает скорость передачи данных между беспроводным роутером и устройствами 802.11g.
- **Включить WMM APSD**: Включить WMM APSD (Автоматический переход в режим энергосбережения) для управления энергосбережением беспроводных устройств. Выберите **Отключить** для отключения WMM APSD.

3.18.7 Черный список роуминга

Эта функция позволяет добавлять устройства в черный список роуминга и запрещать им роуминг между узлами AiMesh.



4 Утилиты

ПРИМЕЧАНИЯ:

- Скачайте и установите утилиты с сайта ASUS:
  - Device Discovery v1.4.7.1 с http://dlcdnet.asus.com/pub/ASUS/**LiveUpdate/Release/Wireless/Discovery.zip**
  - Firmware Restoration v1.9.0.4 с http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
  - Windows Printer v1.0.5.5 с http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip
- Утилиты не поддерживаются в MAC OS.

4.1 Обнаружение устройства

Device Discovery - ASUS WLAN утилита, которая обнаруживает роутер и позволяет его конфигурировать.

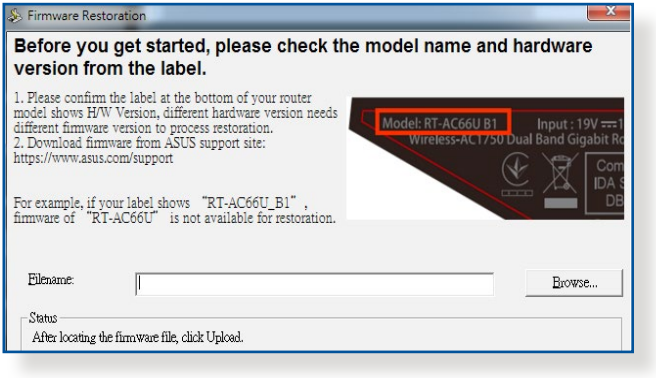
Для запуска утилиты Device Discovery:

- Перейдите **Пуск > Программы > ASUS Utility > Wireless Router > Device Discovery**.

ПРИМЕЧАНИЕ: При установке роутера в режим точки доступа, вам необходимо использовать утилиту Device Discovery для получения IP-адреса роутера.

4.2 Восстановление прошивки

Firmware Restoration - утилита, которая используется в случае ошибки при обновлении прошивки роутера. Она загружает указанную прошивку. Процесс занимает около трех минут.



ОСТОРОЖНО!Перед использованием утилиты Firmware Restoration переключите роутер в режим восстановления.

ПРИМЕЧАНИЕ: Эта функция не поддерживается в MAC OS.

Для запуска утилиты Firmware Restoration:

1. Отключите питание от роутера.
2. Удерживая кнопку Reset, расположенную на задней панели, подключите питание к роутеру. Отпустите кнопку сброса когда индикатор питания, расположенный на передней панели, начнет медленно мигать, означая, что роутер находится в режиме восстановления.
3. Установите статический IP на вашем компьютере и используйте следующие настройки TCP/IP:

   IP-адрес: 192.168.1.x

   Маска подсети: 255.255.255.0

4. Перейдите **Пуск > Программы > ASUS Utility > Wireless Router > Firmware Restoration**.
5. Укажите файл и нажмите **Upload**.

ПРИМЕЧАНИЕ: Это не утилита обновления прошивки и не может быть использована при рабочем роутере. Обычное обновление прошивки можно выполнить через веб-интерфейс. Подробную информацию смотрите в разделе **Глава 3: Конфигурация EBR63**.

5 Устранение неисправностей

В этом разделе представлены инструкции для решения некоторых наиболее часто встречающихся общих проблем с роутером. Если вы столкнулись с проблемами, не упомянутыми в этой главе, посетите сайт ASUS https://www.asus.com/ru/support/ для получения дополнительной информации о продукте или обратитесь в службу техподдержки ASUS.

5.1 Устранение основных неисправностей

При возникновении проблем с роутером сначала попробуйте выполнить инструкции из этого раздела.

Обновите прошивку до последней версии.

1. В меню навигации выберите **Настройки** > **Администрирование** > **Обновление прошивки**. Нажмите **Проверить** для проверки наличия последней версии прошивки.
2. Если доступна новая прошивка, посетите сайт ASUS и скачайте ее.
3. На странице **Обновление прошивки** нажмите **Browse** для нахождения прошивки.
4. Нажмите **Загрузить** для обновления прошивки.

Последовательность перезапуска сети:

1. Выключите модем.
2. Отключите модем.
3. Выключите роутер и компьютеры.
4. Подключите модем.
5. Включите модем и подождите 2 минуты.
6. Включите роутер и подождите 2 минуты.
7. Включите компьютеры.

Убедитесь в правильности установки Ethernet-кабеля.

- При правильном подключении Ethernet-кабеля к модему индикатор WAN будет гореть.
- При правильном подключении Ethernet-кабеля к включенному компьютеру индикатор LAN будет гореть.

Убедитесь, что настройки беспроводной сети компьютера совпадают с роутером.

- При подключении компьютера к роутеру убедитесь в правильности SSID (имя беспроводной сети), шифрования и пароля.

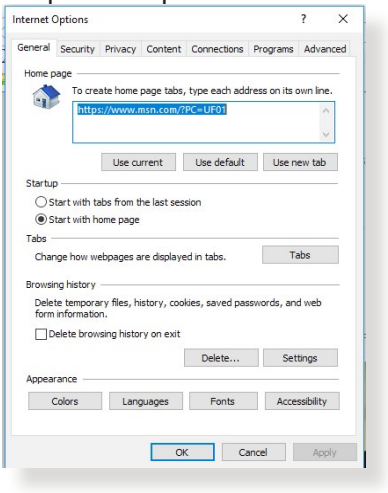
Убедитесь в правильности сетевых настроек.

- Каждый сетевой клиент должен иметь действительный IP-адрес. Для назначения IP-адресов компьютерам вашей сети рекомендует использовать DHCP-сервер роутера.
- Некоторые провайдеры требуют использовать MAC-адрес компьютера, используемого при первом подключении. MAC-адрес можно посмотреть в веб-интерфейсе на странице **Информационная панель** > **Клиенты**.

5.2 Часто задаваемые вопросы (FAQ)

Невозможно войти в веб-интерфейс роутера через браузер

- Если ваш компьютер подключен, проверьте соединение Ethernet-кабеля и состояние индикатора, как описано в предыдущем разделе.
- Убедитесь, что вы используете правильные логин и пароль. Имя пользователя и пароль по умолчанию можно найти на этикетке в нижней части EBR63. Убедитесь, что режим Caps Lock отключен при вводе данных.
- Удалите куки-файлы в браузере.. В браузере Internet Explorer выполните следующие действия:
  1. Запустите Internet Explorer, затем нажмите **Сервис** > **Свойства обозревателя**.
  2. На вкладке **Общие** в области **Просмотр истории** нажмите **Удалить...**, выберите **Временные файлы Интернета** и **Файлы cookie и данные сайта** и нажмите **Удалить**.



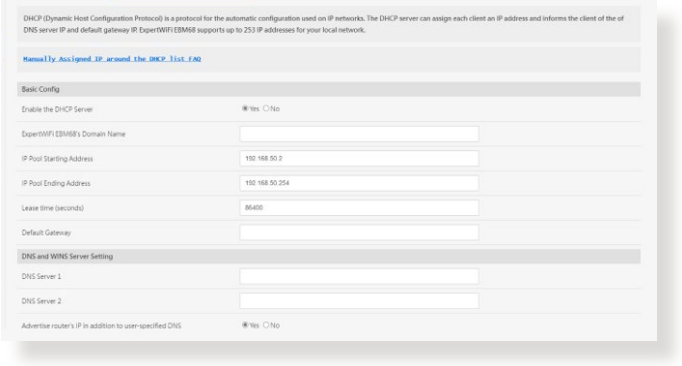
ПРИМЕЧАНИЯ:

- Команды для удаления куки- файлов могут варьироваться в зависимости от браузера.
- Отключите использование прокси-сервера, подключение удаленного доступа, а также настройте TCP/IP для автоматического получения IP-адреса. Подробную информацию смотрите в первой главе этого руководства.
- Убедитесь, что используются Ethernet кабели CAT5e или CAT6.

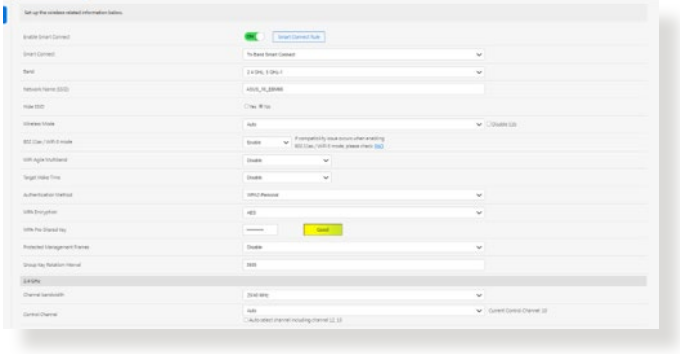
Клиент не может установить беспроводное соединение с роутером.

ПРИМЕЧАНИЕ: При возникновении проблем с подключением к сети 5 ГГц убедитесь, что ваше беспроводное устройство поддерживает частоту 5 ГГц или является двухдиапазонным.

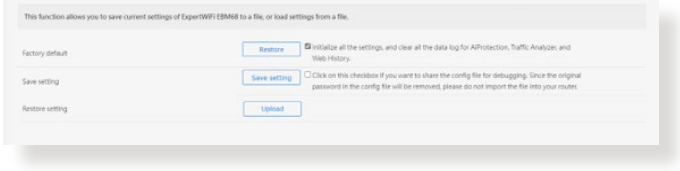
- **Вне зоны покрытия:**
  - Поместите роутер ближе к беспроводному клиенту.
  - Попробуйте настроить антенны роутера как описано в разделе **1.4 Размещение роутера**.
- **DHCP-сервер отключен:**
  1. Войдите в веб-интерфейс. Перейдите в **Информационная панель** > **Клиенты** и найдите устройство, которое нужно подключить к роутеру.
  2. Если **Информационная панель** не отображает устройство, перейдите в **Настройки** > **LAN** > **DHCP-сервер**.



- SSID скрыт. Если устройство может найти SSID другого роутера, но не может найти SSID вашего роутера, перейдите в **Настройки** > **Беспроводная связь** > **Общие**, затем выберите **Нет** в поле **скрыть SSID** и выберите **Авто** в поле **Канал управления**.



- При использовании беспроводного адаптера убедитесь, что используемый беспроводной канал доступен в вашей стране или регионе. Если нет, настройте канал, полосу пропускания и беспроводной режим.
- Если вы все еще не можете подключиться к роутеру, сбросьте его к заводским настройкам по умолчанию. В веб-интерфейсе перейдите в **Настройки** > **Администрирование** > **Восстановить/сохранить/загрузить настройки** и нажмите **Восстановить**.



Интернет недоступен.

- Убедитесь, что роутер может подключиться к вашему провайдеру. Для этого запустите веб-интерфейс и перейдите в **Информационная панель** и проверьте состояние Интернет.
- Если роутер не может подключиться к вашему провайдеру, попробуйте переподключить сеть как описано в разделе **Последовательность перезапуска сети**..
- Если все еще нет доступа к интернету, попробуйте перезагрузить компьютер и проверить IP-адрес и адрес шлюза.
- Проверьте индикаторы состояния на ADSL модеме и беспроводном роутере. Если индикатор WAN на роутере не горит, убедитесь, что все кабели правильно подключены.

Вы забыли SSID (имя сети) или сетевой пароль

- Установите новый SSID и ключ шифрования через проводное соединение (Ethernet-кабель). Войдите в веб-интерфейс, перейдите в **Информационная панель**, нажмите иконку роутера и введите новый SSID и ключ шифрования, затем нажмите **Применить**.
- Выполните сброс роутера к настройкам по умолчанию. Войдите в веб-интерфейс, перейдите в **Настройки** > **Администрирование** > **Восстановить/сохранить/загрузить настройки** и нажмите **Восстановить**. Имя пользователя и пароль по умолчанию можно найти на этикетке в нижней части EBR63.

Как сбросить систему к настройкам по умолчанию?

- Перейдите в **Настройки** > **Администрирование** > **Восстановить/сохранить/загрузить настройки** и нажмите **Восстановить**.

Ошибка обновления прошивки.

Переключите роутер в режим восстановления и запустите утилиту Firmware Restoration. Информацию по использованию утилиты Firmware Restoration смотрите в разделе **4.2 Восстановление прошивки**.

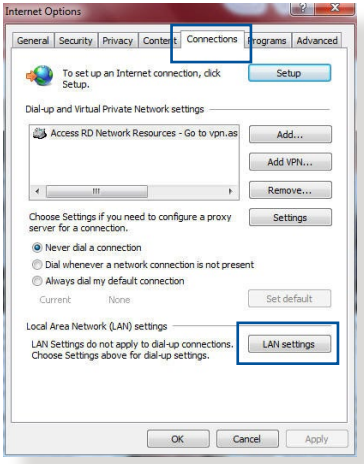
Невозможно подключиться к веб-интерфейсу

Перед конфигурацией роутера выполните инструкции данного раздела для конфигурации компьютера и сетевых клиентов.

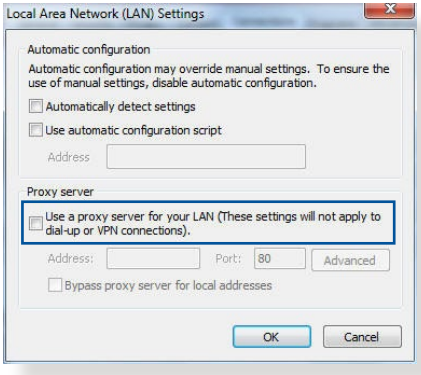
A. Отключите прокси-сервер, если он включен.

Windows

1. Нажмите **Пуск > Internet Explorer** для запуска браузера.
2. Выберите **Сервис** > **Свойства обозревателя** > **Подключения** > **Настройка локальной сети**.

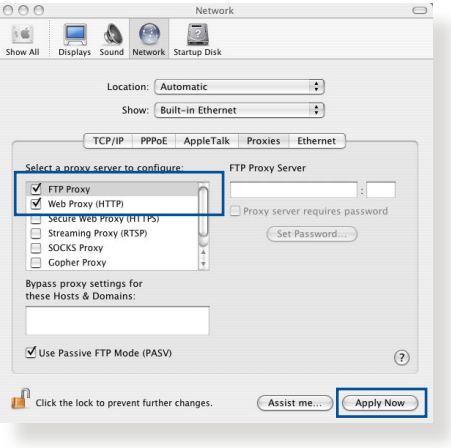


3. На экране **настройки локальной сети** отключите использование прокси-сервера для локальной сети.
4. Нажмите **OK** когда закончите.



MAC OS

1. В браузере Safari нажмите **Safari** > **Preferences** > **Advanced** > **Change Settings...**
2. На экране сеть снимите флажки **FTP Proxy** и **Web Proxy (HTTP)**.
3. Когда закончите, нажмите **Применить**.

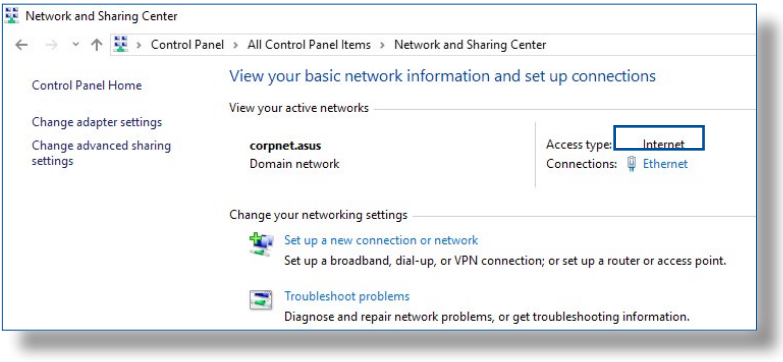


ПРИМЕЧАНИЕ: Для получения подробной информации по отключению использования прокси-сервера, обратитесь к справке браузера.

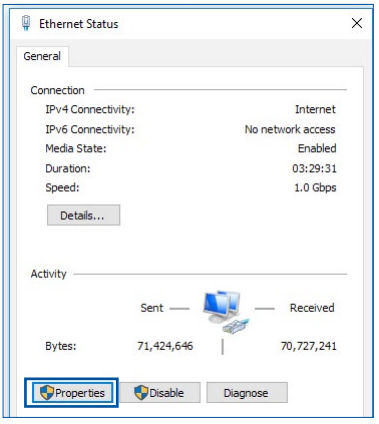
B. Настройте TCP/IP для автоматического получения IP-адреса.

Windows

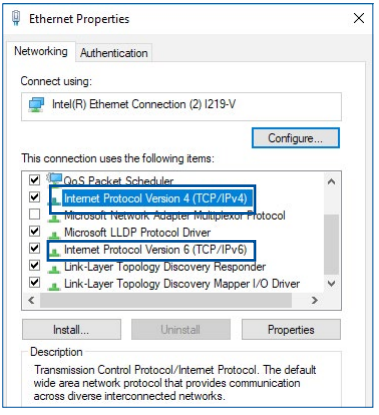
1. Нажмите **Пуск** > **Панель управления** > **Центр управления сетями и общим доступом**, затем нажмите сетевое подключение для отображения его состояния.



2. Нажмите **Свойства** для открытия окна свойств Ethernet.



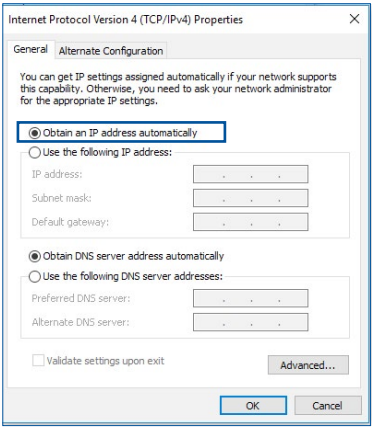
3. Выберите **Протокол Интернета версии 4(TCP/IPv4)** или **Протокол Интернета версии 6(TCP/IPv6)**, затем нажмите **Свойства**.



4. Выберите **Получить IP-адрес автоматически** для автоматического получения IP-адреса.

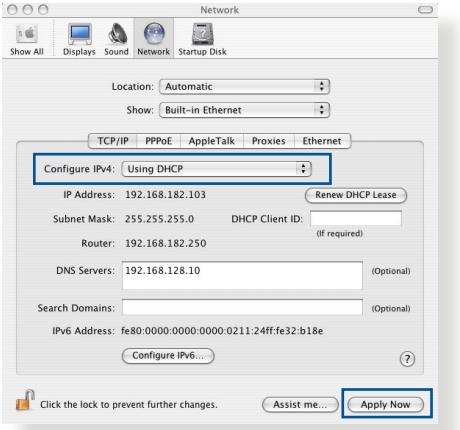
   Выберите **Получить IPv6-адрес автоматически** для автоматического получения IP-адреса IPv6.

5. Нажмите **ОК** когда закончите.



MAC OS

1. Нажмите иконку Apple , расположенную в левом верхнем углу экрана.
2. Нажмите **System Preferences > Network > Configure...**
3. На вкладке TCP/IP в выпадающем списке **Configure IPv4** выберите **Using DHCP**.
4. Когда закончите, нажмите **Применить**.

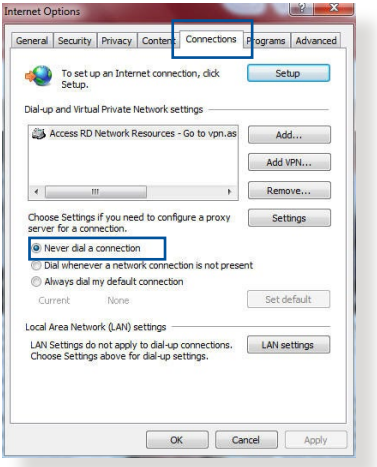


ПРИМЕЧАНИЕ: Подробную информацию по конфигурации настроек TCP/IP смотрите в справке к вашей операционной системе.

C. Отключите подключение удаленного доступа.

Windows

1. Нажмите **Пуск** > **Internet Explorer** для запуска браузера.
2. Выберите **Сервис** > **Свойства обозревателя** > **Подключения**.
3. Установите флажок **Никогда не использовать коммутируемые подключения**.
4. Нажмите **OK** когда закончите.



ПРИМЕЧАНИЕ:Для получения подробной информации по отключению удаленного доступа, обратитесь к справке браузера.

Приложение

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Подробную информацию смотрите на нашем сайте. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee

cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Правила безопасности

При использовании устройства всегда соблюдайте меры предосторожности, включая, помимо прочего, следующие:

ВНИМАНИЕ!

- Шнур питания должен быть подключен к розетке с заземлением. Подключайте устройство к ближайшей, легкодоступной розетке.
- Если устройство неисправно, не пытайтесь исправить его самостоятельно. Эти ограничения рассчитаны на обеспечение защиты в разумных пределах от вредоносных воздействий при установке в жилом помещении.
- Не пользуйтесь поврежденными сетевыми шнурами, аксессуарами и периферийными устройствами.
- Не устанавливайте это оборудование на высоту более 2 метров.
- Рекомендуется использовать продукт при температуре от 0°C до 40°C.
- Перед использованием устройства прочтите инструкции по эксплуатации и ознакомьтесь с допустимым температурным диапазоном.
- Будьте осторожны при использовании данного устройства в аэропортах, больницах, заправочных станциях и гаражах.
- Помехи для медицинских устройств: поддерживайте минимальное расстояние (не менее 15 см) между имплантированными медицинскими устройствами и продуктами ASUS для снижения риска возникновения помех.
- Используйте устройство в условиях хорошего приема для уменьшения уровня излучения.
- Установите устройство подальше от беременных женщин и нижней части живота подростков.
- Не используйте устройство при обнаружение видимых дефектов, когда оно мокрое, повреждено или модифицировано. Обратитесь за помощью в сервисный центр.

ВНИМАНИЕ!

- Не устанавливайте устройство на неровную или неустойчивую поверхность.
- Не кладите на устройство посторонние предметы. Не подвергайте устройство механическим воздействиям, например надавливание, сгибание, прокалывание или измельчение.
- Не разбирайте, не открывайте, не нагревайте, не сжигайте, не красьте и не засовывайте в отверстия устройства посторонние предметы.
- Обратите внимание на этикетку на нижней стороне устройства и убедитесь, что ваш блок питания поддерживает соответствующее напряжение.
- Храните устройство вдали от огня и источников тепла.
- Не подвергайте воздействию жидкостей и не используйте в условиях повышенной влажности. Не пользуйтесь устройством во время грозы.
- Подключайте выходные цепи PoE данного изделия исключительно к сетям PoE, без маршрутизации на внешние устройства.
- Во избежание поражения электричеством, отключите шнур питания от розетки прежде, чем переносить систему с места на место.
- Используйте только аксессуары, одобренные производителем устройства для использования с этой моделью. Использование других типов аксессуаров может привести к аннулированию гарантии или нарушению местных правил и законов, а также может представлять угрозу безопасности. Информацию о наличии авторизованных аксессуаров можно узнать у продавца.
- Использование устройства способом, не рекомендованным в прилагаемых инструкциях, может привести к возгоранию или травме.

Сервис и поддержка

Посетите наш сайт https://www.asus.com/ru/support/.