R26249

REPUBLIC OF GAMERS

# USER MANUAL

ROG Rapture GT6

ROG Rapture AX10000 Tri-band Gaming Mesh Router

ASUS

R26249
Проверенное издание V3
Апрель 2025

# Оглавление

# Оглавление

# Оглавление

# 1 Информация о беспроводном роутере

## 1.1 Приветствие!

Благодарим Вас за приобретение беспроводного роутера ROG Rapture!

Мощный и стильный роутер использует частотные диапазоны 2.4ГГц, 5ГГц-1 и 5ГГц-2 и поддерживает потоковое вещание в высоком качестве, SMB, UPnP AV и FTP сервера для круглосуточного доступа к файлам, одновременную работу до 300,000 сессий; а также технологию ASUS Green Network, обеспечивающую энергосбережение до 70%.

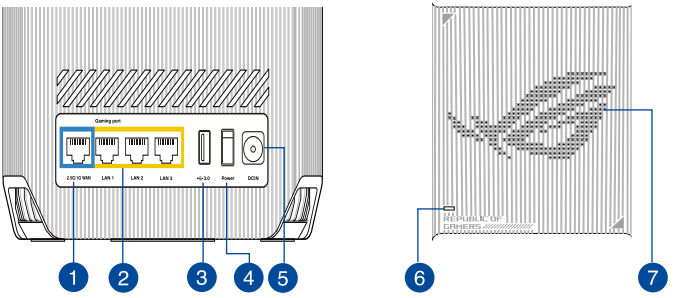
## 1.2 Комплект поставки

- ☑ Игровой роутер ROG Rapture
- ☑ Блок питания
- ☑ Сетевой кабель (RJ-45)
- ☑ Краткое руководство

**ПРИМЕЧАНИЯ:**

- Если какие-либо элементы комплекта поставки отсутствуют или повреждены, обратитесь в службу техподдержки ASUS. Обратитесь к разделу **Сервис и поддержка** 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 | **Порт WAN 2,5 Гбит/с / 1Гбит/с (Интернет)**<br>Подключение сетевого кабеля для установки подключения WAN 2.5/1 Гбит/с. |
| 2 | **Разъемы LAN 1-3**<br>Подключение сетевых устройств. |
| 3 | **Разъем USB 3.2 Gen 1x1**<br>Подключение устройств USB 3.2 Gen 1x1, например жесткого диска USB или USB флэш-диска. |
| 4 | **Кнопка питания**<br>Нажмите эту кнопку включения/отключения системы. |
| 5 | **Разъем питания (DCIN)**<br>Подключение блока питания. |
| 6 | **Индикатор** |
| | Горит синим цветом: роутер готов к настройке. |
| | Горит белым цветом: роутер подключен к сети и готов к работе |
| | Горит красным цветом: Роутер не подключен к интернету / ваш узел отключен от роутера |
| | Горит желтым цветом Плохое качество подключения между узлом и роутером |
| 7 | **Aura RGB:**<br>Позволяет пользователям настраивать или включать / выключать Aura RGB из информационной панели. |

**ПРИМЕЧАНИЯ:**

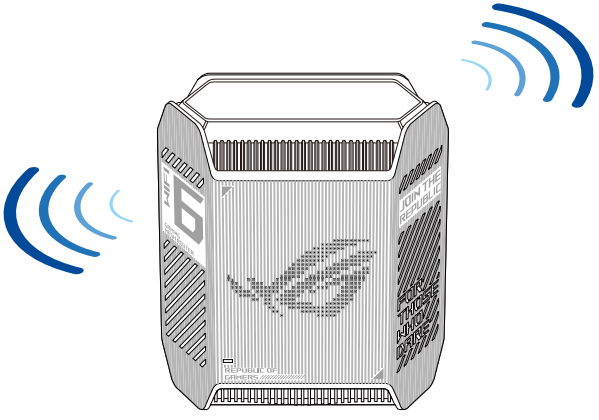
- Используйте только блок питания, поставляемый с устройством. При использовании других блоков питания устройство может быть повреждено.
- **Спецификация:**

| | | | |
|---|---|---|---|
| **Блок питания** | Выходная мощность: 19 В с максимальным током 2,37 А<br>19,5 В с максимальным током 2,31 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 https://www.asus.com.



## 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
- Это лучше убрать
- 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 в трех диапазонах 2.4ГГц, 5ГГц-1 и 5ГГц-2. Это позволяет выполнять интернет-серфинг и работать с электронной почтой, используя частотный диапазон 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, (запятая) могут не поддерживать частотный диапазон 5 ГГц. Обратитесь к спецификации устройства.
- Длина Ethernet кабеля, используемого для подключения сетевых устройств не должна превышать 100 метров.

**ВАЖНО!**

- У некоторых беспроводных адаптеров могут возникнуть проблемы при подключении к точкам доступа Wi-Fi 802.11ax.
- При возникновении такой проблемы убедитесь, что вы используете драйвер последней версии. Для получения драйверов, обновлений и прочей информации посетите сайт производителя.
  - Realtek: https://www.realtek.com
  - Mediatek: https://www.mediatek.com
  - Intel: https://www.intel.com/

# 2 Начало работы

## 2.1 Настройка роутера

**ВАЖНО!**

- 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!**

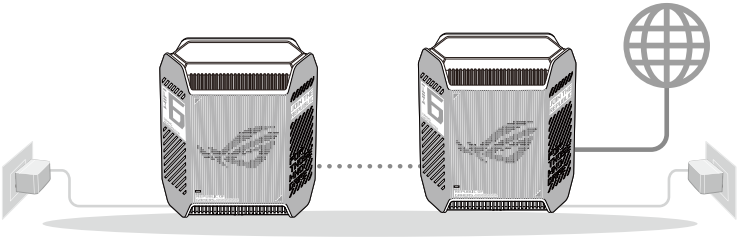
- Шнур питания должен быть подключен к розетке с заземлением. Подключайте устройство к ближайшей, легкодоступной розетке.
- Если устройство неисправно, не пытайтесь исправить его самостоятельно. Эти ограничения рассчитаны на обеспечение защиты в разумных пределах от вредоносных воздействий при установке 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.

## A. Проводное подключение

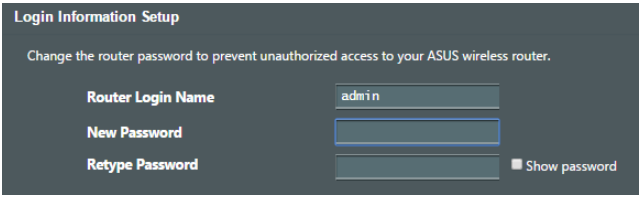
**ПРИМЕЧАНИЕ:** Для проводного подключения можно использовать любой (прямой или перекрестный) сетевой кабель.

**Для настройки беспроводного роутера через проводное подключение:**

1. Подключите роутер к электрической розетке и включите его. С помощью сетевого кабеля подключите компьютер к LAN порту роутера.



2. Веб-интерфейс запускается автоматически при открытии браузера. Если он не запустился автоматически, введите http://www.asusrouter.com
3. Задайте пароль роутера для предотвращения несанкционированного доступа.



## B. Беспроводное подключение

**Для настройки беспроводного роутера через беспроводное подключение:**

1. Подключите роутер к электрической розетке и включите его.


2. Подключитесь к сети (SSID), указанной на этикетке на задней стороне роутера. В целях безопасности смените SSID и назначьте пароль.

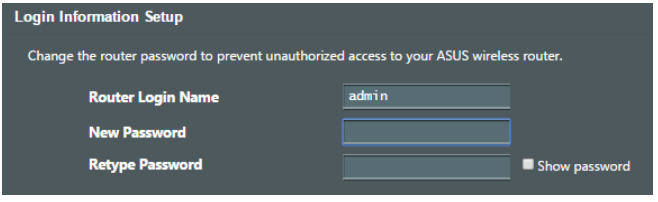

| Имя Wi-Fi (SSID): | ASUS_XX_GT6 |
|---|---|

* **XX** относится к двум последним цифрам MAC-адреса диапазона 2,4 ГГц. Его можно найти на этикетке на задней панели роутера.

3. После подключения, веб-интерфейс запускается автоматически при открытии браузера. Если он не запустился автоматически, введите http://www.asusrouter.com.
4. Задайте пароль роутера для предотвращения несанкционированного доступа.

**ПРИМЕЧАНИЯ:**

- Подробную информацию о подключении к беспроводной сети смотрите в руководстве пользователя для WLAN адаптера.
- Информацию по настройке параметров безопасности смотрите в разделе **Настройка параметров безопасности беспроводной сети** данного руководства.



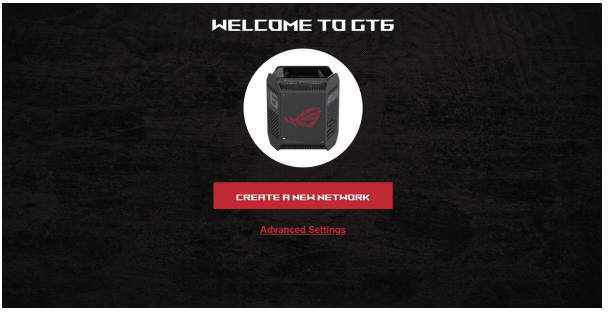
## 2.2 Быстрая настройка Интернет (QIS) с автоопределением

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.

**Для использования QIS с автоматическим определением:**

1. Запустите браузер. Вы будете перенаправлены в мастер настройки (Быстрая настройка Интернет). В противном случае вручную введите http://www.asusrouter.com.



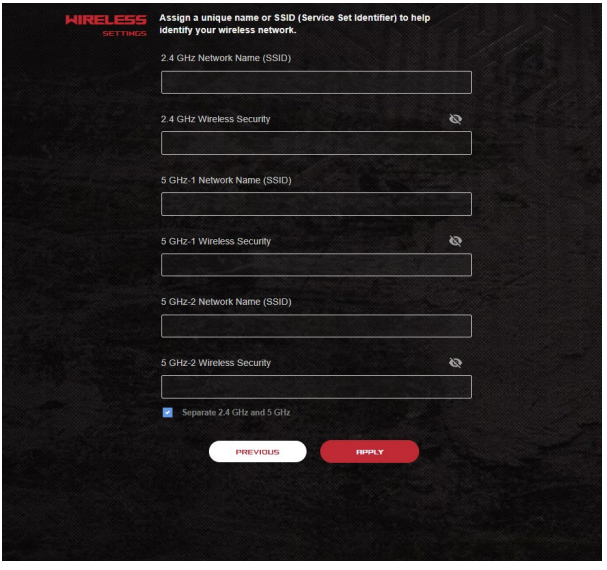

2. Роутер поддерживает следующие типы подключения: **Динамический IP**, **PPPoE**, **PPTP**, **L2TP**. Введите необходимую информацию для вашего типа подключения.

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

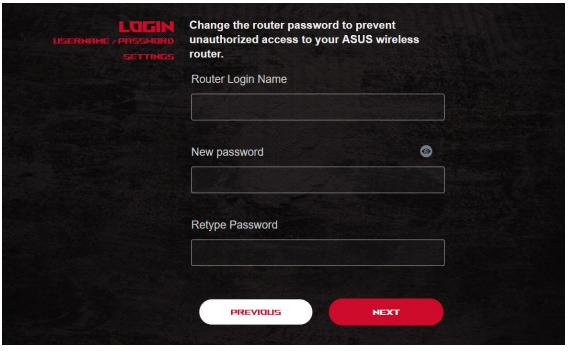
**ПРИМЕЧАНИЯ:**

- 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. Назначьте имя сети (SSID) и ключ безопасности для беспроводных подключений 2,4 ГГц, 5 ГГц-1 и 5 ГГц-2. Когда закончите, нажмите **Применить**.



4. На странице **Конфигурация входа в систему** измените пароль роутера, для предотвращения несанкционированного доступа.




**ПРИМЕЧАНИЕ:** 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.

## 2.3 Подключение к беспроводной сети

После настройки беспроводного роутера через QIS к беспроводной сети можно подключить компьютер и другие устройства.

**Для подключения к вашей сети выполните следующее:**

1. Для просмотра доступных беспроводных сетей щелкните по иконке сети  в области уведомлений.
2. Выберите беспроводную сеть, к которой вы желаете подключиться и нажмите **Подключить**.
3. При доступе к безопасной беспроводной сети введите пароль или сетевой ключ и нажмите **OK**.
4. Дождитесь подключения компьютера к беспроводной сети. Иконка  отображает состояние подключения и мощность сигнала проводного или беспроводного подключения.

**ПРИМЕЧАНИЯ:**

- Подробную информацию по настройке беспроводной сети смотрите в следующей главе.
- Подробную информацию по подключению устройства к беспроводной сети смотрите в руководстве пользователя устройства.

# 3 Конфигурация общих и дополнительных параметров

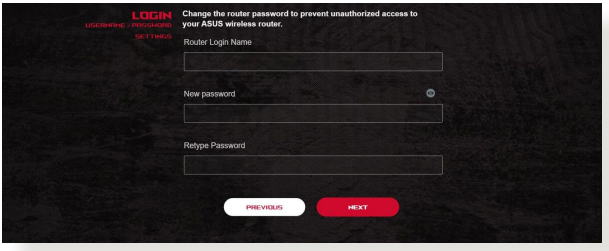
## 3.1 Вход в веб-интерфейс

Данный беспроводной роутер оснащен интуитивно понятным веб-интерфейсом (GUI) - ROG Gaming Center, который дает вам полный контроль над сетью и необходимую информацию, например состояние подключенного устройства или состояние подключения к серверу, а также быстрый доступ ко всем игровым возможностям.

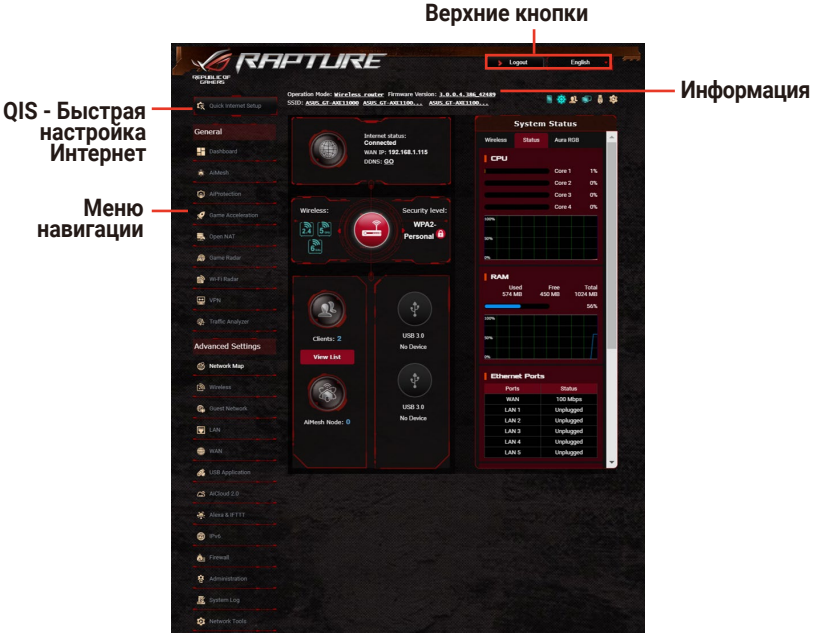
**ПРИМЕЧАНИЕ:** Функции могут изменяться в зависимости от версии прошивки.

**Для входа в веб-интерфейс:**

1. В браузере введите адрес роутера по умолчанию: http://www.asusrouter.com.
2. На странице входа введите имя пользователя и пароль, который вы установили в разделе **2.2 Быстрая настройка Интернет (QIS) с автоопределением**.




3. Теперь можно использовать веб-интерфейс для конфигурации различных параметров роутера.



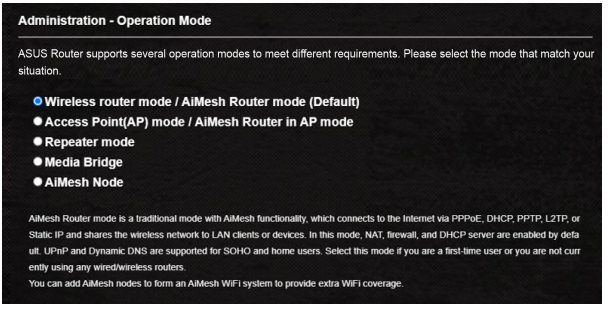

* Изображения предназначены только для справки.

**ПРИМЕЧАНИЕ:** При входе в веб-интерфейс в первый раз автоматически появится страница быстрой настройки Интернет (QIS).

# 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 **Дополнительные настройки** > **Администрирование** > **Режим работы**.
2. Выберите любой из следующих режимов:
   - **Режим беспроводного роутера / режим роутера AiMesh (по умолчанию)**: В режиме беспроводного роутера, роутер подключается к интернету и предоставляет доступ к интернету для устройств в локальной сети.
   - **Режим точки доступа (AP) / AiMesh роутер в режиме точки доступа**: В этом режиме роутер создает новую беспроводную сеть.
   - **Узел AiMesh**: Для этого потребуется хотя бы два роутера ASUS, которые поддерживают AiMesh. Включите узел AiMesh и войдите в веб-интерфейс роутера AiMesh для поиска других узлов AiMesh, которые можно подключить к системе AiMesh. Система AiMesh обеспечивает централизованное управление и покрытие всего дома.
3. Нажмите **Применить**.

**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 **Дополнительные настройки** > **Администрирование** > **Система**.
2. Можно сконфигурировать следующие параметры:
   - **Изменение пароля роутера**: Можно изменить имя пользователя и пароль беспроводного роутера, введя новые.
   - **Часовой пояс**: Выберите часовой пояс для вашей сети.
   - **NTP-сервер**: Для синхронизации времени роутер может подключаться к серверу NTP (Network Time Protocol).
   - **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 веб-доступ из WAN**: Выберите **Да** для разрешения доступа к веб-интерфейсу роутера из Интернет. Выберите **No** для предотвращения доступа.
   - **Разрешить только указанный IP-адрес**: Выберите **Да**, если нужно задать IP-адреса устройств, которым разрешен доступ к веб-интерфейсу роутера из WAN.
   - **Список клиентов**: Введите IP-адреса сетевых устройств, которым разрешен доступ к веб-интерфейсу роутера из WAN. Этот список будет использоваться, если включена опция **Разрешить только определенный IP**.
3. Нажмите **Применить**.

### 3.2.3 Обновление прошивки

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

**Для обновления прошивки:**

1. В меню навигации выберите **Дополнительные 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

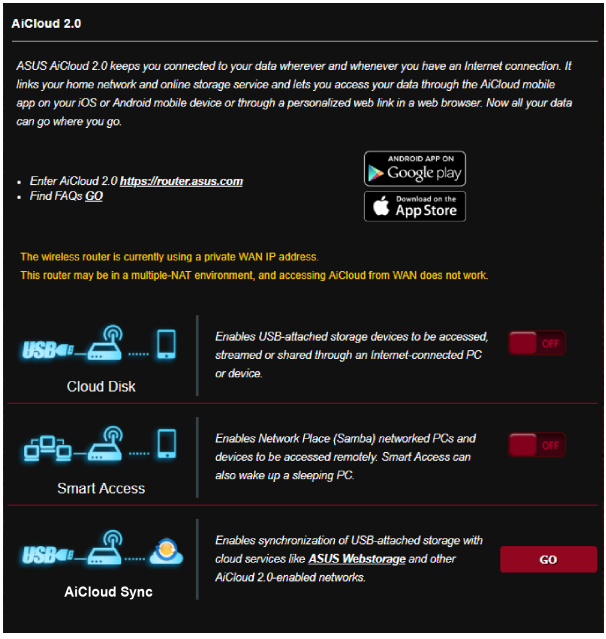
**Для восстановления/сохранения/сброса параметров:**

1. В меню навигации выберите **Дополнительные настройки** > **Администрирование** > **Восстановить/Сохранить/Загрузить настройки**.
2. Выберите задачу:
   - Для восстановления настроек по умолчанию нажмите **Восстановить**, затем **OK** для подтверждения.
   - Для сохранения текущих настроек нажмите **Сохранить**, затем **Сохранить** в окне с указанием пути.
   - Для восстановления сохраненных настроек нажмите **Обзор** для нахождения файла настроек, затем нажмите **Загрузить**.

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

## 3.3 AiCloud 2.0

AiCloud 2.0 - приложение, позволяющее сохранять, синхронизировать, обмениваться файлами.



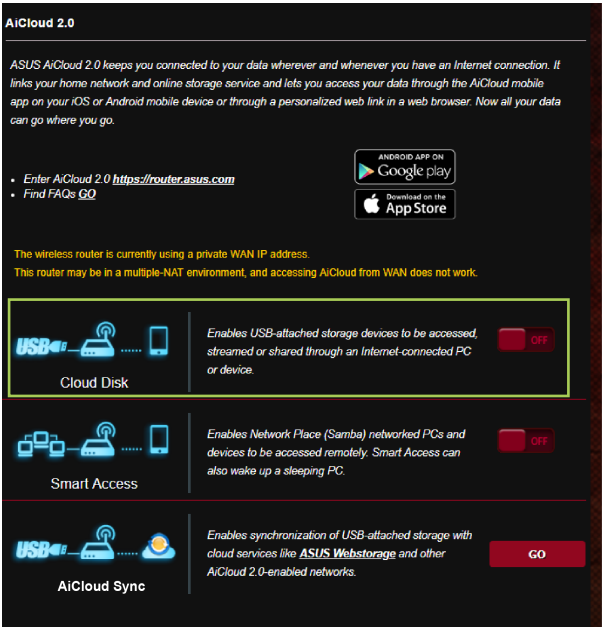

### Для использования AiCloud:

1. Скачайте и установите приложение ASUS AiCloud с Google Play Store или Apple Store.
2. Подключите устройства к сети. Следуйте инструкциям на экране для завершения процесса настройки AiCloud.

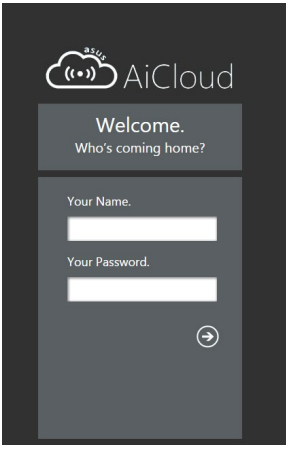
## 3.3.1 Облачный диск

**Для создания облачного диска:**

1. Подключите USB-накопитель к беспроводному роутеру.
2. Включите **Cloud Disk**.

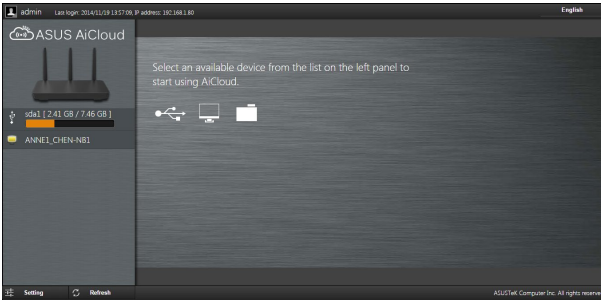


3. Посетите **http://www.asusrouter.com** и введите логин и пароль роутера. Рекомендуется использовать **Google Chrome** или **Firefox**.



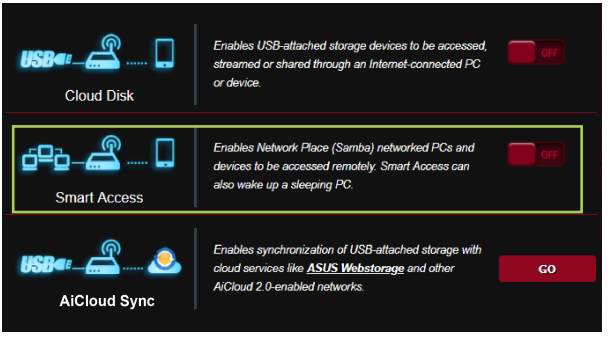

4. Теперь можно подключиться к облачному хранилищу с любого устройства, подключенного к интернету.

**ПРИМЕЧАНИЕ:** При доступе к подключенным к сети устройствам необходимо вручную ввести имя устройства и пароль вручную, поскольку они не сохраняются в AiCloud.



## 3.3.2 Smart Access

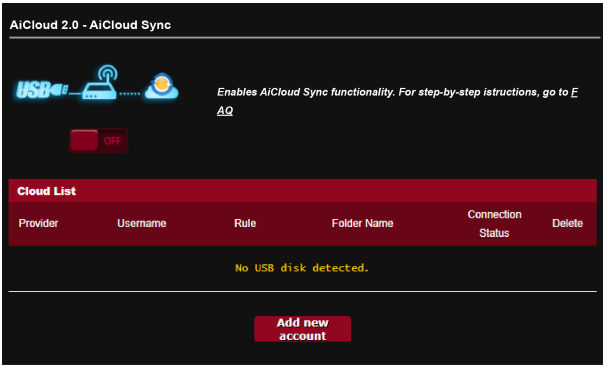
Функция Smart Access позволяет получить доступ к домашней сети через доменное имя роутера.




**ПРИМЕЧАНИЯ:**

- С помощью ASUS DDNS можно создать доменное имя для вашего роутера. Подробную информацию смотрите в разделе **3.20.6 DDNS**.
- AiCloud предоставляет безопасное соединение HTTPS по умолчанию. Для безопасного использования Cloud Disk и Smart Access введите https:// [yourASUSDDNSname]. Asuscomm.com.

## 3.3.3 AiCloud Sync

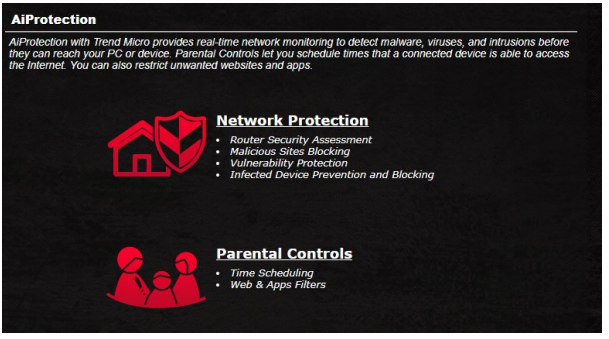



**Для использования AiCloud Sync:**

1. Запустите AiCloud и нажмите **AiCloud Sync** > **Go**.
2. Выберите **ON** для включения AiCloud Sync.
3. Нажмите **Добавить новую учетную запись**.
4. Введите пароль ASUS WebStorage и выберите директорию для синхронизации.
5. 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 планирование времени доступа к интернету.



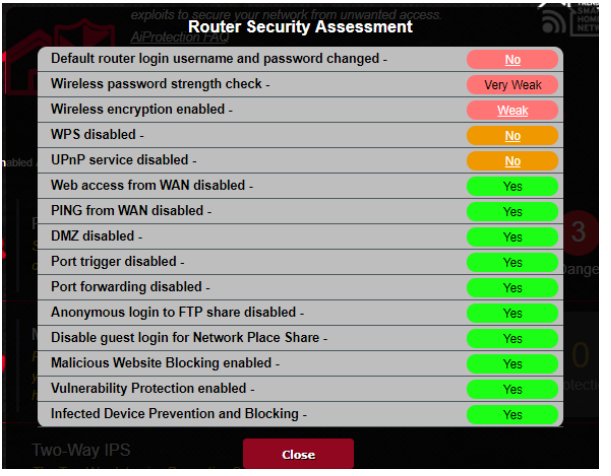
## 3.4.1Конфигурация AiProtection

AiProtection обеспечивает защиту сети от несанкционированного доступа.

**Для конфигурации AiProtection:**

1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице AiProtection нажмите **Сетевая защита**.
3. На вкладке Сетевая защита нажмите **Сканировать**.

Результаты сканирования отобразятся на странице **Оценка безопасности роутера**.




**ВАЖНО!** Поля на странице **Оценка безопасности роутера**, помеченные как **Да** означают безопасно.

4. (Дополнительно) На странице **Оценка безопасности роутера** вручную сконфигурируйте пункты, помеченные как **Нет**, **Слабо** или **Очень слабо**. Для этого:

   a. 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.

5. В подтверждающем сообщении нажмите **ОК**.

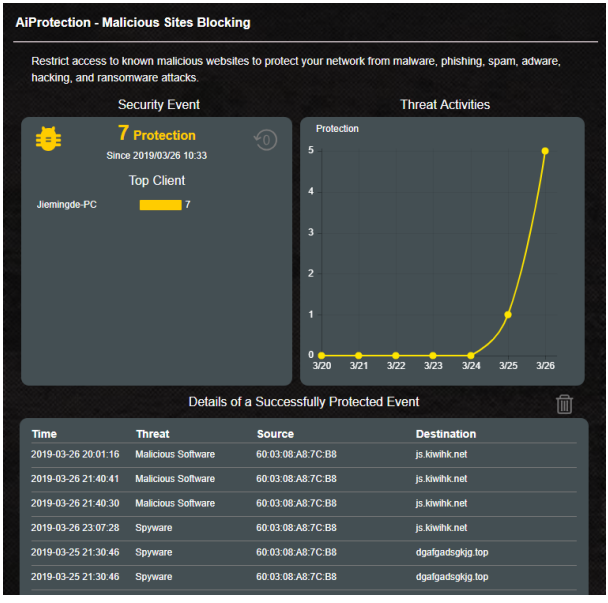
## 3.4.2 Блокировка вредоносных сайтов

Эта функция ограничивает доступ к известным вредоносным сайтам, добавленных в базу данных.

**ПРИМЕЧАНИЕ:** Эта функция включается автоматически при запуске Сканирование роутера.

**Для включения блокировки вредоносных сайтов:**

1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице AiProtection нажмите **Сетевая защита**.
3. В панели **Блокировка вредоносных сайтов** нажмите **ВКЛ**.



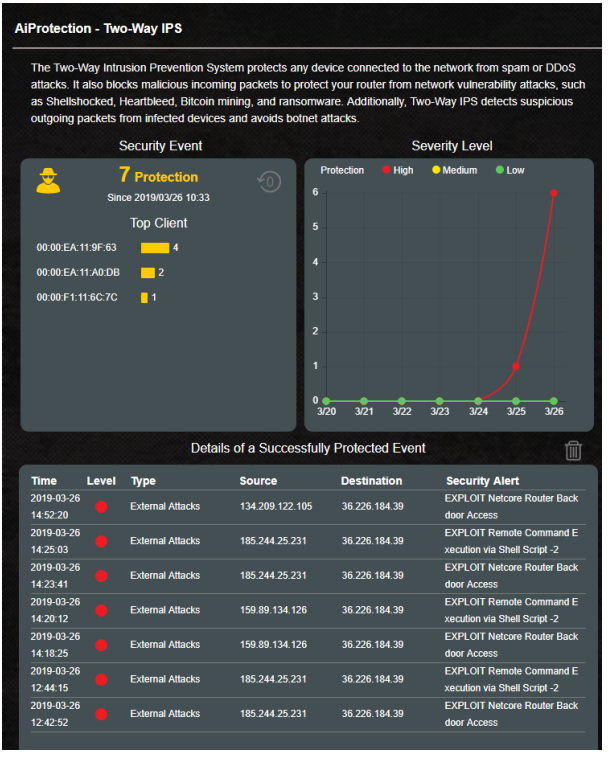
## 3.4.3 Двусторонняя IPS

Эта функция устраняет известные эксплоиты в конфигурации роутера.

**ПРИМЕЧАНИЕ:** Эта функция включается автоматически при запуске Сканирование роутера.

### Для включения двухстороннего IPS:

1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице AiProtection нажмите **Сетевая защита**.
3. В панели **Двусторонний IPS** нажмите **ВКЛ**.



### 3.4.4 Профилактика и блокировка зараженных устройств

Эта функция предотвращает заражение устройств при обмене персональной информацией с внешней стороной.

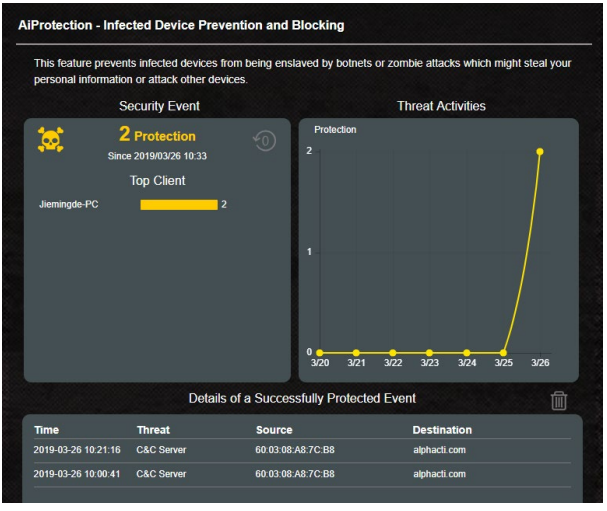
**ПРИМЕЧАНИЕ:** Эта функция включается автоматически при запуске Сканирование роутера.

**Для включения профилактики и блокировки зараженного устройства:**

1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице AiProtection нажмите **Сетевая защита**.
3. В панели **Профилактика и блокировка зараженных устройств** нажмите **ВКЛ**.

**Для конфигурации предпочитаемых оповещений:**

1. В панели Профилактика и блокировка зараженных устройств нажмите **Предпочитаемые оповещения**.
2. Выберите или введите провайдера электронной почты, учетную запись электронной почты и пароль, затем нажмите **Применить**.

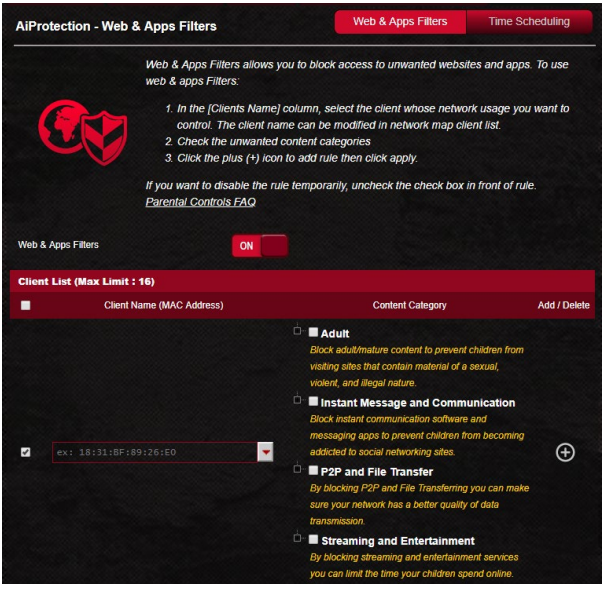


## 3.4.5 Настройка Родительского контроля

Родительский контроль позволяет контролировать время доступа к сети Интернет или ограничивать время использования сети Интернет.

**Для включения двухстороннего IPS:**

1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице AiProtection нажмите **Родительский контроль**.




### Фильтры для веб и приложений

Фильтры для веб и приложений - функция Родительского контроля, которая позволяет блокировать доступ к нежелательным сайтов или приложениям.

**Для конфигурации фильтров для веб и приложений:**

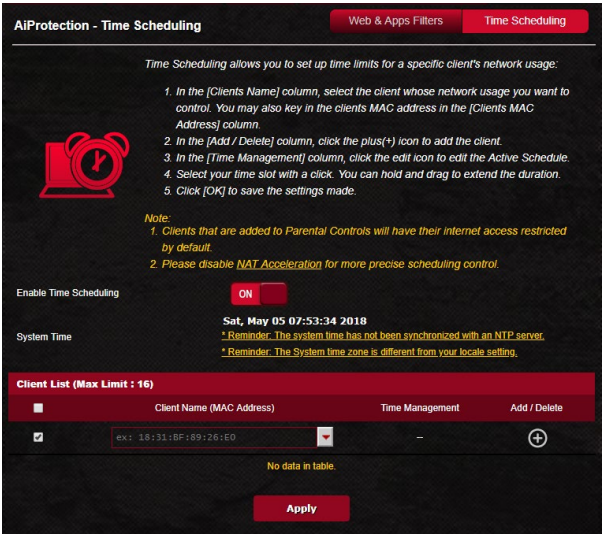
1. В меню навигации выберите **Общие** > **AiProtection**.
2. На главной странице **Aiprotection** нажмите иконку **Родительский контроль** для перехода на вкладку **Родительский контроль**.

3. В панели **Включить фильтры для веб и приложений** нажмите **ВКЛ**.
4 При появлении лицензионного соглашения нажмите **Я согласен**.
5. В столбце **Список клиентов** выберите или введите имя клиента из выпадающего списка.
6. В столбце **Содержимое** выберите фильтры из четырех основных категорий: **Взрослый**, **Мгновенные сообщения и связь**, **P2P и передача файлов** и **Потоковое вещание и развлечения**.
7. Нажмите ⊕ для добавления клиентского профиля.
8. Нажмите **Применить** для сохранения настроек.

## Расписание

Расписание позволяет установить ограничение времени для использования сети клиентом.

**ПРИМЕЧАНИЕ:** Убедитесь, что системное время синхронизировано с NTP-сервером.




### Для конфигурации расписания:

1. В меню навигации выберите **Общие** > **Aiprotection** > **Родительский контроль** > **Расписание**.
2. В панели **Расписание** нажмите **ВКЛ**.
3. В столбце **Имя клиента** введите или выберите имя клиента из выпадающего списка.

   **ПРИМЕЧАНИЕ:** Также можно ввести MAC-адрес клиента в поле MAC-адрес клиента. Убедитесь, что имя клиента не содержит специальных символов или пробелов, поскольку это может вызвать сбой в работе роутера.

4. Нажмите ⊕ для добавления клиентского профиля.
5. Нажмите **Применить** для сохранения настроек.

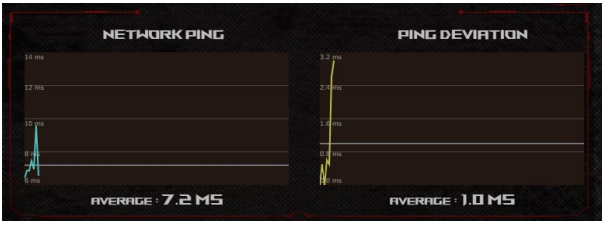
## 3.5 Панель управления

Dash Board позволяет отслеживать трафик в реальном времени для вашей сетевой среды и анализировать сетевой пинг и отклонение пинга в реальном времени.

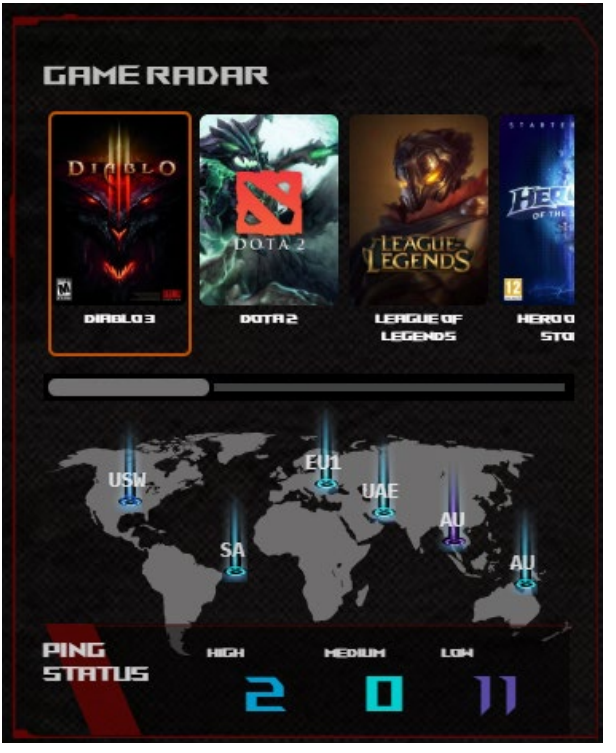

Сетевой пинг влияет на онлайн-игры. Высокий пинг означает более высокую задержку для игр в реальном времени. Для большинства онлайн-игр значение сетевого

пинга менее 99 мс считается хорошим. Если сетевой пинг менее 150 мс, это приемлемо. Как правило, играть в игру сложно при сетевом пинге более 150 мс.

Отклонение пинга также влияет на онлайн-игры. Высокое отклонение пинга может стать причиной отключения при игре в онлайн-игры. Нет значений для отклонения пинга. Тем не менее, низкое отклонение пинга лучше.




- **Game Radar:** Game Radar в информационной панели предоставит информацию о времени пинга для конкретного игрового сервера.



- **Aura RGB:** Позволяет пользователям настраивать или включать / выключать Aura RGB из информационной панели. Можете выбрать любой цвет и любой из пяти шаблонов подсветки.

## 3.6 Брандмауэр

Роутер может функционировать в качестве аппаратного брандмауэра.

**ПРИМЕЧАНИЕ:** Брандмауэр включен по умолчанию.

### 3.6.1 Общие

**Для настройки параметров брандмауэра:**

1. В меню навигации выберите **Дополнительные 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**.

### 3.6.2 Фильтр URL

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

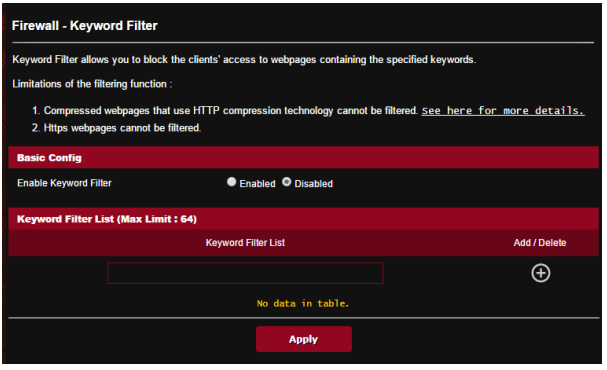
**ПРИМЕЧАНИЕ:** Фильтр URL функционирует на основе запроса DNS. Если сетевой клиент уже посещал сайт, например http://www.abcxxx.com, то сайт заблокирован не будет ( DNS-кэш сохраняет ранее посещенные сайты). Для решения этой проблемы очистите DNS-кэш перед установкой фильтра URL.

**Для настройки фильтра URL:**

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

## 3.6.3 Фильтр ключевых слов

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




**Для настройки фильтра ключевых слов:**

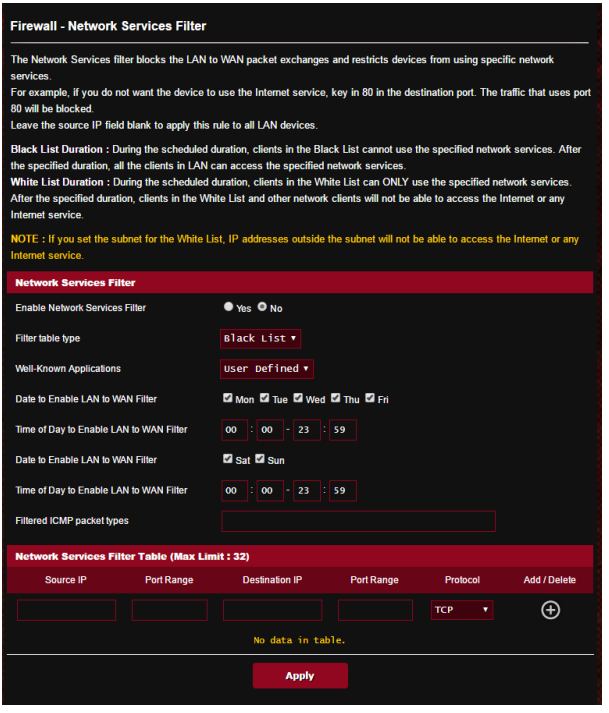
1. В меню навигации выберите **Дополнительные настройки** > **Брандмауэр** > **Фильтр ключевых слов**.
2. В поле **Включить фильтр ключевых слов** выберите **Включить**.
3. Введите слово или фразу и нажмите кнопку ⊕.
4. Нажмите **Применить**.

**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.

## 3.6.4 Фильтр сетевых служб

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



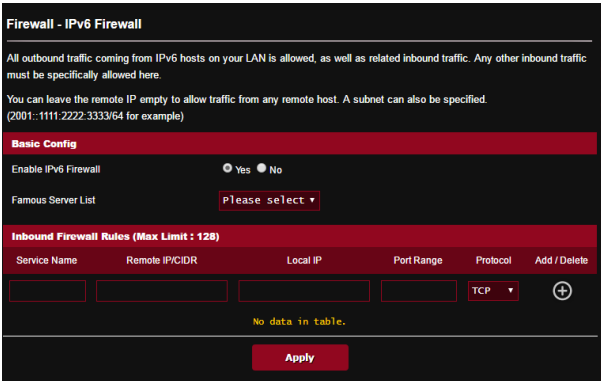

### Для настройки фильтра сетевых служб:

1. В меню навигации выберите **Дополнительные 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 кнопку ⊕.
6. Нажмите **Применить**.

## 3.6.5 Брандмауэр для IPv6

По умолчанию, роутер блокирует весь входящий трафик. Функция Брандмауэр для IPv6 позволяет разрешить входящий трафик с указанных служб.



## 3.7 Ускорение игр

Эта функция позволяет включить Game Boost одним щелчком. Когда Game Boost включен, роутер увеличивает приоритет для игрового трафика для уменьшения задержек в онлайн-играх.

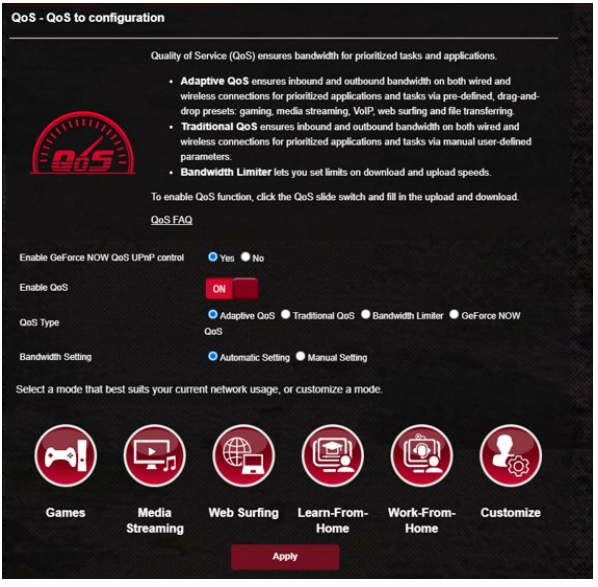

### Game Boost

**Для включения Game Boost:**

В **Game Boost** переместите ползунок **Включить Game Boost** на **ВКЛ**.

## 3.7.1 QoS

Эта функция гарантирует пропускную способность для приоритезированных задач и приложений.




**Для включения функции QoS:**

1. В меню навигации выберите **Общие** > **Ускорение игр** > **QoS**.
2. В панели **Включить QoS** нажмите **ВКЛ**.
3. Выберите тип QoS (Adaptive, Traditional или Bandwidth).

   **ПРИМЕЧАНИЕ:** Описание типа QoS отображается на вкладке QoS.

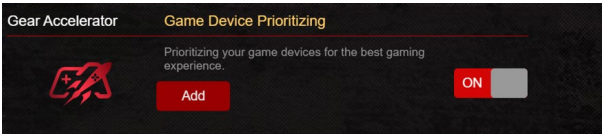
4. Нажмите **Авто-настройка** для автоматического выбора оптимальной полосы пропускания или **Ручная настройка** для установки полосы пропускания для загрузки и скачивания вручную.

   **ПРИМЕЧАНИЕ:** Информацию о ширине канала можно получить у вашего провайдера (ISP). Можно посетить http://speedtest .net и проверить свою пропускную способность.

5. Нажмите **Применить**.

### 3.7.2 Gear Accelerator

Gear Accelerator позволяет назначить приоритет игровым устройствам для обеспечения наилучших игровых возможностей.




**Для конфигурации Gear Accelerator:**

1. В меню навигации выберите **Общие** > **Ускорение игр**.
2. На вкладке **Gear Accelerator** нажмите **ВКЛ**.
3. После применения настроек нажмите **Добавить** для выбора имени клиента.
4. Нажмите для добавления клиентского профиля.
5. Нажмите **Применить** для сохранения настроек.

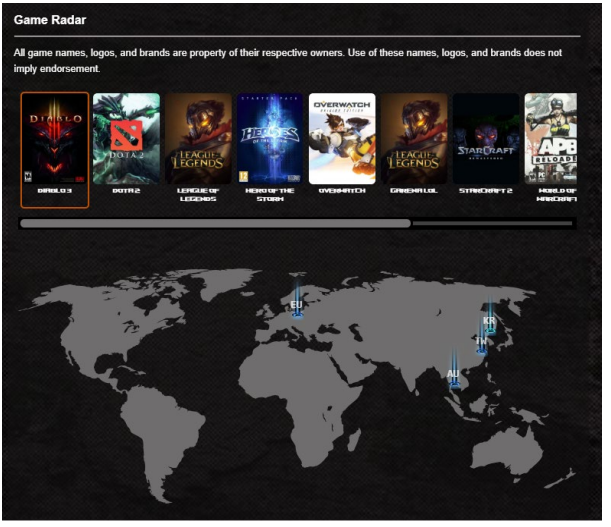
ПРИМЕЧАНИЕ: Для удаления профиля клиента нажмите .

## 3.8 Game Radar

Game Radar - это диагностическая утилита, помогающая определить качество соединения с игровыми серверами.


**Для использования Game Radar:**

1. В меню навигации выберите **Общие** > **Game Radar** и выберите игру из списка.




2. Проверьте **Ping Status** для каждого сервера.
3. Для уменьшения возможных задержек при игре выберите игровой сервер с низким пингом.

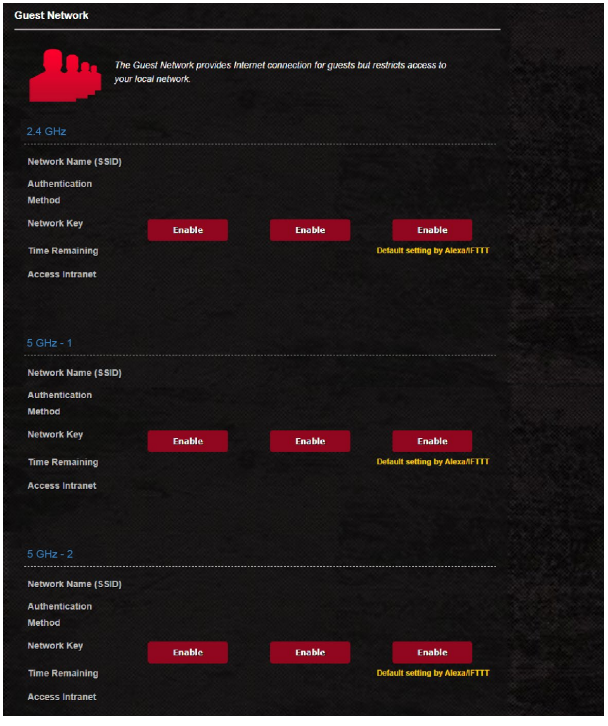
## 3.9 Гостевая сеть

Гостевая сеть предоставляет подключение к интернету для временных посетителей через отдельный SSID без доступа к локальной сети.

**ПРИМЕЧАНИЕ:** Роутер поддерживает до девяти SSID (три SSID для 2.4, три SSID для 5 ГГц-1 и три SSID для 5 ГГц-2).

**Для создания гостевой сети:**

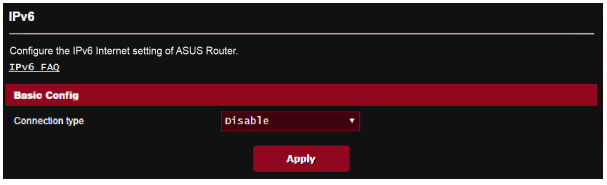
1. В меню навигации выберите **Дополнительные настройки** > **Гостевая сеть**.
2. На экране гостевой сети выберите используемый диапазон: 2,4, 5 ГГц-1 или 5 ГГц-2.
3. Выберите **Включить**.



4. Для изменения гостевых настроек, щелкните по ним. Нажмите **Удалить** для удаления гостевых настроек.
5. В поле Имя сети (SSID) назначьте имя для временной беспроводной сети.
6. Выберите метод аутентификации.
7. При выборе WPA-аутентификации выберите шифрование WPA.
8. Укажите время доступа или выберите пункт **Безграничный**.
9. Включите или отключите **Доступ к Интранет**.
10. Когда закончите, нажмите **Применить**.

## 3.10 IPv6

Данный роутер поддерживает адресацию IPv6, поддерживающую большее количество IP-адресов. Этот стандарт еще не получил широкого распространения. Информацию о поддержке IPv6 можно узнать у вашего провайдера.




**Для настройки IPv6:**

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

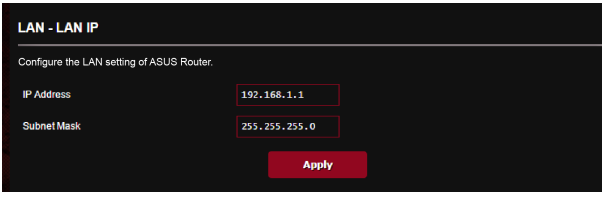
**ПРИМЕЧАНИЕ:** Конкретную информацию по IPv6 можно узнать у вашего провайдера.

# 3.11 LAN

## 3.11.1 IP-адрес локальной сети

На экране LAN IP можно изменить настройки LAN IP роутера.

**ПРИМЕЧАНИЕ:** Любые изменения LAN IP повлияют на настройки DHCP.

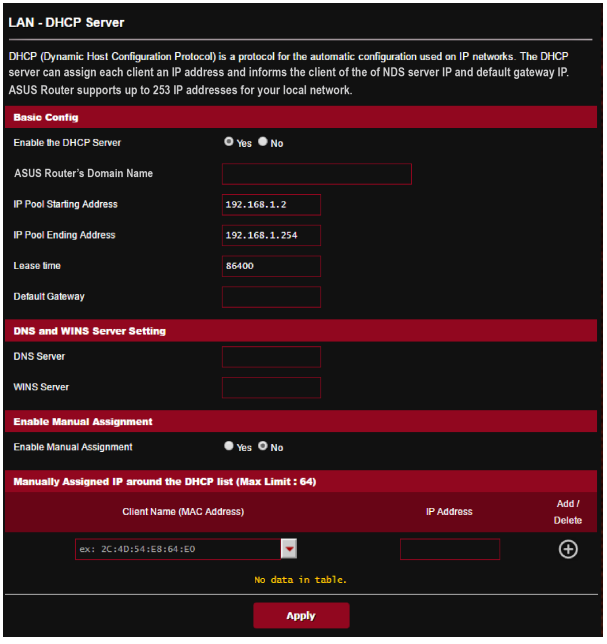



**Для изменения параметров LAN IP:**

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

## 3.11.2 DHCP-сервер

Роутер использует DHCP для автоматического назначения IP-адресов сетевым клиентам. Вы можете назначить диапазон IP-адресов и время аренды.




**Для конфигурации DHCP сервера:**

1. В меню навигации выберите **Дополнительные настройки** > **Брандмауэр** > **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:**

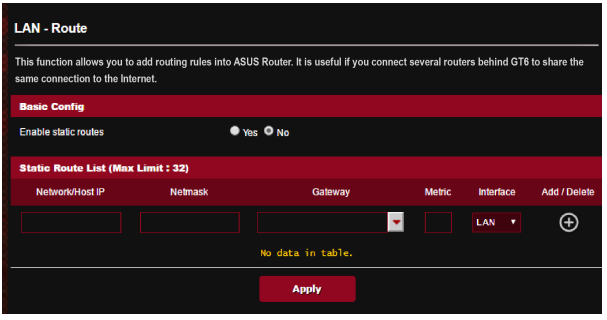
- Рекомендуется использовать IP-адрес в формате: 192.168.1.xxx (где xxx может быть любым числом в диапазоне от 2 до 254).
- Начальный IP-адрес пула не должен быть больше конечного IP-адреса.

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.

## 3.11.3 Маршрутизация

Если в сети используется несколько роутеров, можно настроить таблицу маршрутизации.

**ПРИМЕЧАНИЕ:** Не изменяйте маршруты по умолчанию, если вы не имеете представления о маршрутизации.

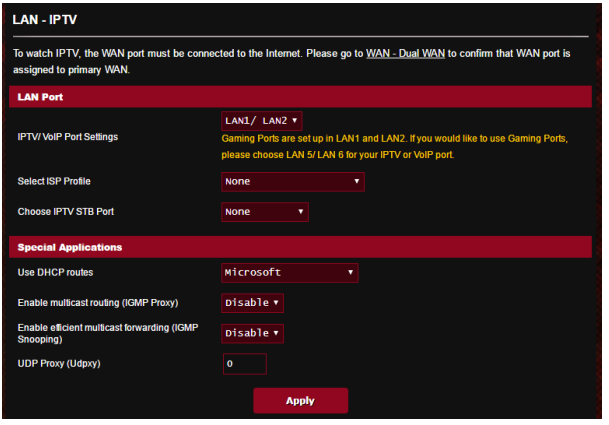



**Для конфигурации таблицы маршрутизации:**

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

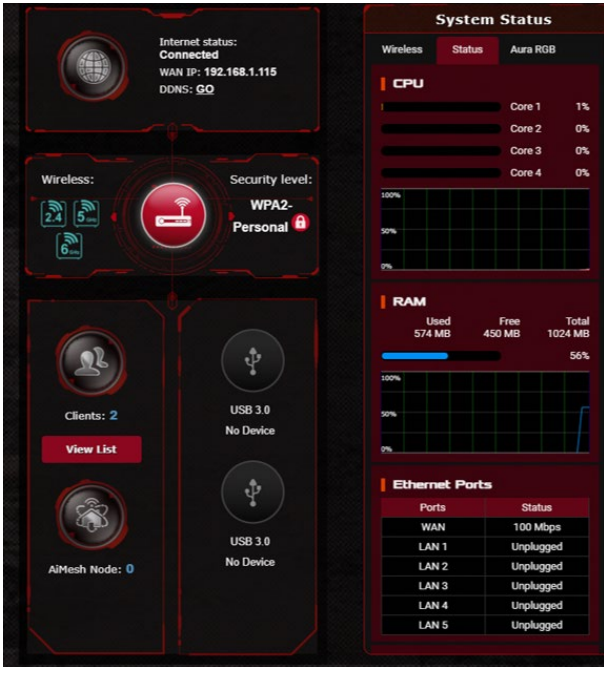
## 3.11.4 IPTV

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.



## 3.12 Карта сети

Карта сети позволяет конфигурировать параметры сетевой безопасности, управлять сетевыми клиентами и USB-устройствами.




### 3.12.1 Настройка параметров безопасности беспроводной сети

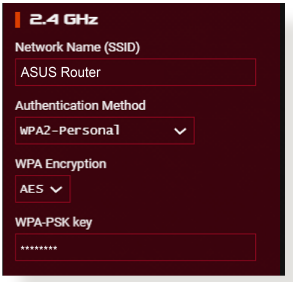
Для защиты беспроводной сети от несанкционированного доступа, необходимо настроить параметры безопасности.

**Для настройки параметров безопасности:**

1. В меню навигации выберите **Дополнительные настройки** > **Карта сети**.
2. На экране карты сети, под областью **Состояние системы** можно сконфигурировать параметры безопасности беспроводной сети, например SSID, уровень безопасности и настройки шифрования.

**ПРИМЕЧАНИЕ:** Можно настроить параметры безопасности для диапазонов 2,4 ГГц , 5 ГГц-1 и 5 ГГц-2.

### Настройки безопасности 2,4 ГГц




### Настройки безопасности 5 ГГц-1


### Настройки безопасности 5 ГГц-2

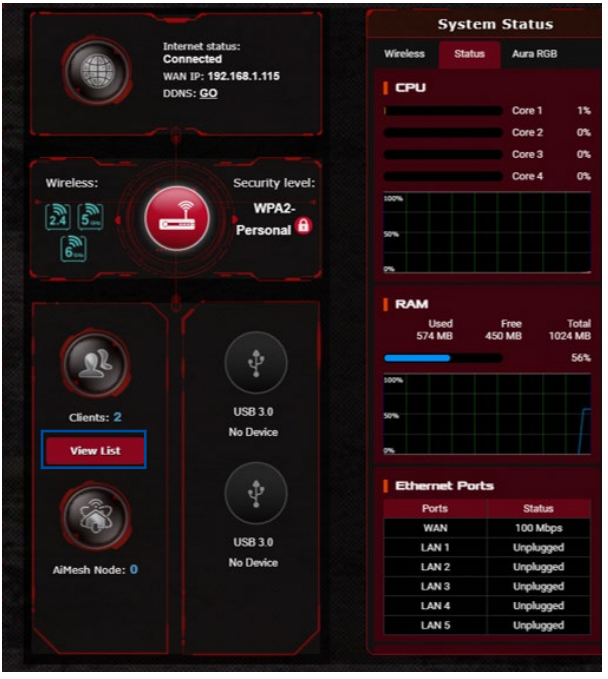

3. В поле **Network Name (SSID)** введите уникальное имя для вашей беспроводной сети.
4. В списке **Метод аутентификации** выберите метод шифрования для беспроводной сети.

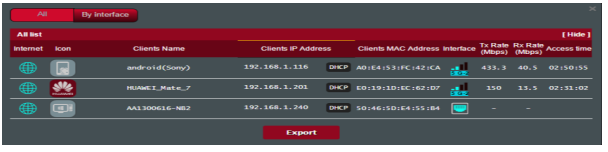
   При выборе метода аутентификации WPA-Personal или WPA-2 Personal необходимо ввести ключ.

**ВАЖНО!** Стандарт IEEE 802.11n/ac не поддерживает высокоскоростного соединения с WEP или WPA-TKIP ключом. Если вы используете эти методы шифрования, скорость передачи данных снизится до IEEE 802.11g 54Mbps.

5 Когда закончите, нажмите **Применить**.

## 3.12.2 Управление сетевыми клиентами



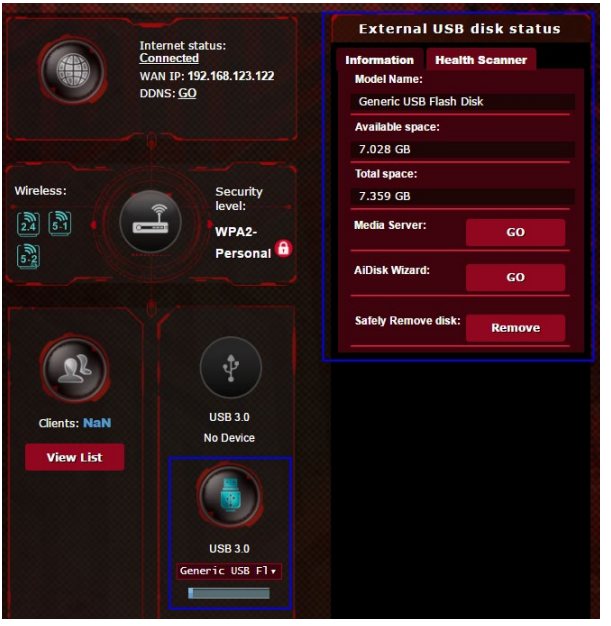




**Для управления сетевыми клиентами:**

1. В меню навигации выберите **Дополнительные настройки** > **Карта сети**.
2. На экране карта сети, выберите иконку **состояние клиента** для отображения информации о сетевых клиентах.
3. Нажмите **Просмотреть список** под иконкой **Клиенты** для отображения всех клиентов.
4. Для блокирования клиента, выберите клиента и нажмите иконку открытого замка.

### 3.12.3 Мониторинг USB-устройства

Беспроводной роутер оснащен двумя портами USB, предназначенными для подключения USB-накопителя или USB-принтера.




**ПРИМЕЧАНИЯ:**

- Для использования этой функции, необходимо подключить USB-накопитель (жесткий диск USB или USB флэш-диск) к разъему USB на задней панели беспроводного роутера. Убедитесь, что USB-накопитель готов к использованию. Список совместимых устройств смотрите на http://event.asus.com/networks/disksupport
- К портам USB одновременно можно подключить два USB-накопителя или один принтер и один USB-накопитель.

**ВАЖНО!** Сначала необходимо создать учетную запись и задать для нее права доступа, позволяющие другим сетевым клиентам доступ к USB-устройству через FTP, Samba или AiCloud. Для получения дополнительной информации смотрите разделы **3.17 использование USB приложений** и **3.3 Использование AiCloud 2.0** в данном руководстве.

**Для мониторинга USB-устройства:**

1. В меню навигации выберите **Дополнительные настройки** > **Карта сети**.
2. Для отображения информации о USB-устройстве на экране карты сети выберите иконку **Состояние USB диска**.
3. В поле **AiDisk Wizard** нажмите **GO** для создания FTP сервера  для обмена файлами в Интернете.

**ПРИМЕЧАНИЯ:**

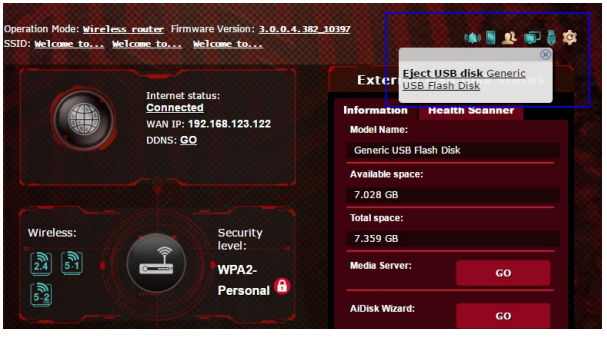
- Дополнительную информацию смотрите в разделе **3.17.2 Использование серверов** данного руководства.
- Беспроводной роутер работает с большинством USB жестких дисков/ флэш-дисков (размером до 4 Тб) и поддерживает чтение и запись для FAT16, FAT32, NTFS и HFS+.

## Безопасное извлечение USB-диска

**ВАЖНО!** Неправильное извлечение USB диска может привести к потере данных.

**Для безопасного извлечения USB-накопителя:**

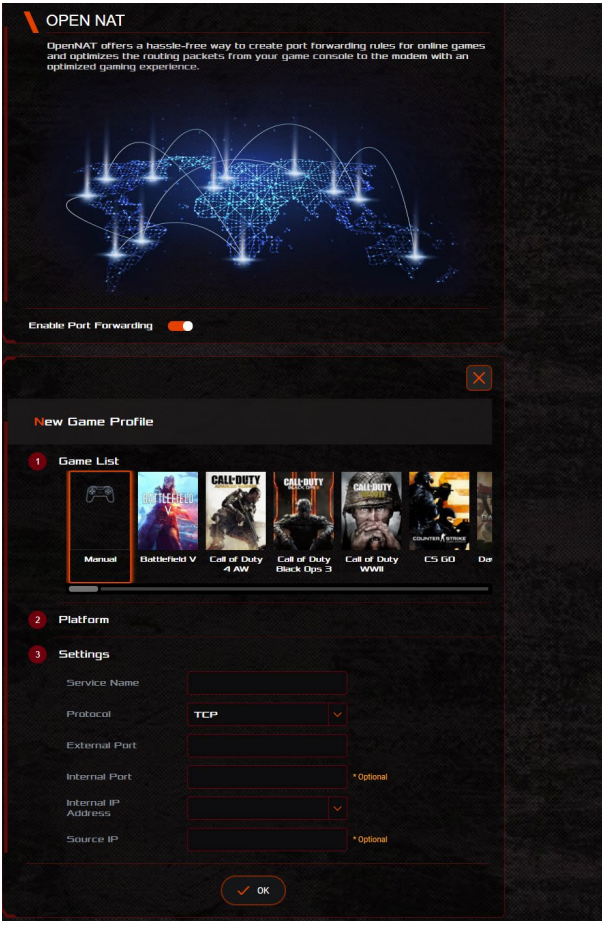
1. В меню навигации выберите **Дополнительные настройки** > **Карта сети**.
2. В правом верхнем углу нажмите  > **Отключить USB-накопитель**. После успешного отключения USB-накопителя состояние изменится на **Отключен**.



## 3.13 Open NAT и игровой профиль

Open NAT предлагает удобный способ переадресации портов для онлайн-игр и оптимизирует маршрутизацию игрового трафика.

При игре в игры могут возникнуть проблемы с подключением из-за настроек провайдера или роутера, например NAT и блокировка портов. Игровой профиль обеспечивает неблокируемое игровое соединение.



**Для конфигурации Open NAT:**

1. В меню навигации выберите **Общие** > **Open NAT**.
2. Переведите **Включить переадресацию портов**.
3. В поле **Список игр** выберите игру и выполните основные настройки.
4. Нажмите **OK**.

## 3.14 Smart Connect

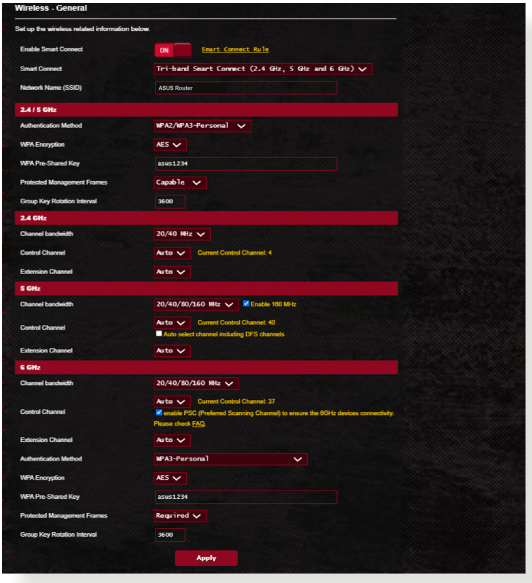
Smart Connect предназначен для автоматического управления клиентами в одном из трех диапазонов (2,4 ГГц, 5 ГГц-1 и 5 ГГц-2) для максимального использования пропускной способности беспроводной сети.

### 3.14.1 Настройка Smart Connect

Smart Connect можно включить из веб-интерфейса следующими двумя способами:

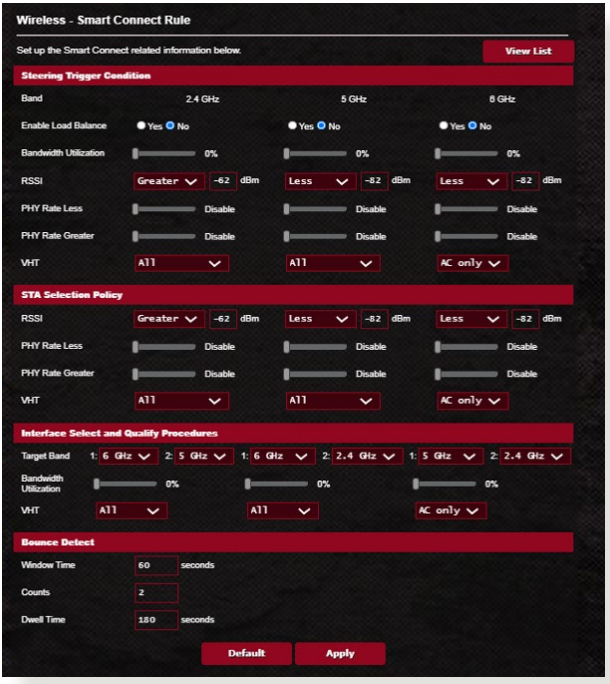
- **Через настройки беспроводной сети**

1. В браузере введите адрес роутера по умолчанию: http://www.asusrouter.com.
2. На странице входа, введите имя пользователя, затем нажмите **OK**. Автоматически появится страница быстрой настройки (QIS).
3. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > **Общие**.
4. Переместите ползунок в поле **Enable Smart Connect** в положение **ВКЛ**. Эта функция автоматически подключает сетевых клиентов к соответствующему диапазону для оптимальной скорости.



## 3.14.2 Правило Smart Connect

ASUSWRT предоставляет настройки по умолчанию для запуска механизма переключения. Условия запуска можно изменить в соответствии с условиями вашей сети. Для изменения настроек перейдите на вкладку **Smart Connect Rule** на экране Сетевые утилиты.

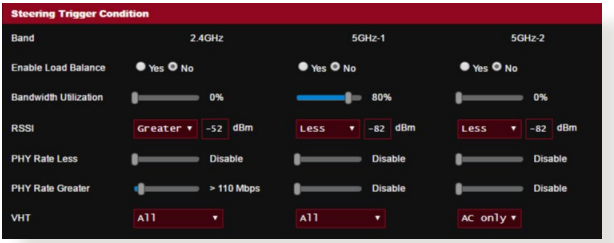



Элементы Smart Connect Rule разделены на четыре раздела:

- Условие Steering Trigger
- Политика выбора STA
- Выбор интерфейса и процедуры подготовки
- Обнаружение отказа

### Условие Steering Trigger

Этот набор элементов устанавливает критерии для переключения диапазонов.




- **Использование пропускной способности**

  Когда использование полосы пропускания превышает этот процент, будет инициализировано переключение диапазонов.

- **Включить балансировку нагрузки**

  Это контролирует балансировку нагрузки.

- **RSSI**

  Если уровень принимаемого сигнала любого подключенного клиента соответствует этим критериям, будет инициировано переключение.

- **PHY Rate Less / PHY Rate Greater**

  Эти элементы определяют скорости передачи STA, при которых запускается переключение.

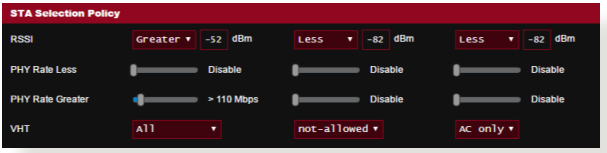
- **VHT**

  Этот элемент определяет, как обрабатываются клиенты 802.11ac и прочие.

  - **ВСЕ** (по умолчанию) означает, что любой тип клиента может инициировать переключение.
  - **Только AC** означает, что клиент должен поддерживать 802.11ac для запуска переключения.
  - **Не разрешается** означает, что все клиенты, кроме 802.11ac, будут запускать переключение, например: 802.11a/b/g/n.g / n.

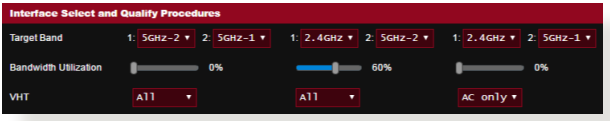
## Политика выбора STA

После запуска переключения ASUSWRT будет следовать политике выбора STA для выбора клиента (STA), который будет направляться в наиболее подходящий диапазон.




## Выбор интерфейса и процедуры подготовки

Эти элементы указывают диапазон для переключаемого клиента. Элементы **Target Band** указывают на первый и второй диапазоны для переключения. Клиенты, соответствующие критериям политики выбора STA будут переключены на первый диапазон, если **Bandwidth Utilization** меньше заданного значения. В противном случае клиент будет переключен на второй диапазон **Target Band**.




## Обнаружение отказа

Этот набор элементов определяет, как часто клиент может быть переключен. Это предназначено для предотвращения постоянного переключения клиентов. Тем не менее, это не препятствует самостоятельному отключению клиентов или считает их переключенными, если они так сделают. Каждый клиент может быть переключен N **Counts** в течение **Window Time**. При достижении максимального количества переключений, клиент не будет переключаться в течение **Dwell Time.**

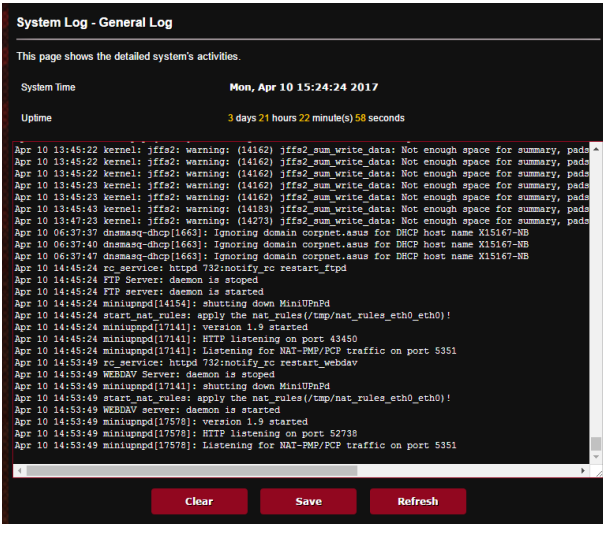
# 3.15 Системный журнал

Системный журнал содержит записанную сетевую активность.

**ПРИМЕЧАНИЕ:** Системный журнал очищается при перезагрузке или выключении роутера.

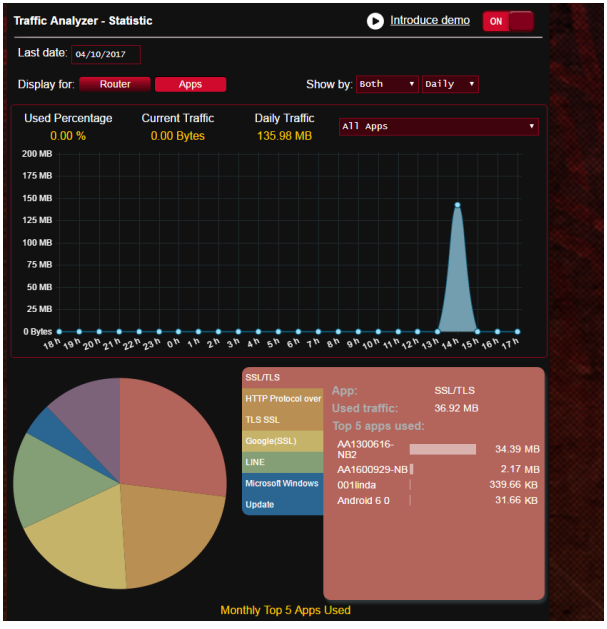
**Для просмотра системного журнала:**

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



# 3.16 Анализатор трафика

Анализатор трафика дает вам представление о том, что происходит в вашей сети, ежедневно, еженедельно или ежемесячно. Он позволяет просмотреть трафик каждого пользователя или устройства или приложения, помогая устранить узкие места в подключении к интернету.
Это также отличный способ отслеживания активности пользователей и использования ими Интернета.



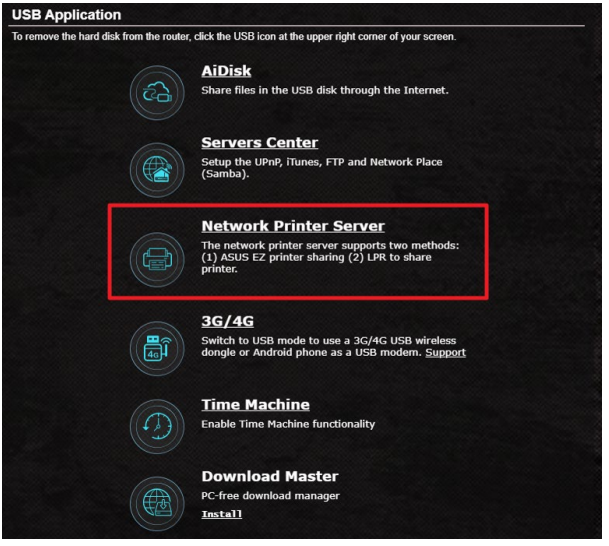

**Для конфигурации анализатора трафика:**

1. В меню навигации выберите **Общие** > **Анализатор трафика**.
2. На главной странице **Анализатора трафика** включите статистику трафика.
3. Выберите дату, для которой нужно отобразить диаграмму.
4. В поле **Отобразить для** выберите роутер или приложения для отображения информации о трафике.
5. В поле **Отобразить поля** выберите способ отображения информации о трафике.

## 3.17 USB-приложение

Функция USB-приложения содержит подменю AiDisk, Серверы, Сервер печати и Download Master.

**ВАЖНО!** Для использования серверных функций необходимо подключить USB-накопитель (жесткий диск USB или USB флэш-диск) к порту USB на задней панели беспроводного роутера. Убедитесь, что USB-накопитель готов к использованию. Таблицу с поддерживаемыми файловыми системами смотрите на сайте ASUS http://event.asus.com/2009/networks/disksupport/.

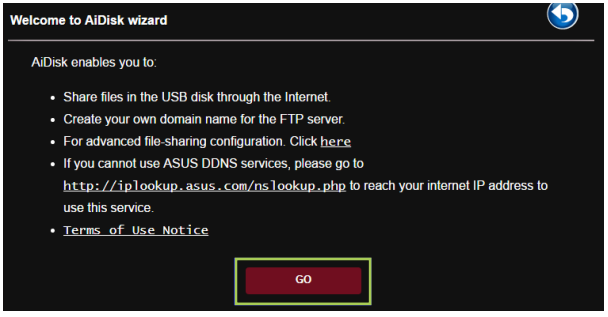


## 3.17.1 Использование AiDisk

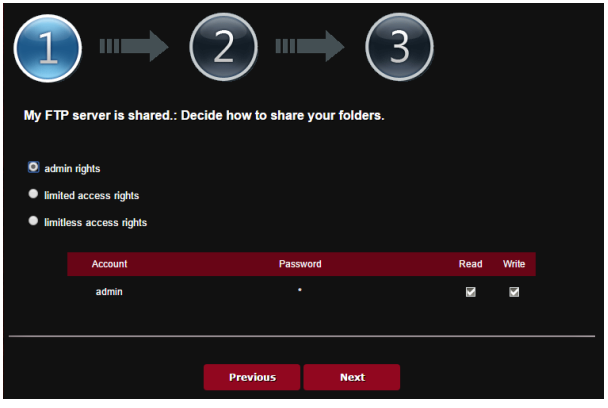
AiDisk позволяет обмениваться файлами, хранящимися на подключенном USB-накопителе через Интернет. AiDisk также позволяет настроить ASUS DDNS и FTP сервер.

**Для использования AiDisk выполните следующее:**

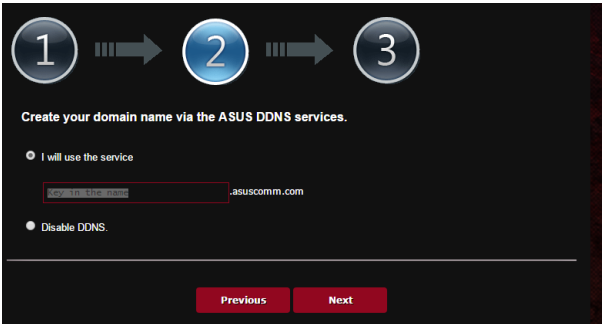
1. В меню навигации нажмите **Дополнительные настройки** > **USB Application**, затем нажмите иконку **AiDisk**.
2. На экране Добро пожаловать в мастер AiDisk нажмите **Go**.




3. Выберите права доступа для клиентов.



4. Создайте собственное доменное имя через службу ASUS DDNS, прочитайте условия использования и выберите "I will use the service and accept the Terms of service" и введите доменное имя. Когда закончите, нажмите **Next**.




Для пропуска настройки DDNS выберите **Пропустить настройку ASUS DDNS** и нажмите **Далее**.

5. Нажмите **Готово** для завершения настройки.
6. Для доступа к созданному FTP серверу запустите браузер или FTP клиент и введите созданную FTP ссылку (**ftp://<domain name>.asuscomm.com**).

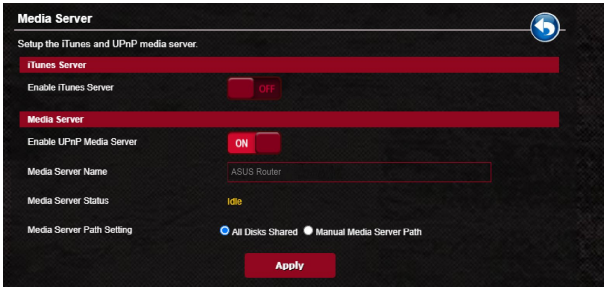
## 3.17.2 Использование службы Серверы

Страница Серверы позволяет осуществить обмен файлами с USB-накопителя по сети с помощью Samba, FTP или медиасервера. Также можно сконфигурировать другие параметры USB-накопителя.

### Использование медиасервера

Беспроводной роутер обеспечивает доступ для UPnP-совместимых устройств к мультимедийным файлам на подключенном USB-накопителе.

> **ПРИМЕЧАНИЕ:** Подключите ваше устройство к локальной сети перед использованием функции UPnP-медиасервера.

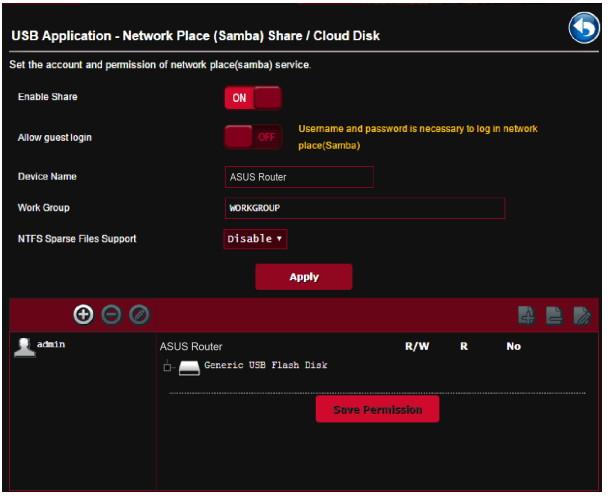



Для открытия страницы настроек медиасервера перейдите **Дополнительные настройки** > **USB-приложение** > **Серверы** > **Медиасервер**. Ознакомьтесь с описанием полей:

- **Включить iTunes сервер?:** Выберите ВКЛ/ОТКЛ для включения/отключения iTunes сервера.
- **Включить UPnP медиасервер:** Выберите ВКЛ/ОТКЛ для включения/отключения UPnP медиасервера.
- **Состояние медиасервера:** Отображает состояние медиасервера.
- **Настройки медиасервера**: Выберите **Общий доступ ко всем дискам** или **Настройка медиасервера вручную**.

## Использование сетевого окружения (Samba)

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




**Для использования Samba сервера:**

1. В меню навигации выберите **Дополнительные настройки** > **USB-приложение** > **Службы и серверы** > **Сетевое окружение (Samba) / Облачный диск**.

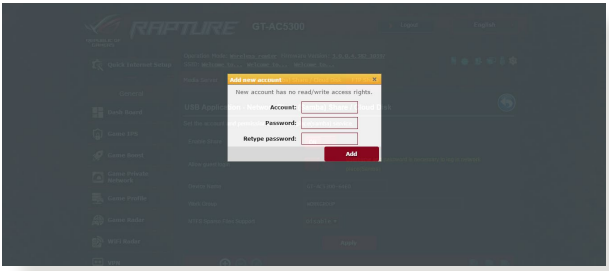
   **ПРИМЕЧАНИЕ:** Сетевое окружение (Samba) по умолчанию включено.

2. Для добавления, удаления или изменения учетной записи выполните следующие действия.

**Для создания учетной записи выполните следующее:**

a) Нажмите для добавления новой учетной записи.

b) В поля **Account** и **Password** введите имя и пароль сетевого клиента. Повторите ввод пароля для подтверждения. Нажмите **Add** для добавления учетной записи.




**Для удаления учетной записи пользователя:**

a) Выберите учетную запись для удаления.

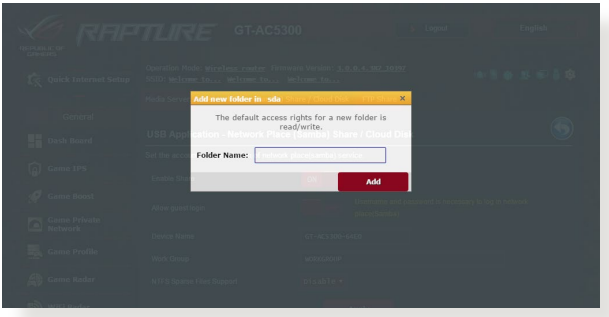
b) Нажмите .

c) При появлении запроса нажмите **Удалить** для подтверждения.

**Для добавления папки:**

a) Нажмите .

b) Введите имя папки и нажмите **Добавить**. Папка будет добавлена в список папок.



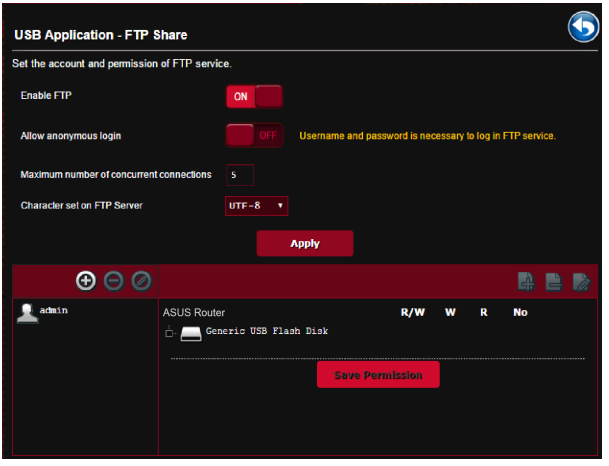

3. В списке папок выберите права доступа:
   - **R/W**: Выберите эту опцию для назначения прав на чтение/запись.
   - **R**: Выберите эту опцию для назначения прав на чтение.
   - **No:** Выберите эту опцию, если вы не хотите сделать папку общей.
4. Для применения изменений нажмите **Apply**.

## Использование FTP сервера

FTP сервер позволяет обмениваться файлами с USB-накопителя по локальной сети или через Интернет.

**ВАЖНО!**

- Убедитесь, что вы безопасно отключили USB диск. Неправильное извлечение USB диска может привести к потере данных.
- Для безопасного извлечения USB-накопителя обратитесь к подразделу **Безопасное извлечение USB-диска** раздела **3.12.3 Мониторинг USB-устройства**.




### Для использования службы FTP:

**ПРИМЕЧАНИЕ:** Убедитесь, что вы настроили FTP сервер с помощью AiDisk. Подробную информацию смотрите в разделе **3.17.1 Использование AiDisk**.

1. В меню навигации нажмите **Дополнительные настройки** > **USB-приложение** > **Общий ресурс в FTP.**
2. В списке папок выберите права доступа:
   - **R/W**: Выберите эту опцию для назначения прав на чтение/запись для указанной папки.
   - **W**: Выберите эту опцию для назначения прав на

запись для указанной папки.

- **R**: Выберите эту опцию для назначения прав на чтение для указанной папки.
- **No:** Выберите эту опцию, если вы не хотите предоставлять общий доступ к конкретной папке.

3. При желании можно включить опцию **Разрешить анонимный вход**.
4. В поле **Максимальное число одновременных подключений** введите количество устройств, которые могут одновременно подключаться к FTP-серверу.
5. Для применения изменений нажмите **Применить**.
6. Для доступа к FTP серверу, в браузере или FTP утилите введите ссылку **FTP://<hostname>.asuscomm.com**, имя пользователя и пароль.

## 3.17.33G/4G

Для доступа к интернету к роутеру можно подключить 3G/4G USB-модем.

**ПРИМЕЧАНИЕ:** Список поддерживаемых USB-модемов можно найти на странице http://event.asus.com/2009/networks/3gsupport/

**Для настройки доступа к интернету через 3G/4G:**

1. В меню навигации нажмите **Дополнительные настройки** > **USB-приложение** > **3G/4G**.
2. В поле **Включить USB-модем** выберите **Да**.
3. Настройте следующее:
   - **Местоположение**: Выберите местоположение вашего 3G/4G провайдера из списка.
   - **Провайдер**: Выберите вашего провайдера (ISP) из списка.
   - **Служба APN (Access Point Name) (опционально)**: Подробную информацию можно получить у вашего 3G/4G провайдера.
   - **Набираемый номер и ПИН-код**: Номер 3G/4G провайдера и ПИН-код для подключения.

   **ПРИМЕЧАНИЕ:** ПИН-код может отличаться в зависимости от провайдера.

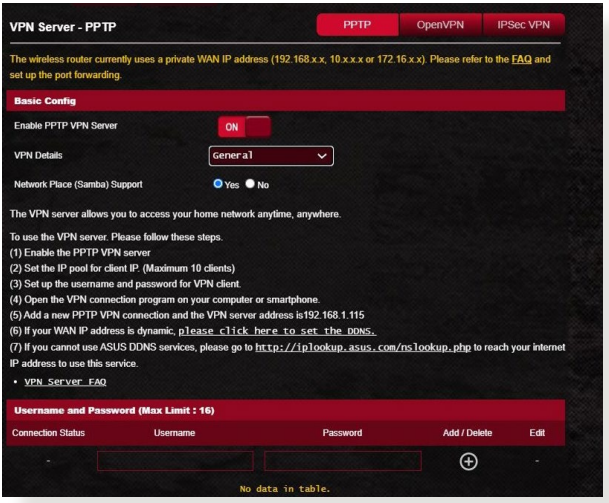
   - **Имя пользователя / Пароль:** Имя пользователя и пароль будут предоставлены 3G/4G провайдером.
   - **USB-адаптер**: Выберите USB 3G/4G адаптер из списка. Если модель вашего USB-адаптера неизвестна или отсутствует в списке, выберите **Авто**.
4. Нажмите **Применить**.

**ПРИМЕЧАНИЕ:** Роутер будет перезагружен для применения изменений.

# 3.18 VPN

VPN (виртуальная частная сеть) обеспечивает безопасное подключение к удаленному компьютеру или сети через публичную сеть, например Интернет.

**ПРИМЕЧАНИЕ:** Перед настройкой VPN-подключения потребуется IP-адрес или доменное имя VPN-сервера.

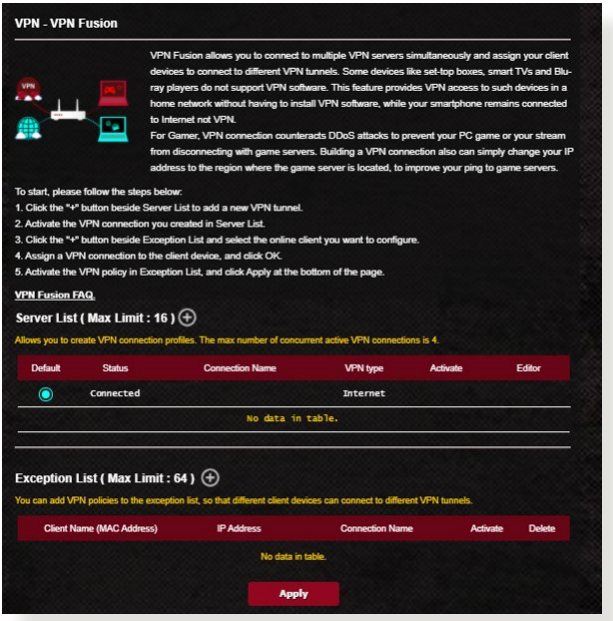



**Для настройки доступа к VPN-серверу:**

1. В меню навигации выберите **Общие** > **VPN**.
2. В поле **Включить VPN-сервер** выберите **ВКЛ**.
3. Если нужно настроить дополнительные параметры VPN, например поддержка трансляции, аутентификация, MPPE-шифрование, а также диапазона IP адресов клиента, в списке **Подробнее о VPN** выберите **Дополнительные настройки**.
4. В поле **Поддержка Сетевого окружения (Samba)** выберите **Да**.
5. Введите имя пользователя и пароль для доступа к VPN-серверу. Нажмите ⊕.
6. Нажмите **Применить**.

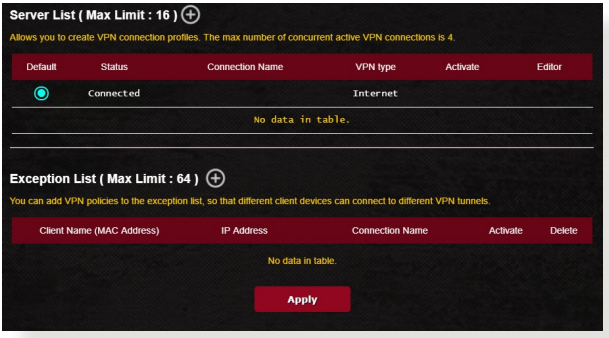
### 3.18.1 VPN Fusion

VPN Fusion позволяет одновременно подключаться к нескольким VPN-серверам и назначать их для сетевых клиентов. Некоторые устройства, например приставки, интеллектуальные телевизоры и Blu-ray-плееры не поддерживают VPN. Эта функция обеспечивает VPN-доступ для таких устройств в домашней сети без необходимости установки программного обеспечения VPN. Для игроков VPN-подключение противодействует DDoS-атакам, предотвращая отключение вас от игровых серверов. Создание VPN-подключения также может просто изменить ваш IP-адрес для соответствия региону, где расположен игровой сервер, что улучшает пинг с игровыми серверами.



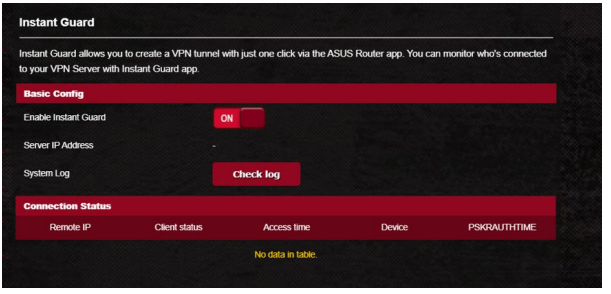
**Для начала выполните следующие действия:**

1. Нажмите кнопку ⊕ рядом со списком серверов для добавления нового туннеля VPN.
2. Активируйте VPN-подключение, созданное в списке серверов.
3. Нажмите кнопку ⊕ рядом со списком исключений и выберите онлайн-клиента для конфигурации.
4. Назначьте VPN-подключение для клиентского устройства и нажмите **ОК**.
5. Активируйте политику VPN в **списке исключений и** нажмите **Применить** в нижней части страницы.



## 3.18.2 Instant Guard

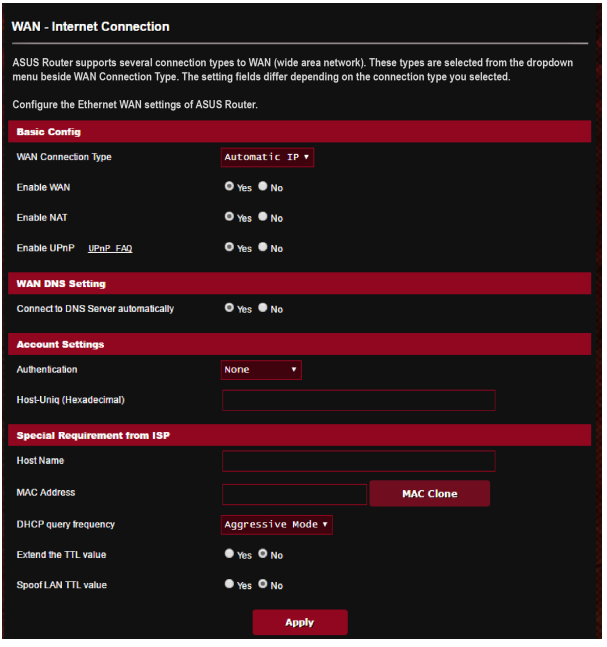
Instant Guard запускает на роутере собственный личный VPN-сервер. При использовании VPN-туннеля, все ваши данные проходят через сервер. С помощью Instant Guard вы полностью контролируете свой собственный сервер, что является самым безопасным решением.



# 3.19 WAN

## 3.19.1 Подключение к интернету

На странице подключение к интернету можно сконфигурировать параметры WAN подключения.




**Для конфигурации параметров WAN:**

1. В меню навигации выберите **Дополнительные 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 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 автоматически**: Позволяет роутеру автоматически получить IP-адрес DNS сервера от провайдера. DNS - это хост в

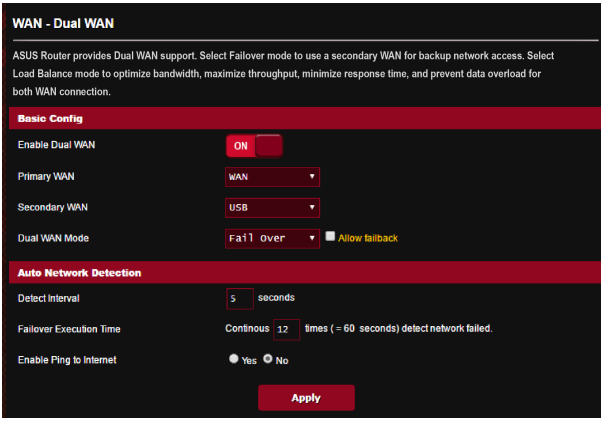
интернете, который транслирует имена Интернет в IP-адреса.

- **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..
- **Частота запросов DHCP**: Изменяет интервала обнаружения DHCP во избежание перегрузки DHCP-сервера.

## 3.19.2 Двойной WAN

Данный беспроводной роутер поддерживает функцию двойной WAN. Функция двойной WAN может функционировать в любом из этих двух режимов:

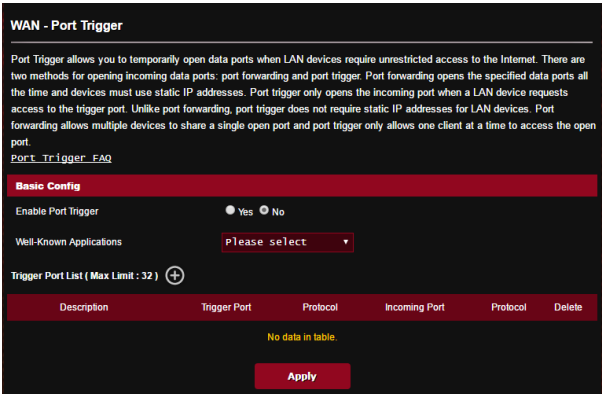
- **Режим отказоустойчивости**: Выберите этот режим для использования вторичного WAN в качестве резервного.
- **Режим балансировки нагрузки**: Выберите этот режим для оптимизации пропускной способности, уменьшения времени отклика и предотвращения перегрузки первичного и вторичного WAN.



## 3.19.3 Переключение портов

Функция переключения портов открывает входящий порт на ограниченный период времени, когда клиент в локальной сети запрашивает исходящее соединение на заданный порт. Переключение портов используется в следующих случаях:

- Нескольким локальным клиентам необходима переадресация портов для одного приложения в разное время.
- Приложению требуются конкретные входящие порты, которые отличаются от исходящих портов.




**Для настройки переключения портов:**

1. В меню навигации выберите **Дополнительные настройки** > **WAN** > **Переключение портов**.
2. В поле **Включить переключение портов** выберите **Да**.
3. В поле **Известные приложения** выберите популярные игры и веб-службы для добавления в список переключения портов.
4. В таблице **Список переключаемых портов** введите следующую информацию:
   - **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.
- **Протокол**: Выберите протокол TCP или UDP.

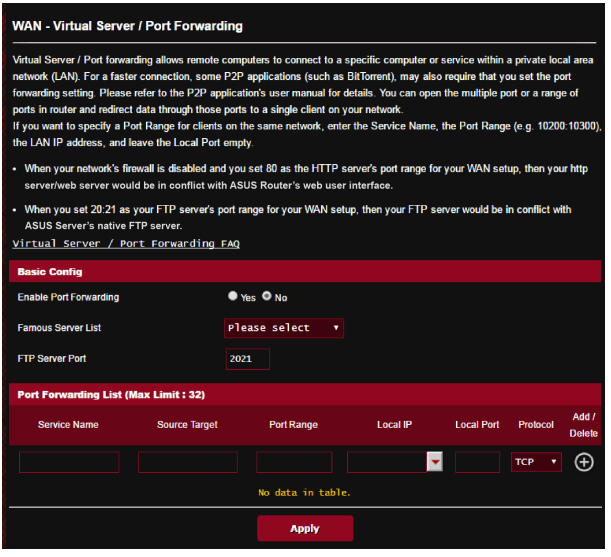
5. Нажмите **Добавить** для добавления информации в список. Нажмите **Удалить** для удаления информации из списка.
6. Когда закончите, нажмите **Применить**.

**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.

## 3.19.4 Виртуальный сервер/Переадресация портов

Переадресация портов - метод для перенаправления сетевого трафика из Интернета на указанный порт или диапазон портов устройства в локальной сети. Настройка переадресации портов на роутере позволяет удаленным компьютерам использовать службы, предоставляемые компьютерами вашей сети.




**Для настройки переадресации портов:**

1. В меню навигации выберите **Дополнительные настройки** > **WAN** > **Виртуальный сервер/ Переадресация портов**.
2. В поле **Включить переадресацию портов** выберите Да.
3. В поле **Список известных серверов** выберите тип службы, к которой нужно получить доступ.
4. В поле **Список известных игр** выберите популярную игру, к которой нужно получить доступ. Этот пункт перечисляет порт для выбранный популярным онлайн-игры работать должным образом.

5. В таблице **Список переадресованных портов** введите следующую информацию:
   - **Имя службы**: Введите имя службы.
   - **Диапазон портов:** 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. Диапазон портов принимает различные форматы, например диапазон портов (300:350), отдельные порты (566,789) или смешанный (1015:1024,3021).

   **ПРИМЕЧАНИЯ:**

   - Когда в Вашей сети отключен брандмауэр и Вы установили 80 порт для использования веб-сервером в локальной сети, этот веб-сервер будет конфликтовать с веб-интерфейсом роутера.
   - Сеть использует порты для обмена данными, где каждому порту присваиваются определенный номер и служба. Например, порт 80 используется для HTTP. Отдельный порт может одновременно использоваться только одним приложением или службой. Следовательно, попытка двух компьютеров получить доступ к данным через один и тот же порт приведет к ошибке. Например, нельзя использовать порт 100 для переадресации портов для двух компьютеров одновременно.

   - **Локальный IP-адрес:** Введите IP-адрес клиента локальной сети.

   **ПРИМЕЧАНИЕ:** Для корректной переадресации используйте для локального клиента статический IP-адрес. Подробную информацию смотрите в разделе **3.11 Локальная сеть**.

   - **Локальный порт:** Введите порт для пересылки пакетов. Оставьте это поле пустым, если хотите перенаправить входящие пакеты на диапазон портов.
   - **Протокол**: Выберите протокол. Если вы не уверены, выберите **BOTH**.
6. Нажмите **Добавить** для добавления информации в список. Нажмите **Удалить** для удаления информации из списка.
7. Когда закончите, нажмите Применить.

**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.

### 3.19.5 DMZ

Virtual DMZ отображает один компьютер в интернете, позволяя ему принимать все входящие пакеты, направленные в локальную сеть.

Входящий трафик из интернета обычно отбрасывается или перенаправляется на указанный компьютер, если настроена переадресация или переключение портов. В режиме DMZ один компьютер получает все входящие пакеты.

Включение DMZ оправдано при открытии неограниченного двухстороннего доступа к компьютеру, например серверу web или e-mail.

**Предупреждение:** Открытие всех портов клиента для сети Интернет делает сеть уязвимой для атак извне. Обратите внимание на риск, связанный с использованием DMZ.

**Для настройки DMZ:**

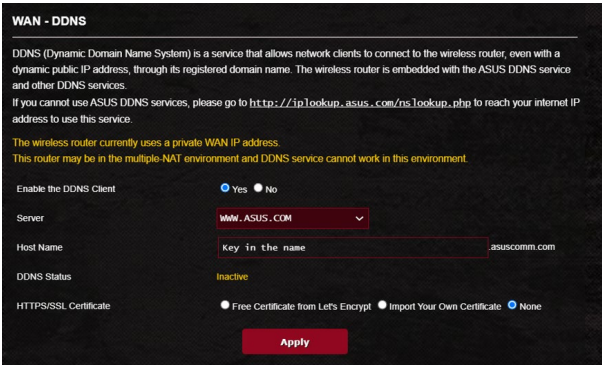
1. В меню навигации выберите **Дополнительные настройки** > **WAN** > **DMZ**.
2. Сконфигурируйте параметры ниже. Когда закончите, нажмите **Применить**.
   - **IP-адрес видимой станции:** Введите LAN IP-адрес клиента, который будет использоваться для DMZ. Убедитесь, что сервер использует статический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

**Для удаления DMZ:**

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

## 3.19.6 DDNS

Настройка DDNS (динамический DNS) позволяет получить доступ к роутеру из Интернет посредством службы ASUS DDNS или другой службы DDNS.




### Для настройки DDNS:

1. В меню навигации выберите **Дополнительные 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:**

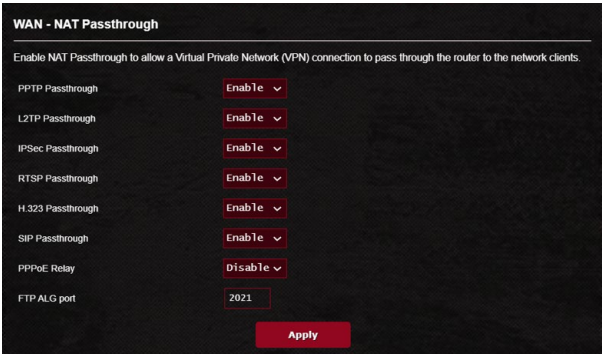
Служба DDNS сервис не будет работать при следующих условиях:

- 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.

## 3.19.7 NAT Passthrough

NAT Passthrough разрешает пакетам (VPN) проходить через роутер к сетевым клиентам. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough и RTSP Passthrough включены по умолчанию.

Для включения /отключения NAT Passthrough перейдите в **Дополнительные настройки** > **WAN** > **NAT Passthrough**. Когда закончите, нажмите **Применить**.



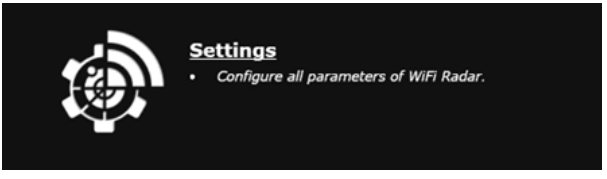
# 3.20 Wi-Fi Radar

Wi-Fi Radar - утилита для анализа беспроводной сети, анализирующая каналы и пакеты данных для устранения неполадок.

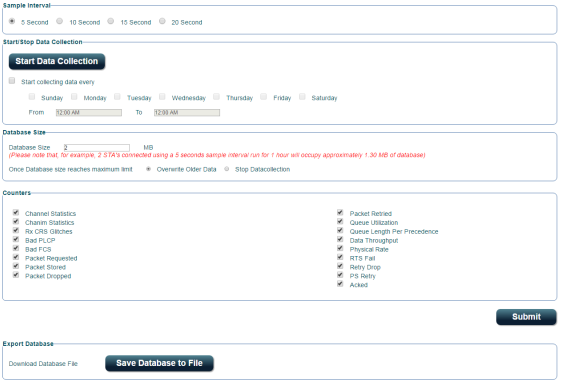
**ПРИМЕЧАНИЕ:** Включение Wi-Fi Radar может привести к снижению производительности беспроводной сети. Включайте Wi-Fi Radar только при необходимости.


### Для использования Wi-Fi Radar:

1. В меню навигации выберите **Общие** > **Wi-Fi Radar** > **Настройки** и сконфигурируйте параметры Wi-Fi Radar.



2. Нажмите **Start Data Collection** и установите расписание для сбора данных.
3. После задания всех параметров нажмите **Submit**.




## 3.20.1 Поиск сетей Wi-Fi

Поиск сетей Wi-Fi позволяет искать беспроводные сети.

## 3.20.2Статистика беспроводного канала

Эта функция показывает использование каналов для всех диапазонов и статистику распределения каналов.

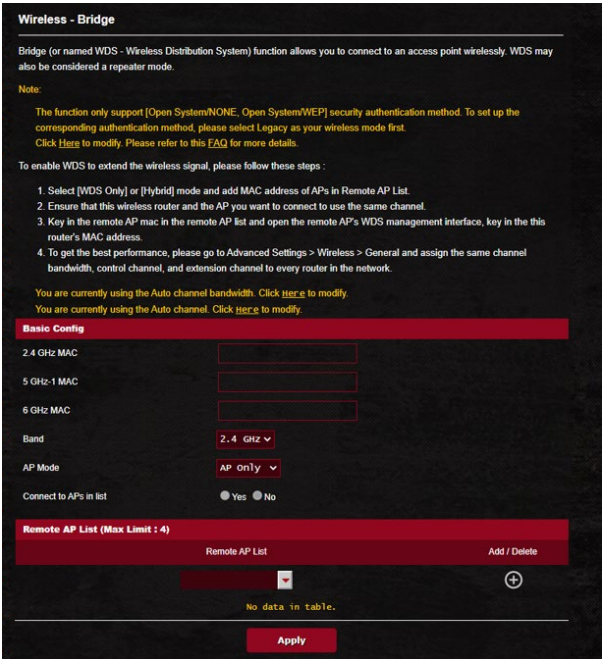

## 3.20.3Дополнительные способы устранения неисправностей

Эта функция показывает статистику сбоев Wi-Fi.

# 3.21 Беспроводная связь

## 3.21.1 Общие

На странице Общие можно сконфигурировать основные параметры беспроводной сети.




**Для конфигурации основных параметры беспроводной сети:**

1. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > **Общие**.
2. Выберите 2,4, 5 ГГц-1 или 5 ГГц-2 в качестве частотного диапазона для беспроводной сети.
3. Для использования функции Smart Connect переместите ползунок в поле **Enable Smart Connect** в положение **ВКЛ**. Эта функция автоматически подключает сетевых клиентов к соответствующему диапазону (2,4 ГГц, 5 ГГц-1 или 5 ГГц-2).

4. Для идентификации вашей беспроводной сети назначьте сетевое имя или SSID (Идентификатор беспроводной сети) длиной до 32 символов. Беспроводные устройства могут подключиться к беспроводной сети через назначенный SSID. SSID на информационном баннере обновляются при сохранении настроек.

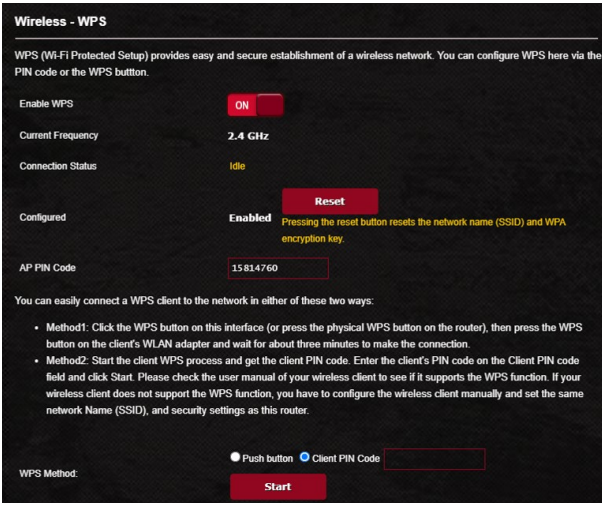
   **ПРИМЕЧАНИЕ:** Можно назначить уникальные SSID для частотных диапазонов 2,4 ГГц, 5 ГГц-1 или 5 ГГц-2.

5. 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.
6. Выберите беспроводной режим, определяющий тип беспроводных устройств, которые могут подключиться к роутеру:
   - **Авто**: Выберите Авто для разрешения подключения к роутеру устройств 802.11ac, 802.11n, 802.11 g и 802.11b.
   - **N only**: Выберите **N only** для максимальной производительности Wireless N. Этот режим запрещает подключение к роутеру устройств 802.11g и 802.11b.
   - **Legacy**: Выберите **Legacy** для разрешения подключения к роутеру устройств 802.11b/g/n. Максимальная скорость для устройств 802.11n будет 54 Мбит/с.
7. Выберите рабочий канал для беспроводного роутера. Выберите **Авто** для автоматического выбора канала с наименьшим количеством помех.
8. Выберите ширину канала для обеспечения высокой скорости передачи данных.
9. Выберите метод аутентификации.
10. Когда закончите, нажмите **Применить**.

## 3.21.2 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 **Дополнительные настройки** > **Беспроводная связь** > **WPS**.
2. В поле **Включить WPS** переместите ползунок в положение **ON**.
3. По умолчанию WPS использует частотный диапазон 2,4 ГГц. Если нужно изменить частотный диапазон 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.

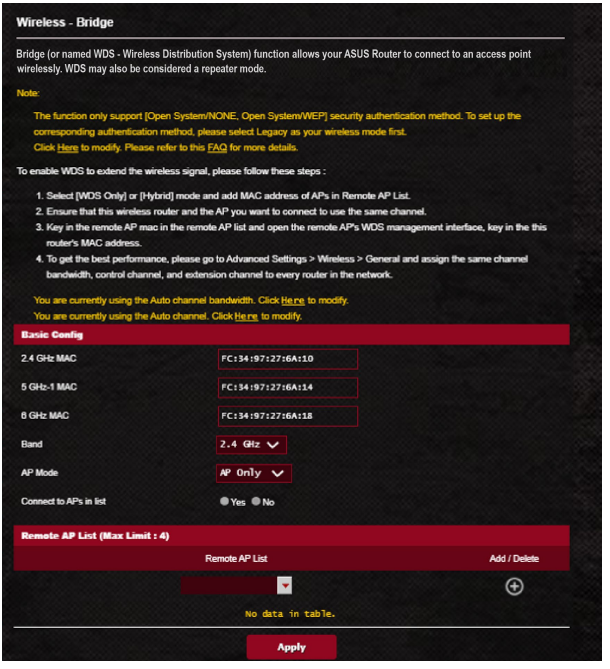
4. В поле Метод WPS выберите **Кнопка Push** или **ПИН-код клиента**. При выборе **Кнопка** перейдите к шагу 5. При выборе **ПИН-код клиента** перейдите к шагу 6.
5. Для настройки WPS с помощью кнопки на роутере, выполните следующие действия:
   a. Нажмите **Пуск** или нажмите кнопку WPS на задней панели 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.
6. 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.

## 3.21.3 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 **Дополнительные настройки** > **Беспроводная связь** > **WDS**.
2. Выберите диапазон частот для беспроводного моста.

3. В поле **Режим AP** выберите любую из следующих опций:
   - **AP Only**: Отключает функцию беспроводного моста.
   - **WDS Only**: Включает функцию беспроводного моста, но запрещает подключение к роутеру других беспроводных устройств.
   - **HYBRID**: Включает функцию беспроводного моста и разрешает подключение к роутеру других беспроводных устройств.

   **ПРИМЕЧАНИЕ:** Беспроводные устройства, подключенные к роутеру в гибридном режиме получат только половину скорости точки доступа.

4. В поле **Подключиться к точкам доступа в списке** выберите **Да**, если необходимо подключиться к точке доступа в списке удаленных AP.
5. По умолчанию, канал беспроводного моста установлен в **Авто**, что позволяет роутеру автоматически выбрать канал с наименьшим количеством помех.

   Канал можно изменить в **Дополнительные настройки** > **Беспроводная связь** > **Общее**.

   **ПРИМЕЧАНИЕ:** Доступность канала зависит от страны или региона.

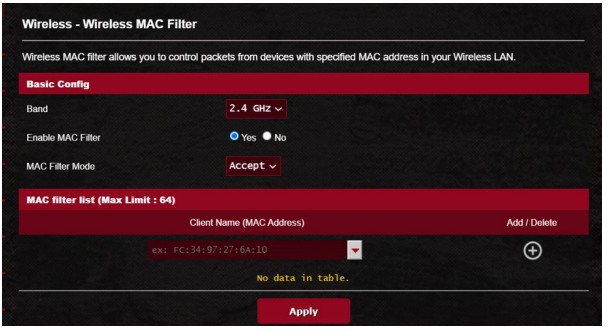
6. В списке удаленных AP введите MAC-адрес и нажмите **Добавить** ⊕ для ввода MAC-адреса доступной точки доступа Access Points.

   **ПРИМЕЧАНИЕ:** Любая добавленная в список точка доступа использовать одинаковый с роутером канал управления.

7. Нажмите **Применить**.

## 3.21.4 Фильтр MAC адресов беспроводной сети

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

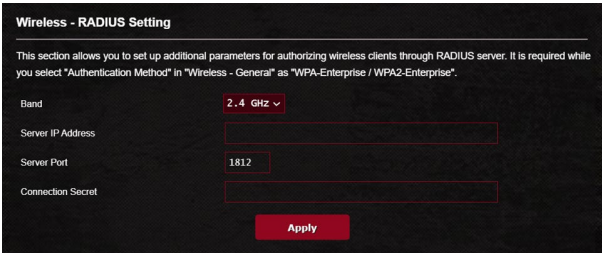



**Для настройки фильтра MAC адресов беспроводной сети:**

1. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > **Фильтр MAC-адресов беспроводной сети**.
2. Выберите диапазон частот.
3. В поле **Включить MAC фильтр** выберите **Да**.
4. 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.
5. В списке MAC-фильтра, нажмите кнопку **Добавить** ⊕ и введите MAC-адрес беспроводного устройства.
6. Нажмите **Применить**.

## 3.21.5 Настройка RADIUS

Настройка RADIUS (Remote Authentication Dial In User Service) обеспечивает дополнительный уровень безопасности при использовании режима аутентификации WPA-Enterprise, WPA2-Enterprise или Radius with 802.1x.




**Для настройки параметров RADIUS:**

1. Убедитесь, что режим аутентификации беспроводного роутера установлен в значение WPA-Enterprise или WPA2-Enterprise.

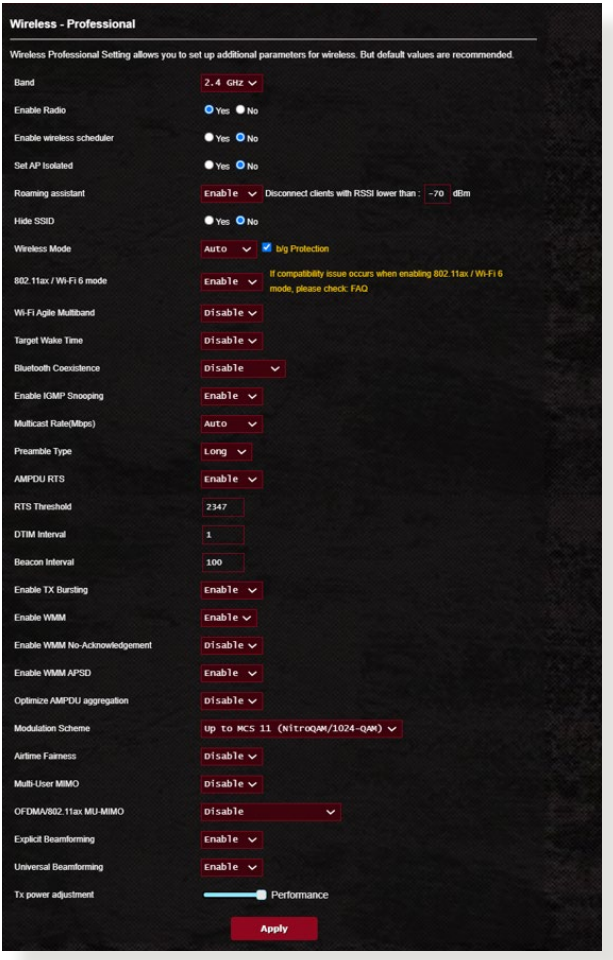
   **ПРИМЕЧАНИЕ:** Настройки режима аутентификации для беспроводного роутера смотрите в разделе **3.21.1 Общие**.

2. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > вкладка **Настройка RADIUS**.
3. Выберите диапазон частот.
4. В поле **IP-адрес сервера** введите IP-адрес сервера RADIUS.
5. В поле **Порт сервера** введите порт сервера.
6. В поле **Ключ соединения** назначьте пароль для доступа к серверу RADIUS.
7. Нажмите **Применить**.

## 3.21.6 Профессиональный

На экране Профессиональный можно сконфигурировать дополнительные параметры.

**ПРИМЕЧАНИЕ:** Мы рекомендуем использовать значения по умолчанию.




На экране **Профессиональные настройки** 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**: Выберите **Да** для включения и конфигурации беспроводного планировщика. Выберите **Нет** для отключения беспроводного планировщика.
  - **Дата включения радиомодуля (рабочие дни)**: Можно указать режим работы беспроводной сети в рабочие дни.
  - **Время включения радиомодуля**: Можно указать время работы беспроводной сети в рабочие дни.
  - **Дата включения радиомодуля (выходные)**: Можно указать режим работы беспроводной сети в выходные дни.
  - **Время включения радиомодуля**: Можно указать время работы беспроводной сети в выходные дни.
- **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.
- **Уменьшение помех USB 3.0:** Включение этой функции обеспечивает наилучшую

производительность беспроводной связи на частоте 2,4 ГГц. Отключение этой функции увеличивает скорость передачи данных по USB 3.0 и может повлиять на радиус действия беспроводной сети в диапазоне 2,4 ГГц.

- **Оптимизация агрегации AMPDU**:  Оптимизируйте максимальное количество MPDU в AMPDU для избежание потерь или повреждения пакетов при передаче их по нестабильным беспроводным каналам
- **Turbo QAM**: Включение этой функции позволяет поддерживать 256-QAM (MCS 8/9) для диапазона 2,4 ГГц для достижения большей дальности и пропускной способности.
- **Распределения эфира**: С помощью распределения эфира, скорость сети не определяется самым медленным трафиком. Распределяя время поровну между клиентами, распределение эфира позволяет каждому пакету двигаться с максимальной скоростью.
- **Явное формирование луча**: Клиентские адаптеры и роутер поддерживают технологию формирования луча. Эта технология позволяет этим устройствам взаимодействовать, оценивать качество канала и управлять направлением сигнала для улучшения скорости передачи данных.
- **Универсальное формирование луча**: Для устаревших беспроводных адаптеров, которые не поддерживают формирование диаграммы направленности, роутер оценивает канал и определяет направление для улучшения скорости передачи данных.

# 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.

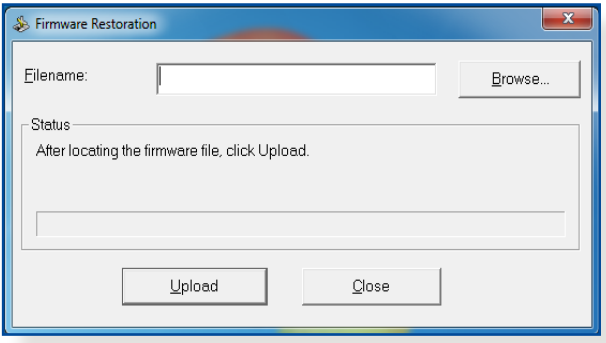
**Для запуска утилиты Device Discovery:**

- Перейдите **Пуск** > **Программы** > **ASUS Utility** > **ASUS 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.




**ВАЖНО!** 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 GT6 Wireless Router** > **Firmware Restoration**.

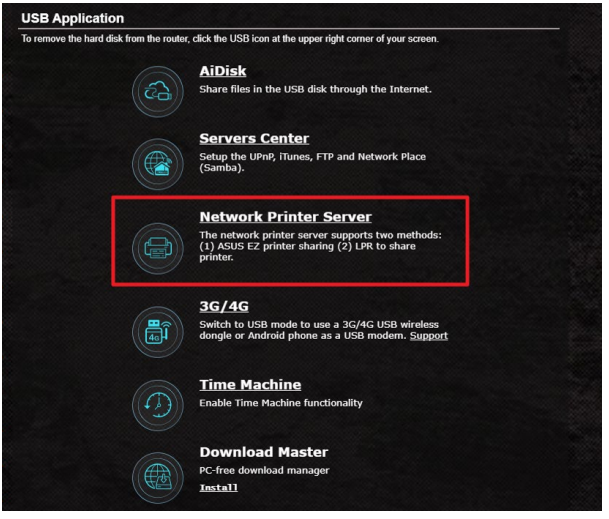
5. Укажите файл и нажмите **Upload**.

**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 главе 3 **Конфигурация общих и дополнительных параметров**.

## 4.3 Настройка сетевого принтера

### 4.3.1 Общий принтер ASUS EZ

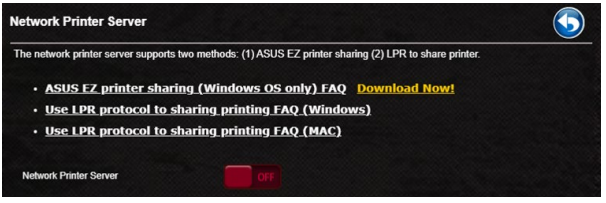
Утилита ASUS EZ Printing позволяет к USB порту роутера подключить USB принтер и настроить сервер печати. Это позволяет сетевым клиентам печатать файлы и сканировать документы.



**ПРИМЕЧАНИЕ:** Функция сетевого принтера поддерживается только в Windows 7/8/8.1/10.

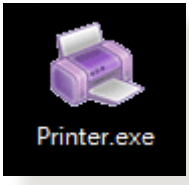
### Для установки утилиты EZ Printer sharing:

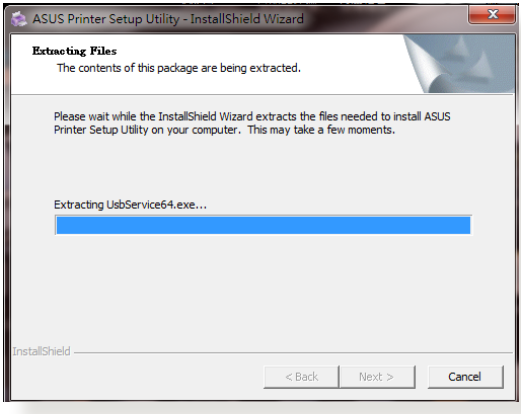
1. В меню навигации выберите **Дополнительные настройки** > **USB-приложение** > **Сервер печати**.
2. Нажмите **Скачать сейчас** для загрузки утилиты сетевого принтера.



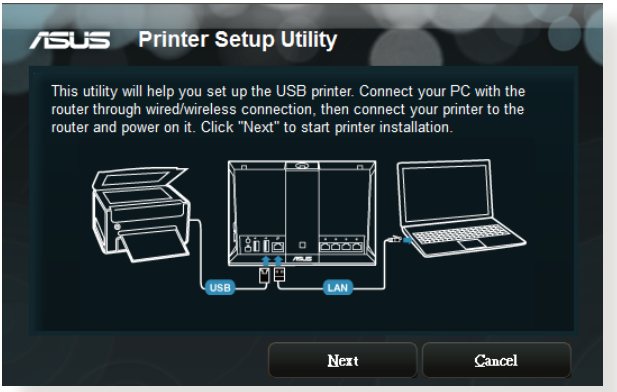

**ПРИМЕЧАНИЕ:** Утилита сетевого принтера поддерживается в Windows 7/8/8.1/10. Для установки утилиты на Mac OS, выберите **Используйте протокол LPR для общей печати**.

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



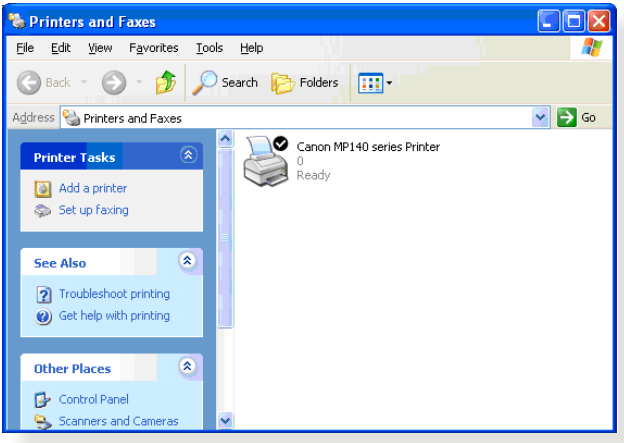
4. Следуйте инструкциям на экране для настройки оборудования, затем нажмите **Next**.




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.



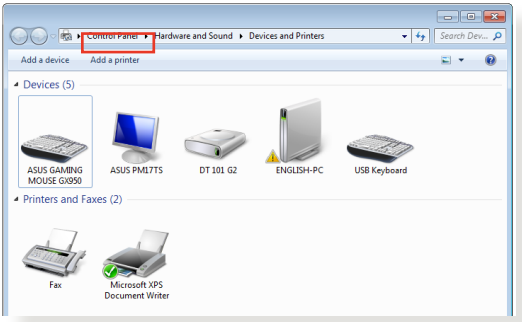
## 4.3.2 Использование LPR для совместного использования принтера

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

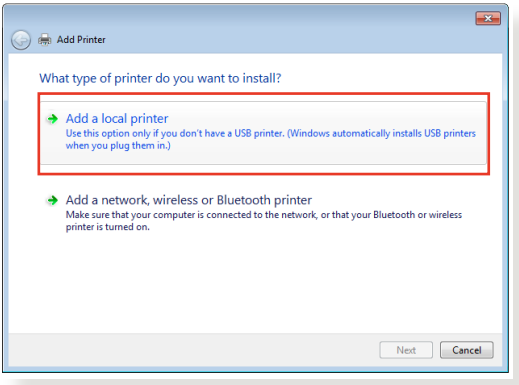
### Совместное использование принтера LPR

**Для совместного использования принтера LPR:**

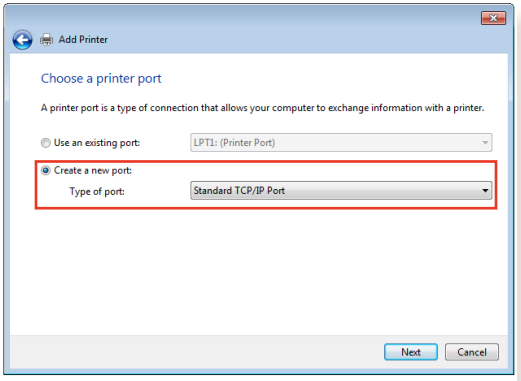
1. Для запуска **Мастера установки принтера** нажмите **Пуск** > **Устройства и принтеры** > **Мастер установки**.



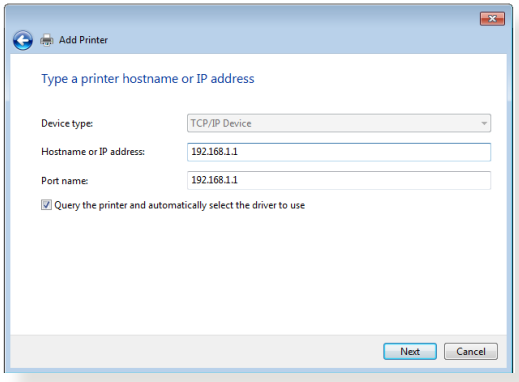

2. Выберите **Добавить локальный принтер**, затем нажмите **Далее**.



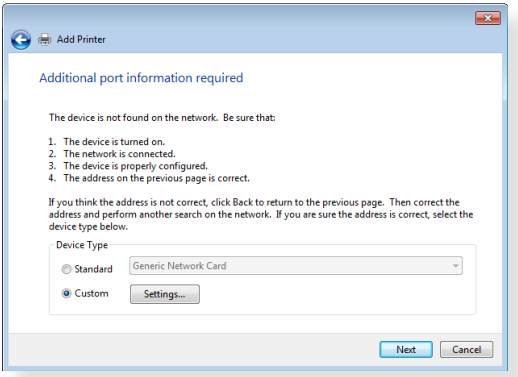
3. Выберите **Создать новый порт**, затем установите **Тип порта** в значение **Стандартный порт TCP/IP**. Нажмите **Далее**.



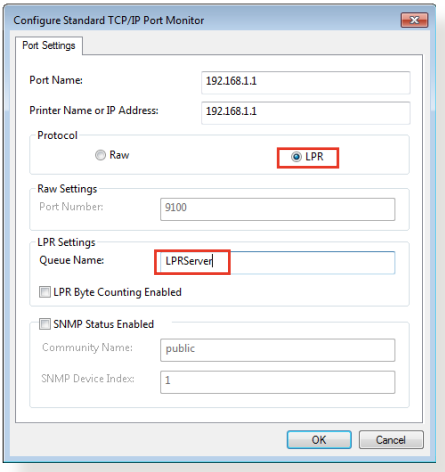

4. В поле **Имя хоста или IP-адрес** введите IP-адрес беспроводного роутера и нажмите **Далее**.



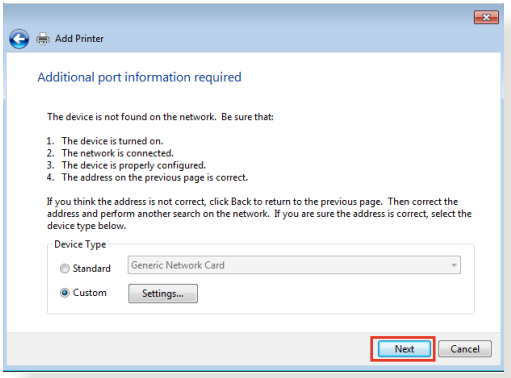
5. Выберите **Пользовательский**, затем нажмите **Настройки**.



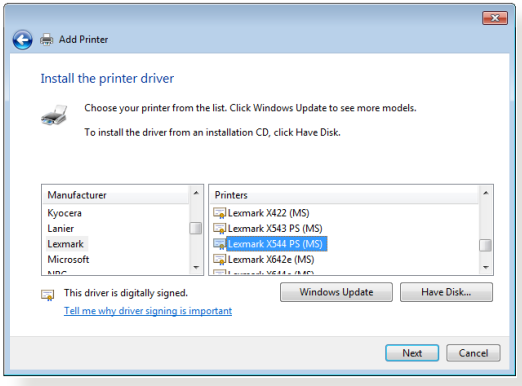

6. Установите **Протокол** в **LPR**. В поле **Имя очереди** введите **LPRServer**, затем нажмите **OK** для продолжения.



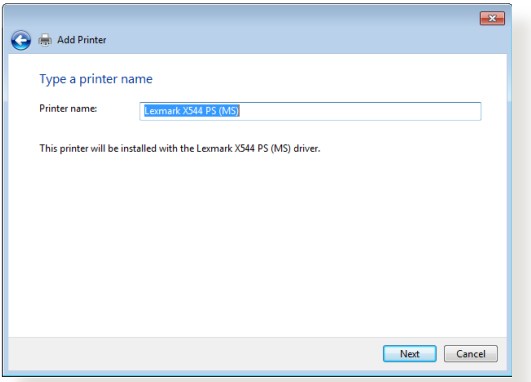
7. Нажмите **Далее** для завершения настройки порта TCP/IP.



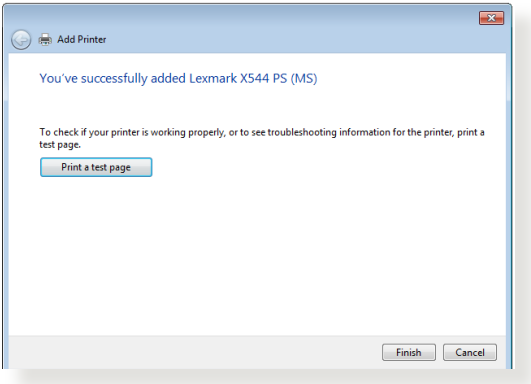

8. Установите драйвер принтера из списка. Если принтер отсутствует в списке, нажмите **Have Disk** для установки драйвера принтера вручную.



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




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



## 4.4 Download Master

Download Master - утилита, позволяющая загружать файлы, даже в то время как ваш компьютер выключен.

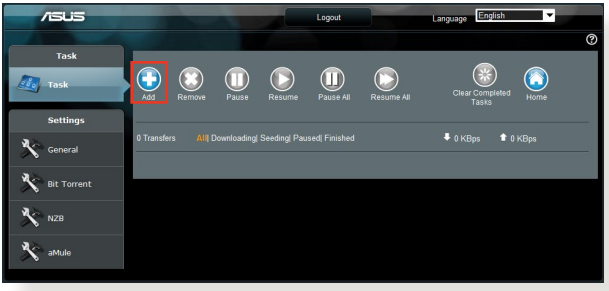
**ПРИМЕЧАНИЕ:** Для использования Download Master необходимо подключить к роутеру USB-накопитель.

**Для использования Download Master:**

1. Нажмите **Дополнительные настройки** > **USB-приложение** > **Download Master** для скачивания и установки утилиты.

   **ПРИМЕЧАНИЕ:** Если у вас несколько USB-накопителей, выберите устройство для хранения скачанных файлов.

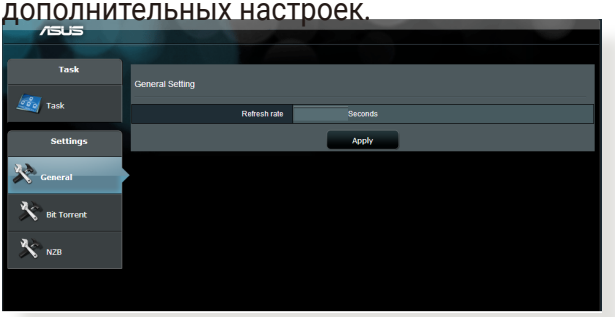
2. После завершения скачивания нажмите иконку Download Master для использования утилиты.
3. Нажмите **Добавить** для добавления закачки.



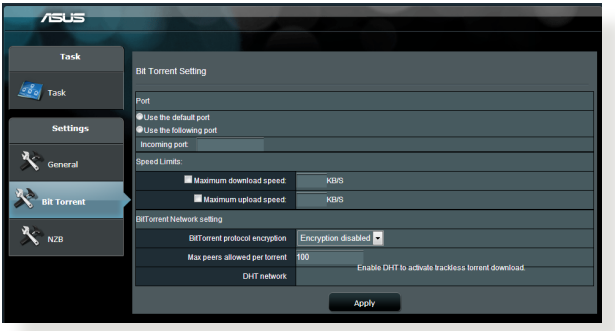

4. Выберите тип загрузки BitTorrent, HTTP или FTP. Введите торрент-файл или URL-адрес для начала загрузки.

   **ПРИМЕЧАНИЕ:** Подробную информацию о Bit Torrent смотрите в разделе **4.4.1 Конфигурация параметров Bit Torrent**.

5. Используйте панель навигации для конфигурации дополнительных настроек.




## 4.4.1Конфигурация параметров Bit Torrent

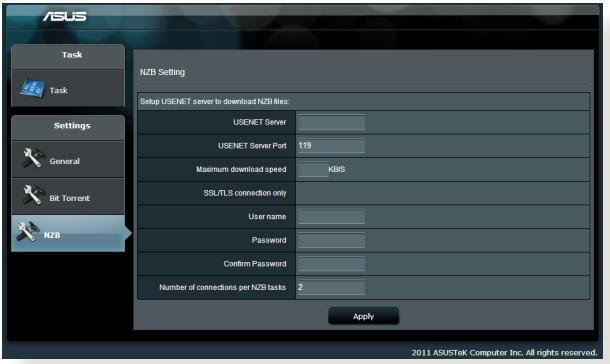



**Для конфигурации параметров BitTorrent:**

1. В панели навигации Download Master нажмите **Bit Torrent** для открытия страницы **Настройки Bit Torrent** .
2. Выберите порт, используемый для загрузки.
3. Во избежание перегрузки сети можно ограничить максимальную скорость скачивания и загрузки в области **Ограничение скорости**.
4. Можно ограничить максимальное количество разрешенных пиров и включить или отключить шифрование файлов во время загрузки.

## 4.4.2 Настройки NZB

Можете настроить сервер USENET для загрузки файлов NZB. После ввода параметров USENET нажмите **Применить**.



# 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/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. Войдите в веб-интерфейс. Перейдите в **Дополнительные настройки** > **Администрирование** > **Обновление прошивки**. Нажмите **Проверить** для проверки наличия последней версии прошивки.
2. Если доступна новая прошивка, посетите сайт ASUS https://rog.asus.com/networking/rog-rapture-GT6-model/helpdesk_download 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.

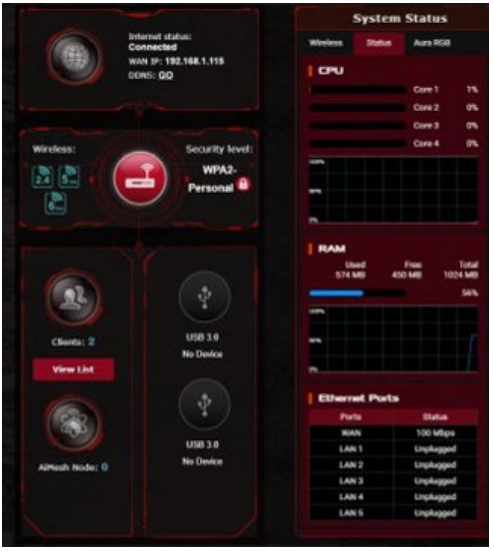
- При правильном подключении Ethernet-кабеля к модему индикатор WAN будет гореть.
- При правильном подключении Ethernet-кабеля к включенному компьютеру индикатор LAN будет гореть.

### 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 **Карта сети** > страница **Клиенты** или навести курсор мыши на устройство в поле **Состояние клиента**.

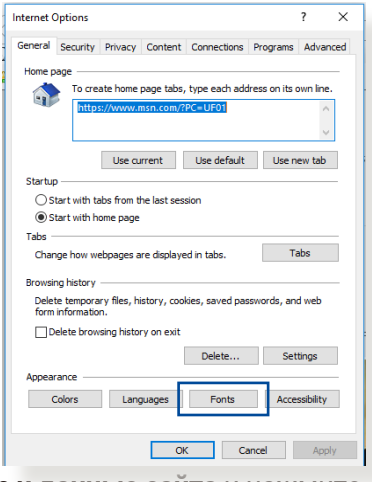


## 5.2 Часто задаваемые вопросы (FAQ)

### 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. 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**.



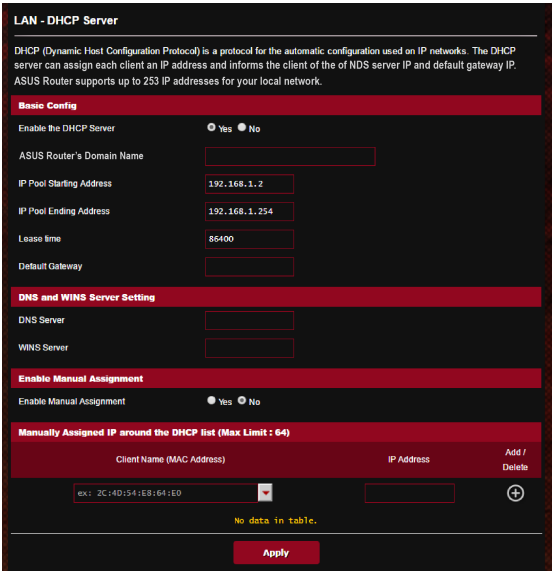

**ПРИМЕЧАНИЯ:**

- 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.

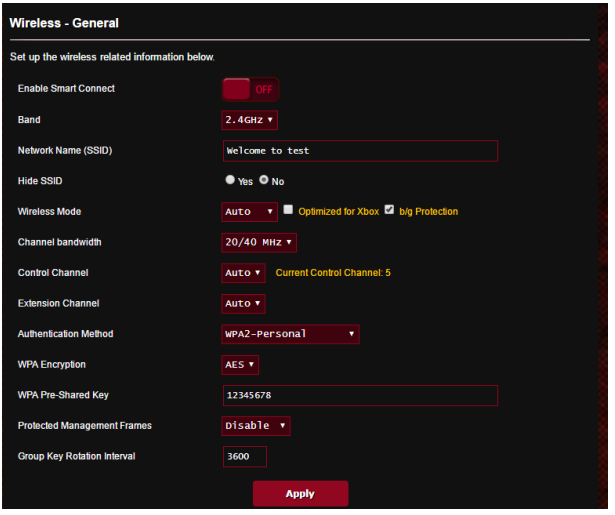
## Клиент не может установить беспроводное соединение с роутером.

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

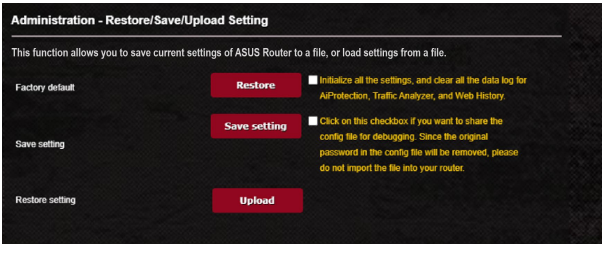
- **Вне зоны покрытия:**
  - Поместите роутер ближе к беспроводному клиенту.
- **DHCP-сервер отключен:**
  1. Войдите в веб-интерфейс. Перейдите в **Общие** > Карта сети > **Клиенты** и найдите устройство, которое нужно подключить к роутеру.
  2. Если не удалось найти устройство на **карте сети**, перейдите в **Дополнительные настройки** > **LAN** > вкладка **DHCP-сервер**, раздел **Основные настройки** и в поле **Включить DHCP-сервер** выберите **Да**.



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




- 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. Войдите в веб-интерфейс, перейдите в **Администрирование** > вкладка **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 **Дополнительные настройки** > **Карта сети** и проверьте **Состояние Интернет**.
- Если роутер не может подключиться к вашему провайдеру, попробуйте переподключить сеть как описано в разделе **Последовательность перезапуска сети**.


- Устройство было заблокировано с помощью функции родительского контроля. Перейдите в **Общие**> **Aiprotection** вкладка **Родительский контроль** и проверьте, находится ли устройство в списке. Если устройство в списке, удалите его, нажав **Delete** или настройте параметры времени.
- 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 **Карта сети**, 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 **Администрирование** > вкладка **Восстановить, Сохранить, Загрузить настройки** и нажмите **Восстановить**.

## Как сбросить систему к настройкам по умолчанию?

- Перейдите в **Администрирование** > вкладка **Восстановить, Сохранить, Загрузить настройки** и нажмите **Восстановить**.

  Параметры системы по умолчанию:

| | |
|---|---|
| **Включен DHCP:** | Да (если WAN кабель подключен) |
| **IP-адрес:** | http://www.asusrouter.com (или 192.168.50.1) |
| **Имя домена:** | (пусто) |
| **Маска подсети:** | 255.255.255.0 |
| **DNS сервер 1:** | 192.168.50.1 |
| **DNS сервер 2:** | (пусто) |
| **SSID (2,4 ГГц):** | ASUS_XX_2G |
| **SSID (5 ГГц-1):** | ASUS_XX_5GHz-1 |
| **SSID (5 ГГц-2):** | ASUS_XX_5GHz-2 |

## 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**.

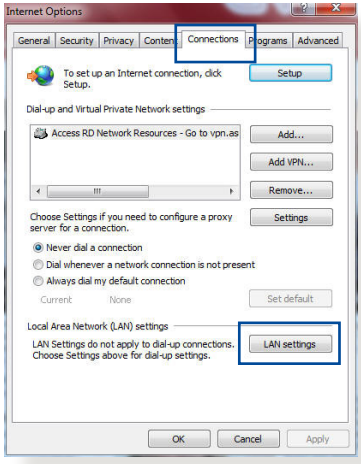
## Невозможно подключиться к веб-интерфейсу

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

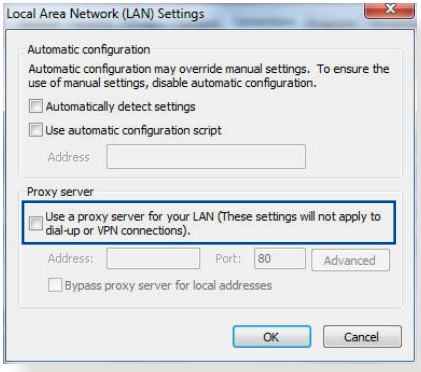
### A. Отключите прокси-сервер, если он включен.

#### Windows

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

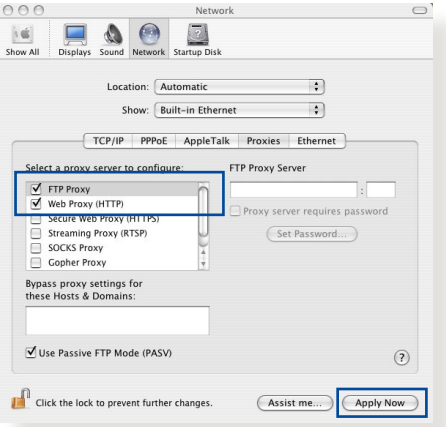



3. На экране **настройки локальной сети** отключите использование прокси-сервера для локальной сети.
4. Нажмите **OK** когда закончите.



### 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**.

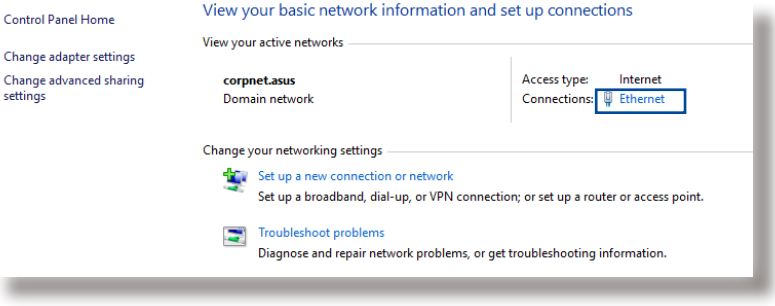



**ПРИМЕЧАНИЕ:** Для получения подробной информации по отключению использования прокси-сервера, обратитесь к справке браузера.

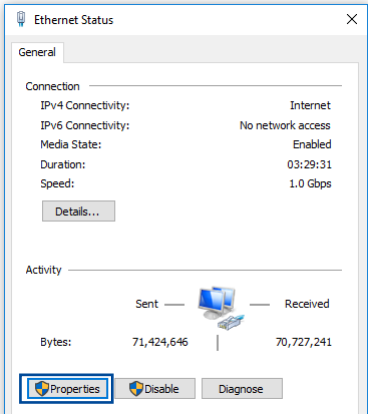
## B. Настройте TCP/IP для автоматического получения IP-адреса.

### Windows

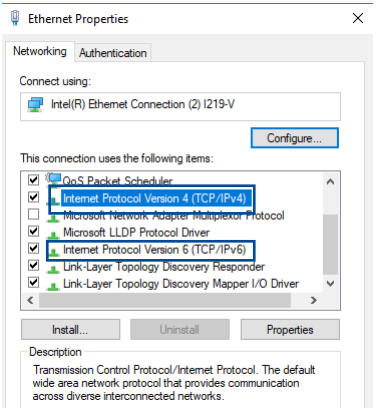
1. Нажмите **Пуск > Панель управления > Центр управления сетями и общим доступом**, затем нажмите сетевое подключение для отображения его состояния.



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



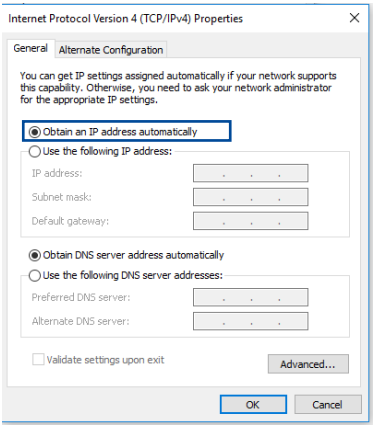

3. Выберите **Протокол Интернета версии 4(TCP/IPv4)** или **Протокол Интернета версии 6(TCP/IPv6)**, затем нажмите **Свойства**.




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

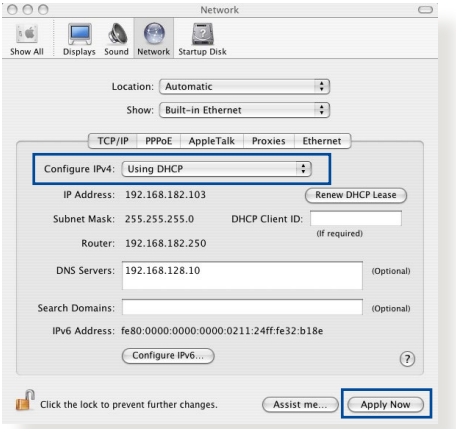
   Выберите **Получить IPv6-адрес автоматически** для автоматического получения IP-адреса IPv6.

5. Нажмите **OK** 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**.

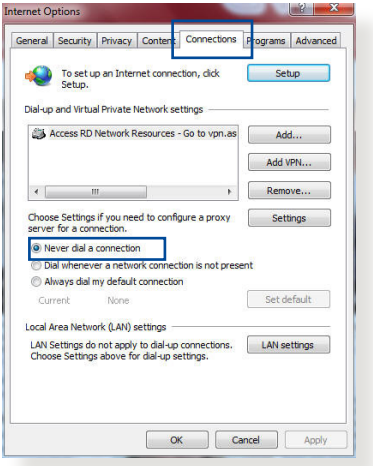



**ПРИМЕЧАНИЕ:** Подробную информацию по конфигурации настроек TCP/IP смотрите в справке к вашей операционной системе.

## 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. Please visit our web site for updated information. 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/.