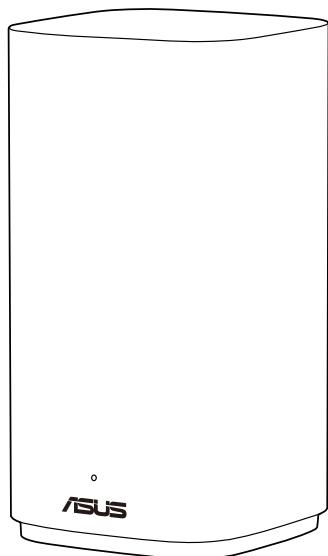


# Руководство пользователя

## ZenWiFi BD4 Outdoor

Двухдиапазонный роутер AX3600



**ASUS**  
IN SEARCH OF INCREDIBLE

R25876

Проверенное издание V2

Январь 2024

**Copyright © 2025 ASUSTeK Computer Inc. Все права защищены.**

Любая часть этого руководства, включая оборудование и программное обеспечение, описанные в нем, не может быть дублирована, передана, преобразована, сохранена в системе поиска или переведена на другой язык в любой форме или любыми средствами, кроме документации, хранящейся покупателем с целью резервирования, без специального письменного разрешения ASUSTeK Computer Inc. ("ASUS").

Гарантия прекращается, если: (1) изделие отремонтировано, модифицировано или изменено без письменного разрешения ASUS; (2) серийный номер изделия поврежден, неразборчив либо отсутствует.

ASUS ПРЕДОСТАВЛЯЕТ ДАННОЕ РУКОВОДСТВО "КАК ЕСТЬ" БЕЗ ГАРАНТИИ ЛЮБОГО ТИПА, ЯВНО ВЫРАЖЕННОЙ ИЛИ ПОДРАЗУМЕВАЕМОЙ, ВКЛЮЧАЯ НЕЯВНЫЕ ГАРАНТИИ ИЛИ УСЛОВИЯ ПОЛУЧЕНИЯ КОММЕРЧЕСКОЙ ВЫГОДЫ ИЛИ ПРИГОДНОСТИ ДЛЯ КОНКРЕТНОЙ ЦЕЛИ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМИ ГАРАНТИЯМИ И УСЛОВИЯМИ. КОМПАНИЯ ASUS, ЕЕ ДИРЕКТОРЫ, РУКОВОДИТЕЛИ, СОТРУДНИКИ ИЛИ ПРЕДСТАВИТЕЛИ НЕ НЕСУТ НИКАКОЙ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ОСОБЫЕ ИЛИ СЛУЧАЙНЫЕ УБЫТКИ (ВКЛЮЧАЯ УБЫТКИ ОТ УПУЩЕННОЙ ВЫГОДЫ, УТРАТУ ДЕЯТЕЛЬНОСТИ, НЕ ИСПОЛЬЗОВАНИЕ ИЛИ ПОТЕРЮ ДАННЫХ, ПРЕРЫВАНИЕ ДЕЯТЕЛЬНОСТИ И ТОМУ ПОДОБНОЕ), ДАЖЕ ЕСЛИ КОМПАНИЯ ASUS БЫЛА ОСВЕДОМЛЕНА О ВОЗМОЖНОСТИ УБЫТКОВ ВСЛЕДСТВИЕ ДЕФЕКТА ИЛИ ОШИБКИ В ДАННОМ РУКОВОДСТВЕ ИЛИ ПРОДУКТЕ.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ И ИНФОРМАЦИЯ, СОДЕРЖАЩИЕСЯ В ДАННОМ РУКОВОДСТВЕ, ПРИВОДЯТСЯ ТОЛЬКО В ЦЕЛЯХ ОЗНАКОМЛЕНИЯ. ОНИ МОГУТ БЫТЬ ИЗМЕНЕНЫ В ЛЮБОЕ ВРЕМЯ БЕЗ УВЕДОМЛЕНИЯ И НЕ ДОЛЖНЫ РАССматРИВАТЬСЯ КАК ОБЯЗАТЕЛЬСТВО СО СТОРОНЫ ASUS. КОМПАНИЯ ASUS НЕ НЕСЕТ НИКАКОЙ ОТВЕТСТВЕННОСТИ И ОБЯЗАТЕЛЬСТВ ЗА ЛЮБЫЕ ОШИБКИ ИЛИ НЕТОЧНОСТИ, КОТОРЫЕ МОГУТ СОДЕРЖАТЬСЯ В НАСТОЯЩЕМ РУКОВОДСТВЕ, ВКЛЮЧАЯ ОПИСАНИЯ ПРОДУКЦИИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

Продукция и названия корпораций, имеющиеся в этом руководстве, могут являться зарегистрированными торговыми знаками или быть защищенными авторскими правами соответствующих компаний и используются только в целях идентификации.

# Оглавление

<b>1</b>	<b>Информация о беспроводном роутере</b>	
1.1	Приветствие!	6
1.2	Комплект поставки	6
1.3	Данный беспроводной роутер	7
1.4	Размещение роутера	8
1.5	Системные требования	9
<b>2</b>	<b>Начало работы</b>	
2.1	Настройка роутера	10
A.	Проводное подключение	11
B.	Беспроводное подключение	12
2.2	Быстрая настройка Интернет (QIS) с автоопределением..	
	14	
2.3	Подключение к беспроводной сети	16
<b>3</b>	<b>Конфигурация общих и дополнительных параметров</b>	
3.1	Вход в веб-интерфейс	17
3.1.1	Настройка параметров безопасности беспроводной сети	19
3.1.2	Управление сетевыми клиентами	20
3.2	Адаптивная QoS	21
3.2.1	Управление QoS (качество обслуживания)	21
3.3	Администрирование	24
3.3.1	Режим работы	24
3.3.2	Система	25
3.3.3	Обновление прошивки	26
3.3.4	Восстановление/сохранение/загрузка настроек..	26
3.4	AiProtection	27
3.4.1	Сетевая защита	27
3.4.2	Настройка Родительского контроля	31

# Оглавление

<b>3.5 Брандмауэр .....</b>	<b>34</b>
3.5.1 Общие.....	34
3.5.2 Фильтр URL.....	35
3.5.3 Фильтр ключевых слов.....	36
3.5.4 Фильтр сетевых служб .....	37
<b>3.6 IPv6 .....</b>	<b>38</b>
<b>3.7 Локальная сеть.....</b>	<b>39</b>
3.7.1 LAN IP .....	39
3.7.2 DHCP-сервер.....	40
3.7.3 Маршрут .....	42
3.7.4 IPTV.....	43
<b>3.8 Сеть .....</b>	<b>44</b>
3.8.1 Основная сеть - Фильтр MAC-адресов .....	44
3.8.2 Гостевая сеть.....	46
3.8.2.1 Гостевая сеть.....	46
3.8.2.2 Мастер умного дома.....	48
<b>3.9 Системный журнал .....</b>	<b>52</b>
<b>3.10 Анализатор трафика.....</b>	<b>53</b>
<b>3.11 WAN .....</b>	<b>54</b>
3.11.1 Подключение к интернету .....	54
3.11.2 Переключение портов.....	57
3.11.3 Виртуальный сервер/Переадресация портов.....	59
3.11.4 DMZ .....	62
3.11.5 DDNS .....	63
3.11.6 NAT Passthrough.....	64
<b>3.12 Беспроводная связь .....</b>	<b>65</b>
3.12.1 Общие .....	65
3.12.2 WPS .....	68

# **Оглавление**

3.12.3 Настройка RADIUS.....	70
3.12.4 Профессиональный.....	71
<b>4 Утилиты</b>	
4.1 Обнаружение устройства.....	74
4.2 Восстановление прошивки .....	74
<b>5 Устранение неисправностей</b>	
5.1 Устранение основных неисправностей.....	76
5.2 Часто задаваемые вопросы (FAQ) .....	79
<b>Приложение</b>	
Правила безопасности .....	97
Сервис и поддержка.....	99

# 1 Информация о беспроводном роутере

## 1.1 Приветствие!

Благодарим вас за приобретение беспроводного роутера ASUS ZenWiFi BD4 Outdoor

ZenWiFi BD4 Outdoor в белом корпусе поддерживает два диапазона 2,4 ГГц и 5 ГГц для непрерывной беспроводной потоковой передачи HD-контента. Он включает в себя SMB-сервер, UPnP AV-сервер и FTP-сервер для обмена файлами в режиме 24/7, способен обрабатывать до 300000 сеансов и включает в себя технологию ASUS Green Network, обеспечивающую энергосбережение до 70%.

## 1.2 Комплект поставки

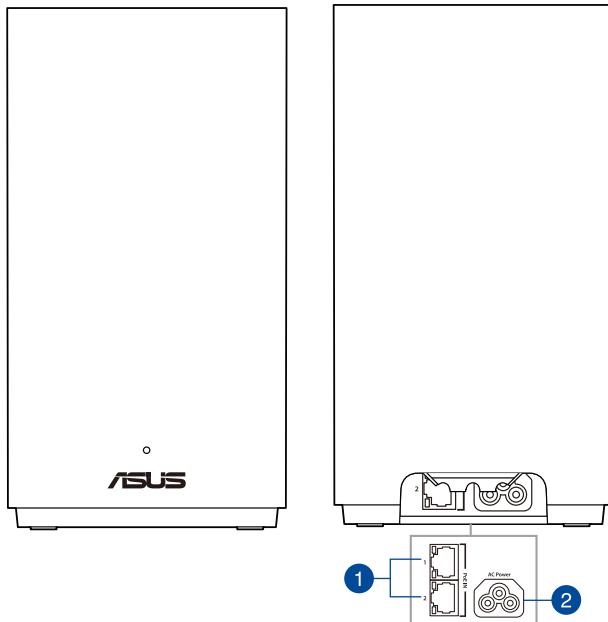
- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Беспроводной роутер<br>ZenWiFi BD4 Outdoor | <input checked="" type="checkbox"/> Сетевой кабель (RJ-45)                       |
| <input checked="" type="checkbox"/> Сетевой шнур                               | <input checked="" type="checkbox"/> Комплект для крепления<br>к стене или столбу |
| <input checked="" type="checkbox"/> Краткое руководство                        | <input checked="" type="checkbox"/> Гарантийный талон                            |

---

### 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 Разъемы 2,5GbE (автоопределение PoE и WAN/LAN)

Разъемы 2,5GbE предназначены для подключения к оптическому модему или к коммутатору или шлюзу PoE+ с помощью сетевого кабеля.

### 2 Разъем питания

Разъем питания предназначен для подключения к розетке с помощью шнура питания.

---

---

## ПРИМЕЧАНИЯ:

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

Входное напряжение	110 В ~ 240 В (50 ~ 60 Гц), 2 А		
Температура при работе	-30~60°C	при хранении	-40~70°C
Влажность при работе	10~90%	при хранении	5~90%

---

## 1.4 Размещение роутера

Для улучшения беспроводной связи между роутером и беспроводными устройствами выполните следующее:

- Поместите беспроводной роутер в центре беспроводной сети для максимального покрытия.
- Поместите устройство подальше от металлических преград и прямых солнечных лучей.
- Для предотвращения помех поместите устройство подальше от устройств стандарта 802.11 или устройств, работающих на частоте 2,4 или 5ГГц, устройств Bluetooth, беспроводных телефонов, трансформаторов, мощных двигателей, флюоресцентных ламп, микроволновых лучей, холодильников и другого промышленного оборудования.
- Используйте последнюю прошивку. Для получения подробной информации о наличии свежей прошивки посетите сайт ASUS <http://www.asus.com>.

## 1.5 Системные требования

Для настройки сети необходим компьютер, соответствующий следующим требованиям:

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

---

### ПРИМЕЧАНИЯ:

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

---

### 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!

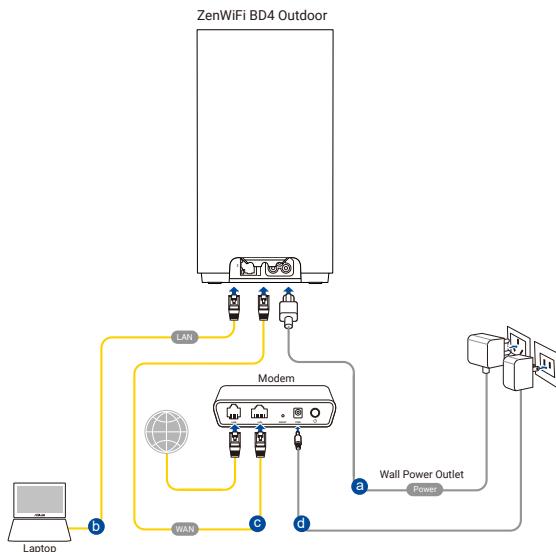
- Шнур питания должен быть подключен к розетке с заземлением. Подключайте устройство к ближайшей, легкодоступной розетке.
- Если шнур питания неисправен, не пытайтесь отремонтировать его самостоятельно. Обратитесь к квалифицированному технику или продавцу.
- Не пользуйтесь поврежденными сетевыми шнурами, аксессуарами и периферийными устройствами.
- Не устанавливайте это устройство 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) кабель.

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

1. Подключите роутер к электрической розетке и включите его. Подключите сетевой кабель от компьютера к разъему 2,5 Гбит/с на роутере.

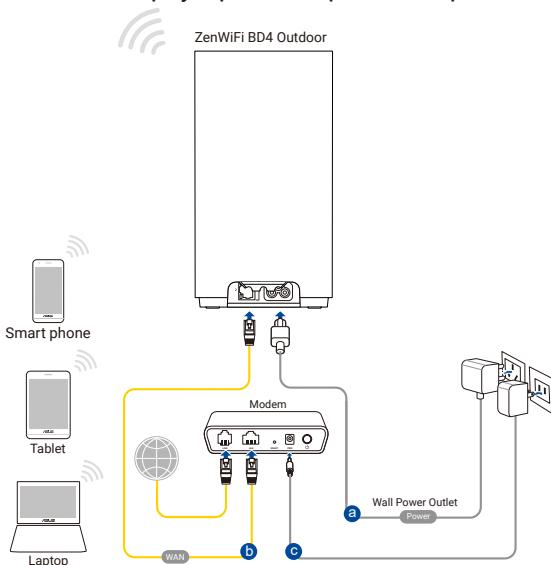


2. Веб-интерфейс запускается автоматически при открытии браузера. Если он не запустился автоматически, введите <http://www.asusrouter.com>
  3. Задайте пароль роутера для предотвращения несанкционированного доступа.

## 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\_BD4 Outdoor

\* 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.
  - Для настройки параметров безопасности сети, обратитесь к разделу **3.1.1 Настройка параметров безопасности беспроводной сети** в данном руководстве.
-

## 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 **Настройки вручную** и вручную сконфигурируйте тип подключения.
- 
3. Назначьте имя сети (SSID) и ключ безопасности для беспроводного подключения WiFi 7. Когда закончите, нажмите **Применить**.
  4. На странице **Конфигурация входа в систему** измените пароль роутера, для предотвращения несанкционированного доступа.

---

**ПРИМЕЧАНИЕ:** Имя пользователя и пароль для входа в роутер отличаются от имени сети Wi-Fi 7 (SSID) и ключа безопасности. Имя пользователя и пароль позволяют войти в веб-интерфейс роутера для конфигурации параметров беспроводного роутера. Имя сети Wi-Fi 7 (SSID) и ключ безопасности позволяют устройствам Wi-Fi подключаться к вашей сети Wi-Fi 7.

---

## 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 сетисмотрите в следующей главе.
  - Подробную информацию по подключению устройства к беспроводной сетисмотрите в руководстве пользователя устройства.
-

### **3 Конфигурация общих и дополнительных параметров**

#### **3.1 Вход в веб-интерфейс**

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

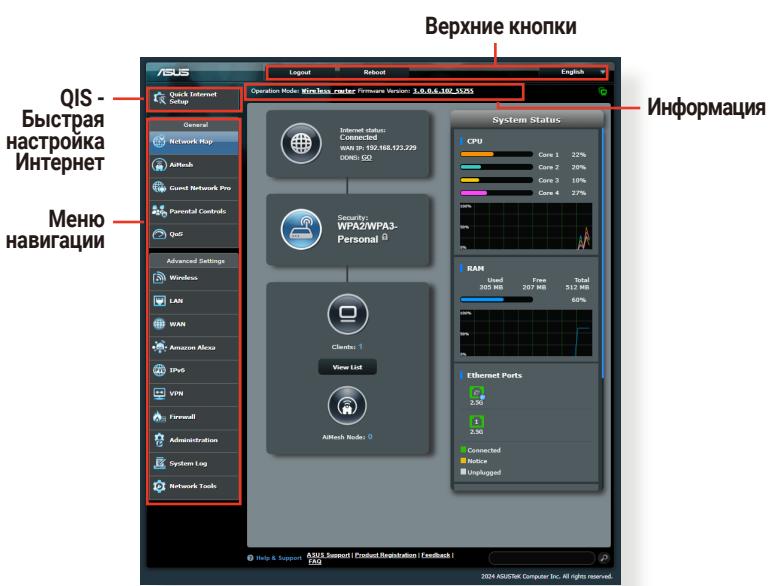
---

**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).

---

### 3.1.1 Настройка параметров безопасности беспроводной сети

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

**Для настройки параметров безопасности:**

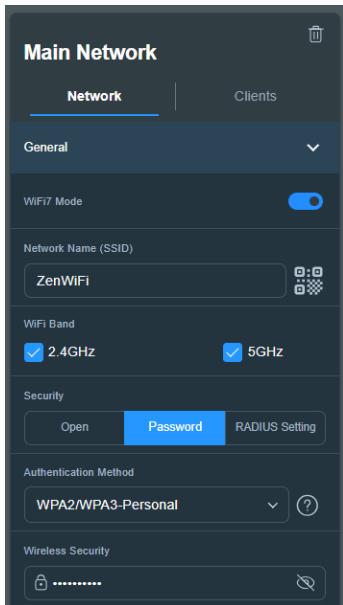
1. В меню навигации выберите **Общие > Карта сети**.
2. Выберите сеть, и вы сможете настроить параметры безопасности беспроводной сети, например SSID, уровень безопасности и параметры шифрования.

---

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

---

#### Настройки безопасности 2,4 ГГц и 5 ГГц



3. В поле **Network Name (SSID)** введите уникальное имя для вашей беспроводной сети.
4. В выпадающем списке **WEP-шифрование** выберите метод шифрования для беспроводной сети.

---

**ВАЖНО!** Стандарт IEEE 802.11n/ac/ax 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. Введите код безопасности.
6. Когда закончите, нажмите **Применить**.

### 3.1.2 Управление сетевыми клиентами



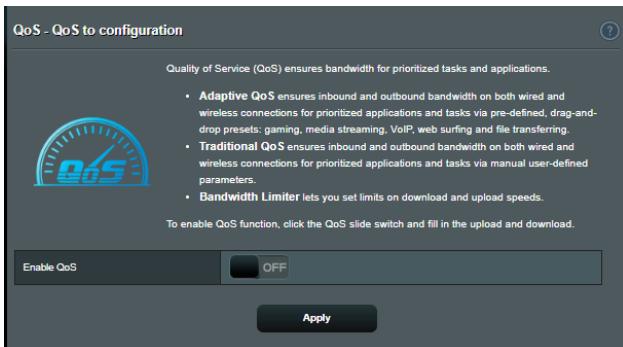
**Для управления сетевыми клиентами:**

1. В меню навигации выберите **Общие > Карта сети**.
2. На экране карта сети, выберите иконку **состояние клиента** для отображения информации о сетевых клиентах.
3. Для блокирования клиента, выберите клиента и нажмите **Block**.

## 3.2 Адаптивная QoS

### 3.2.1 Управление QoS (качество обслуживания)

Качество обслуживания (QoS) позволяет вам установить приоритет и управлять сетевым трафиком.



Для установки приоритета выполните следующее:

1. В меню навигации выберите **Общие > Адаптивная QoS > QoS**.
2. Нажмите **ON** для включения QoS. Заполните поля входящей и исходящей скорости.

---

**ПРИМЕЧАНИЕ:** Информацию о ширине канала можно получить у вашего провайдера (ISP).

---

3. Нажмите **Применить**.

---

**ПРИМЕЧАНИЕ:** Список пользовательских правил предназначен для дополнительных настроек. Если необходимо задать приоритет для сетевых служб, выберите **Определяемые пользователем правила QoS** или **Определяемый пользователем приоритет** в верхнем правом углу.

---

4. На странице **Определяемые пользователем правила QoS** находится четыре типа онлайн-служб по умолчанию: web surf, HTTPS и file transfers. Выберите нужную службу, запол-

ните **Исходный IP или MAC, Порт назначения, Протокол, Передаваемый и Приоритет**, затем нажмите **Применить**. Эта информация появится на экране правил QoS.

---

### **ПРИМЕЧАНИЯ:**

- Для ввода исходного IP или MAC возможны следующие действия:
    - a) Укажите IP-адрес, например "192.168.122.1".
    - b) Введите IP-адреса, находящиеся в одной подсети или в одном IP-пуле, например "192.168.123.\*" или "192.168.\*.\*"
    - c) Введите все адреса как "\*.\*.\*.\*" или оставьте это поле пустым.
    - d) Формат MAC-адрес состоит из шести групп по две шестнадцатеричных цифры, разделенных двоеточием (:) (например 12:34:56:aa:bc:ef)
  - Для исходного порта возможны следующие действия:
    - a) Укажите конкретный порт, например "95".
    - b) Введите диапазон портов, например "103:315", ">100" или "<65535".
  - В столбце **Передаваемый** содержится информация о входящем и исходящем сетевом трафике для одной секции. В этом столбце можно установить ограничение сетевого трафика (в КБ) для конкретной службы. Например, если два сетевых клиента ПК 1 и ПК 2 осуществляют доступ в Интернет (через порт 80), а РС 1 превысил ограничение сетевого трафика, то он получит более низкий приоритет. Если вам не нужно ограничение трафика, оставьте поле пустым.
- 
5. На странице **Определяемый пользователем приоритет** можно выбрать приоритет для сетевых приложений или устройств из списка **Определяемые пользователем правила QoS**. На основе приоритета можете использовать следующие методы для отправки пакетов данных:
- Изменить порядок отправляемых в Интернет пакетов.

- В таблице **Скорость исходящего соединения** установите **Минимальное ограничение ширины канала** и **Максимальное ограничение ширины канала** для нескольких сетевых приложений с разным приоритетом. Исходящая ширина канала для сетевых приложений отображается в процентах.

---

**ПРИМЕЧАНИЯ:**

- Низкоприоритетные пакеты игнорируются для обеспечения передачи высокоприоритетных пакетов.
  - В таблице **Скорость входящего соединения** установите **Максимальное ограничение ширины канала** для сетевых приложений в соответствующем порядке. Высокий приоритет исходящих пакетов вызовет высокий приоритет входящих пакетов.
  - При отсутствии высокоприоритетных пакетов соединение доступно для низкоприоритетных пакетов.
6. Установите пакеты с наивысшим приоритетом. Для игр, например, можно установить ACK, SYN и ICMP в качестве пакетов с наивысшим приоритетом.

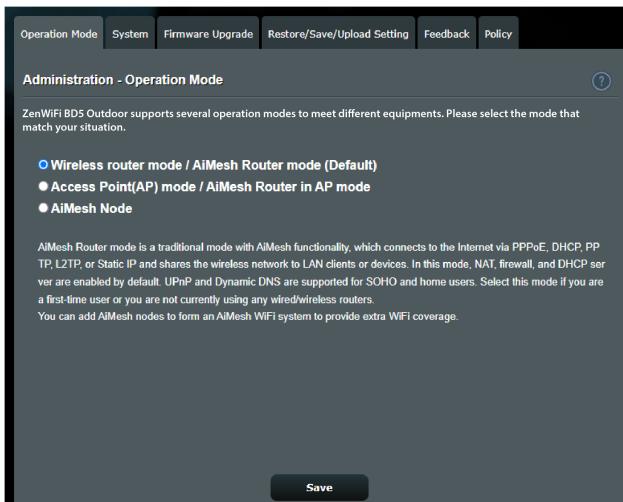
---

**ПРИМЕЧАНИЕ:** Убедитесь, что QoS включено и задано ограничение скорости для загрузки/скачивания.

## 3.3 Администрирование

### 3.3.1 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 (по умолчанию)**: В режиме беспроводного роутера, роутер подключается к интернету и предоставляет доступ к интернету для устройств в локальной сети.
  - **Режим точки доступа**: В этом режиме роутер создает новую беспроводную сеть.
  - **Узел AiMesh**: Можно установить этот роутер в качестве узла AiMesh для расширения существующего Wi-Fi покрытия AiMesh.
3. Нажмите **Сохранить**.

---

**ПРИМЕЧАНИЕ:** При изменении режима роутер перезагрузится.

---

### 3.3.2 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.
  - **Поведение кнопки WPS:** Физическая кнопка WPS используется для активации WPS.
  - **Часовой пояс:** Выберите часовой пояс для вашей сети.
  - **NTP-сервер:** Для синхронизации времени роутер может подключаться к серверу NTP (Network Time Protocol).
  - **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 **Нет** для предотвращения доступа.
  - **Разрешить только определенный IP:** Выберите **Да**, если нужно задать IP-адреса устройств, которым разрешен доступ к веб-интерфейсу роутера из WAN.
3. Нажмите **Применить**.

### 3.3.3 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 **Firmware Version** нажмите **Check** для нахождения загруженного файла.
  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 системысмотрите в разделе **4.2 Восстановление прошивки**.
- 

### 3.3.4 Восстановление/сохранение/загрузка настроек

#### 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 настройки**, укажите папку куда нужно сохранить файл и нажмите **Сохранить**.
  - Для восстановления сохраненных настроек нажмите **Обзор** для нахождения файла настроек, затем нажмите **Открыть**.

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

---

## 3.4 AiProtection

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

### 3.4.1 Сетевая защита

Сетевая защита обеспечивает защиту сети от несанкционированного доступа.

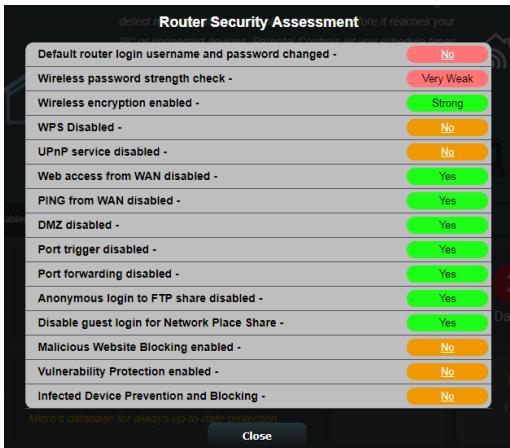


## Конфигурация сетевой защиты

Для конфигурации сетевой защиты:

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

После завершения сканирования утилита отобразит результаты на странице **Оценка безопасности роутера**.



**ВАЖНО!** Поля, помеченные как **Да**, на странице **Оценка безопасности роутера** означают безопасно. Пункты, помеченные как **Нет**, **Слабо** или **Очень слабо** рекомендуется сконфигурировать соответствующим образом.

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

**ПРИМЕЧАНИЕ:** При щелчке по элементу откроется страница его настроек.

- б. 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. Для конфигурации настроек безопасности автоматически нажмите **Защитить роутер**.
6. При появлении подтверждения нажмите **OK**.

## 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**.

## Двусторонняя IPS

Двусторонняя IPS (система предотвращения атак) защищает роутер от сетевых атак, блокируя вредоносные входящие пакеты и обнаруживая подозрительные исходящие пакеты.

---

**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 **Двусторонняя IPS** нажмите **ВКЛ**.

## 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 предпочтаемых оповещений:**

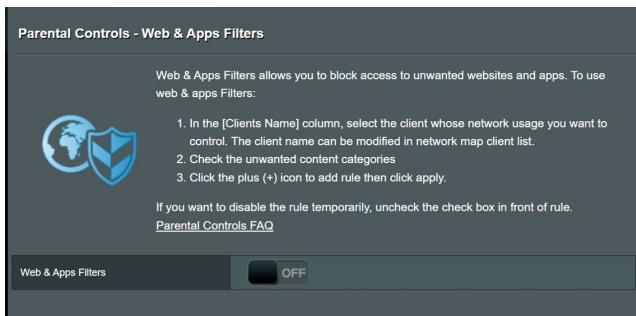
1. В панели **Профилактика и блокировка зараженных устройств** нажмите **Предпочитаемые оповещения**.
2. Выберите или введите провайдера электронной почты, учетную запись электронной почты и пароль, затем нажмите **Применить**.

### 3.4.2 Настройка Родительского контроля

Родительский контроль позволяет контролировать время доступа к интернету или ограничивать время использования интернета.

Для перехода на главную страницу родительского контроля:

В меню навигации выберите **Общие > Родительский контроль**.



#### Фильтры для веб и приложений

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

Для конфигурации фильтров для веб и приложений:

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

## Parental Controls - Web & Apps Filters

Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:



1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.  
[Parental Controls FAQ](#)

Web & Apps Filters		ON	
Client List (Max Limit : 64)			
	Client Name (MAC Address)	Content Category	Add / Delete
<input checked="" type="checkbox"/>	192.168.1.100 (192.168.1.100)	<input type="checkbox"/> <b>Adult</b> Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature. <input type="checkbox"/> <b>Instant Message and Communication</b> Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites. <input type="checkbox"/> <b>P2P and File Transfer</b> By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission. <input type="checkbox"/> <b>Streaming and Entertainment</b> By blocking streaming and entertainment services you can limit the time your children spend online.	
No data in table.			

**Apply**

## Расписание

Расписание позволяет установить ограничение времени для использования сети клиентом.

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

## Parental Controls - Time Scheduling

By enabling Block All Devices, all of the connected devices will be blocked from Internet access.

Enable block all devices													
<p>This feature allows you to set up a scheduled time for specific devices' Internet access.</p> <ol style="list-style-type: none"> <li>In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.</li> <li>In the [Add / Delete] column, click the plus(+) icon to add the client.</li> <li>In [Time Management] column, click the edit icon to set a schedule.</li> <li>Click [Apply] to save the configurations.</li> </ol>													
Enable Time Scheduling													
System Time	Thu, Sep 21 12:34:41 2023												
<b>Client List (Max Limit : 64)</b> <table border="1"> <thead> <tr> <th>Select all</th> <th>Client Name (MAC Address)</th> <th>Time Management</th> <th>Add / Delete</th> </tr> </thead> <tbody> <tr> <td>Time</td> <td>88:1C:7F:15:41:63 (E8)</td> <td>-</td> <td></td> </tr> <tr> <td colspan="4">No data in table.</td> </tr> </tbody> </table>		Select all	Client Name (MAC Address)	Time Management	Add / Delete	Time	88:1C:7F:15:41:63 (E8)	-		No data in table.			
Select all	Client Name (MAC Address)	Time Management	Add / Delete										
Time	88:1C:7F:15:41:63 (E8)	-											
No data in table.													
<b>Apply</b>													

**Для конфигурации расписания:**

1. В меню навигации выберите **Общие** > **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 Брандмаэр

Роутер может функционировать в качестве аппаратного брандмаэра.

**ПРИМЕЧАНИЕ:** Брандмаэр включен по умолчанию.

### 3.5.1 Общие

The screenshot shows the Firewall configuration interface with the following sections:

- General:** Includes options to enable Firewall (Yes), DoS protection (Yes), and ICMP Echo (ping) Request from WAN (Yes). It also lists Logged packets type as None.
- Basic Config:** Shows Enable IPv4 inbound firewall rules set to Yes.
- Inbound Firewall Rules (Max Limit : 128):** A table with columns Source IP, Port Range, Protocol, and Add / Delete. It displays "No data in table."
- IPv6 Firewall:** Describes that all outbound traffic from IPv6 hosts on the LAN is allowed. It includes a note about specifying inbound traffic and a sample IP address (2001:1111:2222:3333:64).
- Basic Config:** Shows Enable IPv6 Firewall set to Yes and Famous Server List set to Please select.
- Inbound Firewall Rules (Max Limit : 128):** A table with columns Service Name, Remote IP/CDR, Local IP, Port Range, Protocol, and Add / Delete. It displays "No data in table."

An **Apply** button is located at the bottom of the interface.

Для настройки параметров брандмаэра:

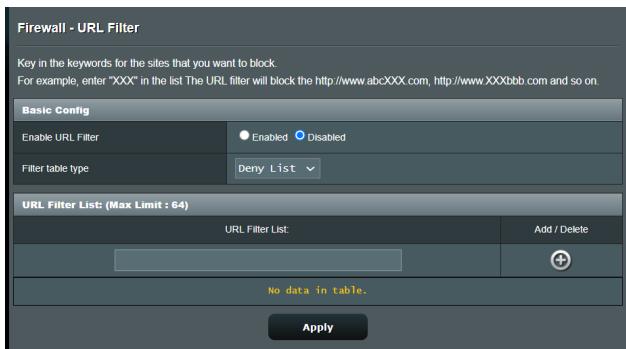
1. В меню навигации выберите **Дополнительные настройки > Брандмаэр > Общие**.
2. В поле **Включить брандмаэр** выберите **Да**.

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**.

### 3.5.2 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 Enable URL Filter выберите **Enabled**.
3. Введите URL и нажмите **(+)**.
4. Нажмите **Применить**.

### 3.5.3 Фильтр ключевых слов

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

The screenshot shows the 'Firewall - Keyword Filter' configuration page. At the top, a note states: 'Keyword Filter allows you to block the clients' access to webpages containing the specified keywords.' Below this is a section titled 'Limitations of the filtering function':

- 1. Compressed webpages that use HTTP compression technology cannot be filtered. [See here for more details.](#)
- 2. Https webpages cannot be filtered.

Under the 'Basic Config' heading, there is a 'Enable Keyword Filter' switch set to 'Enabled'. The 'Keyword Filter List (Max Limit : 64)' section contains a table with one row: a placeholder 'No data in table.' and a 'Add / Delete' button with a plus sign. At the bottom is an 'Apply' button.

**Для настройки фильтра ключевых слов:**

1. В меню навигации выберите **Дополнительные настройки > Брандмаэр > Фильтр ключевых слов.**
2. В поле Enable Keyword Filter выберите **Enabled**.
3. Введите слово или фразу и нажмите **Добавить**.
4. Нажмите **Применить**.

**ПРИМЕЧАНИЯ:**

- Фильтр ключевых слов функционирует на основе запроса DNS. Если сетевой клиент уже посещал сайт, например <http://www.abcxx.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.

### 3.5.4 Фильтр сетевых служб

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

**Firewall - Network Services Filter**

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked). Leave the source IP field blank to apply this rule to all LAN devices.

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.

Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network services.

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

**Network Services Filter**

Enable Network Services Filter	<input checked="" type="radio"/> Yes <input type="radio"/> No
Filter table type	Deny List
Well-Known Applications	User Defined
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Date to Enable LAN to WAN Filter	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Filtered ICMP packet types	

**Network Services Filter Table (Max Limit : 32)**

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	

No data in table.

**Apply**

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 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.

---

## 3.7 Локальная сеть

### 3.7.1 LAN IP

На экране LAN IP можно изменить настройки LAN IP роутера.

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

LAN - LAN IP	
Configure the LAN setting of ASUS Router.	
Host Name	ASUS Router
ASUS Router's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0
<b>Apply</b>	

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**.

### 3.7.2 DHCP-сервер

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

The screenshot shows the 'LAN - DHCP Server' configuration interface. It includes sections for 'Basic Config', 'DNS and WINS Server Setting', 'Manual Assignment', and a table for 'Manually Assigned IP around the DHCP list'. The 'Basic Config' section has fields for enabling the server, setting the domain name, defining the IP pool range (192.168.50.2 to 192.168.50.254), lease time (86400), and default gateway. The 'DNS and WINS Server Setting' section includes fields for DNS servers and WINS server. The 'Manual Assignment' section allows for manual IP assignment, with a table showing a single entry for a client with MAC address 00:0C:29:07:54:11, IP 192.168.50.100, and host name 'ASUS Router'. An 'Apply' button is at the bottom.

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
00:0C:29:07:54:11	192.168.50.100			

Для конфигурации DHCP сервера:

1. В меню навигации выберите **Дополнительные настройки > Брандмаэр > 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.
- 

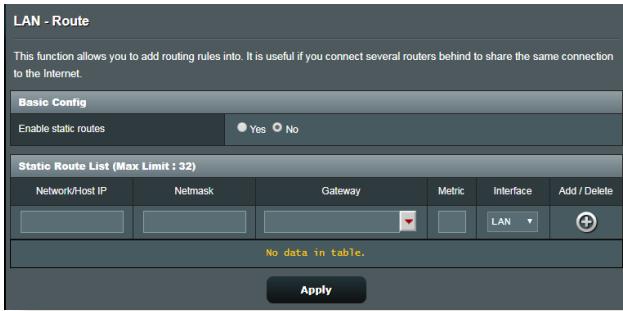
#### **ПРИМЕЧАНИЯ:**

- Рекомендуется использовать IP-адрес в формате: 192.168.50. 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.

### 3.7.3 Маршрут

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**.

### 3.7.4 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.

**LAN - IPTV**

To watch IPTV, the WAN port must be connected to the Internet. Please go to [WAN - Dual WAN](#) to confirm that WAN port is assigned to primary WAN.

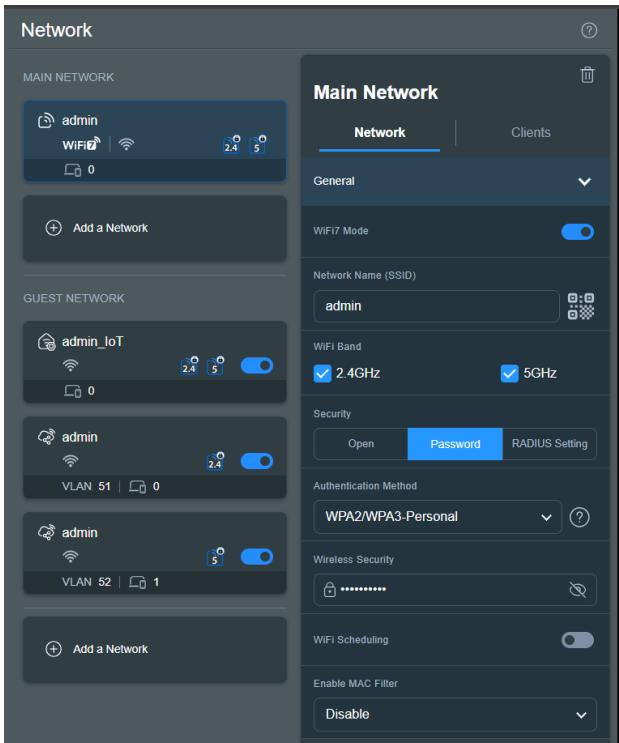
<b>LAN Port</b>	
Select ISP Profile	None
Choose IPTV STB Port	None
<b>Special Applications</b>	
Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
UDP Proxy (UdpProxy)	0

**Apply**

## 3.8 Сеть

### 3.8.1 Основная сеть - Фильтр MAC-адресов

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

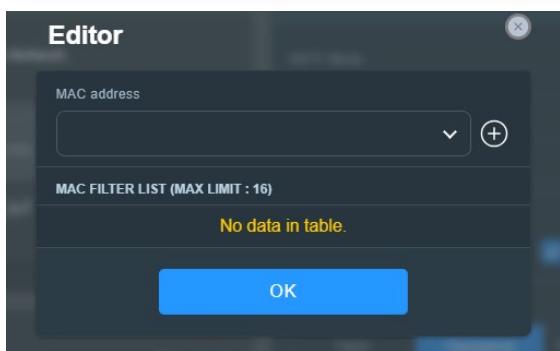
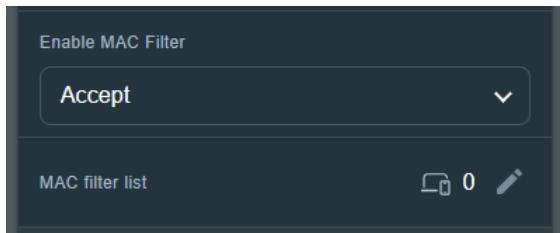


Для настройки фильтра MAC адресов беспроводной сети:

1. В меню навигации выберите **Общие > Сеть > Основная сеть** и выберите имя сети (SSID) основной сети.
2. В поле **Включить MAC фильтр** 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.

**ПРИМЕЧАНИЕ:** Выберите **Отключить**, если вы хотите выключить фильтр MAC адресов.

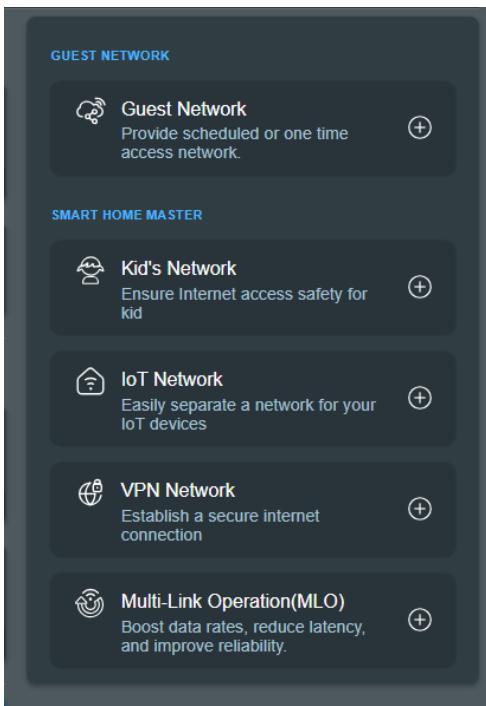
4. В списке фильтрации MAC-адресов нажмите для перехода на страницу **Редактор**, затем нажмите и введите MAC-адрес беспроводного устройства.
5. Нажмите **OK**.



## 3.8.2 Гостевая сеть

### 3.8.2.1 Гостевая сеть

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



---

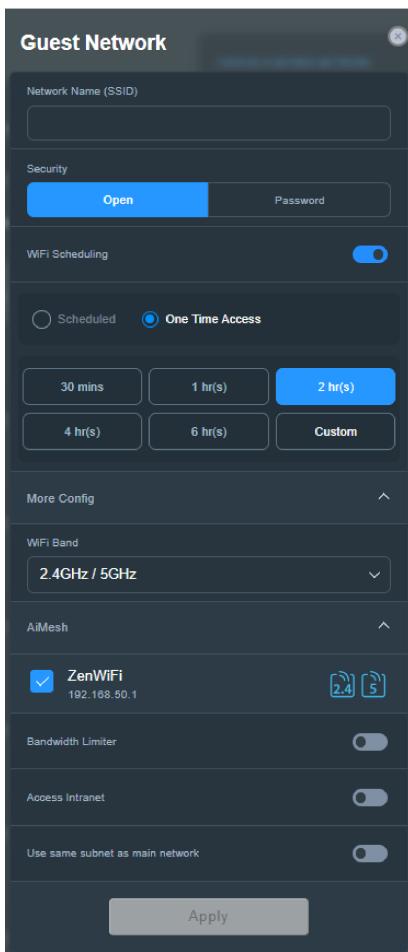
**ПРИМЕЧАНИЕ:** Роутер поддерживает до трех SSID в гостевой сети.

---

Для создания гостевой сети:

1. В меню навигации выберите **Общие > Сеть > Гостевая сеть > Добавить сеть**.
2. Выберите **Гостевая сеть** и назначьте сетевое имя для вашей временной сети в поле **Имя сети (SSID)**.
3. В разделе **Безопасность** выберите метод аутентификации.

4. Укажите время доступа или выберите **По расписанию** для добавления профиля онлайн-расписания.
5. Выберите **Диапазон WiFi** для гостевой сети, которую вы хотите создать.
6. Включите или отключите **Ограничитель скорости**.
7. Включите или отключите **Доступ к Инtranет**.
8. Когда закончите, нажмите **Применить**.

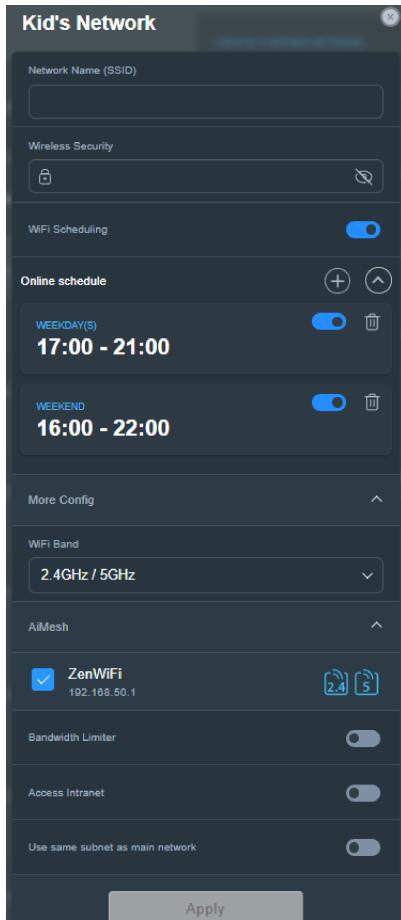


### **3.8.2.2 Мастер умного дома**

Smart Home Master - мощная и удобная утилита для сегментации сети. Она упрощает процесс создания и управления подсетями, например создание выделенного SSID для детских устройств, подключение к VPN через выделенную подсеть или даже создание одного безопасного SSID для устройств IoT.

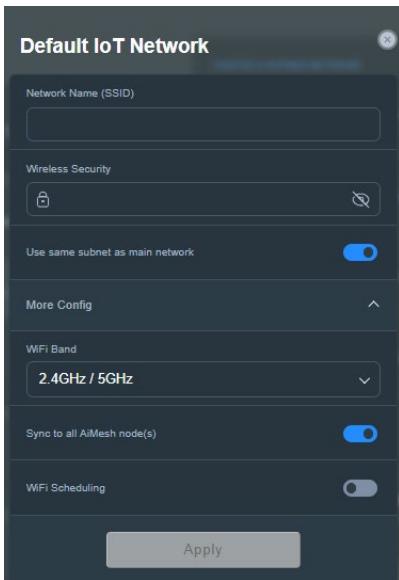
**Для создания детской сети:**

1. В меню навигации выберите **Общие > Сеть > Гостевая сеть > Добавить сеть.**
2. Выберите **Детская сеть** и в полях **Имя сети (SSID)** и **Безопасность беспроводной сети** задайте имя сети и ключ безопасности.
3. В поле **Онлайн-расписание** настройте время подключения к интернету.
4. Выберите **Диапазон WiFi** для детской сети, которую вы хотите создать.
5. Включите или отключите **Ограничитель скорости**.
6. Включите или отключите **Доступ к Интранет**.
7. Когда закончите, нажмите **Применить**.



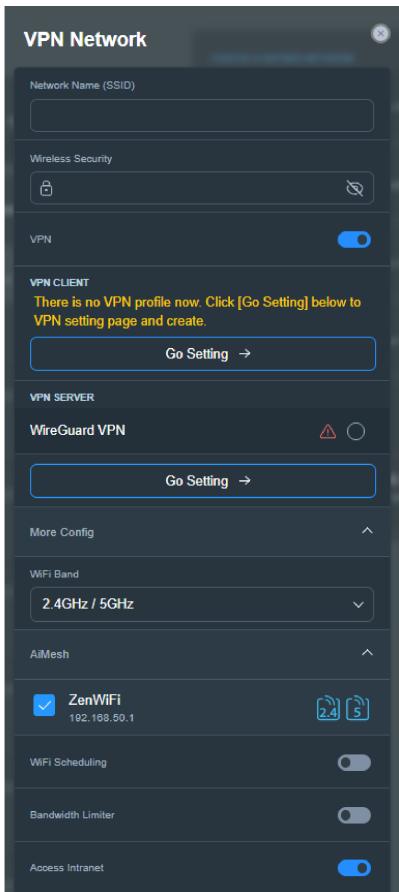
### Для создания сети IoT:

1. В меню навигации выберите **Общие > Сеть > Гостевая сеть > Добавить сеть**.
2. Выберите **Сеть IoT** и в полях **Имя сети (SSID)** и **Безопасность беспроводной сети** задайте имя сети и ключ безопасности.
3. Выберите **Диапазон WiFi** для сети IoT, которую вы хотите создать.
4. Настройте время доступа к интернету, включив **Расписание WiFi**.
5. Когда закончите, нажмите **Применить**.



### Для создания сети VPN:

1. В меню навигации выберите **Общие > Сеть > Гостевая сеть > Добавить сеть**.
2. Выберите **Сеть VPN** и в полях **Имя сети (SSID)** и **Безопасность беспроводной сети** задайте имя сети и ключ безопасности.
3. Если вы еще не настроили профиль VPN для VPN-сервера или VPN-клиента, нажмите **Перейти в Настройки** для создания профиля VPN.
4. Выберите **Диапазон WiFi** для сети VPN, которую вы хотите создать.
5. Настройте время доступа к интернету, включив **Расписание Wi-Fi**.
6. Включите или отключите **Ограничитель скорости**.
7. Включите или отключите **Доступ к Интранет**.
8. Когда закончите, нажмите **Применить**.



## 3.9 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
  - Выберите вкладку Подключения

The screenshot shows the 'System Log - General Log' interface. At the top, it displays the date and time: 'Thu, Aug 23 07:15:34 2018'. Below that, it shows 'Uptime' as '0 days 1 hours 18 minute(s) 11 seconds'. There is a 'Remote Log Server' input field and an 'Apply' button. The main area is a scrollable log window displaying system logs. The logs start with 'Aug 23 06:51:04 miniuupnpd[7139]: version 1.9 started' and continue through various kernel messages and system events until 'Aug 23 07:07:15 miniuupnpd[7729]: Listening for NAT-PMP/PCP traffic on port 5351'. At the bottom of the log window, there are 'Clear' and 'Save' buttons.

```
System Log - General Log

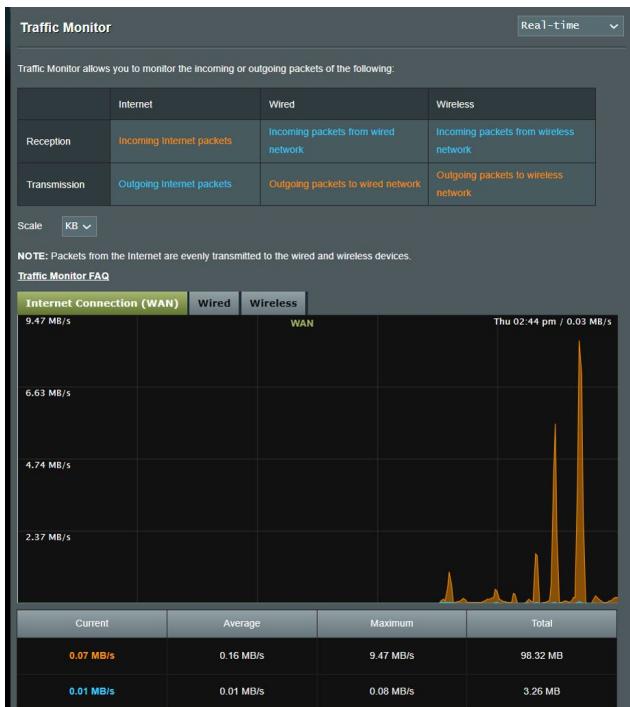
This page shows the detailed system's activities.

System Time | Thu, Aug 23 07:15:34 2018
Uptime | 0 days 1 hours 18 minute(s) 11 seconds
Remote Log Server |  Apply

Aug 23 06:51:04 miniuupnpd[7139]: version 1.9 started
Aug 23 06:51:04 miniuupnpd[7139]: HTTP listening on port 52102
Aug 23 06:51:04 miniuupnpd[7139]: Listening for NAT-PMP/PCP traffic on port 5351
Aug 23 06:58:52 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:52 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:53 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:53 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:55 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 06:58:57 kernel: ^[[0;33;4m[PATHSTAT] path add flow ASSERT: (enroute_pathkey != PATH_IX_INVALID)
Aug 23 07:07:14 miniuupnpd[7139]: shutting down MiniUPnPd
Aug 23 07:07:14 miniuupnpd[7139]: stopping MiniUPnPd on interface eth0
Aug 23 07:07:14 miniuupnpd[7680]: version 1.9 started
Aug 23 07:07:14 miniuupnpd[7680]: HTTP listening on port 60955
Aug 23 07:07:14 miniuupnpd[7680]: Listening for NAT-PMP/PCP traffic on port 5351
Aug 23 07:07:14 wan: finish adding multi routes
Aug 23 07:07:14 ntp: update
Aug 23 07:07:14 miniuupnpd[7680]: stopping down MiniUPnPd
Aug 23 07:07:15 miniuupnpd[7729]: version 1.9 started
Aug 23 07:07:15 miniuupnpd[7729]: HTTP listening on port 58635
Aug 23 07:07:15 miniuupnpd[7729]: Listening for NAT-PMP/PCP traffic on port 5351
```

## 3.10 Анализатор трафика

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



---

**ПРИМЕЧАНИЕ:** Сумма пакетов из интернета равна сумме переданных пакетов для проводных и беспроводных устройств.

---

## 3.11 WAN

### 3.11.1 Подключение к интернету

На странице подключение к интернету можно сконфигурировать параметры WAN подключения.

**WAN - Internet Connection**

ASUS Router supports several connection types to WAN (wide area network). These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of ASUS Router.

**Basic Config**

WAN Connection Type	Automatic IP
Enable WAN	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable NAT	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable UPnP	<input checked="" type="radio"/> Yes <a href="#">UPnP_FAQ</a> <input type="radio"/> No
Enable WAN Aggregation	<input type="radio"/> Yes <input checked="" type="radio"/> No WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). <a href="#">WAN Aggregation FAQ</a>

**WAN DNS Setting**

DNS Server	Default status : Get the DNS IP from your ISP automatically Assign a DNS service to improve security, block advertisement and gain faster performance. <a href="#">Assign</a>
Forward local domain queries to upstream DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable DNS Rebind protection	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable DNSSEC support	<input checked="" type="radio"/> Yes <input type="radio"/> No
Prevent client auto DoH	Auto
DNS Privacy Protocol	None

**DHCP Option**

Class-identifier (Option 60):	
Client-identifier (Option 61):	<input checked="" type="checkbox"/> IAID/DUID
Class-identifier (Option 60):	
Client-identifier (Option 61):	<input checked="" type="checkbox"/> IAID/DUID

**Account Settings**

Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

**Special Requirement from ISP**

Host Name	
MAC Address	
DHCP query frequency	Aggressive Mode
Extend the TTL value	<input checked="" type="radio"/> Yes <input type="radio"/> No
Spoof LAN TTL value	<input type="radio"/> Yes <input checked="" type="radio"/> No

**Apply**

## 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 **Фиксированный IP**. Если вы не знаете тип подключения к интернету, проконсультируйтесь с вашим провайдером.
  - **Включить WAN:** Выберите **Да** для включения доступа к интернету. Выберите **Нет** для отключения доступа к интернету.
  - **Включить функцию трансляции сетевых адресов (NAT):** NAT (трансляция сетевых адресов) представляет собой систему, в которой один публичный IP (WAN IP) используется для предоставления доступа в Интернет для сетевых клиентов с локальным IP-адресом. Локальный IP-адрес каждого сетевого клиента сохраняется в таблице NAT и используется для маршрутизации входящих пакетов данных.
  - **Включить UPnP:** UPnP (Universal Plug и Play) позволяет использовать несколько устройств (роутеры, телевизоры, стереосистемы, игровые приставки, сотовые телефоны), которые будут управляться через IP-сети с или без централизованного управления через шлюз. UPnP соединяет компьютеры любых типов, обеспечивая единую сеть для удаленной конфигурации и передачи данных. Новое сетевое устройство обнаруживается автоматически с помощью UPnP. После подключения к сети, устройства можно дистанционно сконфигурировать для поддержки P2P-приложений, интерактивных игр, видеоконференций и веб- или прокси-серверов. В отличие от перенаправления портов, которое требует ручной настройки, UPnP автоматически настраивает роутер для принятия входящих соединений и передает запросы к определенному компьютеру в локальной сети.
  - **Включить WAN агрегацию:** Агрегация интернет каналов объединяет два сетевых интерфейса, что позволяет увели-

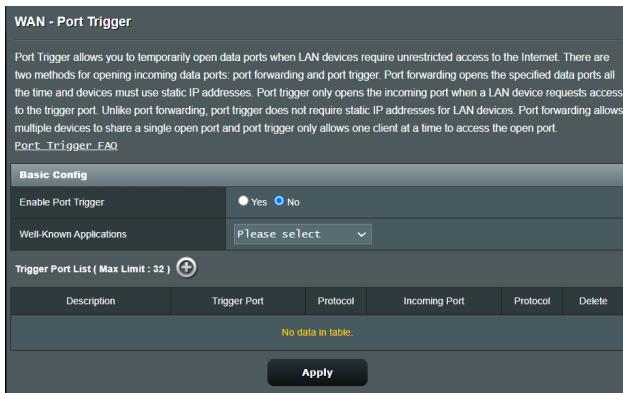
чить пропускную способность канала до 2 Гбит/с. Подключите порты WAN и LAN 4 роутера к LAN-портам модема.

- **Подключение к DNS серверу:** Позволяет роутеру автоматически получить IP-адрес DNS сервера от провайдера. DNS - это хост в интернете, который транслирует имена Интернет в IP-адреса.
- **Аутентификация:** Этот пункт может указываться некоторыми поставщиками услуг Интернета. Уточните у вашего провайдера и заполните в случае необходимости.
- **Имя хоста:** Это поле позволяет указать имя хоста для роутера. Обычно, это специальное требование от провайдера. Введите имя хоста здесь, если ваш провайдер назначил его для вашего компьютера.
- **MAC-адрес:** MAC (Media Access Control) адрес уникальный идентификатор для сетевого устройства. Некоторые провайдеры контролируют MAC-адреса устройств, подключенных к их оборудованию и могут запретить подключение устройства с незнакомым MAC-адресом. Во избежание проблем с подключением из-за незарегистрированного MAC-адреса возможны следующие действия:
  - Обратитесь к вашему провайдеру и попросите обновить MAC адрес.
  - Склонируйте или измените MAC-адрес роутера в соответствии с MAC адресом оригинального устройства.

### 3.11.2 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:

- Несколько 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. Сконфигурируйте нижеследующие параметры. Когда закончите, нажмите **Применить**.
  - **Включить переключение портов:** Выберите **Да** для включения переключения портов.
  - **Известные приложения:** Выберите популярные игры и веб-службы для добавления их в список переключения портов.
  - **Описание:** Введите имя или описание службы.
  - **Переключаемый порт:** Укажите переключаемый порт для приложения.

- **Протокол:** Выберите протокол TCP или UDP.
  - **Входящий порт:** Укажите входящий порт для приема пакетов из интернета.
  - **Протокол:** Выберите протокол TCP или UDP.
- 

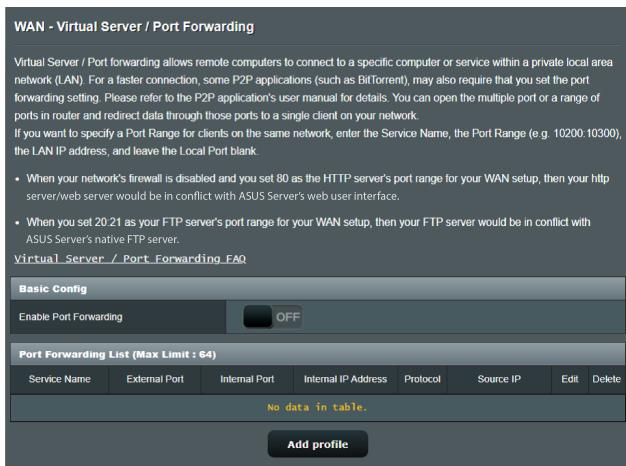
#### **ПРИМЕЧАНИЯ:**

- 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.
-

### 3.11.3 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.

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



Для настройки переадресации портов:

1. В меню навигации выберите **Дополнительные настройки > WAN > Виртуальный сервер/Переадресация портов**.
2. Сконфигурируйте нижеследующие параметры. Когда закончите, нажмите **ВКЛ**.
  - **Включить переадресацию портов:** Выберите **ВКЛ** для включения переадресации портов.
  - **Список известных серверов:** Укажите тип службы, к которой требуется доступ.

- **Список известных игр:** Этот пункт содержит список портов, необходимых для правильной работы популярных онлайн игр.
- **Порт сервера FTP:** Избегайте назначения диапазона портов 20:21 для FTP-сервера, поскольку это будет конфликтовать с родными настройками FTP сервера.
- **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 **3.7 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 **BOTN**.

#### **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.

### 3.11.4 DMZ

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

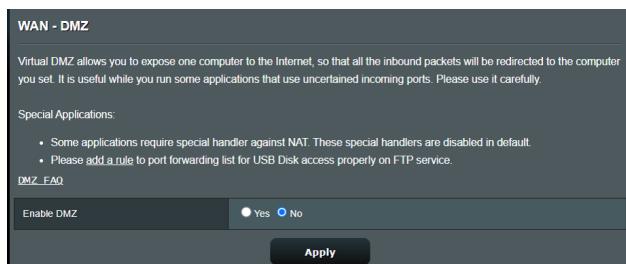
Входящий трафик из интернета обычно отбрасывается или перенаправляется на указанный компьютер, если настроена переадресация или переключение портов. В режиме DMZ один компьютер получает все входящие пакеты.

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

---

**ОСТОРОЖНО:** 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**.

### 3.11.5 DDNS

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

**WAN - DDNS**

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.  
If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.  
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

The host name is successfully registered. You can use "[hostname] asuscomm.com" to access the service in home network from WAN. Use "[hostname] asuscomm.com" to remotely access your network.  
Go to Advanced Settings > WAN to configure the port forwarding or DMZ settings to allow other WAN clients to remotely access your network.  
If you want to remotely configure the wireless router, go to [here](#).

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	<input type="text" value="www.ASUS.COM"/> <input type="button" value="Deregister"/>
Host Name	<input type="text" value="A6878A175D4A6FB54D2E68D6195DB5E7"/> .asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input checked="" type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input type="radio"/> None
<input type="button" value="Apply"/>	

#### 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.

### 3.11.6 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**.

WAN - NAT Passthrough	
Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.	
PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP ALG port	2021

**Apply**

## 3.12 Беспроводная связь

### 3.12.1 Общие

На странице Общие можно сконфигурировать основные параметры беспроводной сети.

The screenshot displays the 'Wireless - General' configuration interface. It includes fields for 'Enable Smart Connect' (OFF), 'Band' (2.4 GHz), 'Network Name (SSID)' (LIAO), 'Hide SSID' (Yes), 'Wireless Mode' (Auto), '802.11ax / WiFi 6 mode' (Enable), 'WiFi Agile Multiband' (Disable), 'Target Wake Time' (Disable), 'Channel bandwidth' (20/40 MHz), 'Control Channel' (Auto), 'Extension Channel' (Auto), 'Authentication Method' (WPA2-Personal), 'WPA Encryption' (AES), 'WPA Pre-Shared Key' (redacted), and 'Group Key Rotation Interval' (3600). A note about compatibility issues with 802.11ax/WiFi 6 mode is present. The 'Apply' button is at the bottom.

**Для конфигурации основных параметры беспроводной сети:**

1. В меню навигации выберите **Дополнительные настройки > Беспроводная связь > Общие**.
2. Выберите 2,4 ГГц или 5 ГГц в качестве диапазона частот для беспроводной сети.
3. 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 и 5 ГГц.

---

4. В поле **Скрыть SSID** выберите **Да** для предотвращения обнаружения SSID другими беспроводными устройствами. Когда эта функция включена, для доступа к беспроводной сети необходимо ввести SSID вручную.
5. Выберите беспроводной режим, определяющий тип беспроводных устройств, которые могут подключиться к роутеру:
  - **Авто:** Выберите **Авто** для разрешения подключения к роутеру устройств 802.11ac, 802.11n, 802.11 g 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.
  - **N only:** Выберите **N only** для максимальной производительности Wireless N. Этот режим запрещает подключение к роутеру устройств 802.11g и 802.11b.
6. Выберите ширину канала для обеспечения высокой скорости передачи данных:

**40 МГц:** Выберите эту ширину канала для максимальной пропускной способности беспроводной сети.

**20 МГц (по умолчанию):** Выберите эту ширину канала, если вы столкнулись с проблемами с беспроводным подключением.
7. Выберите рабочий канал для беспроводного роутера. Выберите **Авто** для автоматического выбора канала с наименьшим количеством помех.
8. Выберите метод аутентификации:
  - **Open System:** Эта опция не обеспечивает безопасности.
  - **Общий ключ:** вы должны использовать WEP шифрование и ввести хотя бы один общий ключ.
  - **WPA/WPA2 Personal/WPA Auto-Personal:** Эта опция обеспечивает высокий уровень безопасности. Можно использовать WPA (с TKIP) или WPA2 (с AES). При выборе этой опции вы должны использовать шифрование TKIP + AES и ввести ключевую фразу WPA (сетевой ключ).

- **WPA/WPA2 Enterprise/WPA Auto-Enterprise:** Эта опция обеспечивает очень высокий уровень безопасности. Она работает с интегрированным EAP-сервером или внешним RADIUS-сервером.
- **Radius with 802.1x**

---

**ПРИМЕЧАНИЕ:** Беспроводной роутер поддерживает максимальную скорость передачи 54 Мбит когда **Режим беспроводной сети** установлен в **Авто**, а **Метод шифрования** - в **WEP** или **TKIP**.

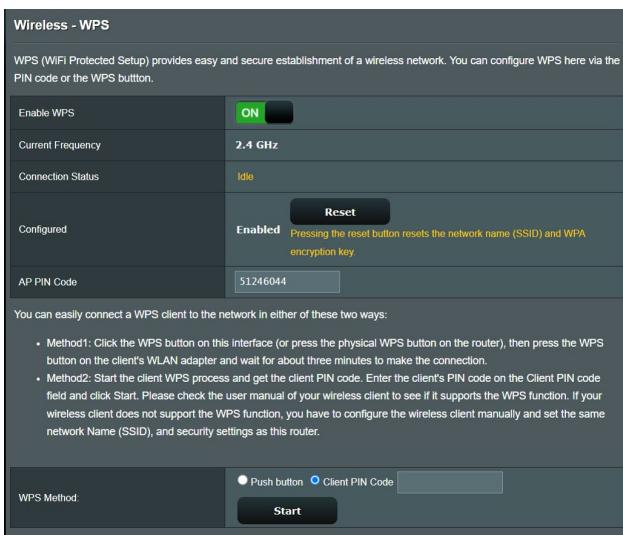
---

9. Выберите шифрование WEP (Wired Equivalent Privacy) для данных, передаваемых по беспроводной сети:
  - **Откл:** Отключает WEP-шифрование
  - **64-бит:** Включает WEP-шифрование
  - **128-бит:** Включает улучшенное WEP-шифрование
10. Когда закончите, нажмите **Применить**.

### 3.12.2 WPS

WPS (Wi-Fi Protected Setup) - стандарт беспроводной безопасности, позволяющий быстро подключать устройства к беспроводной сети. Функцию WPS можно сконфигурировать с помощью PIN-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 2,4 ГГц. Если нужно изменить частоту на 5 ГГц, в поле **Включить WPS** переместите ползунок в положение **OFF**, в поле **Текущая частота** щелкните **Переключить частоту**, затем в поле **Включить WPS** переместите ползунок в положение **ON** еще раз.

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

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

---

**ПРИМЕЧАНИЕ:** Расположение кнопки WPS смотрите в документации беспроводного устройства.

---

- c. Роутер начнет поиск доступных устройств. Если роутер не найдет ни одного устройства, он переключится в режим ожидания.
5. Для настройки WPS с помощью ПИН-кода клиента выполните следующие действия:
  - a. Найдите WPS ПИН-код в руководстве пользователя беспроводного устройства или на самом устройстве.
  - b. Введите ПИН-код клиента в текстовое поле.
  - c. Нажмите **Пуск** для переключения роутера в режим поиска WPS. Индикаторы роутера быстро мигают до завершения настройки WPS.

### 3.12.3 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, WPA2-Enterprise или Radius with 802.1x.
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 **Ключ соединения** назначьте пароль для доступа к серверу RADIUS.
6. Нажмите **Применить**.

### 3.12.4 Профессиональный

На экране Профессиональный можно сконфигурировать дополнительные параметры.

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

**Wireless - Professional**

Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.

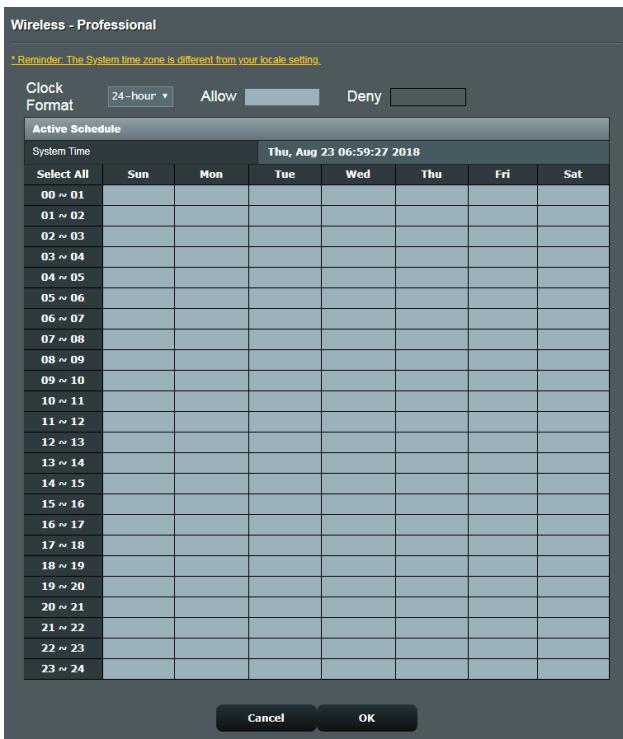
Band	2.4 GHz
Enable Radio	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable wireless scheduler	<input checked="" type="radio"/> Yes <input type="radio"/> No
Set AP Isolated	<input checked="" type="radio"/> Yes <input type="radio"/> No
Roaming assistant	Enable <input type="button" value="Disconnect clients with RSSI lower than : -70 dBm"/>
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Enable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	<input type="button" value="Performance"/>

**Apply**

На экране Профессиональный можно сконфигурировать следующее:

- **Диапазон:** Выберите диапазон, настройки которого нужно изменить.

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



- **Изолировать точку доступа:** Изолирование точки доступа запрещает беспроводным устройствам в сети подключаться друг к другу. Эта функция полезна когда к вашей сети подключается много гостей. Выберите **Да** для включения этой функции или **Нет** для отключения.
- **Скорость многоадресной передачи (Мбит/с):** Скорость многоадресной передачи или нажмите **Отключить** для отключения многоадресной передачи.
- **Тип преамбулы:** Тип преамбулы определяет продолжи-

тельность 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.

- **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.

## 4 Утилиты

### 4.1 Обнаружение устройства

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

Для запуска утилиты Device Discovery:

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

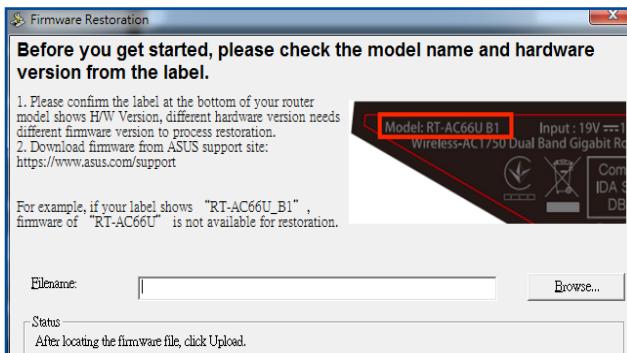
---

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

---

### 4.2 Восстановление прошивки

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



---

**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:  
**Диапазон IP-адресов не может содержать LAN IP: 192.168.1.x**  
**Маска подсети:** 255.255.255.0
4. Перейдите **Пуск > Программы > ASUS Utility > Wireless Router > Firmware Restoration.**
5. Укажите файл и нажмите **Upload.**

---

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

---

# 5 Устранение неисправностей

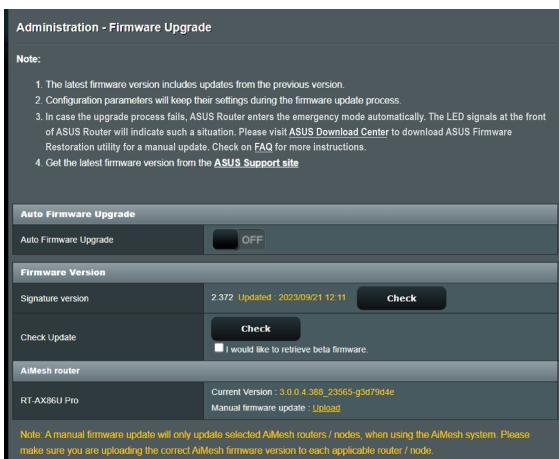
В этом разделе представлены инструкции для решения некоторых наиболее часто встречающихся общих проблем с роутером. Если вы столкнулись с проблемами, не упомянутыми в этой главе, посетите сайт ASUS: <https://www.asus.com/ru/support/> для получения дополнительной информации о продукте или обратитесь в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

## 5.1 Устранение основных неисправностей

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

### Обновите прошивку до последней версии.

1. 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://www.asus.com/Networking/ZenWiFi\\_BD4\\_Outdoor/HelpDesk/](https://www.asus.com/Networking/ZenWiFi_BD4_Outdoor/HelpDesk/) и скачайте ее.
3. На странице **Firmware Version** нажмите **Check** для поиска 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, 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 рекомендуется использовать DHCP-сервер роутера.

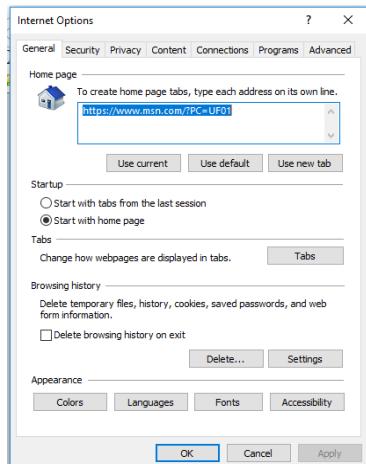
- Некоторые провайдеры требуют использовать MAC-адрес компьютера, используемого при первом подключении. MAC-адрес можно посмотреть в веб-интерфейсе на странице **Карта сети** > страница **Клиенты** или навести курсор мыши на устройство в поле **Состояние клиента**.



## 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:
  - Запустите Internet Explorer, затем нажмите **Сервис > Свойства обозревателя**.
  - На вкладке **Общие** в области **Просмотр истории** нажмите **Удалить...**, выберите **Временные файлы Интернета и Файлы cookie и данные сайта** и нажмите **Удалить**.



#### ПРИМЕЧАНИЯ:

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

## Клиент не может установить беспроводное соединение с роутером.

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

- Вне зоны покрытия:**

- Поместите роутер ближе к беспроводному клиенту.

- DHCP-сервер отключен:**

- Войдите в веб-интерфейс. Перейдите в **Общие > Карта сети > Клиенты** и найдите устройство, которое нужно подключить к роутеру.
- 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**.

**LAN - DHCP Server**

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the DNS server IP and default gateway IP. ASUS Router supports up to 253 IP addresses for your local network.  
Manually Assigned IP around the DHCP list FAQ

Basic Config	
Enable the DHCP Server	<input checked="" type="radio"/> Yes <input type="radio"/> No
ASUS Router's Domain Name	
IP Pool Starting Address	192.168.50.2
IP Pool Ending Address	192.168.50.254
Lease time	86400
Default Gateway	

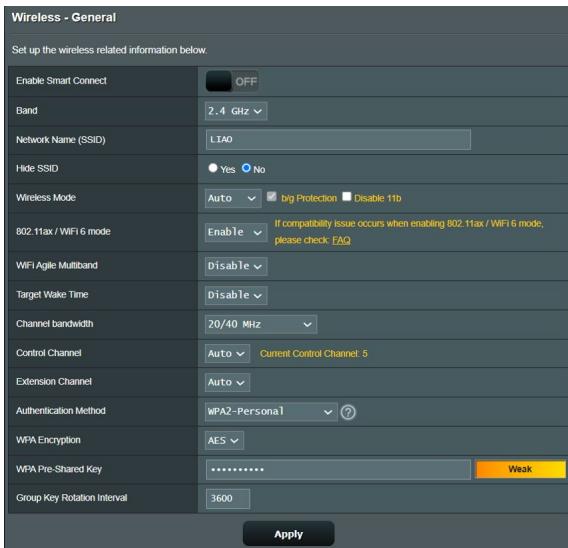
DNS and WINS Server Setting	
DNS Server 1	
DNS Server 2	
Advertise router's IP in addition to user-specified DNS	<input checked="" type="radio"/> Yes <input type="radio"/> No
WINS Server	

Manual Assignment	
Enable Manual Assignment	<input checked="" type="radio"/> Yes <input type="radio"/> No

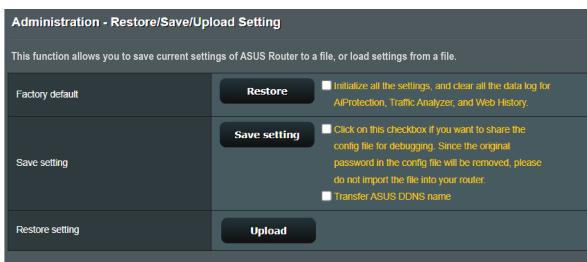
Manually Assigned IP around the DHCP list (Max Limit : 64)				
Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
00:11:00:12:34:56:78:90:12				
No data in table.				

**Apply**

- 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**.

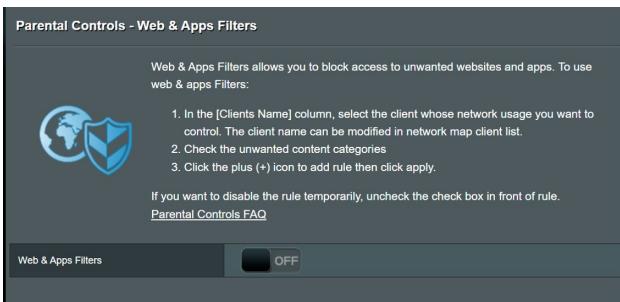


## Интернет недоступен.

- Убедитесь, что роутер может подключиться к вашему провайдеру. Для этого запустите веб-интерфейс и перейдите в **Общие > 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 > 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.

## **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**.

## **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**.

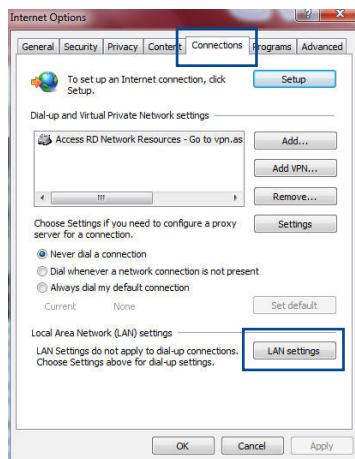
## Невозможно подключиться к веб-интерфейсу

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

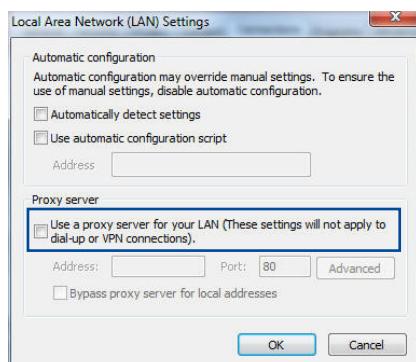
### A. Отключите прокси-сервер, если он включен.

#### Windows

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

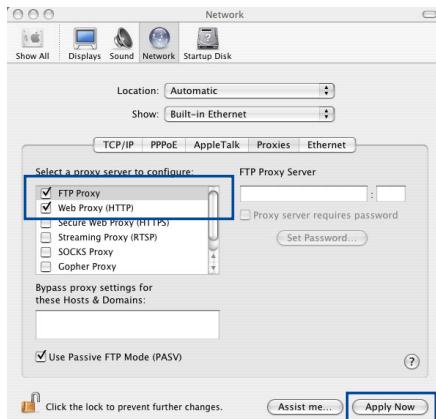


3. На экране **настройки локальной сети** отключите использование прокси-сервера для локальной сети.
4. Нажмите **OK** когда закончите.



## MAC OS

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

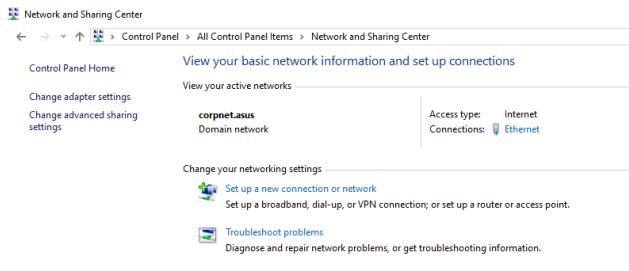


**ПРИМЕЧАНИЕ:** Для получения подробной информации по отключению использования прокси-сервера, обратитесь к справке браузера.

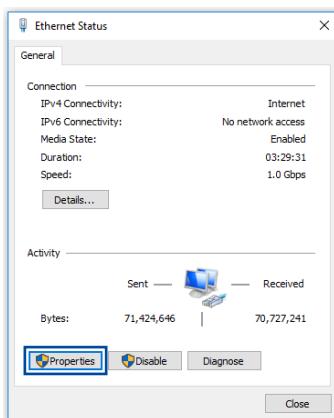
## B. Настройте TCP/IP для автоматического получения IP-адреса.

### Windows

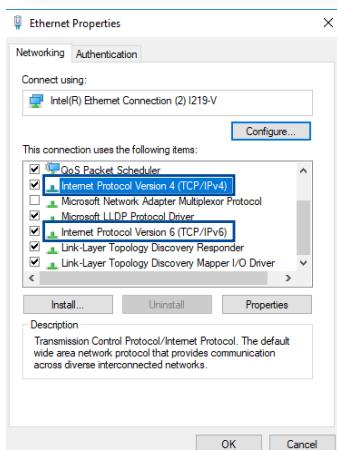
1. Нажмите **Пуск > Панель управления > Центр управления сетями и общим доступом**, затем нажмите сетевое подключение для отображения его состояния.



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



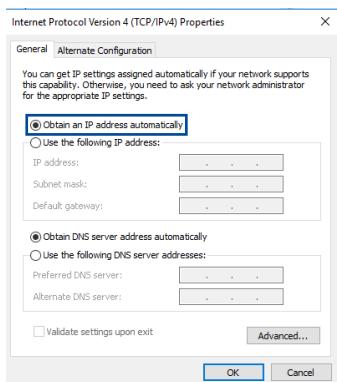
3. Выберите **Протокол Интернета версии 4(TCP/IPv4)** или **Протокол Интернета версии 6(TCP/IPv6)**, затем нажмите **Свойства**.



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

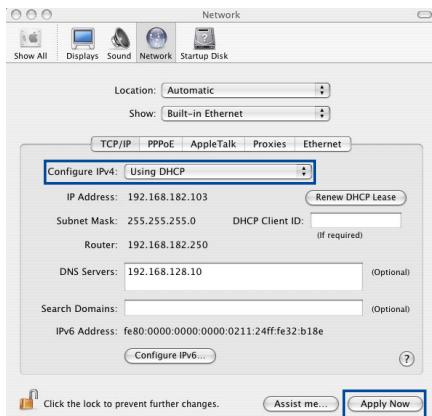
Выберите **Получить IPv6-адрес автоматически** для автоматического получения IPv6-адреса.

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**.

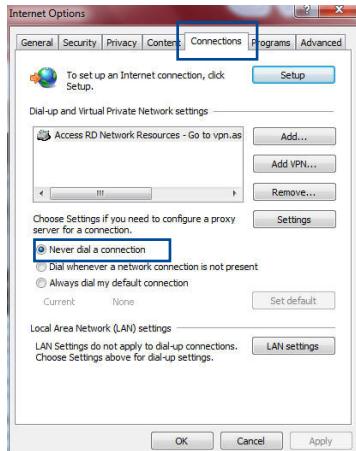


**ПРИМЕЧАНИЕ:** Подробную информацию по конфигурации настроек TCP/IP смотрите в справке к вашей операционной системе.

## 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. Подробную информацию смотрите на нашем сайте. Note that we do not offer direct support for the distribution.

### GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

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

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

### Preamble

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

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

free programs; and that you know you can do these things.

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

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

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

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

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

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

### **Terms & conditions for copying, distribution, & modification**

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative

work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

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

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

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

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
  - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
  - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
  - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for

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

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

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

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

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
  - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
  - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your

- cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
- c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

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

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

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

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

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

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

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

to distribute software through any other system and a licensee cannot impose that choice.

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

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

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

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

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



## **NO WARRANTY**

- 11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
- 12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## Правила безопасности

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



### ВНИМАНИЕ!

- Шнур питания должен быть подключен к розетке с заземлением. Подключайте устройство к ближайшей, легкодоступной розетке.
- Если шнур питания неисправен, не пытайтесь отремонтировать его самостоятельно. Обратитесь к квалифицированному технику или продавцу.
- Не пользуйтесь поврежденными сетевыми шнурами, аксессуарами и периферийными устройствами.
- Не устанавливайте это устройство 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 обнаружении 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 шнур 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/>.

