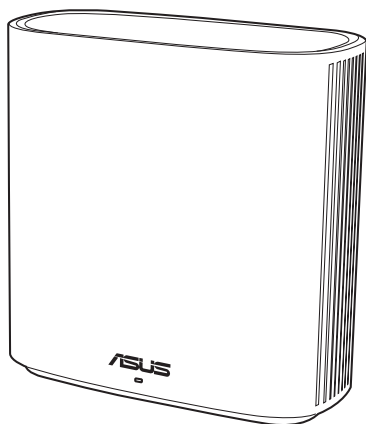


# Руководство пользователя

## ASUS ZenWiFi XD6

Двухдиапазонный роутер AX5400

Модель: XD6



**ASUS**  
IN SEARCH OF INCREDIBLE

R19060

Первое издание

Октябрь 2021

**Copyright © 2021 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.

КОМПАНИЯ ASUS ПРЕДОСТАВЛЯЕТ ДАННОЕ РУКОВОДСТВО НА УСЛОВИИ «КАК ЕСТЬ», БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, ПРЯМЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ, ВКЛЮЧАЯ, В ТОМ ЧИСЛЕ, ЛЮБЫЕ ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ ИЛИ УСЛОВИЯ ГОДНОСТИ ДЛЯ ПРОДАЖИ, ИЛИ ПРИГОДНОСТИ К КОНКРЕТНОЙ ЦЕЛИ ИСПОЛЬЗОВАНИЯ. КОМПАНИЯ ASUS, ЕЕ ДИРЕКТОРА, 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
1.6	Настройка роутера	10
1.6.1	Проводное подключение	11
1.6.2	Беспроводное подключение	12
<b>2</b>	<b>Начало работы</b>	
2.1	Вход в веб-интерфейс	13
2.2	Быстрая настройка Интернет (QIS) с автоопределением	14
2.3	Подключение к беспроводной сети	18
<b>3</b>	<b>Конфигурация общих настроек</b>	
3.1	Использование карты сети	19
3.1.1	Настройка параметров безопасности беспроводной сети	20
3.1.2	Управление сетевыми клиентами	21
3.2	Создание гостевой сети	22
3.3	AiProtection	24
3.3.1	Сетевая защита	25
3.3.2	Настройка Родительского контроля	28
3.4	Использование Диспетчера трафика	30
3.4.1	Управление QoS (качество обслуживания)	30
<b>4</b>	<b>Настройка дополнительных параметров</b>	
4.1	Беспроводная связь	33
4.1.1	Общие	33

## Оглавление

4.1.2	WPS .....	36
4.1.3	Мост.....	38
4.1.4	Фильтр MAC-адресов беспроводной сети .....	40
4.1.5	Настройка RADIUS.....	41
4.1.6	Профессиональный .....	42
<b>4.2</b>	<b>Локальная сеть .....</b>	<b>45</b>
4.2.1	LAN IP .....	45
4.2.2	DHCP-сервер.....	46
4.2.3	Маршрут .....	48
4.2.4	IPTV .....	49
<b>4.3</b>	<b>WAN .....</b>	<b>50</b>
4.3.1	Подключение к интернету.....	50
4.3.2	Переключение портов.....	53
4.3.3	Virtual Server/Port Forwarding.....	55
4.3.4	DMZ.....	58
4.3.5	DDNS .....	59
4.3.6	NAT Passthrough .....	60
<b>4.4</b>	<b>IPv6.....</b>	<b>61</b>
<b>4.5</b>	<b>Брандмауэр .....</b>	<b>62</b>
4.5.1	Общие.....	62
4.5.2	Фильтр URL .....	62
4.5.3	Фильтр ключевых слов .....	63
4.5.4	Фильтр сетевых служб .....	64
<b>4.6</b>	<b>Администрирование .....</b>	<b>66</b>
4.6.1	Режим работы.....	66
4.6.2	Система.....	67
4.6.3	Обновление прошивки .....	69
4.6.4	Восстановить/сохранить/загрузить настройки.....	69

## Оглавление

4.7 Системный журнал.....70

### **5 Утилиты**

5.1 Обнаружение устройства .....71

5.2 Восстановление прошивки.....72

### **6 Устранение неисправностей**

6.1 Устранение основных неисправностей.....74

6.2 Часто задаваемые вопросы (FAQ) .....77

### **Приложение**

Уведомления .....86

Сервис и поддержка..... 102

# 1 Информация о беспроводном роутере

## 1.1 Приветствие!

Благодарим Вас за приобретение беспроводного роутера ASUS ZenWiFi XD6!

Ультратонкий и стильный ZenWiFi XD6 поддерживает частоты 2.4ГГц и 5ГГц, SMB, UPnP AV, FTP сервера для круглосуточного доступа к файлам, одновременную работу до 300,000 сессий; а также технологию ASUS Green Network, обеспечивающую энергосбережение до 70%.

## 1.2 Комплект поставки

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Роутер ASUS ZenWiFi XD6 | <input checked="" type="checkbox"/> Сетевой кабель (RJ-45) |
| <input checked="" type="checkbox"/> Блок питания            | <input checked="" type="checkbox"/> Краткое руководство    |

---

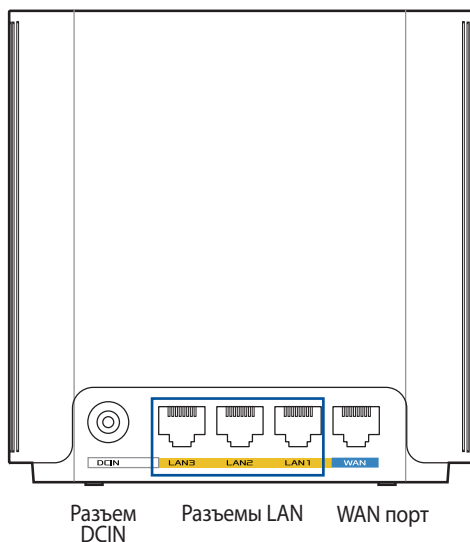
### ПРИМЕЧАНИЯ:

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

## 1.3 Данный беспроводной роутер

- 1 Подключите блок питания к разъему DCIN.
- 2 Индикатор питания загорится при готовности устройства.

### Описание разъемов



---

#### WAN порт

Подключите этому порту модем с помощью сетевого кабеля.

---

#### Разъемы LAN

Подключите компьютер к одному из этих LAN портов с помощью сетевого кабеля.

---

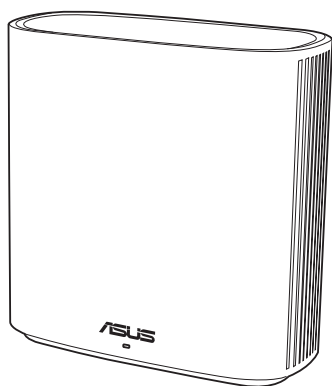
### Спецификация

<b>Блок питания</b>	Выходная мощность: 12 В с максимальным током 2А		
Температура при работе	0~40°C	при хранении	0~70°C
Влажность при работе	50~90%	при хранении	20~90%

## 1.4 Размещение роутера

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

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





## 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
- 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.
  - Беспроводной роутер одновременно поддерживает работу на частотах 2.4 ГГц и 5 ГГц. Это позволяет выполнять интернет-серфинг и работать с электронной почтой, используя частоту 2,4 ГГц и одновременно смотреть потоковое видео высокой четкости, или слушать музыку, используя диапазон 5 ГГц.
  - Некоторые устройства IEEE 802.11n, которые вы хотите подключить к сети могут не поддерживать частоту 5 ГГц. Обратитесь к спецификации устройства.
  - Длина Ethernet кабеля, используемого для подключения сетевых устройств не должна превышать 100 метров.
-

## 1.6 Настройка роутера

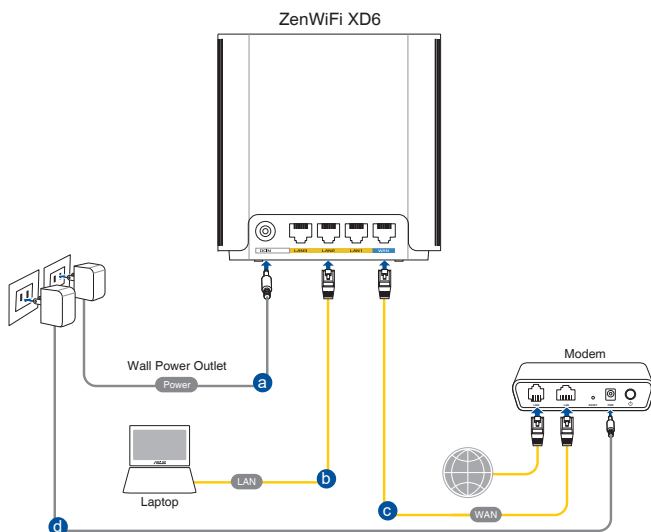
---

### **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).
-

## 1.6.1 Проводное подключение

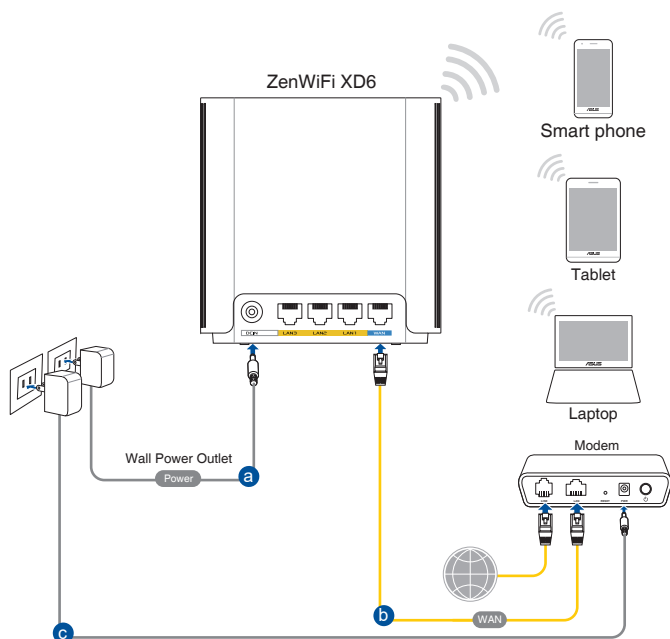
**ПРИМЕЧАНИЕ:** Для проводного подключения можно использовать любой (прямой или перекрестный) кабель.



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

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

## 1.6.2 Беспроводное подключение



### Для настройки беспроводного роутера через беспроводное соединение:

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

### ПРИМЕЧАНИЯ:

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

## 2 Начало работы

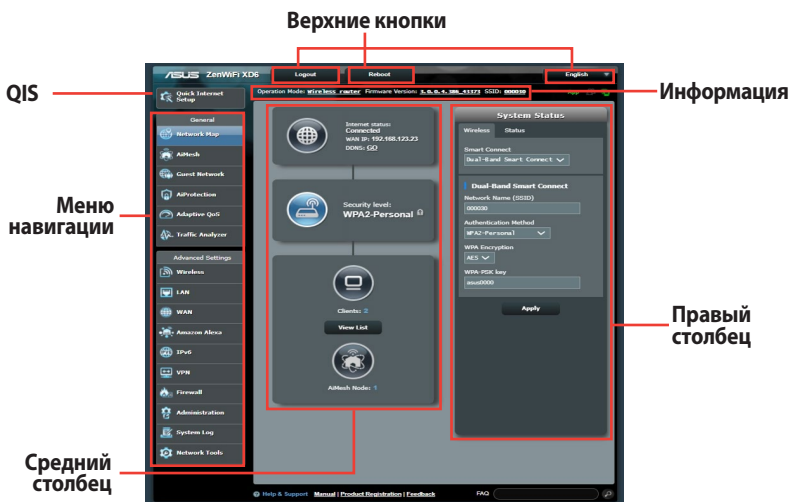
### 2.1 Вход в веб-интерфейс

Данный беспроводной роутер имеет интуитивно понятный графический интерфейс пользователя (GUI), что позволяет легко сконфигурировать его функции через браузер, например 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 <http://router.asus.com>.
2. В окне входа, введите имя пользователя по умолчанию (**admin**) и пароль (**admin**).
3. Теперь можно использовать веб-интерфейс для конфигурации различных параметров роутера.



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

## 2.2 Быстрая настройка Интернет (QIS) с автоопределением

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

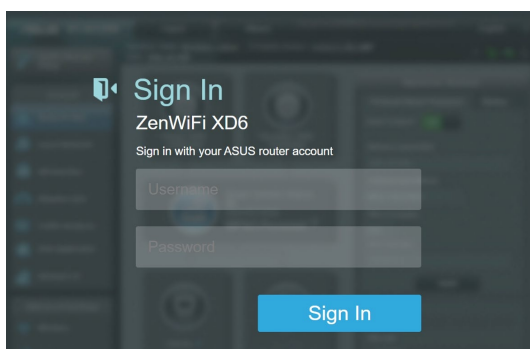
---

**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. Войдите в веб-интерфейс. Автоматически появится страница быстрой настройки (QIS).



---

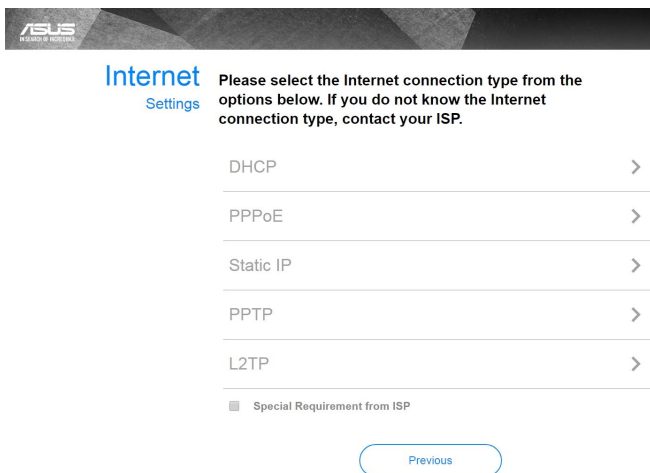
### Примечания:

- Подробную информации об изменении имени пользователя и пароля смотрите в разделе **4.6.2 Система**.
  - Имя пользователя и пароль отличается от имени сети (SSID) и ключа безопасности. Имя пользователя и пароль позволяют войти в веб-интерфейс роутера для конфигурации параметров беспроводного роутера. Имя сети (SSID) и ключ безопасности позволяют беспроводным устройствам подключаться к беспроводной сети.
-

2. Роутер поддерживает следующие типы подключения: **Динамический IP, PPPoE, PPTP, L2TP, Статический IP** и автоматически определяет Динамический IP, PPPoE. Введите необходимую информацию для Вашего типа подключения.

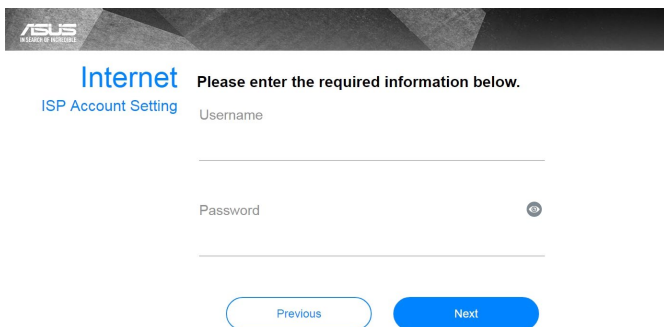
**ВАЖНО!** Необходимую информацию о Вашем подключении к интернету узнайте у Вашего провайдера.

для автоматического IP (DHCP)




The screenshot shows the 'Internet Settings' page on an ASUS router. The title is 'Internet Settings'. Below the title, there is a message: 'Please select the Internet connection type from the options below. If you do not know the Internet connection type, contact your ISP.' There are five radio button options: 'DHCP', 'PPPoE', 'Static IP', 'PPTP', and 'L2TP'. The 'DHCP' option is selected. Below these options is a checkbox labeled 'Special Requirement from ISP'. At the bottom, there is a 'Previous' button.

для PPPoE, PPTP и L2TP



The screenshot shows the 'ISP Account Setting' page on an ASUS router. The title is 'Internet ISP Account Setting'. Below the title, there is a message: 'Please enter the required information below.' There are two input fields: 'Username' and 'Password'. The 'Password' field has a toggle icon to the right. At the bottom, there are two buttons: 'Previous' and 'Next'.

## Для статического IP



**Internet**  
Static IP

**Static IP allows your PC to use a fixed IP address provided by your ISP.**

IP Address  
192.168.1.215

Subnet Mask  
255.255.255.0

Default Gateway  
192.168.1.1

DNS Server1  
192.168.1.1

DNS Server2

Previous Next

---

### Примечания:

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


- 
3. Назначьте имя сети (SSID) и ключ безопасности для беспроводных подключений 2.4 ГГц и 5 ГГц. Когда закончите, нажмите **Применить**.



**Wireless**  
Settings

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

Network Name (SSID)

Wireless Security 

Separate 2.4GHz and 5GHz

[Previous](#) [Apply](#)

---


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

---


**Wireless**  
Settings

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

2.4GHz Network Name (SSID)

2.4GHz Wireless Security 

5GHz-1 Network Name (SSID)

5GHz-1 Wireless Security 



Separate 2.4GHz and 5GHz

[Previous](#) [Apply](#)

## 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 **ОК**.
4. Дождитесь подключения компьютера к беспроводной сети. Иконка  отображает состояние подключения и мощность сигнала проводного или беспроводного подключения.

---

### ПРИМЕЧАНИЯ:

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

## 3 Конфигурация общих настроек

### 3.1 Использование карты сети

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



### 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. На экране карты сети, под областью **Состояние системы** можно сконфигурировать параметры безопасности беспроводной сети, например SSID, уровень безопасности и настройки шифрования.

**ПРИМЕЧАНИЕ:** Вы можете настроить параметры безопасности для диапазонов 2.4 ГГц и 5 ГГц.

#### Настройки 2.4 ГГц



#### Настройки 5 ГГц

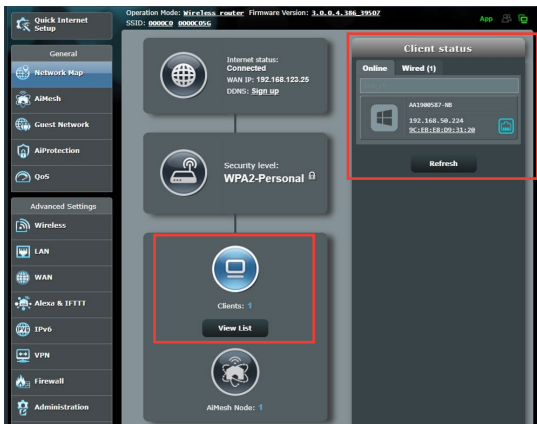


3. В поле **Wireless name (SSID)** введите уникальное имя для Вашей беспроводной сети.
4. В выпадающем списке **WEP-шифрование** выберите метод шифрования для беспроводной сети.

**ВАЖНО!** Стандарт IEEE 802.11n/ac 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 Создание гостевой сети

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

---

**ПРИМЕЧАНИЕ:** Роутер поддерживает до девяти SSID.

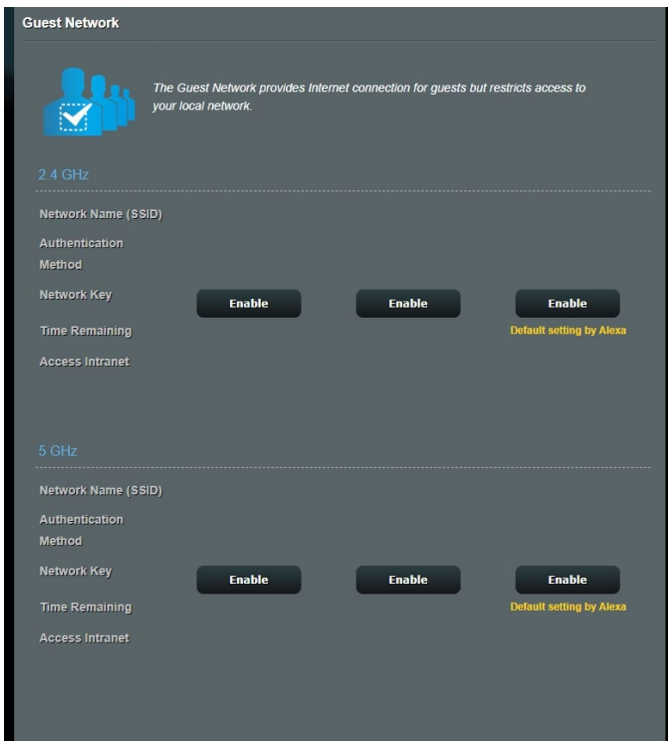
---

### Для создания гостевой сети:

1. В меню навигации выберите **Общие** > **Гостевая сеть**.
2. На экране гостевой сети выберите используемый диапазон: 2.4 или 5 ГГц.
3. Выберите **Включить**.

The screenshot displays the 'Guest Network' configuration page. At the top, there is a header 'Guest Network' and a blue icon of three people with a checkmark. Below the icon is a descriptive text: 'The Guest Network provides Internet connection for guests but restricts access to your local network.' The interface is divided into two sections for different frequency bands: '2.4 GHz' and '5 GHz'. Each section contains the following settings: 'Network Name (SSID)', 'Authentication Method', 'Network Key' (with three 'Enable' buttons), 'Time Remaining', and 'Access Intranet'. A yellow note 'Default setting by Alexa' is visible next to the 'Time Remaining' field in both sections.

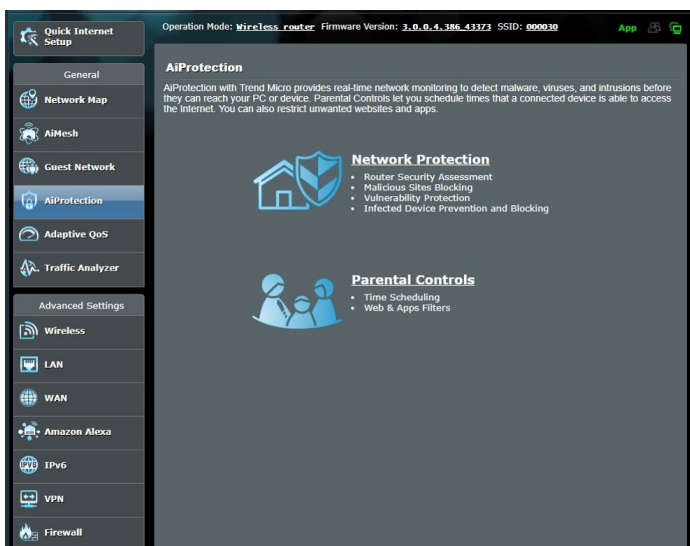
4. Для изменения гостевых настроек, щелкните по ним. Нажмите **Удалить** для удаления гостевых настроек.
5. В поле **Имя сети (SSID)** назначьте имя для временной беспроводной сети.



6. Выберите метод аутентификации.
7. При выборе WPA-аутентификации выберите шифрование WPA..
8. Укажите время доступа или выберите пункт **Безграничный**.
9. Включите или отключите **Доступ к Интранет**.
10. Когда закончите, нажмите **Применить**.

## 3.3 AiProtection

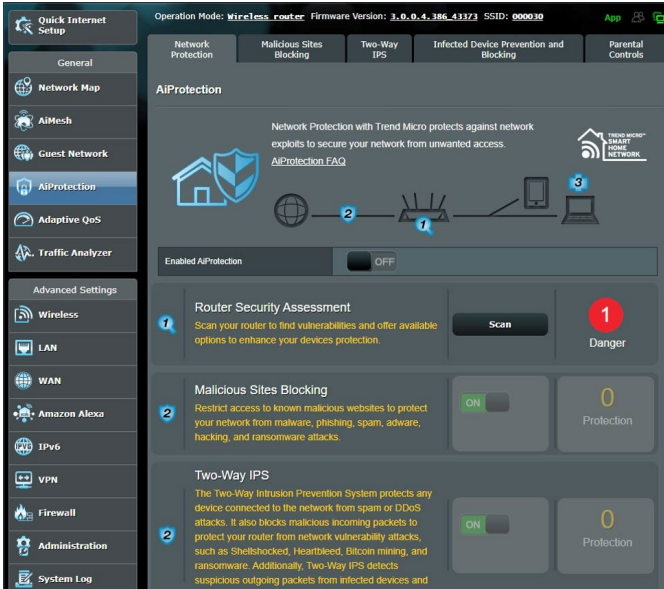
AiProtection обеспечивает мониторинг в режиме реального времени для обнаружения вредоносного программного обеспечения. Также возможна фильтрация нежелательных сайтов и приложений и установка времени доступа к интернету.





### 3.3.1 Сетевая защита

Сетевая защита обеспечивает защиту сети от несанкционированного доступа.

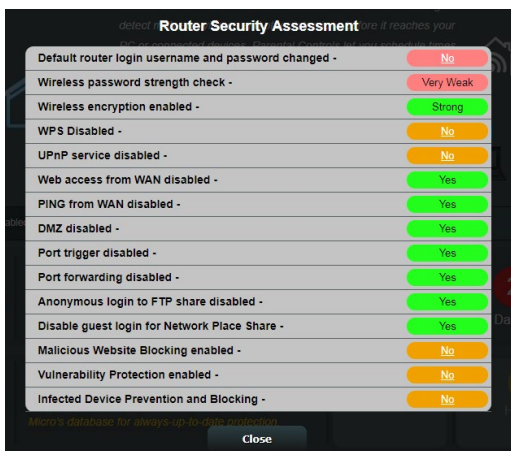


#### Конфигурация сетевой защиты

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** 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:
- Щелкните по элементу.

---

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

---

- На странице настроек безопасности элемента внесите необходимые изменения и нажмите **Применить**.
  - Вернитесь на страницу **Оценка безопасности роутера** и нажмите **Закреть** для закрытия страницы.
5. Для конфигурации настроек безопасности автоматически нажмите **Защитить роутер**.
6. При появлении подтверждения нажмите **ОК**.

## Блокировка вредоносных сайтов

Эта функция ограничивает доступ к известным вредоносным сайтам, добавленным 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**.

## Профилактика и блокировка зараженных устройств

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

---

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

---

### Для включения профилактики и блокировки зараженного устройства:

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

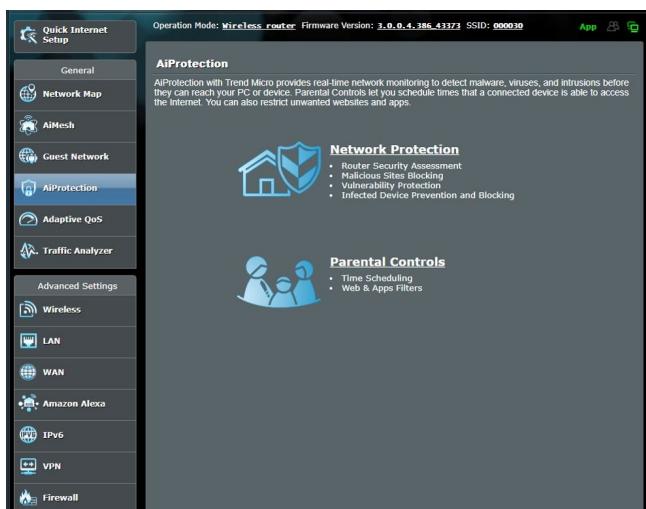
### Для конфигурации предпочитаемых оповещений:

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

### 3.3.2 Настройка Родительского контроля

Родительский контроль позволяет контролировать время доступа к интернету или ограничивать время использования интернета. Для перехода на главную страницу родительского контроля:

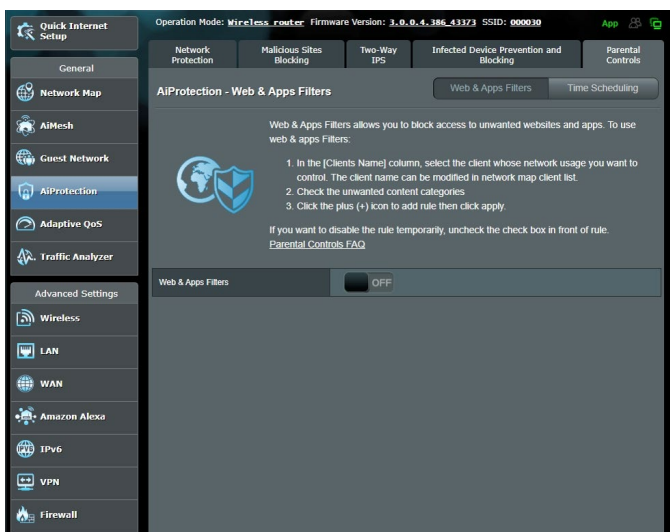
1. В меню навигации выберите **Общие > AiProtection**.
2. На главной странице **AiProtection** нажмите вкладку **Родительский контроль**.



## Расписание

Расписание позволяет установить ограничение времени для использования сети клиентом.

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



**Для конфигурации расписания:**

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

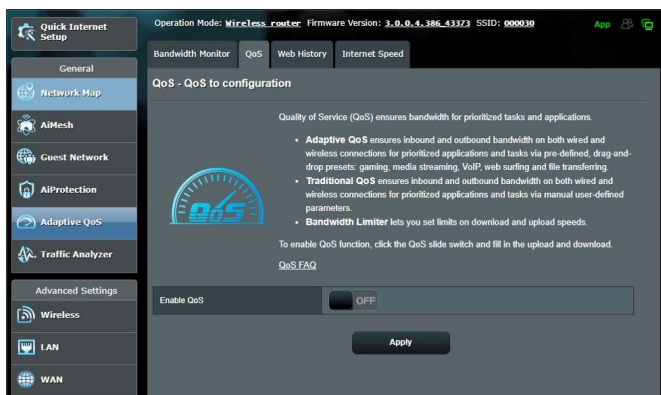
**ПРИМЕЧАНИЕ:** Также можно ввести MAC-адрес клиента в поле **MAC-адрес клиента**. Убедитесь, что имя клиента не содержит специальных символов или пробелов, поскольку это может вызвать сбой в работе роутера.

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

## 3.4 Использование Диспетчера трафика

### 3.4.1 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 > вкладка 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 **Сохранить**.

---

**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, заполните **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 PC 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.

---

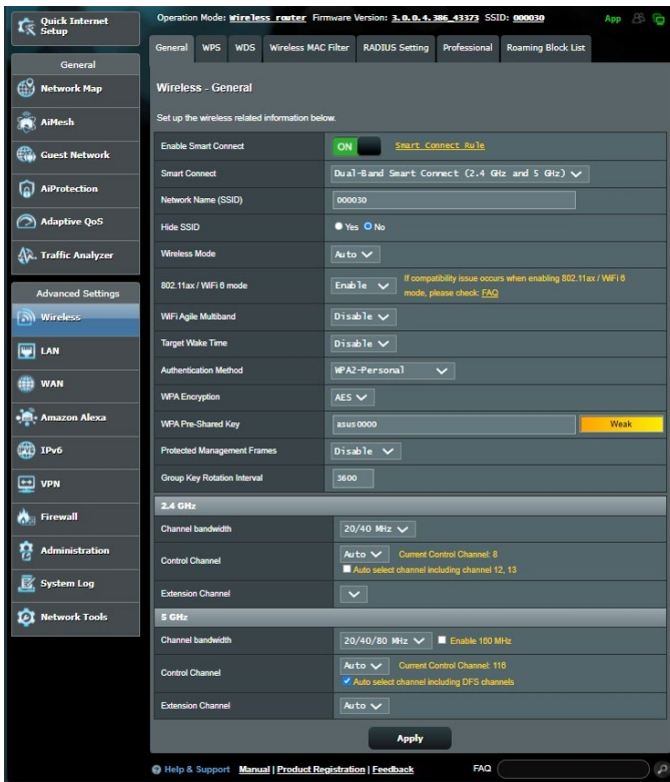


# 4 Настройка дополнительных параметров

## 4.1 Беспроводная связь

### 4.1.1 Общие

На странице Общие можно сконфигурировать основные параметры беспроводной сети.



## Для конфигурации основных параметров беспроводной сети:

1. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > вкладка **Общие**.
2. Выберите 2,4 или 5 ГГц в качестве диапазона частот для беспроводной сети.
3. Для идентификации Вашей беспроводной сети назначьте сетевое имя или SSID (Идентификатор беспроводной сети) 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, 802.11g и 802.11b.
  - **Legacy:** Выберите **Legacy** для разрешения подключения к роутеру устройств 802.11b/g/n. Максимальная скорость для устройств 802.11n будет 54 Мбит/с.
  - **Only:** Выберите **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**.

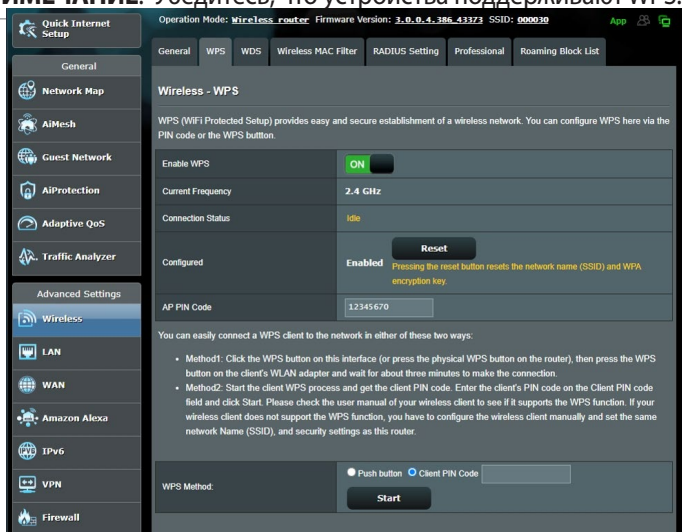
---

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**.

## 4.1.2 WPS

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

**ПРИМЕЧАНИЕ:** Убедитесь, что устройства поддерживают WPS.



### Для включения WPS в беспроводной сети:

1. В меню навигации выберите **Дополнительные настройки** > **Беспроводная связь** > вкладка **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.

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

---

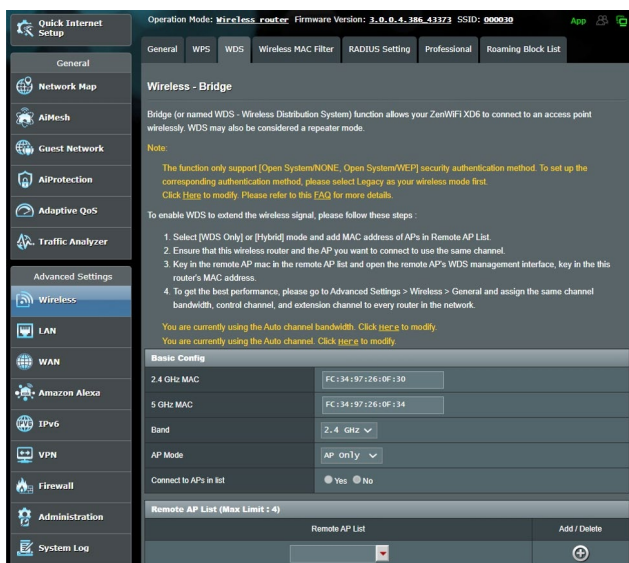
**ПРИМЕЧАНИЕ:** Расположение кнопки WPS смотрите в документации беспроводного устройства.

---

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

## 4.1.3 Мост

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



Для настройки беспроводного моста:

1. В меню навигации выберите **Дополнительные настройки > Беспроводная связь > вкладка WDS.**
2. Выберите диапазон частот для беспроводного моста.
3. В поле **Режим AP** выберите любую из следующих опций:
  - **AP Only:** Отключает функцию беспроводного моста.
  - **WDS Only:** Включает функцию беспроводного моста, но запрещает подключение к роутеру других беспроводных устройств.
  - **HYBRID:** Включает функцию беспроводного моста и разрешает подключение к роутеру других беспроводных устройств.

---

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

---

4. В поле **Подключиться к точкам доступа в списке** выберите **Да**, если необходимо подключиться к точке доступа в списке удаленных AP.
5. В поле **Канал управления** выберите рабочий канал для беспроводного моста. Выберите **Авто** для автоматического выбора канала с наименьшим количеством помех.

---

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

---

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

---

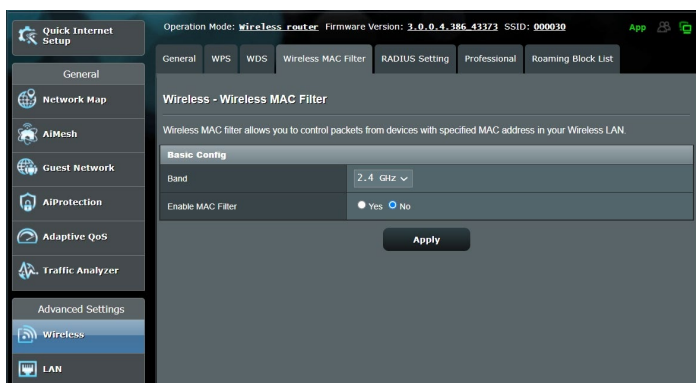
**ПРИМЕЧАНИЕ:** Любая добавленная в список точка доступа использовать одинаковый с роутером канал управления.

---

7. Нажмите **Применить**.

## 4.1.4 Фильтр MAC-адресов беспроводной сети

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



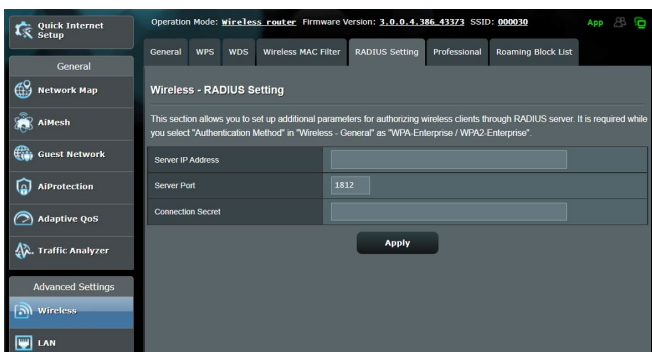
**Для настройки фильтра MAC адресов беспроводной сети:**

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



## 4.1.5 Настройка RADIUS

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



### Для настройки параметров RADIUS:

1. Убедитесь, что режим аутентификации беспроводного роутера установлен в значение WPA-Enterprise, WPA2-Enterprise или Radius with 802.1x.

---

**ПРИМЕЧАНИЕ:** Настройки режима аутентификации для беспроводного роутера смотрите в разделе **4.1.1 Общие**.

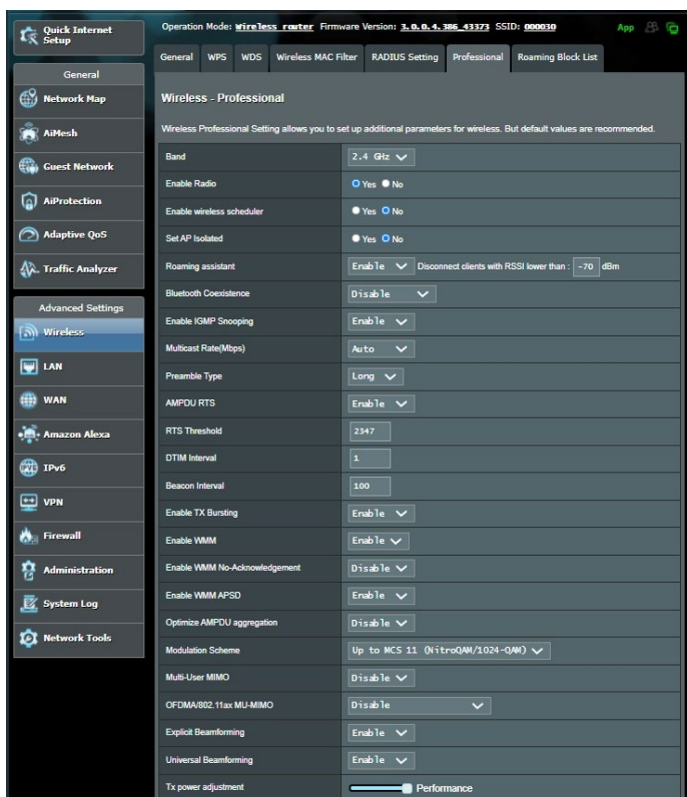
---

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

## 4.1.6 Профессиональный

На экране Профессиональный можно сконфигурировать дополнительные параметры.

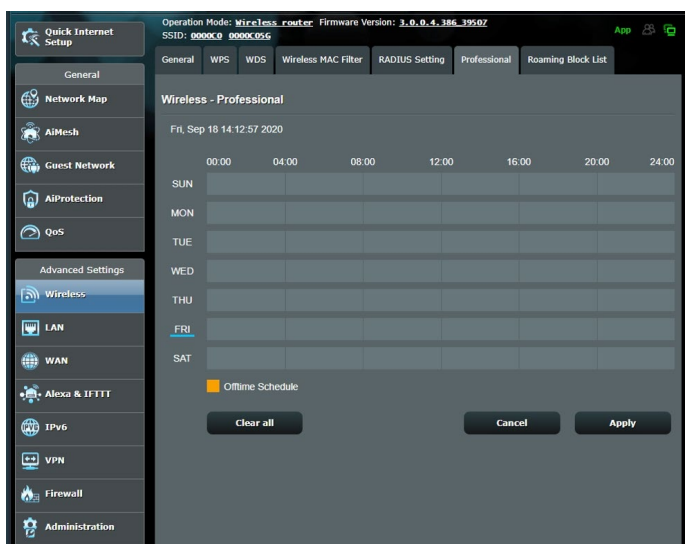
**ПРИМЕЧАНИЕ:** Мы рекомендуем использовать значения по умолчанию.



На экране **Профессиональные настройки** можно сконфигурировать следующее:

- **Диапазон:** Выберите диапазон, настройки которого нужно изменить.
- **Включить радиомодуль:** Выберите **Да** для включения радиомодуля. Выберите **Нет** для отключения радиомодуля.

- **Включить беспроводный планировщик:** 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 **ОК**.



- **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 продолжительность времени, которое требуется роутеру для CRC (Cyclic Redundancy Check). CRC - это метод обнаружения ошибок во время передачи данных. Выберите **Короткая** для беспроводной сети с большим трафиком. Выберите **Длинная** для беспроводной сети со старыми беспроводными устройствами.
- **Порог RTS:** Для беспроводных сетей с большим трафиком и большим количеством беспроводных устройств выберите низкий порог RTS.

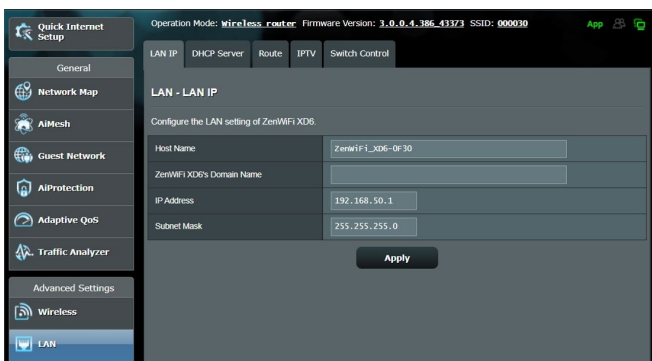
- **Интервал DTIM:** Интервал DTIM (Delivery Traffic Indication Message) или Data Beacon Rate - это интервал времени перед отправкой сигнала беспроводному устройству в спящем режиме, указывая, что пакет данных ожидает доставки. Значение по умолчанию: три миллисекунды.
- **Сигнальный интервал:** Сигнальный 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.

## 4.2 Локальная сеть

### 4.2.1 LAN IP

На экране LAN IP можно изменить настройки LAN IP роутера.

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

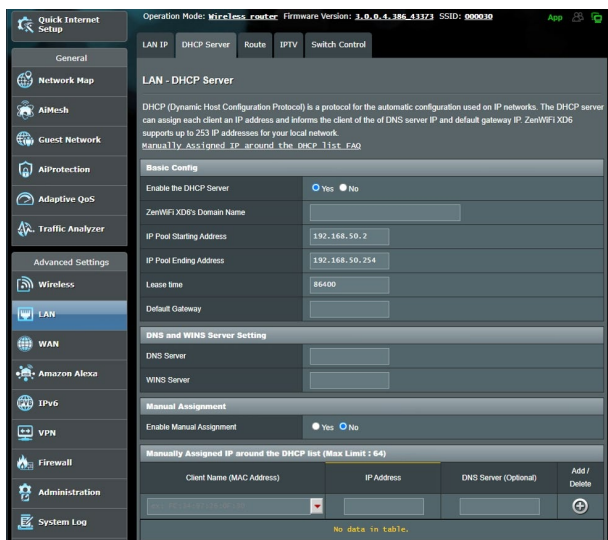


**Для изменения параметров LAN IP:**

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

## 4.2.2 DHCP-сервер

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



**Для конфигурации DHCP сервера:**

1. В меню навигации выберите **Дополнительные настройки > Брандмауэр > вкладка DHCP-сервер.**
2. В поле **Включить DHCP сервер** выберите **Да.**
3. В поле **Имя домена ZenWiFi XD6 Hybrid** введите имя домена для беспроводного роутера.
4. В поле **Начальный адрес пула** введите начальный IP-адрес.
5. В поле **Конечный адрес пула** введите конечный IP-адрес.

6. В поле **Время аренды** введите время аренды IP-адреса. По истечении времени, DHCP сервер назначит новый IP-адрес.

---

**ПРИМЕЧАНИЯ:**

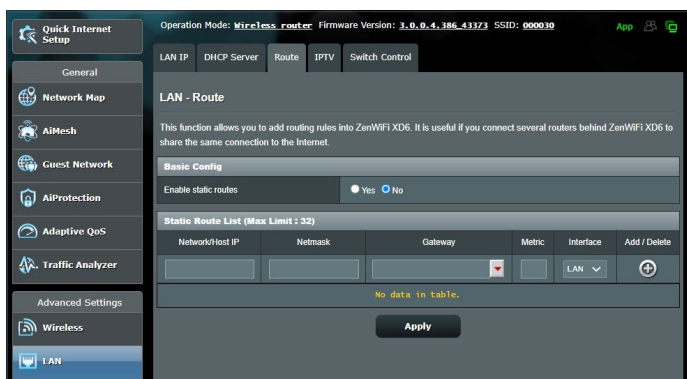
- Рекомендуется использовать IP-адрес в формате: 192.168.1.xxx (где xxx может быть любым числом в диапазоне от 2 до 254).
  - Начальный IP-адрес пула не должен быть больше конечного IP-адреса.
- 

7. Если необходимо, введите IP-адреса DNS и WINS серверов в поля **DNS-сервер** и **WINS-сервер**.
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.

## 4.2.3 Маршрут

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

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



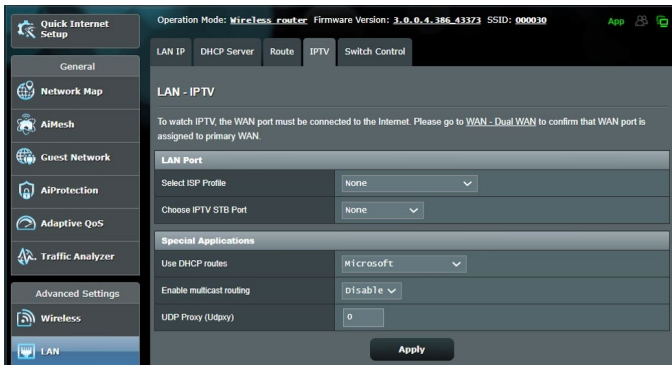
### Для конфигурации таблицы маршрутизации:

1. В меню навигации выберите **Дополнительные настройки** > **LAN** > вкладка **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**.



## 4.2.4 IPTV

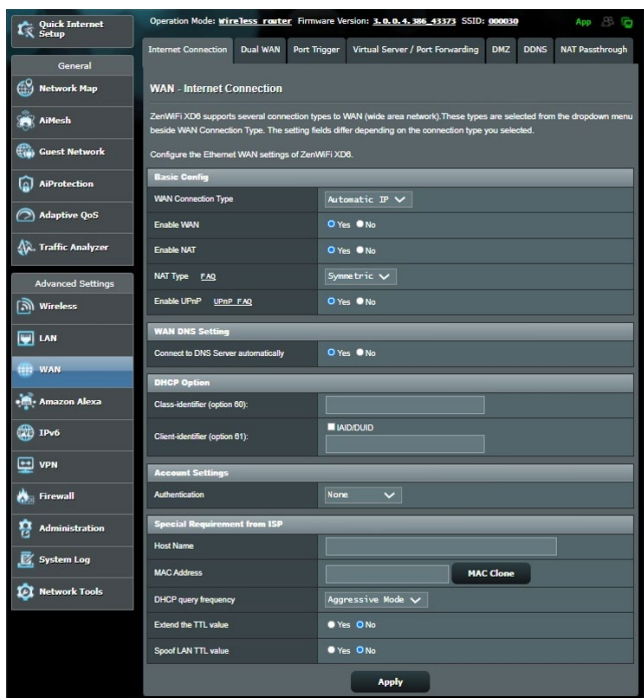
Беспроводной роутер поддерживает подключение к службе IPTV по локальной сети или через провайдера. На вкладке IPTV можно сконфигурировать параметры IPTV, VoIP, групповой рассылки и UDP. Подробную информацию можно получить у Вашего провайдера.



## 4.3 WAN

### 4.3.1 Подключение к интернету

На странице подключения к интернету можно сконфигурировать параметры WAN подключения.



Для конфигурации параметров WAN:

1. В меню навигации выберите **Дополнительные настройки > WAN > вкладка 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.

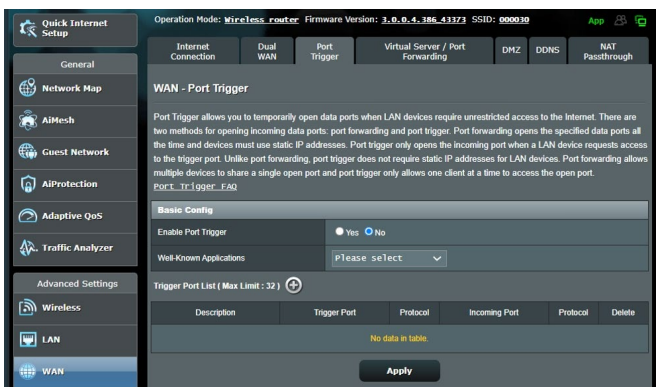
- **Включить WAN:** Выберите **Да** для включения доступа к интернету. Выберите **Нет** для отключения доступа к интернету.
- **Включить функцию трансляции сетевых адресов (NAT):** NAT (трансляция сетевых адресов) представляет собой систему, в которой один публичный IP (WAN IP) используется для предоставления 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 and Play) позволяет использовать несколько устройств (роутеры, телевизоры, стереосистемы, игровые приставки, сотовые телефоны), которые будут управляться через IP-сети с или без централизованного управления через шлюз. UPnP соединяет компьютеры любых типов, обеспечивая единую сеть для удаленной конфигурации и передачи данных. Новое сетевое устройство обнаруживается автоматически с помощью UPnP. После подключения к сети, устройства можно дистанционно сконфигурировать для поддержки P2P-приложений, интерактивных игр, видеоконференций и веб- или прокси-серверов. В отличие от перенаправления портов, которое требует ручной настройки, UPnP автоматически настраивает роутер для принятия входящих соединений и передает запросы к определенному компьютеру в локальной сети.
- **Подключение к DNS серверу автоматически:** Позволяет роутеру автоматически получить IP-адрес DNS сервера от провайдера. DNS - это хост в интернете, который транслирует имена Интернет в IP-адреса.
- **Аутентификация:** Этот пункт может указываться некоторыми поставщиками услуг Интернета. Уточните у Вашего провайдера и заполните в случае необходимости.
- **Имя хоста:** Это поле позволяет указать имя хоста для роутера. Обычно, это специальное требование от провайдера. Введите имя хоста здесь, если ваш провайдер назначил его для вашего компьютера.

- **MAC-адрес:** MAC (Media Access Control) адрес уникальный идентификатор для сетевого устройства. Некоторые провайдеры контролируют MAC-адреса устройств, подключенных к их оборудованию и могут запретить подключение устройства с незнакомым MAC-адресом. Во избежание проблем с подключением из-за незарегистрированного MAC-адреса возможны следующие действия:
  - Обратитесь к Вашему провайдеру и попросите обновить MAC адрес.
  - Склонируйте или измените MAC-адрес роутера в соответствии с MAC адресом оригинального устройства..

## 4.3.2 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:

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



**Для настройки переключения портов:**

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

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

---

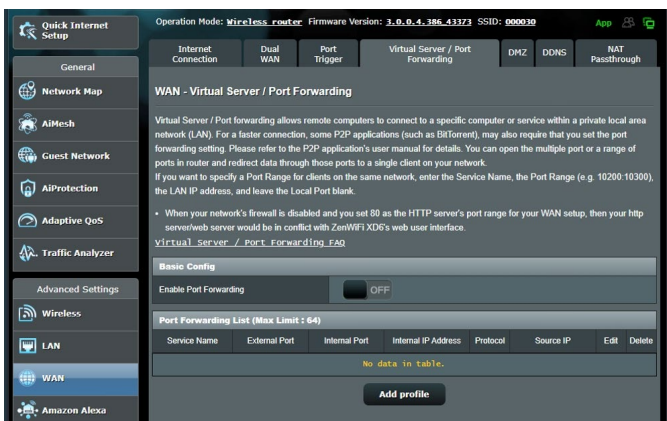
#### **ПРИМЕЧАНИЯ:**

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

## 4.3.3 Virtual Server/Port Forwarding

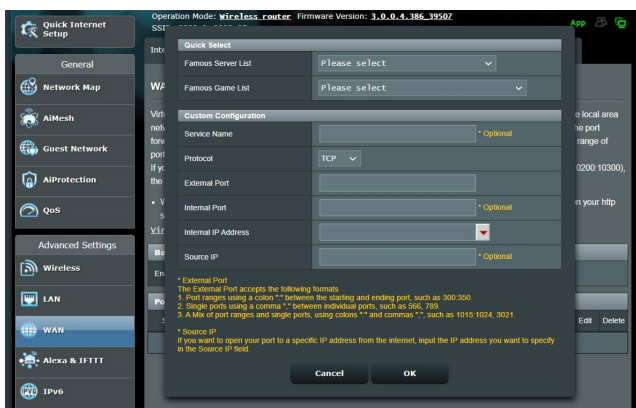
Переадресация портов - метод для перенаправления сетевого трафика из Интернета на указанный порт или диапазон портов устройства в локальной сети. Настройка переадресации портов на роутере позволяет удаленным компьютерам использовать службы, предоставляемые компьютерами вашей сети.

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



**Для настройки переадресации портов:**

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



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



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

---

**ПРИМЕЧАНИЕ:** Для корректной переадресации используйте для локального клиента статический IP-адрес. Подробную информацию смотрите в разделе **4.2 LAN**.

---

### **Для проверки правильной настройки переадресации портов:**

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

### **Различия между переключением портов и перенаправлением портов:**

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

### 4.3.4 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.

---

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

---

#### Для настройки DMZ:

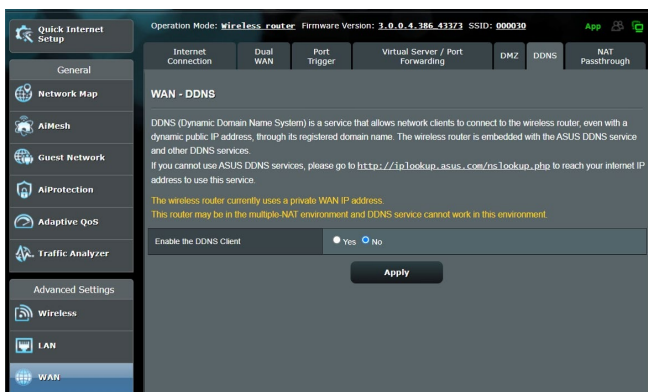
1. В меню навигации выберите **Дополнительные настройки > WAN > вкладка DMZ**.
2. Сконфигурируйте параметры ниже. Когда закончите, нажмите **Применить**.
  - **IP-адрес видимой станции:** Введите LAN IP-адрес клиента, который будет использоваться для DMZ. Убедитесь, что сервер использует статический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

#### Для удаления DMZ:

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

## 4.3.5 DDNS

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



### Для настройки DDNS:

1. В меню навигации выберите **Дополнительные настройки** > **WAN** > вкладка **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:

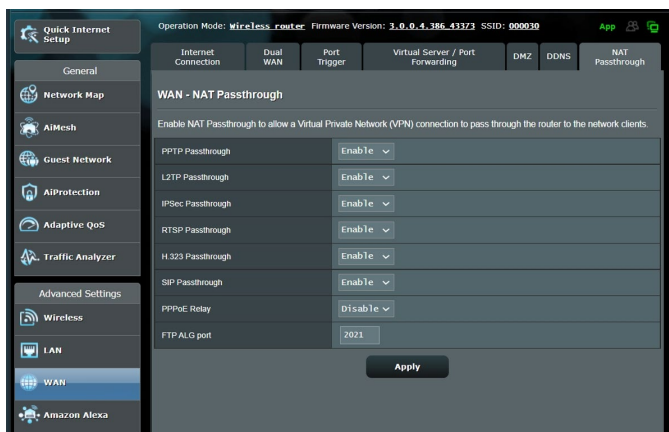
Служба DDNS сервис не будет работать при следующих условиях:

- 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.
- 

### 4.3.6 NAT Passthrough

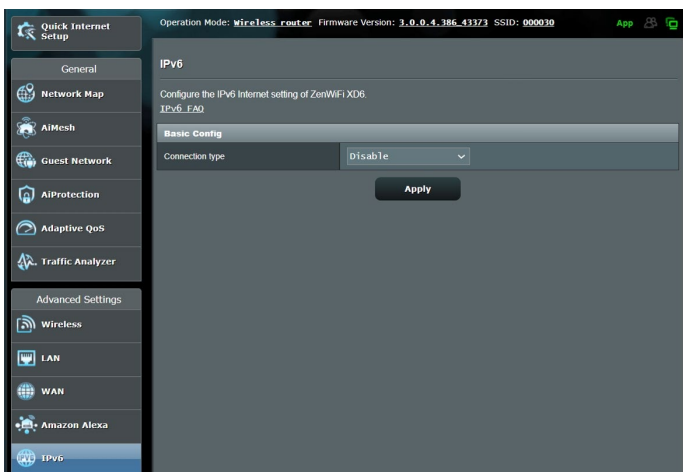
NAT Passthrough разрешает пакетам (VPN) проходить через роутер к сетевым клиентам. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough и RTSP Passthrough включены по умолчанию..

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



## 4.4 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.

---

## 4.5 Брандмауэр

Роутер может функционировать в качестве аппаратного брандмауэра.

---

**ПРИМЕЧАНИЕ:** Брандмауэр включен по умолчанию.

---

### 4.5.1 Общие

**Для настройки параметров брандмауэра:**

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

### 4.5.2 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.

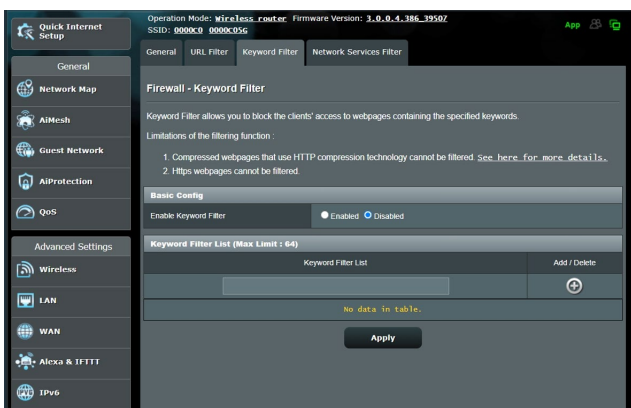
---

## Для настройки фильтра URL:

1. В меню навигации выберите **Дополнительные настройки > Брандмауэр > вкладка Фильтр URL.**
2. В поле Enable URL Filter выберите **Enabled.**
3. Введите URL и нажмите .
4. Нажмите **Применить.**

## 4.5.3 Фильтр ключевых слов

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



## Для настройки фильтра ключевых слов:

1. В меню навигации выберите **Дополнительные настройки > Брандмауэр > вкладка 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.abcsxxx.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.

## 4.5.4 Фильтр сетевых служб

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

Operation Mode: **Wireless router** Firmware Version: **3.0.0.4.386\_43323** SSID: **000030**

General | URL Filter | Keyword Filter | **Network Services Filter**

### 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.

**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  Yes  No

Filter table type: Deny List

Well-Known Applications: User Defined

Date to Enable LAN to WAN Filter: Mon Tue Wed Thu Fri

Time of Day to Enable LAN to WAN Filter: 00 : 00 - 23 : 59

Date to Enable LAN to WAN Filter: Sat 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.



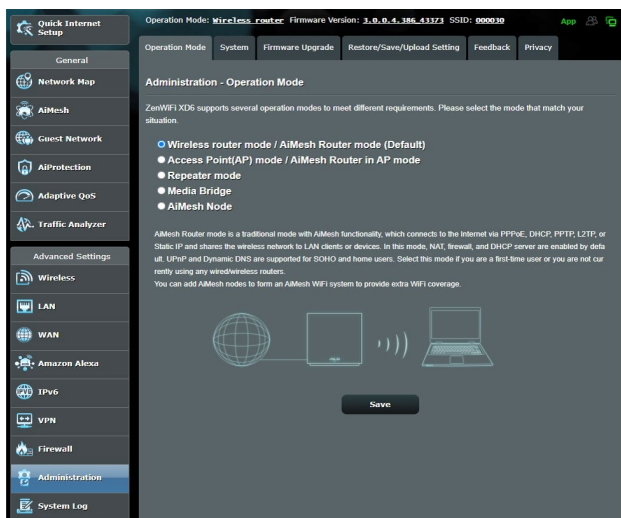
### Для настройки фильтра сетевых служб:

1. В меню навигации выберите **Дополнительные настройки > Брандмауэр >** вкладка **Фильтр сетевых служб**.
2. В поле Включить фильтр сетевых служб выберите **Да**.
3. Выберите режим фильтра. **Черный список** блокирует указанные сетевых службы. **Белый список** предоставляет 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**.

## 4.6 Администрирование

### 4.6.1 Режим работы

На странице режим работы можно выбрать наиболее подходящий режим.



Для настройки режима работы:

1. В меню навигации выберите **Дополнительные настройки** > **Администрирование** > вкладка **Режим работы**.
2. Выберите любой из следующих режимов:
  - **Режим беспроводного роутера / режим роутера AiMesh (по умолчанию):** В режиме беспроводного роутера, роутер подключается к интернету и предоставляет доступ к интернету для устройств в локальной сети.
  - **Режим точки доступа (AP) / роутера AiMesh в режиме AP:** В этом режиме роутер создает новую беспроводную сеть.
  - **Режим повторителя:** В режиме повторителя роутер подключается к существующей беспроводной сети и расширяет покрытие существующей беспроводной сети.
3. Нажмите **Сохранить**.

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

## 4.6.2 Система

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

**Для настройки параметров системы:**

1. В меню навигации выберите **Дополнительные настройки** > **Администрирование** > вкладка **Система**.
2. Можно сконфигурировать следующие параметры:
  - **Изменение пароля роутера:** Можно изменить имя пользователя и пароль беспроводного роутера, введя новые.
  - **Настройка USB:** Можно включить режим гибернации жесткого диска и изменить режим USB.
  - **Поведение кнопки WPS:** Физическая кнопка WPS используется для активации WPS.
  - **Часовой пояс:** Выберите часовой пояс для Вашей сети.
  - **NTP-сервер:** Для синхронизации времени роутер может подключаться к серверу NTP (Network Time Protocol).
  - **Сетевой мониторинг:** Можно включить DNS-запрос для проверки соответствия имени хоста и IP-адреса или включить Ping для проверки целевого адреса.
  - **Автоматический выход:** Можно задать время для автоматического выхода.
  - **Включить уведомление об отключении WAN-интерфейса:** Эта функция позволяет браузеру отображать страницу с предупреждением, когда роутер отключен от Интернета. Когда отключено, страница с предупреждением не появится.
  - **Включить Telnet:** Нажмите **Да** для включения службы Telnet. Выберите **Нет** для отключения Telnet.
  - **Метод аутентификации:** Можно выбрать HTTP, HTTPS или оба протокола для безопасного доступа к роутеру.
  - **Включить планировщик перезагрузки:** Когда включено, можно задать время и дату перезагрузки.
  - **Включить веб-доступ из WAN:** Выберите **Да** для разрешения доступа к веб-интерфейсу роутера из Интернет. Выберите **Нет** для предотвращения доступа.

- **Включить ограничение доступа:** Выберите **Да**, если нужно задать IP-адреса устройств, которым разрешен доступ к веб-интерфейсу роутера из WAN/LAN.
  - **Служба:** Эта функция позволяет настроить Telnet / SSH порт / Разрешить ввод пароля / ключа авторизации / тайм-аут простоя.
3. Нажмите **Применить**.

### 4.6.3 Обновление прошивки

---

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

---

#### Для обновления прошивки:

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

---

#### Примечания:

- После завершения обновления дождитесь перезагрузки системы.
- При ошибке во время обновления беспроводной роутер переходит в аварийный режим и индикатор питания на передней панели медленно мигает. Подробную информацию о восстановлении системы смотрите в разделе **5.2 Восстановление прошивки**.

### 4.6.4 Восстановить/сохранить/загрузить настройки

#### Для восстановления/сохранения/сброса параметров:

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

---

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

---

## 4.7 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. Можно посмотреть сетевую активность на любой из этих вкладок:
  - Общий журнал
  - Журнал беспроводной сети
  - Аренда адресов DHCP
  - IPv6
  - Таблица маршрутизации
  - Переадресация портов
  - Подключения

The screenshot shows the 'System Log - General Log' page of a router. The interface includes a top navigation bar with 'Quick Internet Setup', 'General', 'Network Map', 'AiMesh', 'Guest Network', 'AiProtection', 'Adaptive QoS', and 'Traffic Analyzer'. Below this is an 'Advanced Settings' section with 'Wireless', 'LAN', 'WAN', 'Amazon Alexa', 'IPv6', 'VPN', and 'Firewall' options. The main content area displays system information: 'Operation Mode: Wireless router', 'Firmware Version: 3.0.0.4\_386\_43323', and 'SSID: 600030'. It also shows 'System Log - General Log' with a note that the page shows detailed system activities. The system time is 'Wed, Aug 04 16:44:33 2021' and the uptime is '0 days 6 hour(s) 42 minute(s) 31 seconds'. The 'Remote Log Server' is set to '514'. Below this, a list of log entries is visible, showing various network events such as 'wificlientd: wificlientd\_proc\_event(527)', 'eth6: Auth 26:93:62:64:2D:84', and 'status: Success'.

## 5 Утилиты

---

### ПРИМЕЧАНИЯ:

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

### 5.1 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**.

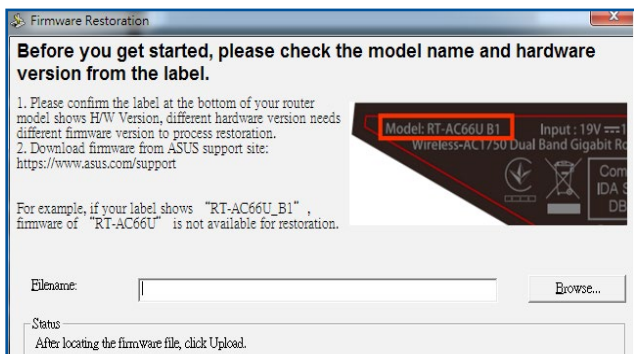
---

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

---

## 5.2 Восстановление прошивки

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



---

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

---

**ПРИМЕЧАНИЕ:** Эта функция не поддерживается в MAC OS.

---

### Для запуска утилиты Firmware Restoration:

1. Отключите питание от роутера.
2. Удерживая кнопку Reset, расположенную на задней панели, подключите питание к роутеру. Отпустите кнопку сброса когда индикатор питания, расположенный на передней панели, начнет медленно мигать, означая, что роутер находится в режиме восстановления.



3. Установите статический IP на Вашем компьютере и используйте следующие настройки TCP/IP:

**IP-адрес:** 192.168.1.x

**Маска подсети:** 255.255.255.0

4. Перейдите **Пуск > Программы > ASUS Utility > 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 4 **Настройка дополнительных параметров.**

---

## 6 Устранение неисправностей

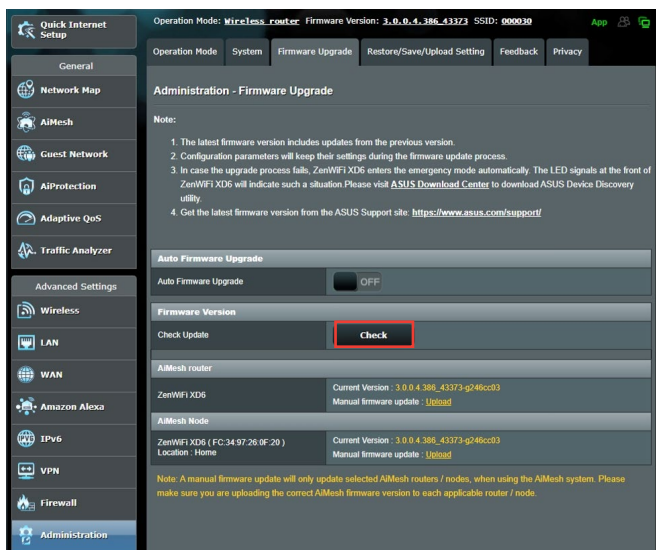
В этом разделе представлены инструкции для решения некоторых наиболее часто встречающихся общих проблем с роутером. Если Вы столкнулись с проблемами, не упомянутыми в этой главе, посетите сайт ASUS <https://www.asus.com/support/> для получения дополнительной информации о продукте или обратитесь в службу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

### 6.1 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** > вкладка **Обновление прошивки**. Нажмите **Проверить** для проверки наличия последней версии прошивки.



2. Если доступна новая прошивка, посетите сайт ASUS <https://www.asus.com/Mesh-WiFi-System/ZenWiFi-XD6/HelpDesk/> и скачайте ее.
3. На странице **Обновление прошивки** нажмите **Browse** для нахождения прошивки.
4. Нажмите **Загрузить** для обновления прошивки.

### **Последовательность перезапуска сети:**

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

### **Убедитесь в правильности подключения Ethernet-кабеля.**

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

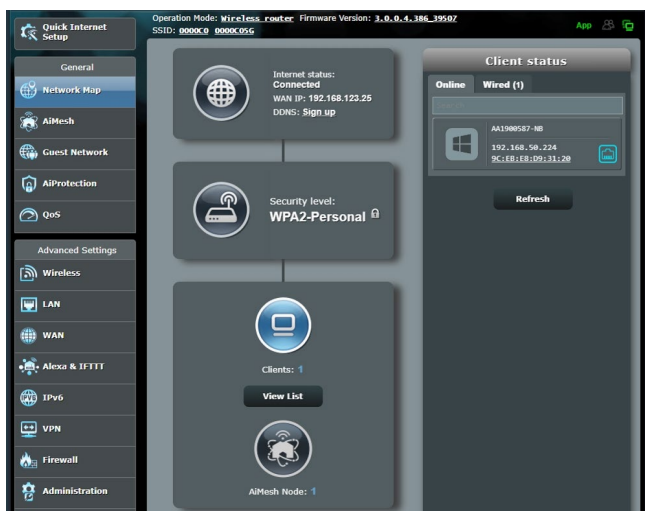
### **Убедитесь, что настройки беспроводной сети компьютера совпадают с роутером.**

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

### **Убедитесь в правильности сетевых настроек.**

- Каждый сетевой клиент должен иметь действительный IP-адрес. Для назначения IP-адресов компьютерам вашей сети рекомендуется использовать DHCP-сервер роутера.

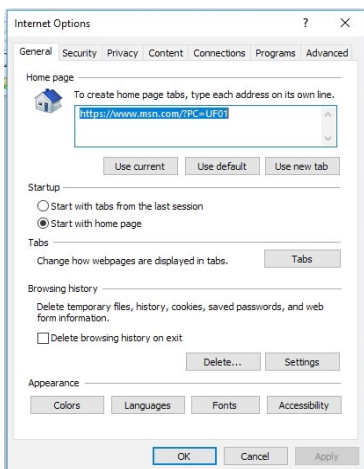
- Некоторые провайдеры требуют использовать MAC-адрес компьютера, используемого при первом подключении. MAC-адрес можно посмотреть в веб-интерфейсе, наведя курсор мыши на устройство в поле **Состояние клиента** на странице **Карта сети > Клиенты**.



## 6.2 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. По умолчанию логин и пароль: "admin/admin". Убедитесь, что режим Caps Lock отключен при вводе данных.
- Удалите куки-файлы в браузере.. В браузере Internet Explorer выполните следующие действия:
  1. Запустите Internet Explorer, затем нажмите **Сервис > Свойства обозревателя**.
  2. На вкладке **Общие** в области **Просмотр истории** нажмите **Удалить...**, выберите **Временные файлы Интернета** и **Файлы cookie и данные сайта** и нажмите **Удалить**.



#### ПРИМЕЧАНИЯ:

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

## Клиент не может установить беспроводное соединение с роутером.

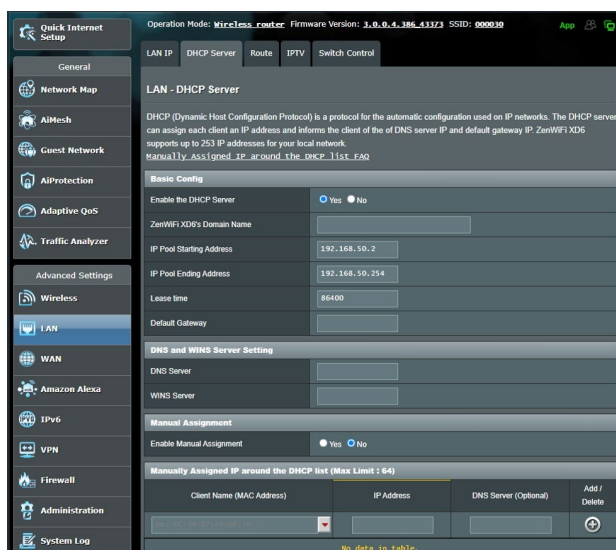
**ПРИМЕЧАНИЕ:** При возникновении проблем с подключением к сети 5 ГГц убедитесь, что ваше беспроводное устройство поддерживает частоту 5 ГГц или является двухдиапазонным.

- **Вне зоны покрытия:**

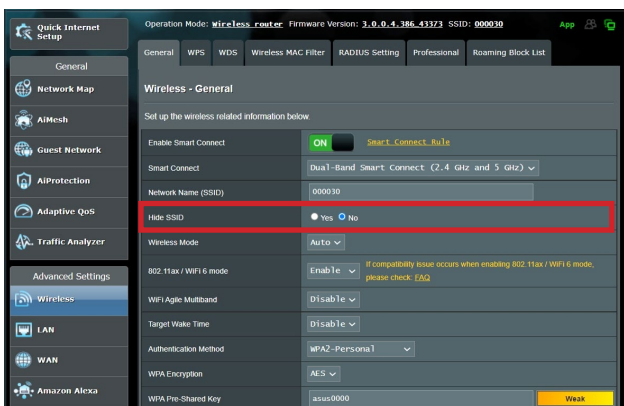
- Поместите роутер ближе к беспроводному клиенту.
- Попробуйте настроить антенны роутера как описано в разделе **1.4 Размещение роутера**.

- **DNCHP-сервер отключен:**

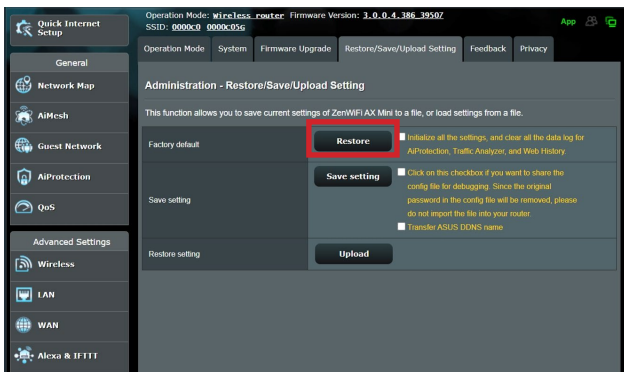
1. Войдите в веб-интерфейс. Перейдите в **Общие > Карта сети > Клиенты** и найдите устройство, которое нужно подключить к роутеру.
2. Если не удалось найти устройство на **карте сети**, перейдите в **Дополнительные настройки > LAN > вкладка DHCP-сервер**, раздел **Основные настройки** и в поле **Включить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



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



- При использовании беспроводного адаптера убедитесь, что используемый беспроводной канал доступен в вашей стране или регионе. Если нет, настройте канал, полосу пропускания и беспроводной режим.
- Если Вы все еще не можете подключиться к роутеру, сбросьте его к заводским настройкам по умолчанию. Войдите в веб-интерфейс, перейдите в **Администрирование > вкладка Восстановить, Сохранить, Загрузить настройки** и нажмите **Восстановить**.



## Интернет недоступен.

- Убедитесь, что роутер может подключиться к Вашему провайдеру. Для этого запустите веб-интерфейс и перейдите в **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** > **AiProtection** > **Родительский контроль** и проверьте, находится ли устройство в списке. Если устройство в списке, удалите его, нажав **Delete** или настройте параметры времени.





- Если все еще нет доступа к интернету, попробуйте перезагрузить компьютер и проверить IP-адрес и адрес шлюза.
- Проверьте индикаторы состояния на ADSL модеме и беспроводном роутере. Если индикатор WAN на роутере не горит, убедитесь, что все кабели правильно подключены.

## Вы забыли SSID (имя сети) или сетевой пароль

- Установите новый SSID и ключ шифрования через проводное соединение (Ethernet-кабель). Войдите в веб-интерфейс, перейдите в **Карта сети**, нажмите иконку роутера и введите новый SSID и ключ шифрования, затем нажмите **Применить**.
- Выполните сброс роутера к настройкам по умолчанию. Войдите в веб-интерфейс, перейдите в **Администрирование** > вкладка **Восстановить, Сохранить, Загрузить настройки** и нажмите **Восстановить**. Логин и пароль по умолчанию "admin".

## Как сбросить систему к настройкам по умолчанию?

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

Параметры системы по умолчанию:

**Включен DHCP:** Да (если WAN кабель подключен)

**IP-адрес:** 192.168.50.1

**Имя домена:** (пусто)

**Маска подсети:** 255.255.255.0

**DNS сервер 1:** router.asus.com

**DNS сервер 2:** (пусто)

**SSID:** ASUS\_XX

## Ошибка обновления прошивки.

Переключите роутер в режим восстановления и запустите утилиту Firmware Restoration. Информацию по использованию утилиты Firmware Restoration смотрите в разделе **5.2 Восстановление прошивки**.

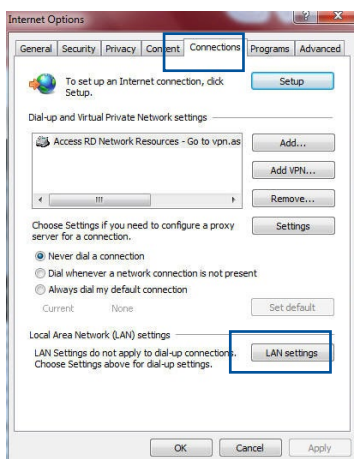
## Невозможно подключиться к веб-интерфейсу

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

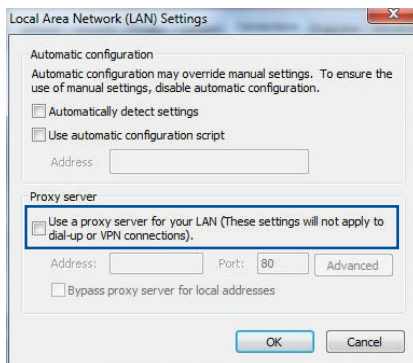
### A. Отключите прокси-сервер, если он включен.

#### Windows

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

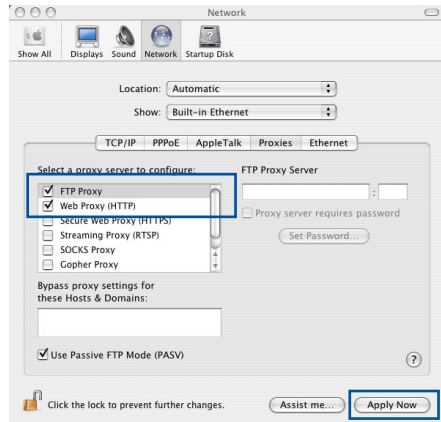


3. На экране **настройки локальной сети** отключите использование прокси-сервера для локальной сети.
4. Нажмите **ОК** когда закончите.



## MAC OS

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

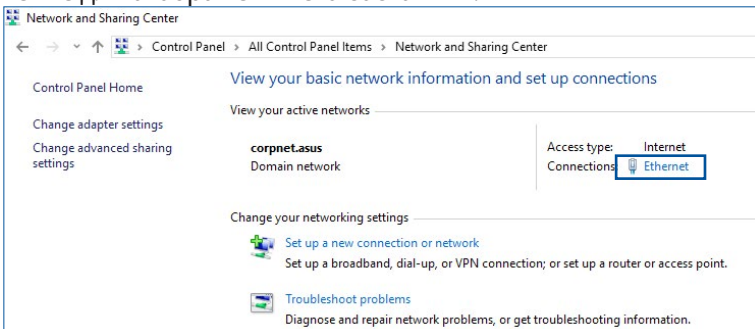


**ПРИМЕЧАНИЕ:** Для получения подробной информации по отключению использования прокси-сервера, обратитесь к справке браузера.

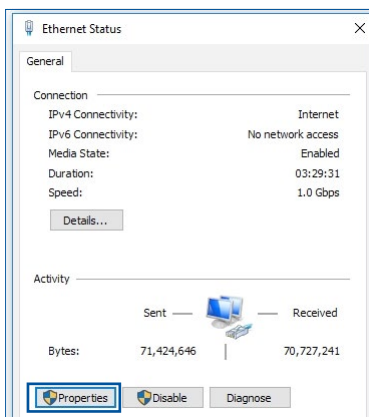
## B. Настройте TCP/IP для автоматического получения IP-адреса.

### Windows

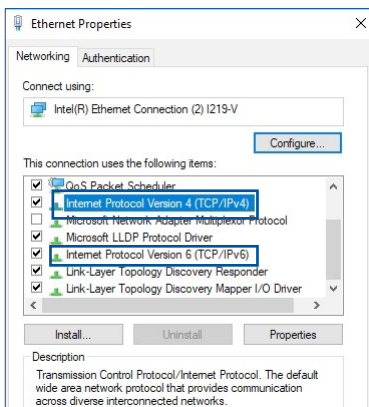
1. Нажмите **Пуск > Панель управления > Центр управления сетями и общим доступом**, затем нажмите сетевое подключение для отображения его состояния.



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



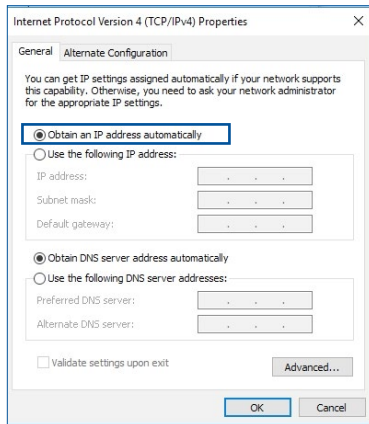
- Выберите **Протокол Интернета версии 4 (TCP/IPv4)** или **Протокол Интернета версии 6 (TCP/IPv6)**, затем нажмите **Свойства**.




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

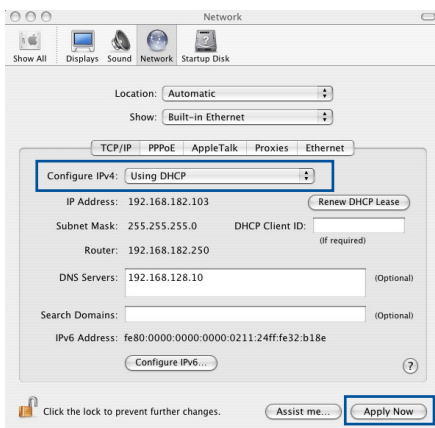
Выберите **Получить IP-адрес автоматически** для автоматического получения IP-адреса.

- Нажмите **ОК** когда закончите.



## MAC OS

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

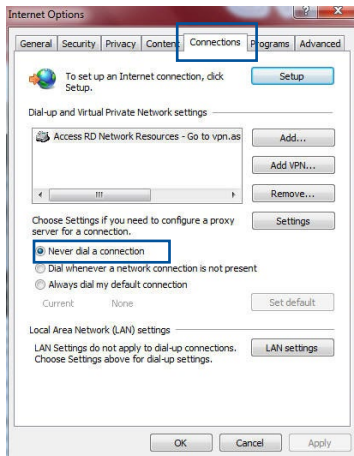


**ПРИМЕЧАНИЕ:** Подробную информацию по конфигурации настроек TCP/IP смотрите в справке к Вашей операционной системе.

## C. Отключите подключение удаленного доступа, если оно включено.

### Windows

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



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

# Приложение

## Уведомления

Данное устройство представляет собой энергопотребляющий продукт (ErP) с высокой доступностью к сети (HiNA). Его потребляемая мощность будет меньше 12 Вт, когда система находится в режиме ожидания сети (режим ожидания),.

## Утилизация и переработка

Компания ASUS берет на себя обязательства по утилизации старого оборудования, исходя из принципов всесторонней защиты окружающей среды. Устройство и его антенна не должны располагаться рядом с другими антеннами и передатчиками. Для получения подробной информации об утилизации и переработке в различных регионах посетите <http://csr.asus.com/english/Takeback.htm>.

## REACH

Согласно регламенту ЕС REACH (Registration, Evaluation, Authorization, and Restriction of Chemicals – Регистрация, Оценка, Разрешения и Ограничения на использование Химических веществ), на сайте ASUS REACH размещен список химических веществ содержащихся в продуктах ASUS: <http://csr.asus.com/english/index.aspx>

## Удостоверение Федеральной комиссии по связи США

Данное устройство соответствует части 15 Правил FCC. Обратитесь к квалифицированному технику или продавцу

- Данное устройство не должно создавать помех.
- На работу устройства могут оказывать влияние внешние помехи, включая те, которые могут вызвать нежелательные режимы его работы.

Данное оборудование было протестировано и сочтено соответствующим ограничениям по цифровым устройствам класса В, в соответствии с частью 15 правил FCC. Эти ограничения рассчитаны на обеспечение защиты в разумных пределах от вредоносных воздействий при установке в жилом помещении.

Данное оборудование генерирует и излучает радиочастотную энергию, которая может создавать помехи в радиосвязи, если устройство установлено или используется не в соответствии с инструкциями производителя. Тем не менее, невозможно гарантировать отсутствие помех в каждом конкретном случае. В случае, если данное оборудование действительно вызывает помехи в радио или телевизионном приеме, что можно проверить, включив и выключив данное оборудование, пользователю рекомендуется попытаться удалить помехи следующими средствами:

- Переориентировать или переместить принимающую антенну.
- Увеличить расстояние между данным прибором и приемником.
- Подключить данное оборудование к розетке другой электроцепи, нежели та, к которой подключен приемник.
- Проконсультироваться с продавцом или квалифицированным радио-/ТВ-техником.

---

**ВАЖНО!** Для уменьшения возможных помех, это устройство, работающее на частоте 5.15 ~ 5.25 ГГц должно использоваться только внутри помещений.

---

**ВНИМАНИЕ:** Изменения или дополнения к данному пункту, не согласованные непосредственно со стороной, ответственной за соответствие правилам, могут сделать недействительным право пользователя на пользование данным оборудованием.

---

### **Размещение**

Устройство и его антенна не должны располагаться рядом с другими антеннами и передатчиками.

## **ВАЖНОЕ ЗАМЕЧАНИЕ:**

**Требования к воздействию радиочастоты** Это оборудование совместимо с ограничениями FCC по радиоизлучению, установленными для неконтролируемого окружения. Конечные пользователи должны следовать инструкциям по эксплуатации для уменьшения воздействия радиочастоты. Для удовлетворения требованиям FCC пожалуйста следуйте инструкциям, описанным в этом руководстве. Это оборудование должно быть установлено и работать на расстоянии не менее 15 см от Вашего тела.



## Меры предосторожности при использовании устройства

- a. Будьте осторожны при использовании данного устройства в аэропортах, больницах, заправочных станциях и гаражах.
- b. Помехи для медицинских устройств: поддерживайте минимальное расстояние (не менее 15 см) между имплантированными медицинскими устройствами и продуктами ASUS для снижения риска возникновения помех.
- c. Используйте продукт ASUS в условиях хорошего приема для уменьшения уровня излучения.
- d. Установите устройство подальше от беременных женщин и нижней части живота подростков.

## Условия эксплуатации:

- Температура эксплуатации устройства: 0-40 °С. Не используйте устройство в условиях экстремально высоких или низких температур.
- Не размещайте устройство вблизи источников тепла, например, рядом с микроволновой печью, духовым шкафом или радиатором.
- Использование несовместимого или несертифицированного адаптера питания может привести к возгоранию, взрыву и прочим опасным последствиям.
- При подключении к сети электропитания устройство следует располагать близко к розетке, к ней должен осуществляться беспрепятственный доступ.
- Утилизация устройства осуществляется в соответствии с местными законами и положениями. Устройство по окончании срока службы должны быть переданы в сертифицированный пункт сбора для вторичной переработки или правильной утилизации.
- Данное устройство не предназначено для детей. Дети могут пользоваться устройством только в присутствии взрослых.
- Не выбрасывайте устройство и его комплектующие вместе с обычными бытовыми отходами.

**EAC**



UA.TR.028

<b>Производитель</b>	<b>ASUSTeK Computer Inc.</b> Телефон: +886-2-2894-3447 Адрес: 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan
<b>Официальный представитель в Европе</b>	<b>ASUS Computer GmbH</b> Адрес: HARKORT STR. 21-23, 40880 RATINGEN, GERMANY

# 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

## EU Declaration of Conformity



We, the undersigned,

**Manufacturer:** ASUSTeK COMPUTER INC.  
**Address:** 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112, Taiwan  
**Authorized representative in Europe:** ASUS COMPUTER GmbH  
**Address, City:** HARKORT STR. 21-23, 40880 RATINGEN  
**Country:** GERMANY

declare the following apparatus:

**Product name:** AX5400 Dual Band WiFi Router  
**Model name:** XD6

**Additional information:** ANNEX I

The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

Radio Equipment Directive – 2014/53/EU

Article 3.1(a)

EN 50385:2017, EN 50665:2017, EN 62311:2008, EN 62368-1:2014/A11:2017

Article 3.1(b)

Draft EN 301 489-1 V2.2.0, Draft EN 301 489-17 V3.2.0, EN 55024:2010/A1:2015, EN 55032:2015/AC:2016, EN 55035:2017, EN 61000-3-2:2014, EN 61000-3-3:2013

Article 3.2

EN 300 328 V2.2.2, EN 301 893 V2.1.1

Radio Equipment Class

Class 2

Ecodesign Directive – 2009/125/EC

(EU) 2019/1782, 1275/2008/EC, EU 801/2013

RoHS Directive – 2011/65/EU

2015/863/EU, EN 50581:2012

Signature:

S.y. Shian, CEO

Place of issue:

Taipei, Taiwan

Date of issue:

12/04/2021

## Сервис и поддержка

Посетите наш сайт <https://www.asus.com/support/>.

