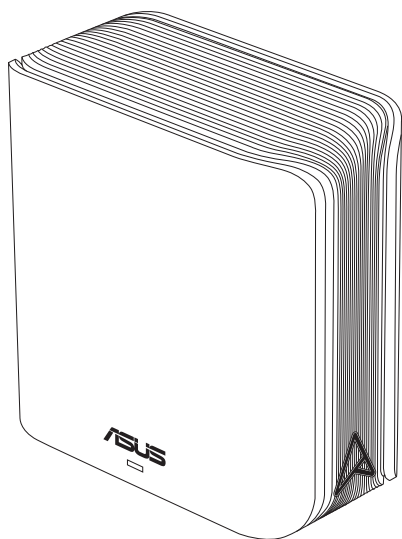


Podręcznik użytkownika

ZenWiFi BD4

Dwupasmowy router BE3600



ASUS
IN SEARCH OF INCREDIBLE

PL23951

Wydanie pierwsze

Sierpień 2024

Copyright © 2024 ASUSTeK COMPUTER INC. Wszelkie prawa zastrzeżone.

Żadnej z części tego podręcznika, włącznie z opisem produktów i oprogramowania, nie można powielać, przenosić, przetwarzać, przechowywać w systemie odzyskiwania danych lub tłumaczyć na inne języki, w jakiegokolwiek formie lub w jakikolwiek sposób, za wyjątkiem wykonywania kopii zapasowej dokumentacji otrzymanej od dostawcy, bez wyraźnego, pisemnego pozwolenia ASUSTeK COMPUTER INC. ("ASUS").

Gwarancja na produkt lub usługa gwarancyjna nie zostanie wydłużona, jeśli: (1) produkt był naprawiany, modyfikowany lub zmieniany, jeśli wykonane naprawy, modyfikacje lub zmiany zostały wykonane bez pisemnej autoryzacji ASUS; lub, gdy (2) została uszkodzona lub usunięta etykieta z numerem seryjnym.

ASUS UDOSTĘPNIŁ TEN PODRĘCZNIK W STANIE "JAKI JEST", BEZ UDZIELANIA JAKIKOLWIEK GWARANCJI, ŻARÓWNO WYRAŹNYCH JAK I DOMNIEMANYCH, WŁĄCZNIE, ALE NIE TYLKO Z DOMNIEMANYMI GWARANCJAMI LUB WARUNKAMI PRZYDATNOŚCI HANDLOWEJ LUB DOPASOWANIA DO OKREŚLONEGO CELU. W ŻADNYM PRZYPADKU FIRMA ASUS, JEJ DYREKTORZY, KIEROWNICY, PRACOWNICY LUB AGENCI NIE BĘDĄ ODPOWIADAĆ ZA JAKIEKOLWIEK NIEBEZPOŚREDNIE, SPECJANE, PRZYPADKOWE LUB KONSEKWENTNE SZKODY (WŁĄCZNIE Z UTRATĄ ZYSKÓW, TRANSAKCJI BIZNESOWYCH, UTRATĄ MOŻLIWOŚCI KORZYSTANIA LUB UTRACENIEM DANYCH, PRZERWAMI W PROWADZENIU DZIAŁANOŚCI ITP.) NAWET, JEŚLI FIRMA ASUS UPREDZIŁA O MOŻLIWOŚCI ZAISTNIENIA TAKICH SZKÓD, W WYNIKU JAKIKOLWIEK DEFEKTÓW LUB BŁĘDÓW W NINIEJSZYM PODRĘCZNIKU LUB PRODUKCIE.

SPECYFIKACJE I INFORMACJE ZNAJDUJĄCE SIĘ W TYM PODRĘCZNIKU, SŁUŻĄ WYŁĄCZNIE CELOM INFORMACYJNYM I MOGĄ ZOSTAĆ ZMIENIONE W DOWOLNYM CZASIE, BEZ POWIADOMIENIA, DLATEGO TEŻ, NIE MOGĄ BYĆ INTERPRETOWANE JAKO WIĄŻĄCE FIRMĘ ASUS DO ODPOWIEDZIALNOŚCI. ASUS NIE ODPOWIADA ZA JAKIEKOLWIEK BŁĘDY I NIEDOKŁADNOŚCI, KTÓRE MOGĄ WYSTĄPIĆ W TYM PODRĘCZNIKU, WŁĄCZNIE Z OPISANYMI W NIM PRODUKTAMI I OPROGRAMOWANIEM.

Produkty i nazwy firm pojawiające się w tym podręczniku mogą, ale nie muszą być zastrzeżonymi znakami towarowymi lub prawami autorskimi ich odpowiednich właścicieli i używane są wyłącznie w celu identyfikacji lub wyjaśnienia z korzyścią dla ich właścicieli i bez naruszania ich praw.

Spis treści

1	Poznanie routera bezprzewodowego	
1.1	Witamy!.....	6
1.2	Zawartość opakowania.....	6
1.3	Router bezprzewodow.....	7
1.4	Ustawianie położenia routera bezprzewodowego.....	8
1.5	Wymagania dotyczące instalacji	9
2	Ustawienia sprzętu	
2.1	Instalacja routera.....	10
	A. Połączenie przewodowe.....	11
	B. Połączenie bezprzewodowe	12
2.2	QIS z autodetekcją Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)	14
2.3	Łączenie z siecią bezprzewodową	16
3	Konfiguracja ustawień ogólnych i zaawansowanych	
3.1	Logowanie do GUI web.....	17
	3.1.1 Wykonanie ustawień zabezpieczenia sieci bezprzewodowej.....	19
	3.1.2 Zarządzanie klientami sieci	20
3.2	Adaptacyjna funkcja QoS.....	21
	3.2.1 Zarządzanie pasmem QoS (Quality of Service)	21
3.3	Administration (Administracja).....	24
	3.3.1 Operation Mode (Tryb działania)	24
	3.3.2 System.....	25
	3.3.3 Aktualizacja firmware	26
	3.3.4 Przywracanie/zapisywanie/przesyłanie ustawień.....	26
3.4	AiProtection	27
	3.4.1 Network Protection	27

Spis treści

3.4.2	Konfiguracja funkcji Parental Controls (Kontrola rodzicielska)	31
3.5	Zapora	34
3.5.1	Ogólne	34
3.5.2	Filtr adresów URL	35
3.5.3	Filtr słów kluczowych.....	36
3.5.4	Network Services Filter (Filtr usług sieciowych).....	37
3.6	IPv6 (Protokół IPv6)	38
3.7	LAN (Sieć LAN).....	39
3.7.1	LAN IP (Adres IP sieci LAN)	39
3.7.2	DHCP Server (Serwer DHCP)	40
3.7.3	Route (Trasa).....	42
3.7.4	IPTV	43
3.8	Sieć	44
3.8.1	Sieć główna - Filtr adresów MAC	44
3.8.2	Guest Network (Sieć gości).....	46
3.8.2.1	Guest Network (Sieć gości)	46
3.8.2.2	Smart Home Master.....	48
3.9	System Log (Dziennik systemu)	52
3.10	Analizator ruchu	53
3.11	WAN (Sieć WAN).....	54
3.11.1	Internet Connection (Połączenie internetowe).....	54
3.11.2	Dwie sieci WAN	57
3.11.3	Port Trigger (Wyzwalanie portów).....	58
3.11.4	Virtual Server/Port Forwarding (Serwer wirtualny/ Przekierowanie portów)	60
3.11.5	DMZ (Strefa DMZ)	63
3.11.6	DDNS (Usługa DDNS).....	64
3.11.7	NAT Passthrough (Przekazywanie NAT)	65

Spis treści

3.12	Wireless (Sieć bezprzewodowa).....	66
3.12.1	WPS	66
3.12.2	Bridge (Mostek).....	68
3.12.3	RADIUS Setting (Ustawienia serwera RADIUS).....	70
3.12.4	Professional (Profesjonalne).....	71

4 Narzędziowych

4.1	Device Discovery	74
4.2	Firmware Restoration	74

5 Rozwiązywanie problemów

5.1	Rozwiązywanie podstawowych problemów	76
5.2	Często zadawane pytania (FAQs)	79

Załączniki

	Uwagi dotyczące bezpieczeństwa	97
	Obsługę i Pomoc	99

1 Poznanie routera bezprzewodowego

1.1 Witamy!

Dziękujemy za zakup routera bezprzewodowego ZenWiFi BD4 firmy ASUS!

ZenWiFi BD4, w minimalistycznej białej obudowie z metalicznymi akcentami w kolorze monogramu A, obsługuje dwupasmowy 2,4 GHz i 5 GHz, oferując bezkonkurencyjną, równoległą, bezprzewodową transmisję strumieniową w jakości HD; serwer SMB; serwer UPnP AV i serwer FTP do wymiany plików 24 godz/7 dni w tygodniu; możliwość obsługi 300.000 sesji. Technologia ASUS Green Network Technology zapewnia do 70% oszczędności energii.

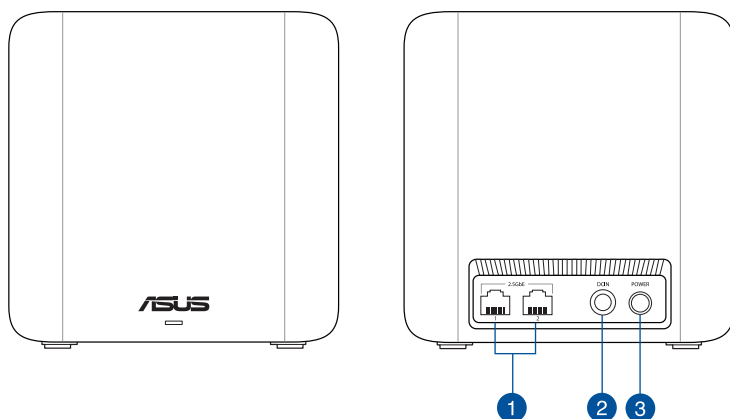
1.2 Zawartość opakowania

- | | |
|--|---|
| <input checked="" type="checkbox"/> Router bezprzewodowy ZenWiFi BD4 | <input checked="" type="checkbox"/> Kabel RJ45 |
| <input checked="" type="checkbox"/> Adapter zasilania | <input checked="" type="checkbox"/> Instrukcja szybkiego uruchomienia |
| <input checked="" type="checkbox"/> Karta gwarancyjna | |

UWAGI:

- Jeżeli którykolwiek z elementów jest uszkodzony lub brakuje go, skontaktować się z firmą ASUS celem uzyskania pomocy technicznej. Patrz **Obsługa i Pomoc** na tylnej stronie okładki niniejszej instrukcji obsługi.
 - Zachować oryginalne opakowanie na wypadek skorzystania w przyszłości z usług gwarancyjnych takich jak naprawa lub wymiana.
-

1.3 Router bezprzewodowy



- 1 Gniazda 2.5GbE (Automatyczne wykrywanie sieci WAN/LAN)**
Służą do podłączania kabli sieciowych celem ustanowienia 2.5GbE WAN/LAN sieciowego.
- 2 Gniazdo zasilania (DCIN)**
Służy do podłączenia wtyczki zasilacza prądu przemiennego wchodzącego w skład zestawu i podłączenia routera do zasilacza.
- 3 Przycisk zasilania**
Naciśnij ten przycisk w celu włączenia lub wyłączenia zasilania systemu.

UWAGI:

- Stosować tylko zasilacz dołączony do zestawu. Zastosowanie innych zasilaczy może spowodować uszkodzenie urządzenia.
- **Dane techniczne:**

Zasilacz sieciowy prądu stałego	Wyjście prądu stałego: +12V przy prądzie maks. 1,5 A		
Temperatura pracy	0~40°C	Przechowywanie	0~70°C
Wilgotność działania	50~90%	Przechowywanie	20~90%

1.4 Ustawianie położenia routera bezprzewodowego

Dla zapewnienia najlepszej transmisji sygnału bezprzewodowego pomiędzy routerem bezprzewodowym a podłączonymi urządzeniami sieciowymi należy upewnić się, że:

- Router bezprzewodowy należy umieścić centralnie, aby zapewnić maksymalny zasięg transmisji bezprzewodowej do urządzeń sieciowych w pomieszczeniu bądź w budynku.
- Urządzenie trzymać z dala od metalowych przeszkód oraz bezpośredniego działania promieniowania słonecznego.
- W celu zapobieżenia zakłóceniom lub utratom sygnału trzymać urządzenie z dala od urządzeń Wi-Fi obsługujących wyłącznie pasma 802.11g lub 20 MHz, komputerowych urządzeń peryferyjnych 2,4 GHz, urządzeń Bluetooth, telefonów bezprzewodowych, transformatorów, silników do wysokich obciążeń, świetlówek, kuchenek mikrofalowych, lodówek oraz innego wyposażenia przemysłowego.
- Zawsze zaktualizować oprogramowanie do najnowszej wersji oprogramowania sprzętowego. Najnowsze informacje dotyczące aktualizacji oprogramowania można uzyskać na stronie internetowej ASUS pod adresem <http://www.asus.com>.

1.5 Wymagania dotyczące instalacji

Do wykonania ustawień sieci potrzeba jednego lub dwóch komputerów, które spełniają następujące wymagania systemowe:

- Port Ethernet RJ-45 (LAN) (10Base-T/100Base-TX/1000BaseTX)
- Obsługa sieci bezprzewodowej IEEE 802.11a/b/g/n/ac/ax
- Zainstalowana usługa TCP/IP
- Przeglądarka sieci web, taka jak Internet Explorer, Firefox, Safari lub Google Chrome

UWAGI:

- Jeśli komputer nie posiada wbudowanej obsługi sieci bezprzewodowej, w celu połączenia z siecią WLAN, można zainstalować w komputerze adapter WLAN IEEE 802.11a/b/g/n/ac/ax.
- Technologia dwupasmowy pasma, router dwupasmowy obsługuje równoległe bezprzewodowe sygnały 2,4 GHz i 5 GHz. Umożliwia to wykonywanie działań powiązanych z Internetem, takich jak surfowanie po Internecie lub czytanie/pisanie wiadomości e-mail z wykorzystaniem pasma 2,4GHz, przy równoległym przesyłaniu strumieni wysokiej jakości plików audio/wideo, takich jak filmy lub muzyka, z wykorzystaniem pasma 5GHz.
- Niektóre urządzenia IEEE 802.11n, które można połączyć z siecią, mogą nie obsługiwać częstotliwości 5 GHz. Należy sprawdzić specyfikacje w podręczniku danego urządzenia.
- Kable Ethernet RJ-45 wykorzystywane do połączenia z urządzeniami sieciowymi nie powinny być dłuższe niż 100 metrów.

WAŻNE!

- W niektórych kartach sieci bezprzewodowej może wystąpić problem z połączeniem się z punktami dostępu WiFi 802.11ax.
- W razie wystąpienia takiego problemu sprawdź, należy zaktualizować sterownik do najnowszej wersji. Przejdź do oficjalnej witryny pomocy technicznej producenta, gdzie można uzyskać sterowniki oprogramowania, aktualizacje i inne powiązane informacje.
 - Realtek: <https://www.realtek.com/en/downloads>
 - Mediatek: <https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi>
 - Intel: <https://downloadcenter.intel.com/>

2 Ustawienia sprzętu

2.1 Instalacja routera

WAŻNE!

- Router bezprzewodowy należy zainstalować za pomocą połączenia przewodowego, aby uniknąć możliwych problemów z instalacją.
 - Przed skonfigurowaniem routera bezprzewodowego ASUS wykonać następujące czynności:
 - W przypadku zastępowania istniejącego routera odłączyć router od sieci.
 - Odłączyć kable/przewody od istniejącego modemu. Jeżeli modem ma baterię zasilania awaryjnego należy ją również wyciągnąć.
 - Ponownie uruchomić komputer (zalecane).
-



OSTRZEŻENIE!

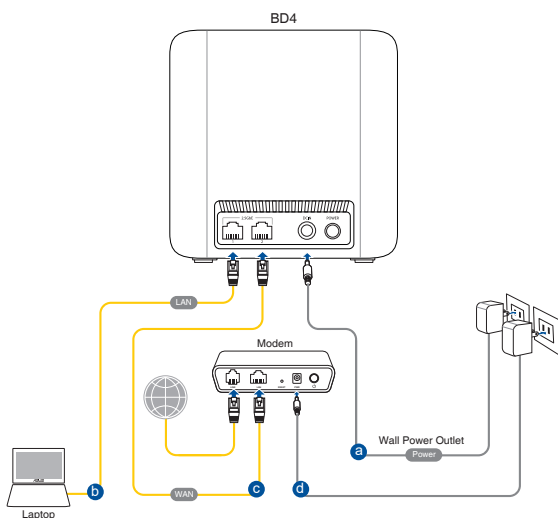
- Przewody zasilające należy podłączać do gniazd elektrycznych o odpowiednim uziemieniu. Urządzenie należy podłączyć wyłącznie do znajdującego się w pobliżu gniazda elektrycznego, które jest łatwo dostępne.
 - Jeśli uszkodzony został zasilacz nie należy próbować naprawiać go samemu. Należy skontaktować się z wykwalifikowanym technikiem serwisu lub ze sprzedawcą.
 - NIE NALEŻY przykrywać szczelin wentylacyjnych komputera desktop PC, aby zapobiec przegrzaniu systemu.
 - NIE NALEŻY montować tego urządzenia na wysokości większej niż 2 metry.
 - Ten produkt należy używać w miejscach o temperaturze otoczenia w zakresie 0°C (32°F) do 40°C (104°F).
-

A. Połączenie przewodowe

UWAGA: Do podłączenia przewodowego można użyć kabla prostego lub skrosowanego.

W celu wykonania ustawienia routera bezprzewodowego poprzez połączenie przewodowe:

1. Podłącz router do gniazda elektrycznego i włącz go. Podłącz kabel sieciowy do komputera i portu 2.5GbE routera.

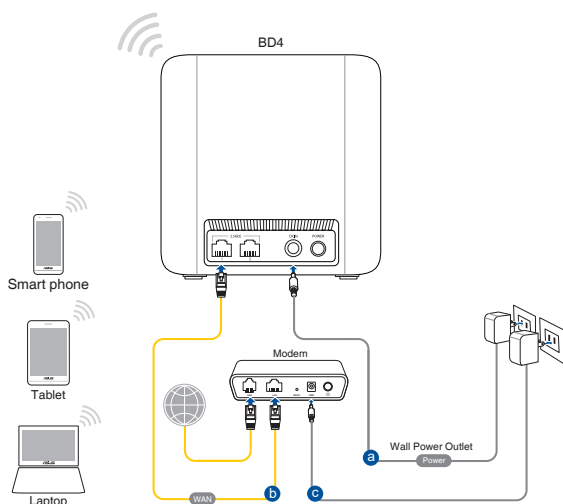


2. Po uruchomieniu przeglądarki, automatycznie otwiera się sieciowy, graficzny interfejs użytkownika. Jeżeli nie uruchomi się automatycznie, wpisz adres <http://www.asusrouter.com>.
3. Ustaw hasło dla routera w celu zabezpieczenia go przed nieautoryzowanym dostępem.

B. Połączenie bezprzewodowe

W celu wykonania ustawienia routera bezprzewodowego poprzez połączenie:

1. Podłącz router do gniazda elektrycznego i włącz go.



2. Nawiąż połączenie z siecią o nazwie (identyfikator SSID) wskazanej na etykiecie produktu z tyłu routera. Aby lepiej zabezpieczyć sieć, zmień identyfikator SSID na unikatowy i przypisz hasło.

Nazwa Wi-Fi (SSID):	ASUS_XX
---------------------	---------

- * **XX** to dwie ostatnie cyfry adresu MAC 2,4 GHz. Można go znaleźć na etykiecie z tyłu routera ZenWiFi BD4.

3. Po połączeniu, przy uruchamianiu przeglądarki, automatycznie otwiera się sieciowy, graficzny interfejs użytkownika. Jeżeli nie uruchomi się automatycznie, wpisz adres <http://www.asusrouter.com>.
4. Ustaw hasło dla routera w celu zabezpieczenia go przed nieautoryzowanym dostępem.

UWAGI:

- Szczegółowe informacje dotyczące połączenia z siecią bezprzewodową znajdują się w podręczniku użytkownika adaptera WLAN.
 - Informacje na temat konfiguracji ustawień zabezpieczeń sieci można znaleźć w części **Wykonanie ustawień zabezpieczenia sieci bezprzewodowej** w rozdziale **3.1.1** niniejszego podręcznika użytkownika.
-

2.2 QIS z autodetekcją Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)

Funkcja QIS (Quick Internet Setup (Szybkie ustawienia połączenia z Internetem)) pomaga w szybkim wykonaniu połączenia z Internetem.

UWAGA: Podczas ustawiania połączenia z Internetem pierwszy raz, naciśnij i przytrzymaj przycisk Reset na routerze bezprzewodowym w celu przywrócenia jego ustawień fabrycznych.

Aby użyć QIS z autodetekcją:

1. Uruchom przeglądarkę internetową. Nastąpi przekierowanie do kreatora konfiguracji ASUS (szybka konfiguracja połączenia z Internetem). Jeśli nie, wprowadź ręcznie adres <http://www.asusrouter.com>.
2. Router bezprzewodowy automatycznie wykryje, czy typ połączenia ISP to **Dynamic IP (Dynamiczny adres IP)**, **PPPoE**, **PPTP** oraz **L2TP**. Wprowadź niezbędne informacje dla typu połączenia ISP.

WAŻNE! Uzyskaj niezbędne informacje dotyczące połączenia z Internetem od ISP.

UWAGI:



- Automatyczne wykrywanie typu połączenia ISP jest wykonywane przy pierwszej konfiguracji routera bezprzewodowego lub po zresetowaniu routera bezprzewodowego do ustawień domyślnych.
 - Jeżeli funkcja QIS nie może wykryć typu połączenia z Internetem, kliknij polecenie **Manual Setting (Ustawień Ręcznych)** (patrz zrzut ekranu w etapie 1) i ręcznie skonfiguruj ustawienia połączenia.
-
3. Przydziel nazwę sieci (SSID) i klucz zabezpieczenia dla połączenia bezprzewodowego Sieć WiFi 7. Po zakończeniu kliknij **Apply (Zastosuj)**.
 4. Na stronie **Login Information Setup (Ustawienia informacji logowania)** zmień hasło logowania do routera, aby zapobiec nieautoryzowanemu dostępowi do routera bezprzewodowego.

UWAGA: Nazwa logowania i hasło routera bezprzewodowego są inne niż nazwa (identyfikator SSID) sieci WiFi 7 i klucz zabezpieczeń. Za pomocą nazwy logowania i hasła routera bezprzewodowego można logować się do sieciowego interfejsu graficznego routera bezprzewodowego w celu konfiguracji jego ustawień. Za pomocą nazwy (identyfikatora SSID) sieci WiFi 7 i klucza zabezpieczeń urządzenia Wi-Fi logują się i łączą z siecią WiFi 7.

2.3 Łączenie z siecią bezprzewodową

Po skonfigurowaniu routera bezprzewodowego za pomocą funkcji QIS można połączyć komputer lub inne urządzenia inteligentne z siecią bezprzewodową.

W celu połączenia z siecią:

1. Kliknij ikonę sieci  w obszarze powiadomień komputera, aby wyświetlić dostępne sieci bezprzewodowe.
2. Wybierz sieć bezprzewodową do połączenia, a następnie kliknij przycisk **Connect (Połącz)**.
3. Może być konieczne wprowadzenie klucza zabezpieczeń sieciowych w celu uzyskania dostępu do zabezpieczonej sieci bezprzewodowej; następnie kliknij przycisk **OK**.
4. Poczekaj na pomyślne ustanowienie połączenia między komputerem a siecią bezprzewodową. Stan połączenia jest wyświetlany za pomocą ikony sieci .

UWAGI:

- Szczegółowe informacje na temat konfiguracji ustawień sieci bezprzewodowej można znaleźć w następujących rozdziałach.
 - Szczegółowe informacje na temat łączenia danego urządzenia z siecią bezprzewodową można znaleźć w dołączonym do niego podręczniku użytkownika.
-

3 Konfiguracja ustawień ogólnych i zaawansowanych

3.1 Logowanie do GUI web

Dla routera bezprzewodowego ASUS dostępny jest intuicyjny sieciowy, graficzny interfejs użytkownika (GUI), który umożliwia łatwą konfigurację jego różnych funkcji w przeglądarce internetowej, takiej jak Internet Explorer, Firefox, Safari lub Google Chrome.

UWAGA: Funkcje mogą się różnić w zależności od wersji oprogramowania sprzętowego.

Aby zalogować się do GUI web:

1. W przeglądarce sieci web, takiej jak Internet Explorer, Firefox, Safari lub Google Chrome, ręcznie wprowadź domyślny adres IP routera bezprzewodowego: <http://www.asusrouter.com>.
2. Na stronie logowania, wprowadź nazwę użytkownika i hasło ustawione w części **2.2 QIS (Quick Internet Setup [Szybkie ustawienia połączenia z Internetem])** z autodetekcją.
3. Można rozpocząć konfigurację różnych ustawień routera bezprzewodowego firmy ASUS za pomocą sieciowego interfejsu graficznego.

QIS (Szybka konfiguracja połączenia z Internetem) - Inteligentne podłączenie

Panel nawigacji

Górne przyciski poleceń

Pasek informacyjny



* Rysunek ma wyłącznie charakter informacyjny.

UWAGA: Po zalogowaniu się do sieciowego interfejsu graficznego po raz pierwszy nastąpi automatyczne przekierowanie na stronę Quick Internet Setup (QIS) (Szybka konfiguracja połączenia z Internetem).

3.1.1 Wykonanie ustawień zabezpieczenia sieci bezprzewodowej

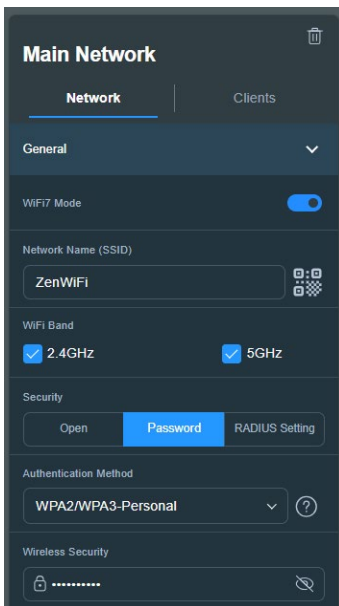
Aby zabezpieczyć sieć bezprzewodową przed nieautoryzowanym dostępem należy skonfigurować ustawienia zabezpieczenia.

W celu wykonania ustawień zabezpieczenia sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > Network Map (Mapa sieci)**.
2. Wybierz sieć i aby wyświetlić ustawienia zabezpieczenia sieci bezprzewodowej takie jak SSID, poziom zabezpieczenia i ustawienia szyfrowania.

UWAGA: Można ustawić różne zabezpieczenia sieci bezprzewodowej dla pasm 2,4GHz i 5GHz.

Ustawienia zabezpieczenia 2,4GHz/5GHz



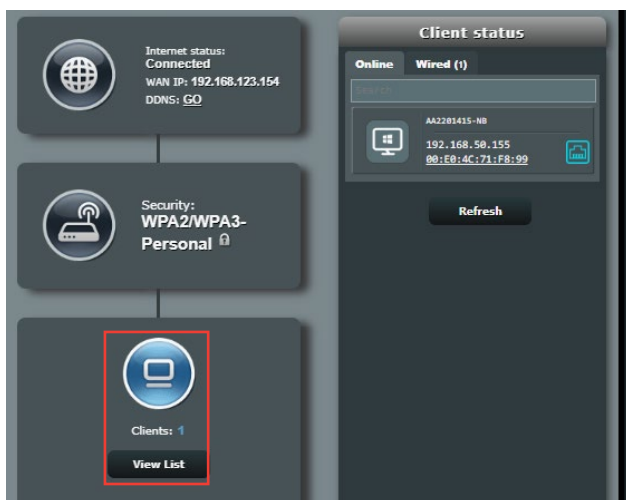
3. W polu **Network Name (SSID) [Nazwa sieci (SSID)]**, wprowadź unikalną nazwę dla własnej sieci bezprzewodowej.

4. Na rozwijanej liście **WEP Encryption (Szyfrowanie WEP)**, wybierz metodę szyfrowania dla sieci bezprzewodowej.

WAŻNE! Standard IEEE 802.11n/ac/ax zakazuje używania wysokiej przepustowości z WEP lub WPA-TKP, jako pojedynczego szyfru. Jeśli używane są te metody szyfrowania, szybkość danych spadnie do szybkości połączenia 54Mbps IEEE 802.11g.

5. Wprowadź klucz hasła zabezpieczenia.
6. Po wykonaniu kliknij **Apply (Zastosuj)**.

3.1.2 Zarządzanie klientami sieci



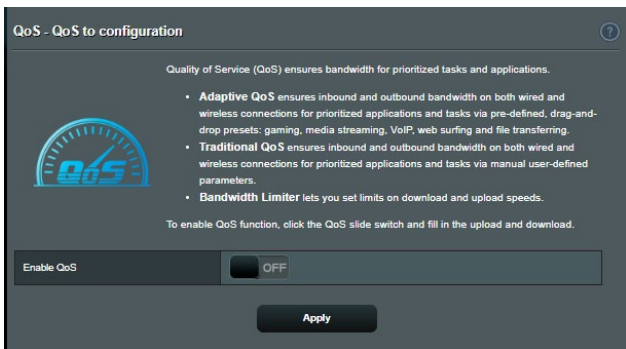
W celu zarządzania klientami sieci:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > wybierz zakładkę **Network Map (Mapa sieci)**.
2. Na ekranie **Network Map (Mapa sieci)**, wybierz ikonę **Client Status (Stan klienta)**, aby wyświetlić informacje o klientach sieciowych.
3. Aby zablokować dostęp klienta do sieci, wybierz klienta i kliknij pozycję **block (zablokuj)**.

3.2 Adaptacyjna funkcja QoS

3.2.1 Zarządzanie pasmem QoS (Quality of Service)

QoS (Quality of Service) umożliwia ustawienie priorytetu pasma i zarządzanie ruchem sieciowym.



Aby ustawić priorytet szerokości pasma:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > Adaptive QoS (Adaptacyjna funkcja QoS) > QoS (Jakość usługi)**.
2. Kliknij **ON (Włącz)**, aby włączyć domyślną zasadę i wypełnij pola pasma dla przesyłanie i pobieranie.

UWAGA: Uzyskaj informacje dotyczące pasma od ISP.

3. Kliknij przycisk **Apply (Zastosuj)**.

UWAGA: Lista User Specify Rule List (Lista reguł określonych przez użytkownika) należy do ustawień zaawansowanych. Aby nadać priorytet określonym aplikacjom sieciowym lub usługom sieciowym, należy wybrać pozycję **User-defined QoS rules (Definiowane przez użytkownika reguły QoS)** lub **User-defined Priority (Priorytet definiowany przez użytkownika)** z listy rozwijanej w prawym górnym rogu ekranu.

4. Na stronie **User-defined QoS rules (Definiowane przez użytkownika reguły QoS)** dostępne są cztery domyślne typy usług online — korzystanie z sieci Web, HTTPS i transferowanie plików. Wybierz preferowaną usługę, wypełnij pola **Source IP or MAC (Adres IP lub MAC źródła)**, **Destination Port (Port docelowy)**, **Protocol (Protokół)**, **Transferred (Przetransferowano)** i **Priority (Priorytet)**, a następnie kliknij przycisk **Apply (Zastosuj)**. Informacje zostaną skonfigurowane na ekranie reguł QoS.

UWAGI

- W celu wprowadzenia adresu IP lub MAC źródła można:
 - a) Wprowadzić określony adres IP, np. „192.168.122.1”.
 - b) Wprowadzić adresy IP z jednej podsieci lub z tej samej puli adresów IP, np. „192.168.123.*” lub „192.168.*.*”.
 - c) Wprowadzić wszystkie adresy IP jako „*.*.*.*” lub pozostawić puste pole.
 - d) Format adresu MAC to sześć grup po dwie cyfry szesnastkowe, oddzielone dwukropkami (:), w kolejności transmisji (np. 12:34:56:aa:bc:ef).
- W przypadku zakresu portu źródłowego lub docelowego można:
 - a) Wprowadzić określony port, np. „95”.
 - b) Wprowadzić porty z zakresu, np. „103:315”, „>100” lub „<65535”.
- W kolumnie **Transferred (Przetransferowano)** znajdują się informacje dotyczące ruchu przesyłania i pobierania (wychodzącego i przychodzącego ruchu sieciowego) dla jednej sekcji. W kolumnie tej można ustawić limit ruchu sieciowego (w KB) dla danej usługi w celu ustalenia priorytetów dla usługi przypisanej do określonego portu. Jeśli na przykład dwaj klienci sieciowi, PC 1 i PC 2, uzyskują dostęp do Internetu (ustawiony na porcie 80), ale klient PC 1 przekracza limit ruchu sieciowego z powodu zadań pobierania, klient PC 1 będzie miał niższy priorytet. Aby nie ustawiać limitu ruchu, należy pozostawić puste pole.

5. Na stronie **User-defined Priority (Priorytet definiowany przez użytkownika)**, dla aplikacji lub urządzeń sieciowych można określić jeden z pięciu poziomów priorytetu za pomocą listy rozwijanej **User-defined QoS rules (Definiowane przez użytkownika reguły QoS)**. W zależności od poziomu priorytetu, pakiety danych można wysyłać za pomocą następujących metod:
- Zmień kolejność przesyłanych pakietów sieciowych, które są wysyłane do Internetu.
 - W tabeli **Upload Bandwidth (Przepustowość przesyłania)** ustaw pozycję **Minimum Reserved Bandwidth (Minimalna zarezerwowana przepustowość)** i **Maximum Bandwidth Limit (Ograniczenie maksymalnej przepustowości)** dla wielu aplikacji sieciowych o różnych poziomach priorytetu. Wartości procentowe wskazują współczynniki przepustowości przesyłania dostępne dla określonych aplikacji sieciowych.

UWAGI:

- Pakiety o niskim priorytecie są odrzucane w celu zapewnienia transmisji pakietów o priorytecie wysokim.
- W tabeli **Download Bandwidth (Przepustowość pobierania)** ustaw pozycję **Maximum Bandwidth Limit (Ograniczenie maksymalnej przepustowości)** dla wielu aplikacji sieciowych w odpowiedniej kolejności. Im wyższy jest priorytet pakietów przesyłanych, tym wyższy będzie priorytet pakietów pobieranych.
- W przypadku braku przesyłania pakietów przez aplikacje o wysokim priorytecie cała szybkość transmisji połączenia internetowego będzie dostępna dla pakietów o niskim priorytecie.

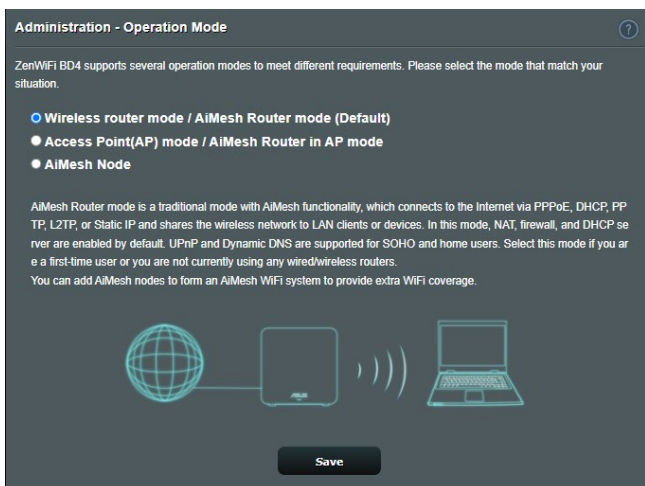
-
6. Ustaw pakiet o najwyższym priorytecie. W celu zapewnienia płynności grania w gry online jako pakiet o najwyższym priorytecie można ustawić ACK, SYN i ICMP.

UWAGA: Należy najpierw włączyć pozycję QoS (Jakość usługi) i skonfigurować limity szybkości przesyłania i pobierania.

3.3 Administration (Administracja)

3.3.1 Operation Mode (Tryb działania)

Na stronie Operation Mode (Tryb działania) można wybrać odpowiedni tryb sieci.



W celu skonfigurowania trybu działania:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > wybierz Operation Mode (Tryb działania)**.
2. Wybierz jeden z podanych trybów działania:
 - **Tryb routera bezprzewodowego (domyślny):** W trybie routera bezprzewodowego router bezprzewodowy łączy się z Internetem i zapewnia dostęp do Internetu urządzeniom dostępnym w jego własnej sieci lokalnej.
 - **Tryb punktu dostępowego:** W tym trybie router tworzy nową sieć bezprzewodową w sieci już istniejącej.
 - **AiMesh Node (Węzeł AiMesh):** Router ZenWiFi BD4 można skonfigurować jako węzeł AiMesh w celu zwiększenia zasięgu sieci Wi-Fi istniejących routerów AiMesh.
3. Kliknij przycisk **Save (Zapisz)**.

UWAGA: Po zmianie trybu nastąpi ponowne uruchomienie routera.

3.3.2 System

Na stronie **System** można skonfigurować ustawienia routera bezprzewodowego.

W celu skonfigurowania ustawień System:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > wybierz System.**
2. Można skonfigurować następujące ustawienia:
 - **Zmień hasło logowania routera:** Hasło i nazwę logowania routera bezprzewodowego można zmienić, wprowadzając nową nazwę i hasło.
 - **Zachowanie przycisku WPS:** Za pomocą fizycznego przycisku WPS na routerze bezprzewodowym można uaktywnić funkcję WPS.
 - **Strefa czasowa:** Wybierz strefę czasową sieci.
 - **Serwer NTP:** Router bezprzewodowy może uzyskiwać dostęp do serwera NTP (Network time Protocol) w celu synchronizacji godziny.
 - **Włącz usługi Telnet:** Kliknij pozycję **Yes (Tak)**, aby włączyć usługi Telnet w sieci. Kliknij pozycję **No (Nie)**, aby wyłączyć usługi Telnet.
 - **Metoda uwierzytelniania:** Jako zabezpieczenie dostępu do routera można wybrać protokół HTTP, HTTPS lub oba.
 - **Włącz dostęp do sieci Web z sieci WAN:** Wybierz pozycję **Yes (Tak)**, aby urządzenia spoza sieci mogły uzyskiwać dostęp do ustawień interfejsu graficznego routera bezprzewodowego. Wybierz opcję **No (Nie)**, aby uniemożliwić dostęp.
 - **Zezwalaj tylko na określone adresy IP:** Kliknij pozycję **Yes (Tak)**, jeśli chcesz określić adresy IP urządzeń, które mogą uzyskiwać dostęp do ustawień interfejsu graficznego routera bezprzewodowego z sieci WAN.
3. Kliknij przycisk **Apply (Zastosuj).**

3.3.3 Aktualizacja firmware

Uwaga: Pobierz najnowszy firmware ze strony sieci web ASUS, pod adresem <http://www.asus.com>.

Aktualizacja firmware:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**.
 2. W polu **Firmware Version (Wersja oprogramowania sprzętowego)** kliknij pozycję **Check (Sprawdź)**, aby zlokalizować pobrany plik.
 3. Kliknij **Upload (Prześlij)**.
-

UWAGI:

- Po ukończeniu procesu uaktualniania należy poczekać, aż system uruchomi się ponownie.
 - Jeśli aktualizacja nie powiedzie się, router bezprzewodowy automatycznie przejdzie do trybu awaryjnego, lub zacnie wolno migać wskaźnik LED zasilania na panelu przednim. Aby przywrócić system, zapoznaj się z sekcją **4.2 Odtwarzanie oprogramowania sprzętowego**.
-

3.3.4 Przywracanie/zapisywanie/przesyłanie ustawień

Aby przywrócić/zapisać/przesłać ustawienia:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Ładuj ustawienia)**.
 2. Wybierz zadanie:
 - Aby przywrócić domyślne ustawienia fabryczne, kliknij **Restore (Przywróć)** i kliknij **OK** w komunikacie potwierdzenia.
 - W celu zapisania aktualnych ustawień systemu kliknij przycisk **Save setting (Zapisz ustawienie)**, przejdź do folderu, w którym chcesz zapisać plik i kliknij pozycję **Save (Zapisz)**.
 - Aby przywrócić poprzednie ustawienia systemu, kliknij **Upload (Prześlij)**, zlokalizuj plik systemowy do przywrócenia, a następnie kliknij **Open (Otwórz)**.
-

WAŻNE! W razie wystąpienia problemu należy załadować najnowszą wersję oprogramowania sprzętowego i skonfigurować nowe ustawienia. Nie należy przywracać ustawień domyślnych routera.

3.4 AiProtection

Funkcja AiProtection zapewnia monitorowanie w czasie rzeczywistym, które umożliwia wykrywanie złośliwego oprogramowania, programów szpiegujących oraz niechcianego dostępu. Filtruje ona także niechciane witryny i aplikacje, a także umożliwia ustalenie harmonogramu dostępu do Internetu przez połączone urządzenie.

3.4.1 Network Protection

Funkcja Network Protection (Ochrona sieci) zapobiega wykorzystywaniu luk w sieci oraz zabezpiecza przed niechcianym dostępem do sieci.

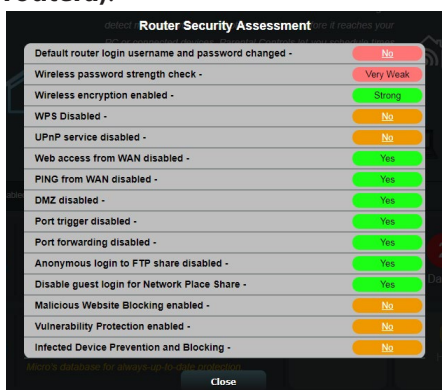


Konfiguracja funkcji Network Protection (Ochrona sieci)

Aby skonfigurować funkcję Network Protection (Ochrona sieci):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij kartę **Network Protection (Ochrona sieci)**.
3. Na karcie **Network Protection (Ochrona sieci)** kliknij przycisk **Scan (Skanuj)**.

Wyniki ukończonego skanowania zostaną wyświetlone na stronie **Router Security Assessment (Ocena zabezpieczeń routera)**.



WAŻNE! Stan pozycji z oznaczeniem **Yes (Tak)** na stronie **Router Security Assessment (Ocena zabezpieczeń routera)** uważa się za **bezpieczny**. W przypadku pozycji z oznaczeniem **No (Nie)**, **Weak (Słabe)** lub **Very Weak (Bardzo słabe)** zalecana jest odpowiednia konfiguracja.

4. (Opcjonalnie) Na stronie **Router Security Assessment (Ocena zabezpieczeń routera)** skonfiguruj ręcznie pozycje z oznaczeniem **No (Nie)**, **Weak (Słabe)** lub **Very Weak (Bardzo słabe)**. Aby to zrobić:
 - a. Kliknij pozycję.

UWAGA: Po kliknięciu pozycji w narzędziu wyświetlona zostanie strona ustawień pozycji.

- b. Na stronie ustawień zabezpieczeń danej pozycji wykonaj konfigurację i wprowadź wymagane zmiany, a po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

- c. Wróć na stronę **Router Security Assessment (Ocena zabezpieczeń routera)** i kliknij przycisk **Close (Zamknij)**, aby zamknąć stronę.
5. W celu automatycznej konfiguracji ustawień zabezpieczeń kliknij przycisk **Secure Your Router (Zabezpiecz swój router)**.
6. Po wyświetleniu komunikatu kliknij przycisk **OK**.

Blokowanie niebezpiecznych witryn

Funkcja ta ogranicza dostęp do niebezpiecznych witryn określonych w bazie danych w chmurze w celu zapewnienia zawsze aktualnej ochrony.

UWAGA: Funkcja ta jest uaktywniana automatycznie w przypadku uruchomienia skanowania **Router Weakness Scan (Skanowanie słabych punktów routera)**.

Aby włączyć funkcję **Malicious Sites Blocking (Blokowanie niebezpiecznych witryn)**:

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij kartę **Network Protection (Ochrona sieci)**.
3. W panelu **Malicious Sites Blocking (Blokowanie niebezpiecznych witryn)** kliknij pozycję **ON (WŁ.)**.

Dwukierunkowy system IPS

Dwukierunkowy system IPS (ang. Intrusion Prevention System) chroni router przed atakami sieciowymi, blokując złośliwe pakiety przychodzące i usuwając podejrzane pakiety wychodzące

UWAGA: Funkcja ta jest uaktywniana automatycznie w przypadku uruchomienia skanowania **Router Weakness Scan (Skanowanie słabych punktów routera)**.

Aby włączyć funkcję **Two-Way IPS (Dwukierunkowy system IPS)**:

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij kartę **Network Protection (Ochrona sieci)**.
3. W panelu **Two-Way IPS (Dwukierunkowy system IPS)** kliknij pozycję **ON (WŁ.)**

Wykrywanie i blokowanie zainfekowanych urządzeń

Funkcja ta zapobiega przesyłaniu informacji osobistych lub zainfekowanego stanu przez zainfekowane urządzenia do urządzeń zewnętrznych.

UWAGA: Funkcja ta jest uaktywniana automatycznie w przypadku uruchomienia skanowania **Router Weakness Scan (Skanowanie słabych punktów routera)**.

Aby włączyć funkcję Vulnerability protection (Ochrona przed wykorzystywaniem luk):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij kartę **Network Protection (Ochrona sieci)**.
3. W panelu **Infected Device Prevention and Blocking (Wykrywanie i blokowanie zainfekowanych urządzeń)** kliknij pozycję **ON (WŁ.)**.

Aby skonfigurować funkcję Alert Preference (Preferencje dotyczące alertów):

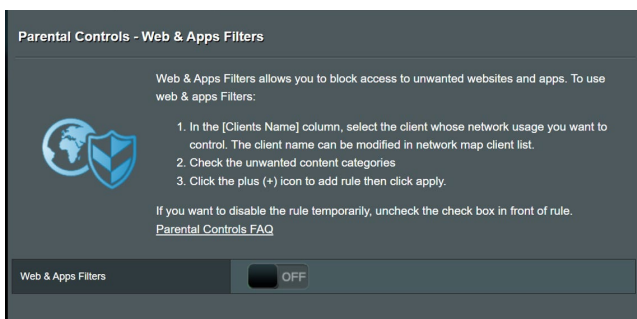
1. W panelu **Infected Device Prevention and Blocking (Wykrywanie i blokowanie zainfekowanych urządzeń)** kliknij przycisk **Alert Preference (Preferencje dotyczące alertów)**.
2. Wybierz lub wprowadź dostawcę poczty e-mail, konto e-mail oraz hasło, a następnie kliknij przycisk **Apply (Zastosuj)**.

3.4.2 Konfiguracja funkcji Parental Controls (Kontrola rodzicielska)

Kontrola rodzicielska zapewnia kontrolę nad czasem dostępu do Internetu oraz umożliwia ustawienie ograniczenia czasu używania sieci klienta.

Aby przejść na stronę główną funkcji Parental Controls (Kontrola rodzicielska):

W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne)** > **Parental Controls (Kontrola rodzicielska)**.



Filtry sieci Web i aplikacji

Web & Apps Filters (Filtry sieci Web i aplikacji) to funkcja pozycji **Parental Controls (Kontrola rodzicielska)**, która umożliwia blokowanie dostępu do niechcianych witryn lub aplikacji.


Aby skonfigurować funkcję Web & Apps Filters (Filtry sieci Web i aplikacji):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne)** > **Parental Controls (Kontrola rodzicielska)**.
2. W panelu **Web & Apps Filters (Filtry sieci Web i aplikacji)** kliknij pozycję **ON (WŁ.)**.
3. Po pojawieniu się komunikatu End Users License Agreement (EULA) [Umowa licencyjna użytkownika oprogramowania (EULA)] kliknij pozycję **I agree (Zgadzam się)**, aby kontynuować.
4. W kolumnie **Client List (Lista klientów)** wprowadź lub wybierz z listy rozwijanej nazwę klienta.

5. W kolumnie **Content Category (Kategoria zawartości)** wybierz filtry z czterech głównych kategorii: **Adult (Dla dorosłych)**, **Instant Message and Communication (Wiadomości błyskawiczne i komunikacja)**, **P2P and File Transfer (Sieć P2P i transfer plików)** oraz **Streaming and Entertainment (Przesyłanie strumieniowe i rozrywka)**.
6. Kliknij ikonę  w celu dodania profilu klienta.
7. Kliknij przycisk **Apply (Zastosuj)**, aby zapisać ustawienia.

Parental Controls - Web & Apps Filters

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




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

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

Web & Apps Filters ON

Client List (Max Limit : 64)

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

Apply

Ustawianie harmonogramu

Funkcja Time Scheduling (Ustawianie harmonogramu) umożliwia ustawienie ograniczenia czasu używania sieci klienta.

UWAGA: Należy upewnić się, że czas systemowy jest zsynchronizowany z serwerem NTP.

Parental Controls - Time Scheduling

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

Enable block all devices OFF

This feature allows you to set up a scheduled time for specific devices' Internet access.

1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling ON

System Time Thu, Sep 21 12:34:41 2023

Client List (Max Limit : 64)

Select	Client Name (MAC Address)	Time Management	Add / Delete
Time		-	+

No data in table.

Apply

Aby skonfigurować funkcję Time Scheduling (Ustawianie harmonogramu):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > Parental Controls (Kontrola rodzicielska) > Time Scheduling (Ustawianie harmonogramu)**.
2. W panelu **Enable Time Scheduling (Włącz ustalanie harmonogramu)** kliknij pozycję **ON (WŁ.)**.
3. W kolumnie **Clients Name (Nazwa klienta)** wprowadź lub wybierz z listy rozwijanej nazwę klienta.

UWAGA: Można także wprowadzić adres MAC klienta w kolumnie **Client MAC Address (Adres MAC klienta)**. Nazwa klienta nie może zawierać znaków specjalnych ani spacji, ponieważ mogłyby one spowodować nieprawidłowe działanie routera.

4. Kliknij ikonę w celu dodania profilu klienta.
5. Kliknij przycisk **Apply (Zastosuj)**, aby zapisać ustawienia.

3.5 Zapora

Router bezprzewodowy może pełnić funkcję zapory sprzętowej w sieci.

UWAGA: Funkcja Firewall (Zapora) jest domyślnie włączona.

3.5.1 Ogólne

Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.
[DoS Protection FAQ](#)

Enable Firewall Yes No

Enable DoS protection Yes No

Logged packets type

Respond ICMP Echo (ping) Request from WAN Yes No

Basic Config

Enable IPv4 inbound firewall rules Yes No

Inbound Firewall Rules (Max Limit : 128)

Source IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>
No data in table.			

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified.
(2001::1111:2222:3333:64 for example)

Basic Config

Enable IPv6 Firewall Yes No

Famous Server List

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	TCP	<input type="button" value="⊕"/>
No data in table.					

W celu skonfigurowania podstawowych ustawień pozycji Firewall (Zapora):

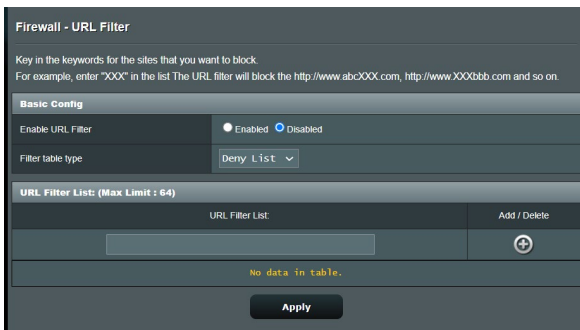
1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) > General (Ogólne)**.
2. W polu **Enable Firewall (Włącz zaporę)** zaznacz pozycję **Yes (Tak)**.

3. W pozycji **Enable DoS protection (Włącz ochronę przed atakami typu DoS)** zaznacz pozycję **Yes (Tak)**, aby zapewnić ochronę sieci przed atakami typu „odmowa usługi” (DoS, Denial of Service), chociaż może to mieć wpływ na wydajność routera.
4. Można także monitorować wymianę pakietów między połączeniami w sieci LAN i WAN. W pozycji **Logged packets type (Typ zarejestrowanych pakietów)** wybierz opcję **Dropped (Porzucone), Accepted (Zaakceptowane)** lub **Both (Oba)**.
5. Kliknij przycisk **Apply (Zastosuj)**.


3.5.2 Filtr adresów URL

Można określić słowa kluczowe lub adresy sieci Web, aby uniemożliwić dostęp do pewnych adresów URL.

UWAGA: Pozycja URL Filter (Filtr adresów URL) zależy od zapytania DNS. Jeśli klient sieciowy uzyskał już dostęp do witryny sieci Web, np. `http://www.abcxxx.com`, witryna ta nie zostanie zablokowana (odwiedzone wcześniej witryny sieci Web są zapisywane w pamięci podręcznej DNS). Aby rozwiązać ten problem, należy wyczyścić pamięć podręczną DNS przed skonfigurowaniem pozycji URL Filter (Filtr adresów URL).

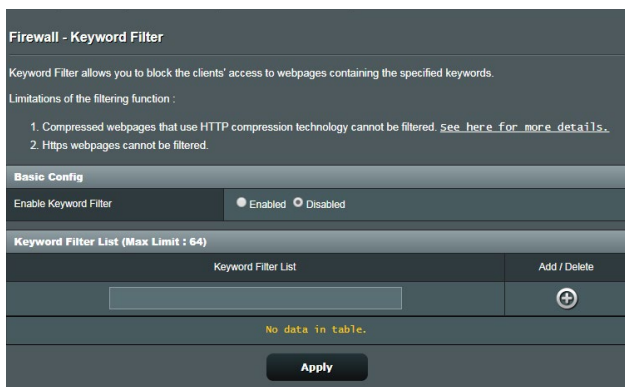


W celu skonfigurowania filtra adresów URL:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) > URL Filter (Filtr adresów URL)**.
2. W polu **Enable URL Filter (Włącz filtr adresów URL)** wybierz pozycję **Enabled (Włączono)**.
3. Wprowadź adres URL i kliknij przycisk .
4. Kliknij przycisk **Apply (Zastosuj)**.

3.5.3 Filtr słów kluczowych

Filtr słów kluczowych blokuje dostęp do stron sieci Web zawierających określone słowa kluczowe.



W celu skonfigurowania filtra słów kluczowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) > Keyword Filter (Filtr słów kluczowych)**.
2. W polu Enable Keyword Filter (Włącz filtr słów kluczowych) wybierz pozycję **Enabled (Włączono)**.
3. Wprowadź słowo lub wyrażenie i kliknij przycisk **Add (Dodaj)**.
4. Kliknij przycisk **Apply (Zastosuj)**.

UWAGI:

- Pozycja Keyword Filter (Filtr słów kluczowych) zależy od zapytania DNS. Jeśli klient sieciowy uzyskał już dostęp do witryny sieci Web, np. <http://www.abcxxx.com>, witryna ta nie zostanie zablokowana (odwiedzone wcześniej witryny sieci Web są zapisywane w pamięci podręcznej DNS). Aby rozwiązać ten problem, należy wyczyścić pamięć podręczną DNS przed skonfigurowaniem pozycji Keyword Filter (Filtr słów kluczowych).
- Nie można filtrować stron sieci Web skompresowanych za pomocą kompresji protokołu HTTP. Przy użyciu filtra słów kluczowych nie można także blokować stron HTTPS.

3.5.4 Network Services Filter (Filtr usług sieciowych)

Za pomocą pozycji Network Services Filter (Filtr usług sieciowych) blokowana jest wymiana pakietów z sieci LAN do sieci WAN oraz ograniczany jest dostęp klientów sieciowych do określonych usług sieci Web, takich jak Telnet lub FTP.

Firewall - Network Services Filter

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

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

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

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.

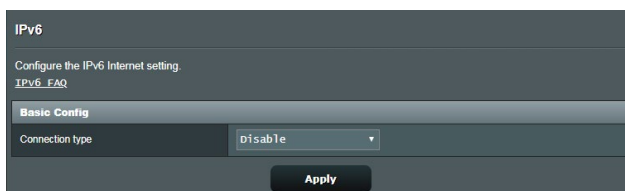
Apply

W celu skonfigurowania filtra usług sieciowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) > wybierz Network Service Filter (Filtr usług sieciowych)**.
2. W polu Enable Network Services Filter (Włącz filtr usług sieciowych) zaznacz pozycję **Yes (Tak)**.
3. Wybierz opcję dla pozycji Filter table type (Typ tabeli filtrów). Pozycja **Deny (Odmów)** umożliwia blokowanie określonych usług sieciowych. Pozycja **Allow (Zezwól)** umożliwia ograniczenie dostępu do określonych usług sieciowych.
4. Określ przedziały czasu i dni, w które filtry mają być aktywne.
5. Aby określić, które usługi sieciowe mają być filtrowane, wprowadź wartości dla pozycji Source IP (Adres IP źródła), Destination IP (Docelowy adres IP), Port Range (Zakres portu) i Protocol (Protokół). Kliknij przycisk .
6. Kliknij przycisk **Apply (Zastosuj)**.

3.6 IPv6 (Protokół IPv6)

Niniejszy router bezprzewodowy obsługuje adresowanie IPv6, system obsługujący więcej adresów IP. Standard ten nie jest jeszcze powszechnie dostępny. W celu sprawdzenia, czy dana usługa internetowa obsługuje protokół IPv6 należy skontaktować się z usługodawcą internetowym.



W celu skonfigurowania protokołu IPv6:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia Zaawansowane) > IPv6 (Protokół IPv6)**.
2. Wybierz opcję dla pozycji **Connection type (Typ połączenia)**. Opcje konfiguracji różnią się w zależności od wybranego typu połączenia.
3. Wprowadź ustawienia sieci LAN i DNS dla protokołu IPv6.
4. Kliknij przycisk **Apply (Zastosuj)**.

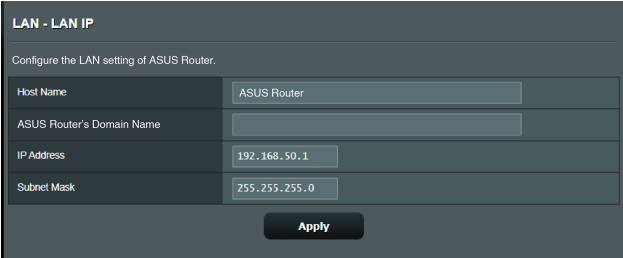
UWAGA: W celu uzyskania określonych informacji dotyczących protokołu IPv6 dla danej usługi internetowej należy skontaktować się z usługodawcą internetowym.

3.7 LAN (Sieć LAN)

3.7.1 LAN IP (Adres IP sieci LAN)

Na ekranie LAN IP (Adres IP sieci LAN) można modyfikować ustawienia adresu IP sieci LAN routera bezprzewodowego.

UWAGA: Wszelkie zmiany adresu IP sieci LAN zostaną odzwierciedlone w ustawieniach DHCP.



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

W celu zmodyfikowania ustawień adresu IP sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > LAN (Sieć LAN) > LAN IP (Adres IP sieci LAN)**.
2. Zmodyfikuj pozycje **IP address (Adres IP)** i **Subnet Mask (Maska podsieci)**.
3. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

3.7.2 DHCP Server (Serwer DHCP)

Router bezprzewodowy korzysta z serwera DHCP do automatycznego przypisywania adresów IP w sieci. Można określić zakres adresów IP oraz czas dzierżawy dla klientów w sieci.

The screenshot shows the 'LAN - DHCP Server' configuration page. It includes a description of DHCP, a 'Basic Config' section with fields for enabling the server, domain name, IP pool (192.168.0.2 to 192.168.0.254), lease time (86400), and default gateway. A 'DNS and WINS Server Setting' section includes fields for DNS servers and a checkbox for advertising the router's IP. A 'Manual Assignment' section has a checkbox for enabling manual IP assignment. At the bottom, there is a table for manually assigned IP addresses with columns for Client Name, IP Address, DNS Server, Host Name, and an Add/Delete button. The table is currently empty, showing 'No data in table.' and an 'Apply' button at the bottom.

LAN - DHCP Server

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

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

W celu wykonania ustawień serwera DHCP:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > LAN (Sieć LAN) > DHCP Server (Serwer DHCP)**.
2. W polu **Enable the DHCP Server (Włączyć serwer DHCP?)** zaznacz **Yes (Tak)**.

3. W polu tekstowym **Domain Name (Nazwa domeny)** wprowadź nazwę domeny routera bezprzewodowego.
4. W polu **IP Pool Starting Address (Adres początkowy zakresu IP)** wprowadź adres początkowy IP.
5. W polu **IP Pool Ending Address (Adres końcowy zakresu IP)** wprowadź adres końcowy IP.
6. W polu **Lease Time (Czas dzierżawy)** wprowadź czas zakończenia ważności adresów IP, po czym router bezprzewodowy automatycznie przydzieli nowe adresy IP klientom sieci.

UWAGI:

- Podczas określania zakresu adresów IP zalecane jest stosowanie formatu adresów IP: 192.168.50.xxx (xxx może być dowolną liczbą pomiędzy 2 a 254).
- Pozycja IP Pool Starting Address (Adres początkowy zakresu IP) nie powinna być wyższa niż pozycja IP Pool Ending Address (Adres końcowy zakresu IP).

-
7. W części **DNS and WINS Server Settings (Ustawienia serwera DNS i WINS)** wprowadź w razie potrzeby adres IP serwera DNS i WINS.
 8. Router bezprzewodowy może także ręcznie przypisywać adresy IP urządzeniom w sieci. W polu **Enable Manual Assignment (Włącz przypisywanie ręczne)** wybierz opcję **Yes (Tak)**, aby przypisać adres IP do określonych adresów MAC w sieci. W celu ręcznego przypisywania do listy DHCP można dodać maksymalnie 32 adresy MAC.

3.7.3 Route (Trasa)

Jeśli dana sieć korzysta z więcej niż jednego routera bezprzewodowego, można skonfigurować tabelę routingu w celu współdzielenia tej samej usługi internetowej.

UWAGA: Jeśli użytkownik nie posiada specjalistycznej wiedzy na temat tabel routingu, zalecane jest pozostawienie domyślnych ustawień trasy.

LAN - Route

This function allows you to add routing rules into. It is useful if you connect several routers behind to share the same connection to the Internet.

Basic Config

Enable static routes Yes No



Static Route List (Max Limit : 32)

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	+

No data in table.

Apply

W celu skonfigurowania tabeli routingu sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > LAN (Sieć LAN) > Route (Trasa)**.
2. W polu **Enable static routes (Włącz trasy statyczne)** zaznacz pozycję **Yes (Tak)**.
3. W obszarze **Static Route List (Lista tras statycznych)** wprowadź informacje o sieci dotyczące innych punktów dostępowych lub węzłów. Kliknij przycisk **Add (Dodaj)**  lub **Delete (Usuń)**  w celu dodania urządzenia do listy lub usunięcia go z niej.
4. Kliknij przycisk **Apply (Zastosuj)**.

3.7.4 IPTV

Router bezprzewodowy obsługuje połączenia z usługami IPTV udostępniane przez usługodawcę internetowego lub sieć LAN. Zakładka IPTV zawiera ustawienia konieczne do konfiguracji pozycji IPTV, VoIP, multimediami i UDP dla danej usługi. W celu uzyskania konkretnych informacji dotyczących usługi należy skontaktować się z usługodawcą internetowym.

LAN - IPTV

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

LAN Port

Select ISP Profile	None ▾
Choose IPTV STB Port	None ▾

Special Applications

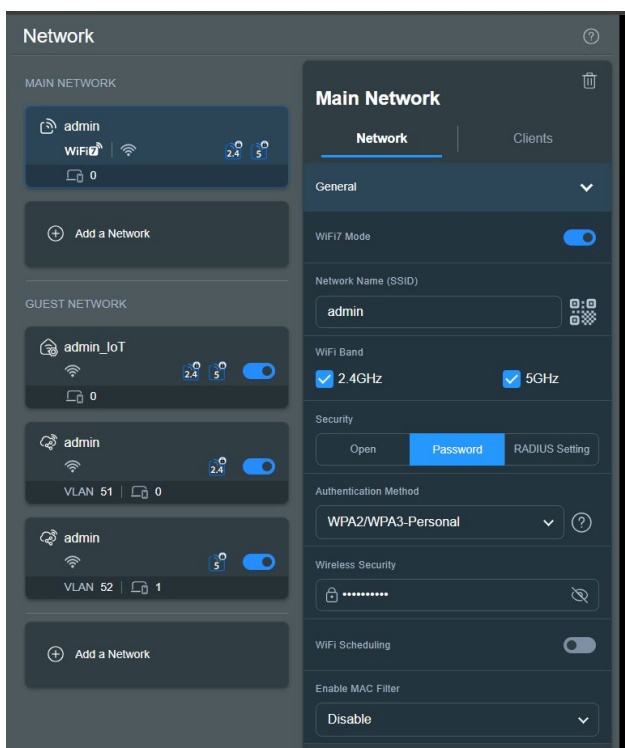
Use DHCP routes	Microsoft ▾
Enable multicast routing (IGMP Proxy)	Disable ▾
UDP Proxy (Udpxy)	0

Apply

3.8 Sieć

3.8.1 Sieć główna - Filtr adresów MAC

Pozycja Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych) zapewnia kontrolę nad pakietami przesyłanymi na określony adres MAC (Media Access Control) w danej sieci bezprzewodowej.





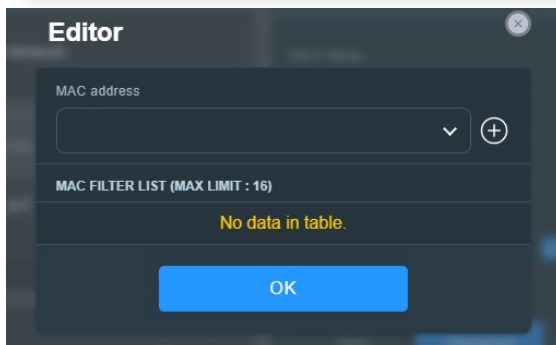
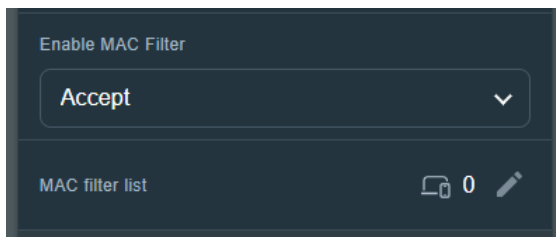
W celu skonfigurowania filtra adresów MAC urządzeń bezprzewodowych:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > **Network (Sieć)** > **Main Network (Sieć główna)** i wybierz nazwę (SSID) sieci głównej.
2. Z listy rozwijanej **Enable Mac Filter (Włącz filtr adresów MAC)** wybierz opcję **Accept (Akceptuj)** lub **Reject (Odrzuć)**.

- Wybierz opcję **Accept (Akceptuj)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) mogły łączyć się z siecią bezprzewodową.
- Wybierz opcję **Reject (Odrzuć)**, aby urządzenia z listy MAC filter list (Lista filtrowanych adresów MAC) nie mogły łączyć się z siecią bezprzewodową.

UWAGA: Wybierz opcję **Disable (Wyłącz)**, jeśli chcesz wyłączyć opcję **Enable MAC Filter (Włącz filtr adresów MAC)**.

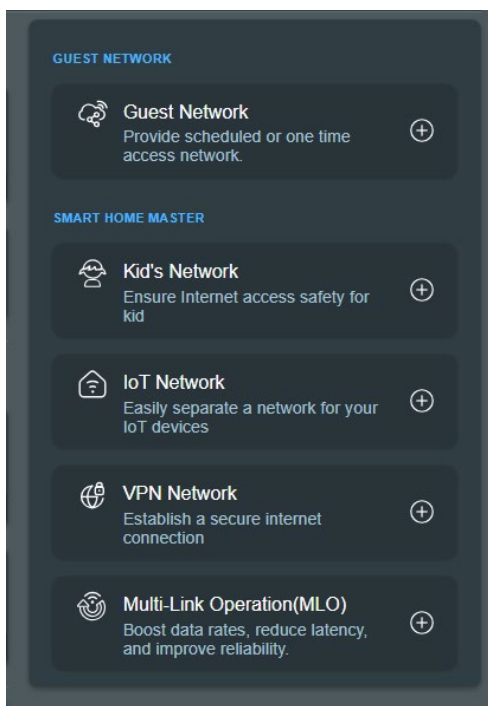
3. W obszarze MAC filter list (Lista filtrowanych adresów MAC) kliknij  w celu przejścia na stronę **Editor (Edytor)**, a następnie kliknij  i wprowadź adres MAC urządzenia bezprzewodowego.
4. Kliknij przycisk **OK**.



3.8.2 Guest Network (Sieć gości)

3.8.2.1 Guest Network (Sieć gości)

Pozycja Guest Network (Sieć gości) udostępnia tymczasowym użytkownikom możliwość połączenia z Internetem za pomocą oddzielnych identyfikatorów SSID lub sieci, bez zapewniania dostępu do sieci prywatnej.



UWAGA: ZenWiFi BD4 obsługuje do trzech identyfikatorów SSID w Guest Network (Sieć gości).

W celu utworzenia sieci gości:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > **Network (Sieć)** > **Guest Network (Sieć Gości)** > **Add a Network (Dodaj sieć)**.
2. Wybierz **Guest Network (Sieć Gości)** i przypisz nazwę sieci tymczasowej w polu **Network Name (SSID) [Nazwa sieci (SSID)]**.

3. Wybierz metodę uwierzytelniania w obszarze **Security (Bezpieczeństwo)**.
4. Określ czas dostępu lub wybierz **Scheduled (Zaplanowane)**, aby dodać profil harmonogramu online.
5. Wybierz **WiFi Band (Pasma WiFi)** dla sieci gościnnej, którą chcesz utworzyć.
6. Włącz lub wyłącz **Bandwidth Limiter (Ogranicznik przepustowości)**.
7. Włącz lub wyłącz **Access Intranet (Dostęp do Intranetu)**.
8. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

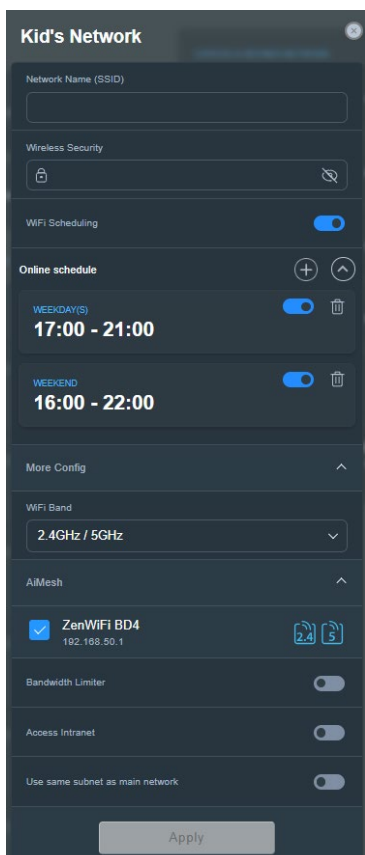
The screenshot shows the 'Guest Network' configuration page. At the top, there is a 'Network Name (SSID)' input field. Below it, the 'Security' section has two options: 'Open' (selected) and 'Password'. The 'WiFi Scheduling' section is turned on and has 'One Time Access' selected over 'Scheduled'. Under 'One Time Access', there are buttons for '30 mins', '1 hr(s)', '2 hr(s)' (selected), '4 hr(s)', '6 hr(s)', and 'Custom'. A 'More Config' section is expanded, showing 'WiFi Band' set to '2.4GHz / 5GHz'. The 'AiMesh' section is also expanded, showing 'ZenWiFi BD4' with IP '192.168.50.1' and icons for 2.4 and 5 GHz bands. At the bottom, there are three toggle switches: 'Bandwidth Limiter' (off), 'Access Intranet' (off), and 'Use same subnet as main network' (off). An 'Apply' button is at the very bottom.

3.8.2.2 Smart Home Master

Smart Home Master to efektywne i przyjazne dla użytkownika narzędzie do segmentacji sieci. Upraszcza proces tworzenia zaawansowanych scenariuszy podsieci i zarządzania nimi, np. tworzenie dedykowanego identyfikatora SSID dla urządzeń dzieci, łączenie się z siecią VPN przez dedykowaną podsieć, a nawet tworzenie jednego bezpiecznego identyfikatora SSID dla wszystkich urządzeń IoT.

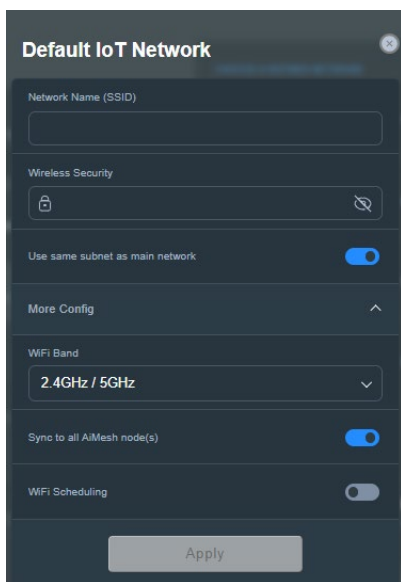
W celu utworzenia Sieć dla dzieci:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > **Network (Sieć)** > **Guest Network (Sieć Gości)** > **Add a Network (Dodaj sieć)**.
2. Wybierz opcję **Kid's Network (Sieć dla dzieci)** i przypisz nazwę sieci oraz klucz zabezpieczeń w polach **Network Name (SSID) [Nazwa sieci (SSID)]** i **Wireless Security (Zabezpieczenia sieci bezprzewodowej)**.
3. Dostosuj czas dostępu do Internetu w polu **Online schedule (Harmonogram online)**.
4. Wybierz **WiFi Band (Pasma WiFi)** dla sieć dla dzieci, którą chcesz utworzyć.
5. Włącz lub wyłącz **Bandwidth Limiter (Ogranicznik przepustowości)**.
6. Włącz lub wyłącz **Access Intranet (Dostęp do Intranetu)**.
7. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.



W celu utworzenia Sieć IoT:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > **Network (Sieć)** > **Guest Network (Sieć Gości)** > **Add a Network (Dodaj sieć)**.
2. Wybierz opcję **IoT Network (Sieć IoT)** i przypisz nazwę sieci oraz klucz zabezpieczeń w polach **Network Name (SSID) [Nazwa sieci (SSID)]** i **Wireless Security (Zabezpieczenia sieci bezprzewodowej)**.
3. Wybierz **WiFi Band (Pasma WiFi)** dla sieć IoT, którą chcesz utworzyć.
4. Dostosuj czas dostępu do Internetu, włączając **WiFi Scheduling (Harmonogram Wi-Fi)**.
5. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.



W celu utworzenia Sieć VPN:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne)** > **Network (Sieć)** > **Guest Network (Sieć Gości)** > **Add a Network (Dodaj sieć)**.
2. Wybierz opcję **VPN Network (Sieć VPN)** i przypisz nazwę sieci oraz klucz zabezpieczeń w polach **Network Name (SSID)** [Nazwa sieci (SSID)] i **Wireless Security (Zabezpieczenia sieci bezprzewodowej)**.
3. Jeśli nie skonfigurowałeś profilu VPN dla serwera VPN lub klienta VPN, kliknij **Go Setting (Przejdź do ustawień)**, aby utworzyć profil VPN.
4. Wybierz **WiFi Band (Pasma WiFi)** dla sieć VPN, którą chcesz utworzyć.
5. Dostosuj czas dostępu do Internetu, włączając **WiFi Scheduling (Harmonogram Wi-Fi)**.
6. Włącz lub wyłącz **Bandwidth Limiter (Ogranicznik przepustowości)**.
7. Włącz lub wyłącz **Access Intranet (Dostęp do Intranetu)**.
8. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.



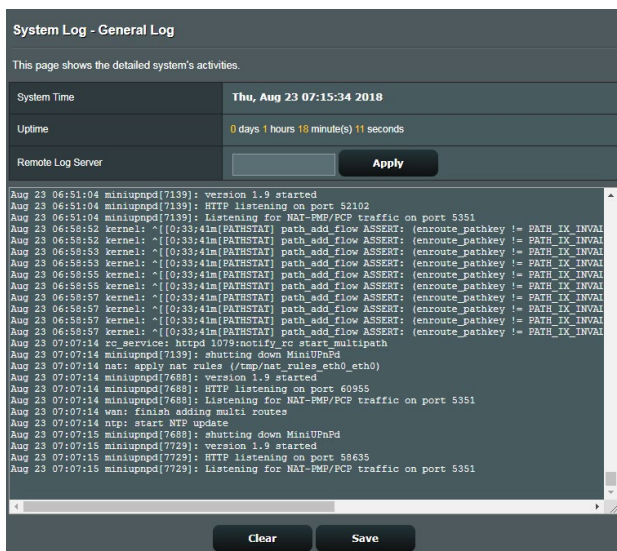
3.9 System Log (Dziennik systemu)

W pozycji System Log (Dziennik systemu) znajduje się lista zarejestrowanych aktywności w sieci.

UWAGA: Po ponownym uruchomieniu lub wyłączeniu routera dziennik systemu jest resetowany.

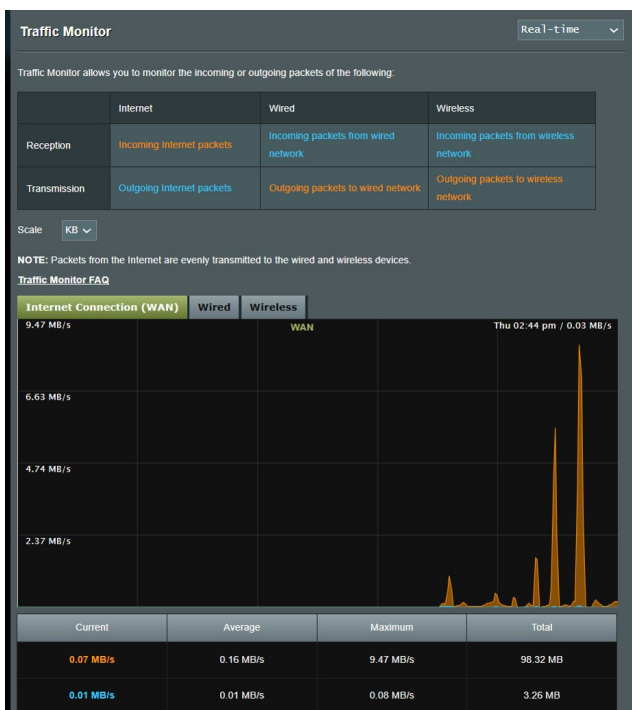
W celu wyświetlenia dziennika systemu:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > System Log (Dziennik systemu)**.
2. Aktywności w sieci można sprawdzić na dowolnej z poniższych zakładek:
 - Dziennik ogólny
 - Dziennik sieci bezprzewodowej
 - Dzierżawy DHCP
 - IPv6
 - Tabela routingu
 - Przekierowanie portów
 - Połączenia



3.10 Analizator ruchu

Funkcja monitorowania ruchu zapewnia informacje dotyczące przepustowości i szybkości połączenia z Internetem, siecią przewodową lub bezprzewodową. Umożliwia ona monitorowanie ruchu sieciowego w czasie rzeczywistym lub na poziomie każdego dnia. Zapewnia ponadto opcję wyświetlania informacji o ruchu sieciowym z ostatnich 24 godzin.



UWAGA: Pakiety z Internetu są równomiernie przesyłane do urządzeń przewodowych i bezprzewodowych.

3.11 WAN (Sieć WAN)

3.11.1 Internet Connection (Połączenie internetowe)

Na ekranie Internet Connection (Połączenie internetowe) można skonfigurować ustawienia różnego typu połączeń WAN.

WAN - Internet Connection

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

Configure the Ethernet WAN settings of ASUS Router.

Basic Config

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

WAN DNS Setting

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

DHCP Option

Class Identifier (Option 60)	<input type="text"/>
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>
Class Identifier (Option 60)	<input type="text"/>
Client Identifier (Option 61)	<input checked="" type="checkbox"/> IAID/DUID <input type="text"/>

Account Settings

Authentication	None
PPP Echo Interval	6
PPP Echo Max Failures	10

Special Requirement from ISP

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

Apply

W celu skonfigurowania ustawień połączenia WAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > Internet Connection (Połączenie internetowe)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Typ połączenia WAN:** Wybierz typ połączenia udostępniany przez usługodawcę internetowego. Dostępne opcje to **Automatic IP (Automatyczny adres IP)**, **PPPoE**, **PPTP**, **L2TP** lub **fixed IP (Stały adres IP)**. W przypadku braku pewności co do typu połączenia WAN lub braku możliwości uzyskania przez router prawidłowego adresu IP należy skontaktować się z usługodawcą internetowym.
 - **Włącz sieć WAN:** Wybierz opcję **Yes (Tak)**, aby router mógł uzyskać dostęp do Internetu. Wybierz opcję **No (Nie)**, aby wyłączyć dostęp do Internetu.
 - **Włącz NAT:** Translator adresów sieciowych NAT (Network Address Translation) to system, w którym jeden publiczny adres IP (adres IP sieci WAN) jest używany do zapewniania dostępu do Internetu klientom sieciowym o prywatnym adresie IP w sieci LAN. Prywatny adres IP każdego klienta sieciowego jest zapisywany w tabeli NAT i używany do rozsyłania przychodzących pakietów danych.
 - **Włącz UPnP:** Protokół UPnP (Universal Plug and Play) umożliwia sterowanie kilkoma urządzeniami (takimi jak routery, telewizory, zestawy stereo, konsole do gier i telefony komórkowe) w sieci z obsługą adresów IP ze sterowaniem centralnym za pomocą bramy lub bez niego. Protokół UPnP łączy komputery o dowolnym współczynniku postaci, zapewniając bezproblemowe połączenie sieciowe do konfiguracji zdalnej i przesyłania danych. Podczas korzystania z protokołu UPnP nowe urządzenie sieciowe jest wykrywane automatycznie. Po połączeniu z siecią urządzenia można skonfigurować zdalnie w celu zapewnienia obsługi aplikacji P2P, gier interaktywnych, konferencji wideo oraz serwerów sieci Web lub proxy. W przeciwieństwie do przekierowania portów, które wymaga ręcznej konfiguracji ustawień portów, protokół UPnP automatycznie konfiguruje router w celu zapewnienia przyjmowania połączeń przychodzących i bezpośrednich żądań do określonego komputera w sieci lokalnej.

- **Enable WAN Aggregation (Włącz agregację WAN):** Agregacja WAN łączy dwa połączenia sieciowe w celu zwiększenia szybkości sieci WAN do 2 Gb/s. Połącz port WAN i port LAN 4 routera z portami LAN modemu.
- **Łączenie z serwerem DNS:** Umożliwia automatyczne uzyskiwanie adresu IP serwera DNS przez router od usługodawcy internetowego. DNS to host w Internecie, który tłumaczy nazwy internetowe na numeryczne adresy IP.
- **Uwierzytelnianie:** Ta pozycja może być określana przez niektórych usługodawców internetowych. Jeśli to konieczne, sprawdź u usługodawcy internetowego i wprowadź.
- **Nazwa hosta:** W tym polu można wprowadzić nazwę hosta danego routera. Jest to zwykle specjalny wymóg usługodawcy internetowego. Jeśli usługodawca internetowy przypisał nazwę hosta do komputera, wprowadź ją w tym polu.
- **Adres MAC:** Pozycja MAC (Media Access Control) address (Adres MAC) to unikatowy identyfikator urządzenia sieciowego. Niektórzy usługodawcy internetowi monitorują adresy MAC urządzeń sieciowych, które łączą się z ich usługą i odrzucają wszelkie próby połączeń urządzeń nierozpoznanych. Aby uniknąć problemów z połączeniami spowodowanych niezarejestrowanym adresem MAC, można:
 - Skontaktować się z usługodawcą internetowym i zaktualizować adres MAC skojarzony z jego usługą.
 - Sklonować lub zmienić adres MAC routera bezprzewodowego firmy ASUS w celu jego dopasowania do adresu MAC poprzedniego urządzenia sieciowego rozpoznawanego przez usługodawcę internetowego.

3.11.2 Dwie sieci WAN

Pozycja Dual WAN (Dwie sieci WAN) umożliwia ustawienie w routerze połączeń od dwóch usługodawców internetowych — podstawowa sieć WAN i dodatkowa sieć WAN.

Aby skonfigurować pozycję Dual WAN (Dwie sieci WAN):

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN)**.
2. Przejdź na kartę **Dual WAN (Dwie sieci WAN)** i kliknij pozycję **ON (WŁ)**.
3. Wybierz sieć w pozycji **Primary WAN (Podstawowa sieć WAN)** i **Secondary WAN (Dodatkowa sieć WAN)**. Dostępne opcje to dwa 2.5GbE WAN/LAN.
4. Wybierz pozycję **Fail Over (Praca awaryjna)** lub **Load Balance (Równoważenie obciążenia)**.
5. Kliknij przycisk **Apply (Zastosuj)**.

UWAGA: Szczegółowe informacje można znaleźć w sekcji FAQ w witrynie pomocy technicznej firmy <https://www.asus.com/support/FAQ/1011719>

WAN - Dual WAN

ZenWiFi BD4 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. [Dual WAN FAQ](#)

Basic Config

Enable Dual WAN OFF

Primary WAN

Auto Network Detection

Detailed explanations are available on the [ASUS Support Site FAQ](#), which may help you use this function effectively.

Detect Interval Every seconds

Internet Connection Diagnosis When the current WAN fails continuous times, it is deemed a disconnection.

Network Monitoring DNS Query Ping

Apply

3.11.3 Port Trigger (Wyzwalanie portów)

Wyzwalanie zakresu portu otwiera wstępnie określony port przychodzący na ograniczony czas za każdym razem, gdy klient w sieci lokalnej nawiązuje połączenie wychodzące z określonym portem. Wyzwalanie portów jest używane w następujących przypadkach:

- Więcej niż jeden klient lokalny wymaga przekierowania portu dla tej samej aplikacji, ale w innym czasie.
- Aplikacja wymaga określonych portów przychodzących innych niż porty wychodzące.

WAN - Port Trigger

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.
[Port_Trigger_FAQ](#)

Basic Config

Enable Port Trigger: Yes No

Well-Known Applications:

Trigger Port List (Max Limit : 32)

Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
No data in table					

W celu skonfigurowania pozycji Port Trigger (Wyzwalanie portów):

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > wybierz Port Trigger (Wyzwalanie portów)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Włącz wyzwalanie portów:** Wybierz opcję **Yes (Tak)**, aby włączyć funkcję Port Trigger (Wyzwalanie portów).
 - **Dobrze znane aplikacje:** Wybierz popularne gry i usługi sieci Web w celu ich dodania do pozycji Port Trigger List (Lista portów wyzwalania).
 - **Opis:** Wprowadź krótką nazwę lub opis usługi.

- **Port wyzwalania:** Określ port wyzwalający otwarcie portu przychodzącego.
- **Protokół:** Wybierz protokół TCP lub UDP.
- **Port przychodzący:** Określ port przychodzący do odbierania danych przychodzących z Internetu.

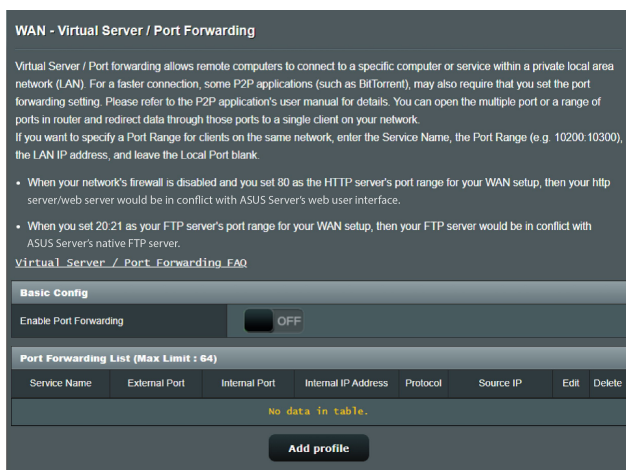
UWAGI:

- Podczas łączenia z serwerem IRC komputer kliencki nawiązuje połączenie wychodzące zgodnie z zakresem portu wyzwalania 66660–7000. Serwer IRC odpowiada poprzez weryfikację nazwy użytkownika i nawiązanie nowego połączenia z komputerem klienckim przez port przychodzący.
- Jeśli funkcja Port Trigger (Wyzwalanie portów) jest wyłączona, router odrzuca połączenia, ponieważ nie może określić, który komputer zgłasza żądanie dostępu do serwera IRC. Po włączeniu funkcji Port Trigger (Wyzwalanie portów) router przypisze port przychodzący do odbierania danych przychodzących. Ten port przychodzący zamknie się po upływie określonego czasu z powodu braku możliwości określenia przez router czasu wyłączenia aplikacji.
- Funkcja wyzwolania portów umożliwia korzystanie z określonej usługi i konkretnego portu przychodzącego w danym czasie tylko przez jednego klienta w sieci.
- Do jednoczesnego wyzwolenia portu w więcej niż jednym komputerze nie można używać tej samej aplikacji. Router przekieruje port z powrotem do ostatniego komputera w celu wysłania żądania/pakietu wyzwolania do routera.

3.11.4 Virtual Server/Port Forwarding (Serwer wirtualny/Przekierowanie portów)

Przekierowanie portów to metoda kierowania ruchu sieciowego z Internetu przychodzącego na określony port lub zakres portów do urządzenia lub urządzeń w sieci lokalnej. Po skonfigurowaniu funkcji Port Forwarding (Przekierowanie portów) routera komputery spoza sieci będą mogły uzyskiwać dostęp do określonych usług zapewnianych przez komputer w sieci.

UWAGA: Po włączeniu przekierowania portów router firmy ASUS blokuje niechciany ruch przychodzący z Internetu i zezwala wyłącznie na odpowiedzi na żądania wychodzące z sieci LAN. Klient sieciowy nie ma bezpośredniego dostępu do Internetu i odwrotnie.



W celu skonfigurowania pozycji Port Forwarding (Przekierowanie portów):

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > Virtual Server / Port Forwarding (Serwer wirtualny/Przekierowanie portów)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **ON (WŁ)**.
 - **Włącz przekierowanie portów:** Kliknij pozycję **ON (WŁ)**, aby włączyć przekierowanie portów.

- **Lista znanych serwerów:** Określ typ usługi, do której chcesz uzyskiwać dostęp.
- **Lista znanych gier:** Pozycja ta zawiera listę portów wymaganych do prawidłowego działania popularnych gier online.
- **Port serwera FTP:** Do serwera FTP nie należy przypisywać zakresu portu 20:21, ponieważ spowodowałoby to konflikt z natywnym ustawieniem przypisania serwera FTP zapewnianym przez router.
- **Nazwa usługi:** Wprowadź nazwę usługi.
- **Zakres portu:** Aby określić wartość pozycji Port Range (Zakres portu) dla klientów w tej samej sieci, wprowadź wartość pozycji Service Name (Nazwa usługi), Port Range (Zakres portu) (np. 10200:10300), adres IP sieci LAN i pozostaw puste pole Local Port (Port lokalny). Wartość pozycji Port Range (Zakres portu) może mieć różny format: zakres portu (300:350), pojedyncze porty (566,789) lub format mieszany (1015:1024,3021).

UWAGI:

- Jeśli zaporą sieciową jest wyłączona, a w konfiguracji sieci WAN jako zakres portu serwera HTTP ustawiono wartość 80, wówczas serwer http/serwer sieci Web będzie w konflikcie z interfejsem sieciowym routera.
 - Porty są używane do wymiany danych w sieci, gdzie każdy port ma przypisany numer portu i określone zadanie. Na przykład port 80 jest używany do obsługi protokołu HTTP. Określony port może być w danym czasie używany wyłącznie przez jedną aplikację lub usługę. Dlatego też próba jednoczesnego uzyskania dostępu do danych przez ten sam port w przypadku dwóch komputerów zakończy się niepowodzeniem. Nie można na przykład ustawić przekierowania portu na port 100 dla dwóch komputerów w tym samym czasie.
-
- **Lokalny adres IP:** Wprowadź adres IP sieci LAN klienta.

UWAGA: W celu zapewnienia prawidłowego działania funkcji przekierowania portów należy wprowadzić statyczny adres IP klienta lokalnego. Informacje na ten temat znajdują się w części **3.8 LAN (Sieć LAN)**.

- **Local Port (Port lokalny):** Wprowadź określony port do odbierania przekierowanych pakietów. Pozostaw to pole puste, jeśli chcesz, aby pakiety przychodzące były przekierowywane na określony zakres portu.
- **Protocol (Protokół):** Wybierz protokół. W przypadku braku pewności wybierz opcję **BOTH (OBA)**.

W celu sprawdzenia, czy funkcja Port Forwarding (Przekierowanie portów) została pomyślnie skonfigurowana:

- Upewnij się, że serwer lub aplikacja są skonfigurowane i uruchomione.
- Konieczny będzie klient spoza sieci LAN, ale posiadający dostęp do Internetu (nazywany „klientem internetowym”). Klient ten nie powinien być połączony z routerem firmy ASUS.
- W kliencie internetowym wprowadź adres IP sieci WAN routera w celu zapewnienia dostępu do serwera. Jeśli przekierowanie portów zostało wykonane pomyślnie, dostęp do plików lub aplikacji zostanie zapewniony.

Różnice między wyzwalaniem portów a przekierowaniem portów:

- Wyzwalanie portów działa nawet bez skonfigurowania określonego adresu IP sieci LAN. W przeciwieństwie do przekierowania portów, które wymaga statycznego adresu IP sieci LAN, wyzwalanie portów umożliwia dynamiczne przekierowanie portów przy użyciu routera. Wstępnie określone zakresy portów są konfigurowane w celu przyjmowania połączeń przychodzących w ograniczonym czasie. W przypadku wyzwalania portów na wielu komputerach mogą być uruchomione aplikacje, które normalnie wymagałyby ręcznego przekierowania tych samych portów do każdego komputera w sieci.
- Wyzwalanie portów jest bezpieczniejsze niż przekierowanie portów, ponieważ porty przychodzące nie są zawsze otwarte. Są one otwarte tylko wtedy, gdy aplikacja nawiązuje połączenie wychodzące przez port wyzwalania.

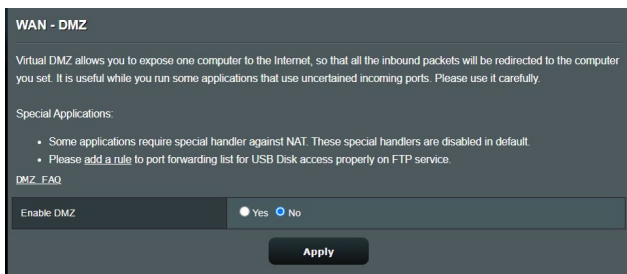
3.11.5 DMZ (Strefa DMZ)

W wirtualnej strefie DMZ dostęp do Internetu ma jeden klient, który odbiera wszystkie pakiety przychodzące do danej sieci lokalnej.

Ruch przychodzący z Internetu jest zwykle odrzucany i kierowany do określonego klienta tylko wtedy, gdy w danej sieci skonfigurowane zostało przekierowanie portów lub wyzwalamie portów. W przypadku konfiguracji strefy DMZ tylko jeden klient sieciowy odbiera wszystkie pakiety przychodzące.

Skonfigurowanie strefy DMZ w sieci jest przydatne, jeśli porty przychodzące mają być otwarte lub w przypadku hostowania serwera domeny, sieci Web lub poczty e-mail.

PRZESTROGA: Otwarcie wszystkich portów klienta na ruch z Internetu naraża sieć na ataki z zewnątrz. Należy wziąć pod uwagę zagrożenia bezpieczeństwa związane z korzystaniem ze strefy DMZ.



W celu skonfigurowania strefy DMZ:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > DMZ (Strefa DMZ)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **IP address of Exposed Station (Adres IP uwidocznionej stacji):** Wprowadź adres IP sieci LAN klienta, który będzie obsługiwał usługę strefy DMZ i będzie miał dostęp do Internetu. Klient serwera musi mieć statyczny adres IP.

W celu usunięcia strefy DMZ:

1. Usuń adres IP sieci LAN klienta z pola tekstowego **IP Address of Exposed Station (Adres IP uwidocznionej stacji)**.
2. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

3.11.6 DDNS (Usługa DDNS)

Skonfigurowanie usługi DDNS (Dynamic DNS) umożliwia uzyskiwanie dostępu do routera spoza sieci za pomocą usługi ASUS DDNS lub innej usługi DDNS.

WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.

If you cannot use ASUS DDNS services, please go to <https://iplookup.asus.com/nslookup.php> to reach your internet IP address to use this service.

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

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

Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No
Server	www.asus.com <input type="button" value="Deregister"/>
Host Name	A8878A175D4A6FD5402C68D6195DB5EF7 asuscomm.com
DDNS Status	Active
DDNS Registration Result	Registration is successful.
HTTPS/SSL Certificate	<input type="radio"/> Free Certificate from Let's Encrypt <input type="radio"/> Import Your Own Certificate <input checked="" type="radio"/> None

W celu skonfigurowania usługi DDNS:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > DDNS (Usługa DDNS)**.
2. Skonfiguruj poniższe ustawienia. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.
 - **Włącz klienta usługi DDNS:** Włącz usługę DDNS w celu zapewnienia dostępu do routera firmy ASUS za pomocą nazwy DNS, a nie adresu IP sieci WAN.
 - **Nazwa serwera i hosta:** Wybierz usługę ASUS DDNS lub inną usługę DDNS. Aby korzystać z usługi ASUS DDNS, w pozycji Host Name (Nazwa hosta) wprowadź wartość w formacie xxx.asuscomm.com (xxx to nazwa hosta).

- Aby korzystać z innej usługi DDNS, kliknij pozycję FREE TRIAL (BEZPŁATNA WERSJA PRÓBNA) i zarejestruj się w trybie online. Uzupełnij pola User Name or E-mail Address (Nazwa użytkownika lub adres e-mail) i Password or DDNS key (Hasło lub klucz DDNS).
- **Włącz symbole wieloznaczne:** Włącz obsługę symboli wieloznacznych, jeśli jest to wymagane przez usługę DDNS.

UWAGI:

Usługa DDNS nie będzie działać w poniższych przypadkach:

- Router bezprzewodowy korzysta z prywatnego adresu IP sieci WAN (192.168.x.x, 10.x.x.x lub 172.16.x.x), na co wskazuje tekst w kolorze żółtym.
- Router może być w sieci, która korzysta z wielu tabel NAT.

3.11.7 NAT Passthrough (Przekazywanie NAT)

Funkcja NAT Passthrough (Przekazywanie NAT) umożliwia przekazywanie połączeń wirtualnej sieci prywatnej (VPN) przez router do klientów sieciowych. Pozycje PPTP Passthrough (Przekazywanie PPTP), L2TP Passthrough (Przekazywanie L2TP), IPsec Passthrough (Przekazywanie IPsec) i RTSP Passthrough (Przekazywanie RTSP) są domyślnie włączone.

Aby włączyć/wyłączyć ustawienia funkcji NAT Passthrough (Przekazywanie NAT), przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > wybierz NAT Passthrough (Przekazywanie NAT)**. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

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

3.12 Wireless (Sieć bezprzewodowa)

3.12.1 WPS

WPS (Wi-Fi Protected Setup) to standard zabezpieczeń sieci bezprzewodowej, który ułatwia łączenie urządzeń z siecią bezprzewodową. Funkcję WPS można skonfigurować za pomocą kodu PIN lub przycisku WPS.

UWAGA: Należy upewnić się, że urządzenia obsługują funkcję WPS.

Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS button.

Enable WPS	<input checked="" type="checkbox"/>
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled <input type="button" value="Reset"/> <small>Pressing the reset button resets the network name (SSID) and WPA encryption key.</small>
AP PIN Code	51246044

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method: Push button Client PIN Code

W celu włączenia funkcji WPS w sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > WPS**.
2. W polu **Enable WPS (Włącz funkcję WPS)** przesunij suwak do opcji **ON (WŁ.)**.
3. Funkcja WPS korzysta domyślnie z częstotliwości 2,4 GHz. Aby zmienić częstotliwość na 5 GHz, ustaw dla funkcji WPS opcję **OFF (WYŁ.)**, kliknij pozycję **Switch Frequency (Przełącz częstotliwość)** w polu **Current Frequency (Bieżąca częstotliwość)**, a następnie ponownie ustaw dla funkcji WPS opcję **ON (WŁ.)**.

UWAGA: Funkcja WPS obsługuje uwierzytelnianie za pomocą metody Open System (Otwarty system), WPA-Personal i WPA2-Personal. Funkcja WPS nie obsługuje sieci bezprzewodowych korzystających z metody szyfrowania Shared Key (Klucz wspólny), WPA-Enterprise, WPA2-Enterprise ani RADIUS.

4. W polu WPS Method (Metoda WPS) wybierz opcję **Push Button (Przycisk polecenia)** lub **Client PIN Code (Kod PIN klienta)**. Po wybraniu opcji **Push Button (Przycisk polecenia)** przejdź do kroku 5. Po wybraniu opcji **Client PIN Code (Kod PIN klienta)** przejdź do kroku 6.
5. Aby skonfigurować funkcję WPS za pomocą przycisku WPS routera, należy wykonać poniższe czynności:
 - a. Kliknij przycisk **Start** lub naciśnij przycisk WPS z tyłu routera bezprzewodowego.
 - b. Naciśnij przycisk WPS na urządzeniu bezprzewodowym. Jest on zwykle oznaczony logo WPS.

UWAGA: Należy poszukać przycisku WPS na urządzeniu bezprzewodowym lub sprawdzić jego lokalizację w podręczniku użytkownika.

- c. Router bezprzewodowy rozpocznie wyszukiwanie dostępnych urządzeń WPS. Jeśli router bezprzewodowy nie znajdzie żadnych urządzeń WPS, przełączy się do trybu wstrzymania.
6. Aby skonfigurować funkcję WPS za pomocą kodu PIN klienta, należy wykonać poniższe czynności:
 - a. Znajdź kod PIN funkcji WPS na urządzeniu bezprzewodowym lub w jego podręczniku użytkownika.
 - b. Wprowadź kod PIN klienta w polu tekstowym.
 - c. Kliknij przycisk **Start** w celu przełączenia routera bezprzewodowego do trybu wyszukiwania funkcji WPS. Wskaźniki LED routera będą migać szybko trzy razy do momentu ukończenia konfiguracji WPS.

3.12.2 Bridge (Mostek)

Dzięki funkcji Bridge (Mostek) lub WDS (Wireless Distribution System) router bezprzewodowy firmy ASUS może łączyć się z innym bezprzewodowym punktem dostępowym w trybie wyłączności, przy jednoczesnym braku dostępu innych urządzeń lub stacji bezprzewodowych do routera bezprzewodowego firmy ASUS. Można to także traktować jako repeater bezprzewodowy, za pomocą którego router bezprzewodowy firmy ASUS komunikuje się z innym punktem dostępowym lub urządzeniem bezprzewodowym.

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your ASUS Router to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first. [Click Here to modify](#). Please refer to this [FAQ](#) for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. [Click Here to modify](#)

You are currently using the Auto channel. [Click Here to modify](#)

Basic Config

2.4 GHz MAC	<input type="text" value="C8:7F:54:12:69:C8"/>
5 GHz MAC	<input type="text" value="C8:7F:54:12:69:CC"/>
Band	<input type="text" value="2.4 GHz"/>
AP Mode	<input type="text" value="AP Only"/>
Connect to APs in list	<input type="radio"/> Yes <input type="radio"/> No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
<input type="text"/>	<input type="button" value="⊕"/>
No data in table.	

W celu skonfigurowania mostka bezprzewodowego:


1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz WDS.**
2. Wybierz pasmo częstotliwości mostka bezprzewodowego.
3. W polu **AP Mode (Tryb AP)** wybierz jedną z dostępnych opcji:

- **Tylko AP:** Wyłączenie funkcji mostka bezprzewodowego.
- **Tylko WDS:** Włączenie funkcji mostka bezprzewodowego bez możliwości łączenia się innych urządzeń/stacji bezprzewodowych z routerem.
- **HYBRID (HYBRYDOWY):** Włączenie funkcji mostka bezprzewodowego z możliwością łączenia się innych urządzeń/stacji bezprzewodowych z routerem.

UWAGA: W trybie Hybrid (Hybrydowy) urządzenia bezprzewodowe połączone z routerem bezprzewodowym firmy ASUS będą miały zapewnioną tylko połowę szybkości połączenia punktu dostępowego.

4. W polu **Connect to APs in list (Nawiążuj połączenia z punktami dostępowymi z listy)** kliknij opcję **Yes (Tak)**, aby połączenia były nawiązywane z punktami dostępowymi z listy Remote AP List (Lista zdalnych punktów dostępowych).
5. W polu **Control Channel (Kanał kontrolny)** wybierz kanał działania mostka bezprzewodowego. Wybierz opcję **Auto (Automat.)**, aby router automatycznie wybierał najmniej zakłócony kanał.

UWAGA: Dostępność kanałów zależy od kraju lub regionu.

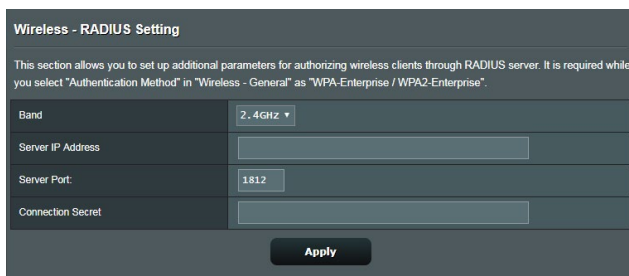
6. W obszarze **Remote AP List (Lista zdalnych punktów dostępowych)** wprowadź adres MAC i kliknij przycisk **Add (Dodaj)**  w celu wprowadzenia adresu MAC innego dostępnego punktu dostępowego.

UWAGA: Ustawienie Control Channel (Kanał kontrolny) każdego dodanego do listy punktu dostępowego powinno być takie samo jak w przypadku routera bezprzewodowego firmy ASUS.

7. Kliknij przycisk **Apply (Zastosuj)**.

3.12.3 RADIUS Setting (Ustawienia serwera RADIUS)

Pozycja RADIUS (Remote Authentication Dial In User Service) Setting (Ustawienia serwera RADIUS) zapewnia dodatkową warstwę zabezpieczeń w przypadku wybrania metody uwierzytelniania WPA-Enterprise, WPA2-Enterprise lub Radius with 802.1x (Radius z 802.1x).



Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	2.4GHz ▼
Server IP Address	<input type="text"/>
Server Port	1812
Connection Secret	<input type="text"/>

Apply

W celu skonfigurowania ustawień serwera RADIUS w sieci bezprzewodowej:

1. Upewnij się, że wybrana metoda uwierzytelniania routera bezprzewodowego to WPA-Enterprise, WPA2-Enterprise lub Radius with 802.1x (Radius z 802.1x).
2. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz zakładkę RADIUS Setting (Ustawienia serwera RADIUS).**
3. Wybierz pasmo częstotliwości.
4. W polu **Server IP Address (Adres IP serwera)** wprowadź adres IP serwera RADIUS.
5. W polu **Connection Secret (Tajne połączenie)** przypisz hasło zapewniające dostęp do serwera RADIUS.
6. Kliknij przycisk **Apply (Zastosuj).**

3.12.4 Professional (Profesjonalne)

Na ekranie Professional (Profesjonalne) dostępne są opcje konfiguracji zaawansowanej.

UWAGA: Zalecane jest zachowanie wartości domyślnych tego ekranu.

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

Na ekranie **Professional Settings (Ustawienia profesjonalne)**

można skonfigurować następujące pozycje:

- **Band (Pasma):** Wybierz pasmo częstotliwości dla pozycji, dla których zastosowanie mają ustawienia profesjonalne.
- **Włącz łączność radiową:** Wybierz opcję **Yes (Tak)**, aby włączyć sieć bezprzewodową. Wybierz opcję **No (Nie)**, aby wyłączyć sieć bezprzewodową.

- **Enable wireless scheduler (Włącz harmonogram sieci bezprzewodowej):** Można wybrać 24-godzinny lub 12-godzinny format zegara. Kolor w tablicy wskazuje Allow (Zezwól) lub Deny (Odmów) . Kliknij każdą ramkę, aby zmienić ustawienia godziny dni tygodnia i po zakończeniu kliknij OK .

Wireless - Professional

* Reminder: The System time zone is different from your locale setting.

Clock Format: 24-hour ▾ Allow Deny

Active Schedule

System Time: Thu, Aug 23 06:59:27 2018

Select All	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00 ~ 01							
01 ~ 02							
02 ~ 03							
03 ~ 04							
04 ~ 05							
05 ~ 06							
06 ~ 07							
07 ~ 08							
08 ~ 09							
09 ~ 10							
10 ~ 11							
11 ~ 12							
12 ~ 13							
13 ~ 14							
14 ~ 15							
15 ~ 16							
16 ~ 17							
17 ~ 18							
18 ~ 19							
19 ~ 20							
20 ~ 21							
21 ~ 22							
22 ~ 23							
23 ~ 24							

Cancel OK

- **Ustawiaj izolowany punkt dostępowy:** Pozycja Set AP isolated (Ustawiaj izolowany punkt dostępowy) uniemożliwia wzajemną komunikację urządzeń bezprzewodowych połączonych z daną siecią. Funkcja ta jest przydatna, jeśli z daną siecią często łączy się lub rozłącza wielu gości. Wybierz opcję **Yes (Tak)**, aby włączyć tę funkcję lub wybierz opcję **No (Nie)**, aby ją wyłączyć.
- **Szybkość multimiisji (Mb/s):** Wybierz szybkość przesyłania w ramach multimiisji lub wybierz opcję **Disable (Wyłącz)** w celu wyłączenia jednoczesnych pojedynczych transmisji.

- **Typ preambuły:** Za pomocą pozycji Preamble Type (Typ preambuły) określany jest czas, w którym router przeprowadza kontrolę CRC (Cyclic Redundancy Check). CRC jest metodą wykrywania błędów podczas transmisji danych. Wybierz opcję **Short (Krótko)** w przypadku zajętej sieci bezprzewodowej o dużym ruchu sieciowym. Wybierz opcję **Long (Długo)**, jeśli sieć bezprzewodowa jest złożona ze starszych modeli urządzeń bezprzewodowych.
- **Próg RTS:** Wybierz niższą wartość dla pozycji RTS (Request to Send) Threshold (Próg RTS) w celu usprawnienia komunikacji bezprzewodowej w przypadku zajętej lub zakłócannej sieci bezprzewodowej o dużym ruchu sieciowym i z wieloma urządzeniami bezprzewodowymi.
- **Interwał DTIM:** Pozycja DTIM (Delivery Traffic Indication Message) Interval (Interwał DTIM) lub Data Beacon Rate (Częstotliwość wysyłania ramek beacon) to czas do momentu wysłania sygnału do urządzenia bezprzewodowego w trybie uśpienia z informacją o oczekującej dostawie pakietu danych. Domyślna wartość to trzy milisekundy.
- **Częstotliwość wysyłania ramek beacon:** Pozycja Beacon Interval (Częstotliwość wysyłania ramek beacon) to czas między jednym pakietem DTIM a kolejnym. Domyślna wartość to 100 milisekund. W przypadku niestabilnego połączenia bezprzewodowego lub urządzeń korzystających z roamingu należy ustawić mniejszą wartość pozycji Beacon Interval (Częstotliwość wysyłania ramek beacon).
- **Włącz tryb TX Bursting:** Pozycja Enable TX Bursting (Włącz funkcję TX Bursting) umożliwia zwiększenie szybkości transmisji między routerem bezprzewodowym a urządzeniami 802.11g.
- **Włącz tryb WMM APSD:** Pozycja Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) (Włącz tryb WMM APSD) usprawnia zarządzanie energią urządzeń bezprzewodowych. Wybierz opcję **Disable (Wyłącz)**, aby wyłączyć tryb WMM APSD.

4 Narzędziowych

4.1 Device Discovery

Device Discovery to narzędzie ASUS WLAN, które wykrywa wersję routera bez przewodowego ASUS, i umożliwia konfigurację ustawień sieci bezprzewodowej.

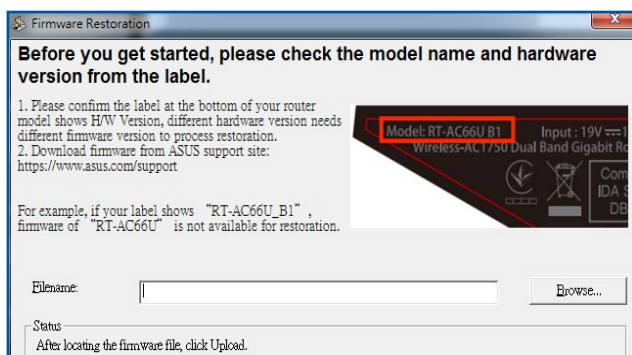
Uruchamianie narzędzia Device Discovery:

- Na pulpicie komputera, kliknij **Start > All Programs (Wszystkie programy) > ASUS Utility > Wireless Router (Router Bezprzewodowy) > Device Discovery.**

UWAGA: W przypadku ustawienia routera w trybie punktu dostępowego w celu uzyskania adresu IP routera należy skorzystać z narzędzia Device Discovery (Wykrywanie urządzeń).

4.2 Firmware Restoration

Narzędzie Firmware Restoration (Odtwarzanie oprogramowania) wykorzystywane jest w routerze bezprzewodowym ASUS w przypadku niepowodzenia procesu aktualizacji oprogramowania. Umożliwia ono wczytanie określonego oprogramowania. Proces trwa około trzech do czterech minut.



WAŻNE! Przed skorzystaniem z narzędzia Firmware Restoration (Odtwarzanie oprogramowania) uruchomić tryb ratunkowy.

UWAGA: Funkcja ta nie jest obsługiwana w systemie MAC OS.

Uruchomienie trybu ratunkowego i użycie narzędzia Firmware Restoration (Odtwarzanie oprogramowania sprzętowego):

1. Odłącz router bezprzewodowy od źródła zasilania.
2. Przytrzymaj wciśnięty przycisk Reset na tylnym panelu i jednocześnie podłącz router bezprzewodowy do zasilania. Kiedy dioda zasilania na panelu czołowym powoli miga wskazując, że znajduje się on w trybie ratunkowym, zwolnij przycisk Reset.
3. Ustaw statyczny adres IP komputera i wprowadź poniższe wartości w celu skonfigurowania ustawień protokołu TCP/IP:

Adres IP: 192.168.1.x

Maska podsieci: 255.255.255.0

4. Na pulpicie komputera kliknąć **Start (Start) > All Programs (Wszystkie programy) > ASUS Utility (Narzędzie ASUS) > Wireless Router (Router bezprzewodowy) > Firmware Restoration (Odtwarzanie oprogramowania sprzętowego)**.
5. Wybrać plik oprogramowania, a następnie kliknąć przycisk **Upload (Prześlij)**.

UWAGA: Nie jest to narzędzie do aktualizacji oprogramowania sprzętowego i nie może być używane na pracującym routerze bezprzewodowym ASUS. Normalna aktualizacja oprogramowania sprzętowego musi być wykonywana przez interfejs przeglądarki sieciowej. Dodatkowe informacje, patrz **Rozdział 3: Konfiguracja ustawień ogólnych i zaawansowanych**.

5 Rozwiązywanie problemów

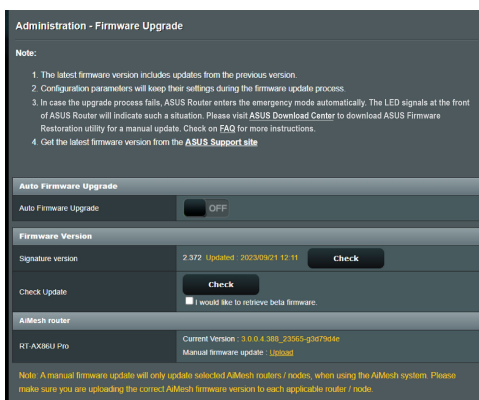
W rozdziale tym omówiono rozwiązania problemów, które mogą wystąpić podczas korzystania z routera. W przypadku pojawienia się problemów, których nie opisano w tym rozdziale, należy przejść do witryny pomocy technicznej firmy ASUS dostępnej pod adresem: <https://www.asus.com/support> w celu uzyskania dalszych informacji o produkcie oraz szczegółowych danych kontaktowych działu pomocy technicznej firmy ASUS.

5.1 Rozwiązywanie podstawowych problemów

W przypadku wystąpienia problemu z routerem należy najpierw wykonać podstawowe czynności opisane w poniższej części, a dopiero potem poszukać innych rozwiązań.

Uaktualnij oprogramowanie sprzętowe do najnowszej wersji.

1. Uruchom sieciowy interfejs graficzny. Przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**. Kliknij przycisk **Check (Sprawdź)** w celu sprawdzenia dostępności najnowszej wersji oprogramowania sprzętowego.



2. Jeśli najnowsza wersja oprogramowania sprzętowego będzie dostępna, przejdź do witryny globalnej firmy ASUS [https://www.asus.com/Networking/ZenWiFi BD4/HelpDesk/](https://www.asus.com/Networking/ZenWiFi_BD4/HelpDesk/) i pobierz najnowszą wersję oprogramowania sprzętowego.
3. Na stronie **Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)** kliknij przycisk **Browse (Przeglądaj)**, aby zlokalizować plik oprogramowania sprzętowego.
4. Kliknij przycisk **Upload (Załaduj)**, aby uaktualnić oprogramowanie sprzętowe.

Uruchom ponownie sieć, wykonując czynności w następującej kolejności:

1. Wyłącz modem.
2. Odłącz modem od zasilania.
3. Wyłącz router i komputery.
4. Podłącz modem do zasilania.
5. Włącz modem i odczekaj 2 minuty.
6. Włącz router i odczekaj 2 minuty.
7. Włącz komputery.

Sprawdź, czy ustawienia sieci bezprzewodowej komputera są zgodne z ustawieniami routera.

- Podczas nawiązywania połączenia bezprzewodowego między komputerem i routerem należy upewnić się, że identyfikator SSID (nazwa sieci bezprzewodowej), metoda szyfrowania i hasło są prawidłowe.

Sprawdź, czy ustawienia sieciowe są prawidłowe.

- Każdy klient w sieci powinien mieć odpowiedni adres IP. Firma ASUS zaleca przypisywanie adresów IP komputerom w sieci za pomocą serwera DHCP routera bezprzewodowego.

- W przypadku niektórych dostawców usług internetowych zapewnianych przez modem kablowy wymagane jest używanie adresu MAC komputera, dla którego zarejestrowano wstępnie konto. Adres MAC można sprawdzić za pomocą sieciowego interfejsu graficznego, na stronie **Network Map (Mapa sieci) > Clients (Klienci)** po umieszczeniu wskaźnika myszy nad urządzeniem w pozycji **Client status (Stan klienta)**.

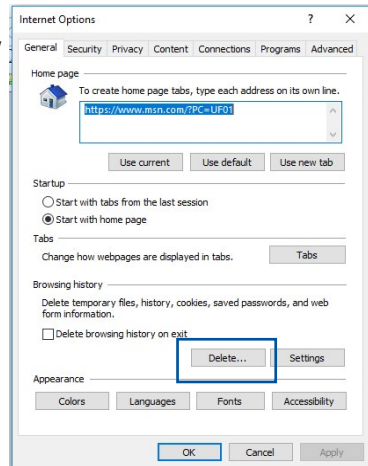


5.2 Często zadawane pytania (FAQs)

Nie mogę uzyskać dostępu do interfejsu graficznego routera przy użyciu przeglądarki sieci Web.

- Jeśli komputer jest podłączony w sposób przewodowy, sprawdź połączenie kabla Ethernet i stan diody LED zgodnie z opisem w poprzedniej części.
- Upewnij się, że używane dane logowania są prawidłowe. Upewnij się, że podczas wprowadzania danych logowania klawisz Caps Lock jest wyłączony.
- Usuń pliki cookie i pliki w przeglądarce sieci Web. W przypadku programu Internet Explorer należy wykonać poniższe czynności:
 1. Uruchom program Internet Explorer, a następnie kliknij kolejno pozycje **Tools (Narzędzia) > Internet Options (Opcje internetowe)**.

2. Na karcie **General (Ogólne)**, w obszarze **Browsing history (Historia przeglądania)** kliknij przycisk **Delete... (Usuń...)**, wybierz pozycję **Temporary Internet Files and website files (Tymczasowe pliki internetowe pliki witryn internetowych)** i **Cookies and website data (Cookie i dane witryny internetowej)**, a następnie kliknij przycisk **Delete (Usuń)**.



UWAGI:

- Polecenia usuwania plików cookie i plików zależą od przeglądarki sieci Web.
- W celu automatycznego uzyskiwania adresów IP należy wyłączyć ustawienia serwera proxy, anulować połączenie telefoniczne i wprowadzić ustawienia protokołu TCP/IP. Bardziej szczegółowe informacje można znaleźć w rozdziale 1 niniejszego podręcznika użytkownika.
- Należy używać kabli Ethernet CAT5e lub CAT6.

Klient nie może ustanowić połączenia bezprzewodowego z routerem.

UWAGA: W przypadku wystąpienia problemów z nawiązaniem połączenia z siecią 5 Ghz należy sprawdzić, czy urządzenie sieciowe obsługuje częstotliwość 5 Ghz i czy jest wyposażone w funkcje podwójnego pasma.

- **Poza zakresem:**
 - Przesuń router bliżej klienta bezprzewodowego.
- **Wyłączono serwer DHCP:**
 1. Uruchom sieciowy interfejs graficzny. Przejdź kolejno do pozycji **General (Ogólne)** > **Network Map (Mapa sieci)** > **Clients (Klienci)** i wyszukaj urządzenie, które chcesz połączyć z routerem.
 2. Jeśli nie można znaleźć urządzenia w pozycji **Network Map (Mapa sieci)**, przejdź kolejno do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **LAN (Sieć LAN)** > **DHCP Server (Serwer DHCP)**, lista **Basic Config (Konfiguracja podstawowa)**, zaznacz opcję **Yes (Tak)** dla pozycji **Enable the DHCP Server (Włącz serwer DHCP)**.

LAN - DHCP Server

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

Basic Config

Enable the DHCP Server Yes No

ASUS Router's Domain Name

IP Pool Starting Address

IP Pool Ending Address

Lease time

Default Gateway

DNS and WINS Server Setting

DNS Server 1

DNS Server 2

Advertise router's IP in addition to user-specified DNS Yes No

WINS Server

Manual Assignment

Enable Manual Assignment Yes No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Host Name (Optional)	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="⊕"/>

No data in table.

Apply

- Ukryto identyfikator SSID. Jeśli urządzenie wyszukuje identyfikatory SSID innych routerów, ale nie może znaleźć identyfikatora SSID posiadanego routera, przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > General (Ogólne)**, zaznacz opcję **(Nie)** dla pozycji **Hide SSID (Ukryj SSID)** i zaznacz opcję **Auto (Automat.)** dla pozycji **Control Channel (Kanał kontrolny)**.

Wireless - General

Set up the wireless related information below.

Enable Smart Connect	<input type="checkbox"/> OFF
Band	2.4 GHz
Network Name (SSID)	L.LAO
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Mode	Auto <input checked="" type="checkbox"/> Inty Protection <input type="checkbox"/> Disable 11b
802.11ax / WiFi 6 mode	Enable <small>If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check FAQ</small>
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 Mhz
Control Channel	Auto <small>Current Control Channel: 5</small>
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	***** Weak
Group Key Rotation Interval	3600

Apply

- Jeśli używana jest karta sieci bezprzewodowej, sprawdź, czy używany kanał bezprzewodowy jest zgodny z kanałami dostępnymi w danym kraju/regionie. Jeśli nie, dostosuj kanał, pasmo kanału i tryb bezprzewodowy.
- Jeśli nawiązanie połączenia bezprzewodowego z routerem jest nadal niemożliwe, można przywrócić domyślne ustawienia fabryczne routera. W interfejsie graficznym routera kliknij kolejno pozycje **Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Administration - Restore/Save/Upload Setting

This function allows you to save current settings of ASUS Router to a file, or load settings from a file.

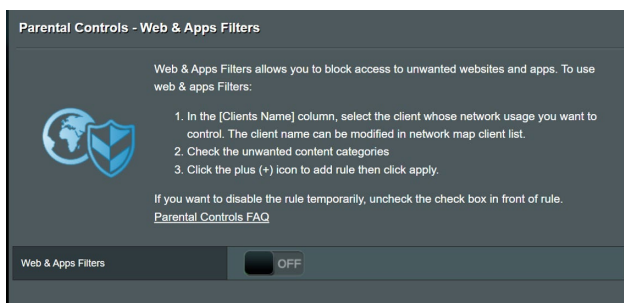
Factory default	<input type="checkbox"/> Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History
Save setting	<input type="checkbox"/> Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.
Restore setting	<input type="checkbox"/> Transfer ASUS DNS name

Niedostępny Internet.

- Sprawdź, czy router może nawiązać połączenie z adresem IP sieci WAN usługodawcy internetowego. Aby to zrobić, uruchom sieciowy interfejs graficzny, przejdź do pozycji **General (Ogólne) > Network Map (Mapa sieci)** i sprawdź pozycję **Internet Status (Stan połączenia z Internetem)**.
- Jeśli router nie może nawiązać połączenia z adresem IP sieci WAN usługodawcy internetowego, uruchom ponownie sieć zgodnie z opisem w części **Restart your network in following sequence (Uruchom ponownie sieć, wykonując czynności w następującej kolejności)** w rozdziale **Rozwiązywanie podstawowych problemów**.



- Urządzenie zostało zablokowane za pomocą funkcji Parental Control (Kontrola rodzicielska). Przejdź do pozycji **General (Ogólne) > Parental Controls (Kontrola rodzicielska)** i sprawdź, czy urządzenie znajduje się na liście. Jeśli urządzenie znajduje się na liście **Client Name (Nazwa klienta)**, usuń je za pomocą przycisku **Delete (Usuń)** lub dostosuj ustawienia Time Management (Zarządzanie czasem).



- Jeśli dostęp do Internetu jest nadal niemożliwy, uruchom ponownie komputer, a następnie sprawdź adres IP i adres bramy sieci.

Nie pamiętam identyfikatora SSID (nazwy sieci) lub hasła sieciowego.

- Skonfiguruj nowy identyfikator SSID i klucz szyfrowania za pomocą połączenia przewodowego (kabel Ethernet). Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Network Map (Mapa sieci)**, kliknij ikonę routera, wprowadź nowy identyfikator SSID i klucz szyfrowania, a następnie kliknij przycisk **Apply (Zastosuj)**.
- Przywróć ustawienia domyślne routera. Uruchom sieciowy interfejs graficzny, przejdź do pozycji **Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Jak przywrócić domyślne ustawienia systemu?

- Przejdź do pozycji **Administration (Administracja) > Restore/Save/Upload Setting (Przywróć/Zapisz/Załaduj ustawienia)** i kliknij przycisk **Restore (Przywróć)**.

Niepowodzenie uaktualnienia oprogramowania sprzętowego.

Uruchom tryb ratunkowy i skorzystaj z narzędzia Firmware Restoration (Odtwarzanie oprogramowania sprzętowego). Informacje na temat korzystania z narzędzia Firmware Restoration (Odtwarzanie oprogramowania sprzętowego) można znaleźć w części **4.2 Odtwarzanie oprogramowania sprzętowego**.

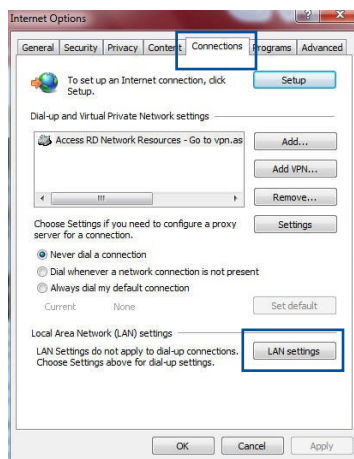
Nie można uzyskać dostępu do sieciowego interfejsu graficznego

Przed konfiguracją routera bezprzewodowego wykonać czynności opisane w tej części dla komputera hosta i klientów sieciowych.

A. Wyłączyć serwer proxy jeżeli jest włączony

Windows®

1. Kliknij przycisk **Start** > **Internet Explorer** w celu uruchomienia przeglądarki internetowej.
2. Kliknij przycisk **Tools (Narzędzia)** > **Internet options (Opcje internetowe)** > **Connections (Połączenia)** > **LAN settings (Ustawienia sieci LAN)**.

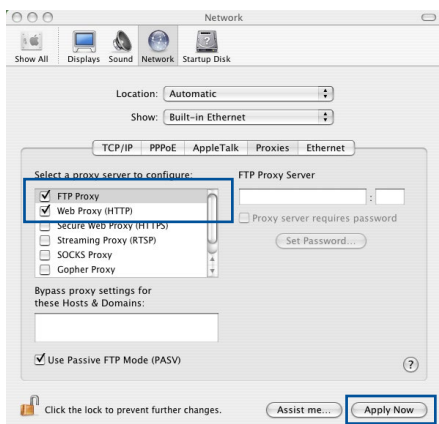


3. Na ekranie Local Area Network (LAN) Settings (Ustawienia sieci lokalnej (LAN)) odznacz opcję **Use a proxy server for your LAN (Użyj serwera proxy dla sieci LAN)**.
4. Po zakończeniu kliknij przycisk **OK**.



MAC OS

1. W przeglądarce Safari kliknąć **Safari > Preferences (Preferencje) > Advanced (Zaawansowane) > Change Settings... (Zmień ustawienia...)**.
2. Na ekranie Network (Sieć) usunąć zaznaczenie **FTP Proxy (Proxy FTP) i Web Proxy (HTTP) (Proxy www (HTTP))**.
3. Po zakończeniu kliknąć przycisk **Apply Now (Zastosuj teraz)**.

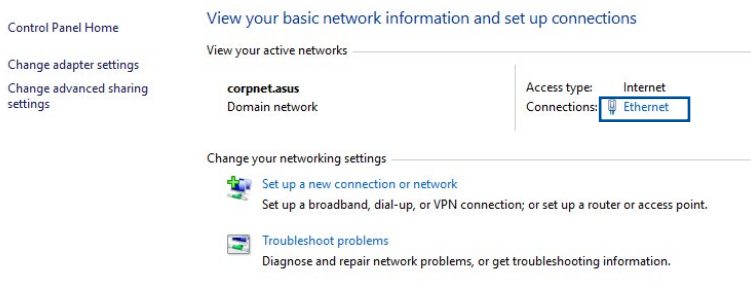


UWAGA: Szczegółowe informacje dotyczące wyłączenia serwera proxy, patrz funkcja pomocy danej przeglądarki.

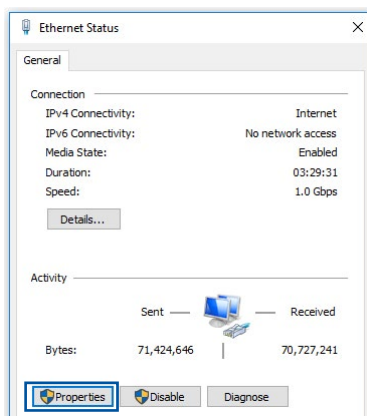
B. Skonfigurować ustawienia TCP/IP do automatycznego uzyskiwania adresu IP.

Windows®

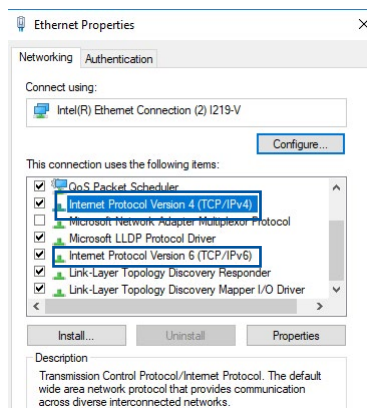
1. Kliknij przycisk **Start > Control Panel (Panel Sterowania) > Network and Sharing Center (Centrum sieci i udostępniania)**, następnie kliknij połączenie sieciowe, aby wyświetlić okno stanu.



2. Kliknij pozycję **Properties** (**Właściwości**), aby wyświetlić okno Ethernet Properties (**Właściwości sieci Ethernet**).



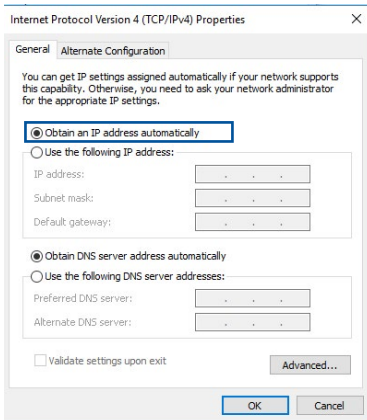
3. Zaznacz opcję **Internet Protocol Version 4 (TCP/IPv4)** (**Protokół internetowy w wersji 4 (TCP/IPv4)**) lub **Internet Protocol Version 6 (TCP/IPv6)** (**Protokół internetowy w wersji 6 (TCP/IPv6)**), a następnie kliknij przycisk **Properties** (**Właściwości**).




4. W celu automatycznego uzyskania ustawień IPv4 IP, zaznacz opcję **Obtain an IP address automatically** (**Automatycznie uzyskaj adres IP**).

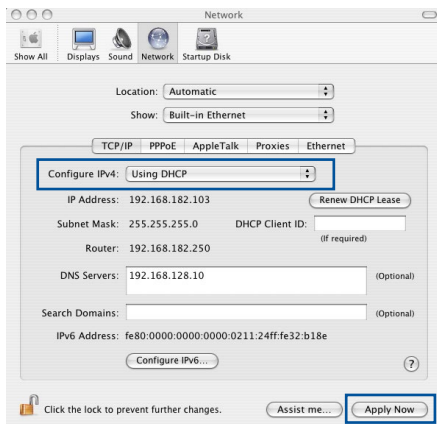
W celu automatycznego uzyskania ustawień IPv6 IP, zaznacz opcję **Obtain an IPv6 address automatically** (**Automatycznie uzyskaj adres IPv6**).

5. Po zakończeniu kliknij przycisk **OK**.



MAC OS

1. Kliknij ikonę Apple  umieszczoną w górnej lewej części ekranu.
2. Kliknij polecenie **System Preferences (Preferencje systemu) > Network (Sieć) > Configure... (Konfiguruj...)**.
3. Na zakładce **TCP/IP** **wybierz Using DHCP (Z użyciem DHCP)** na liście rozwijalnej **Configure IPv4 (Konfiguruj IPv4)**.
4. Po zakończeniu kliknąć przycisk **Apply Now (Zastosuj teraz)**.

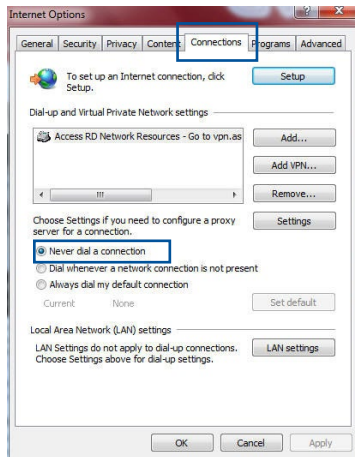


UWAGA: Informacje dotyczące konfiguracji ustawień połączenia TCP/IP komputera patrz pomoc systemu operacyjnego i funkcje wsparcia.

C. Wyłączyć połączenie dial-up jeżeli jest włączone.

Windows®

1. Kliknij przycisk **Start > Internet Explorer** w celu uruchomienia przeglądarki internetowej.
2. Kliknij przycisk **Tools (Narzędzia) > Internet options (Opcje internetowe) > Connections (Połączenia)**.
3. Zaznaczyć opcję **Never dial a connection (Nigdy nie wybieraj połączenia)**.
4. Po zakończeniu kliknij przycisk **OK**.



UWAGA: Szczegółowe informacje o wyłączeniu połączenia dial-up, patrz funkcja pomocy przeglądarki sieciowej.

Załączniki

GNU General Public License

Licensing information

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

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

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

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

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

Preamble

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

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

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

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

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

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

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

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

Terms & conditions for copying, distribution, & modification

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

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

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

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

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

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

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

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

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

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

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

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

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

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

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

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

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

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

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

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

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

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

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

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

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

NO WARRANTY

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

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

END OF TERMS AND CONDITIONS

Uwagi dotyczące bezpieczeństwa

Podczas korzystania z tego urządzenia należy zawsze stosować się do podstawowych zasad bezpieczeństwa, w tym m.in. do poniższych:



OSTRZEŻENIE!

- Przewody zasilające należy podłączać do gniazd elektrycznych o odpowiednim uziemieniu. Urządzenie należy podłączyć wyłącznie do znajdującego się w pobliżu gniazda elektrycznego, które jest łatwo dostępne.
- Jeśli uszkodzony został zasilacz nie należy próbować naprawiać go samemu. Należy skontaktować się z wykwalifikowanym technikiem serwisu lub ze sprzedawcą.
- NIE NALEŻY przykrywać szczelin wentylacyjnych komputera desktop PC, aby zapobiec przegrzaniu systemu.
- NIE NALEŻY montować tego urządzenia na wysokości większej niż 2 metry.
- Ten produkt należy używać w miejscach o temperaturze otoczenia w zakresie 0°C (32°F) do 40°C (104°F).
- Przed rozpoczęciem korzystania z urządzenia należy przeczytać instrukcję obsługi i zapoznać się z podanymi zakresami temperatur.
- W przypadku korzystania z tego urządzenia na lotniskach, w szpitalach, na stacjach benzynowych czy w warsztatach samochodowych należy zwrócić szczególną uwagę na kwestię ochrony bezpieczeństwa osobistego.
- Zakłócenia działania urządzeń medycznych: Między wszczepionymi urządzeniami medycznymi a produktami firmy ASUS należy zachować odległość wynoszącą co najmniej 15 cm (6 cali) w celu ograniczenia ryzyka wystąpienia zakłóceń w pracy tych urządzeń.
- Z urządzeń firmy ASUS należy korzystać w miejscach o dobrym sygnale, aby zminimalizować poziom promieniowania.
- Kobiety w ciąży nie powinny znajdować się blisko urządzenia, a także należy zachować odpowiednią odległość od dolnych partii brzucha w przypadku nastolatków.
- NIE NALEŻY korzystać z tego urządzenia w przypadku występowania widocznych defektów lub jeśli zostało ono zamoczone, uszkodzone lub przerobione. W takiej sytuacji urządzenie należy oddać do serwisu.



OSTRZEŻENIE!

- NIE NALEŻY umieszczać urządzeń na nierównych lub niestabilnych powierzchniach roboczych.
 - NIE NALEŻY umieszczać ani upuszczać przedmiotów na to urządzenie. Urządzenia nie należy wystawiać na wstrząsy mechaniczne, takie jak przygniecenia, wygięcia, nakłuwanie lub niszczenie.
 - NIE NALEŻY urządzenia demontować, otwierać, podgrzewać w kuchence mikrofalowej, spalać, malować ani wpychać jakichkolwiek przedmiotów do jego wnętrza.
 - Należy sprawdzić tabliczkę znamionową na spodzie produktu i upewnić się, że zasilacz jest zgodny z podanymi wartościami.
 - Urządzenie powinno znajdować się z dala od ognia i źródeł ciepła.
 - NIE NALEŻY umieszczać, upuszczać lub wpychać żadnych obcych obiektów na produkt. NIE NALEŻY korzystać z urządzenia podczas burz z wyładowaniami elektrycznymi.
 - Obwody wyjściowe PoE tego urządzenia należy łączyć wyłącznie z sieciami PoE, nie kierując ich do instalacji zewnętrznych.
 - Aby zapobiec porażeniu prądem elektrycznym, przed przeniesieniem systemu należy odłączyć kabel zasilający od gniazdka elektrycznego.
 - Należy korzystać wyłącznie z akcesoriów, które zostały zatwierdzone przez producenta urządzenia do użytku z tym modelem. Używanie innego rodzaju akcesoriów może spowodować unieważnienie gwarancji lub naruszenie lokalnych przepisów prawnych, a także może stanowić zagrożenie dla bezpieczeństwa. Aby uzyskać informacje o zatwierdzonych akcesoriach, należy skontaktować się z lokalnym sprzedawcą.
 - Korzystanie z tego urządzenia w sposób niezgodny z instrukcją obsługi może stwarzać ryzyko wystąpienia pożaru lub obrażeń ciała.
-

Obsługę i Pomoc

Odwiedź naszą wielojęzyczną witrynę internetową pod adresem <https://www.asus.com/support>.

