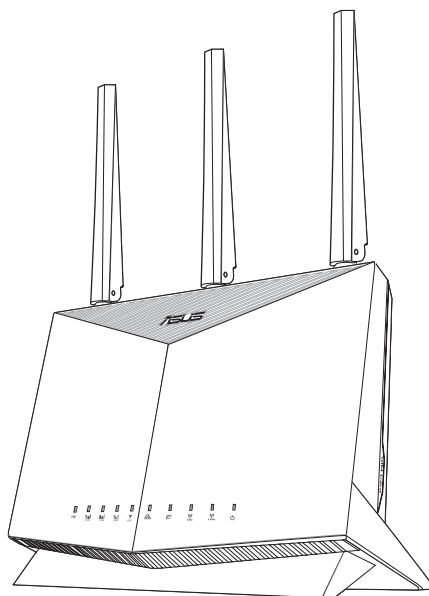


Podręcznik użytkownika

4G-AC86U

Bezprzewodowy router LTE
AC2600 Cat.12



ASUS
IN SEARCH OF INCREDIBLE

PL18231

Wydanie pierwsze

Maj 2021

Copyright © 2021 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 usługę gwarancyjną 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 WYRAŻNYCH 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 AGENCJI 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 UPREDZAŁA O MOŻLIWOŚCI ZAISTNIENIA TAKICH SZKÓD, W WYNIKU JAKIKOLWIEK DEFECTÓW 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!.....	7
1.2	Zawartość opakowania.....	7
1.3	Router bezprzewodow.....	8
1.4	Własności urządzenia	10
1.5	Instalacja karty nano SIM w routerze.....	11
2	Ustawienia sprzętu	
2.1	Instalacja routera.....	12
	A. Połączenie przewodowe.....	13
	B. Połączenie bezprzewodowe	14
2.2	QIS (Quick Internet Setup [Szybkie ustawienia połączenia z Internetem]) z autodetekcją.....	16
3	Konfiguracja ustawień ogólnych	
3.1	Korzystanie z pozycji Network Map (Mapa sieci)	21
	3.1.1 Wykonanie ustawień zabezpieczenia sieci bezprzewodowej.....	22
	3.1.2 System Status	23
	3.1.3 Zarządzanie klientami sieci	24
	3.1.4 Monitorowanie stanu Internetu	26
	3.1.5 Monitorowanie urządzenia USB	27
3.2	Tworzenie Guest Network (Sieć gości)	28
3.3	AiProtection	30
	3.3.1 Network Protection	31
	3.3.2 Konfiguracja funkcji Parental Controls (Kontrola rodzicielska)	35
3.4	Adaptacyjna funkcja QoS.....	39
	3.4.1 Monitor przepustowości	39

Spis treści

3.4.2	QoS.....	40
3.4.3	Historia stron sieci Web.....	41
3.5	Analizator ruchu	42
3.6	Używanie aplikacji USB.....	43
3.6.1	Korzystanie z funkcji AiDisk	43
3.6.2	Korzystanie z funkcji Servers Center (Centrum serwerów)	46
3.7	Korzystanie z aplikacji AiCloud 2.0	51
3.7.1	Funkcja Cloud Disk (Dysk w chmurze).....	51
3.7.2	Funkcja Smart Access (Dostęp inteligentny).....	53
3.7.3	Smart Sync.....	53
3.7.4	Serwer synchronizacji.....	55
3.7.5	Ustawienia	58
3.8	Obsługa wiadomości SMS.....	59
3.8.1	Wysyłanie wiadomości.....	59
3.8.2	Inbox.....	60
4	Konfiguracja ustawień zaawansowanych	
4.1	Wireless (Sieć bezprzewodowa)	61
4.1.1	General (Ogólne).....	61
4.1.2	WPS	63
4.1.3	WDS.....	65
4.1.4	Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych).....	67
4.1.5	RADIUS Setting (Ustawienia serwera RADIUS)	68
4.1.6	Professional (Profesjonalne).....	69
4.2	LAN (Sieć LAN).....	72
4.2.1	LAN IP (Adres IP sieci LAN).....	72
4.2.2	DHCP Server (Serwer DHCP)	73
4.2.3	Route (Trasa).....	75

4.2.4	IPTV	76
4.2.5	Sterowanie przełączaniem.....	76
4.3	WAN (Sieć WAN).....	77
4.3.1	Internet Connection (Połączenie internetowe).....	77
4.3.2	IPv6 (Protokół IPv6)	85
4.3.3	Dwie sieci WAN	86
4.3.4	Port Trigger (Wyzwalanie portów).....	88
4.3.5	Virtual Server/Port Forwarding (Serwer wirtualny/ Przekierowanie portów)	90
4.3.6	DMZ (Strefa DMZ)	93
4.3.7	DDNS (Usługa DDNS).....	94
4.3.8	NAT Passthrough (Przekazywanie NAT).....	95
4.4	IPv6 (Protokół IPv6)	96
4.5	Serwer sieci VPN	97
4.6	Zapora	98
4.6.1	Ogólne	98
4.6.2	Filtr adresów URL	98
4.6.3	Filtr słów kluczowych.....	99
4.6.4	Network Services Filter (Filtr usług sieciowych).....	99
4.6.5	Zapora IPv6	100
4.7	Administration (Administracja).....	101
4.7.1	Operation Mode (Tryb działania)	101
4.7.2	System.....	102
4.7.3	Aktualizacja firmware	104
4.7.4	Przywracanie/zapisywanie/przesyłanie ustawień..	105
4.8	System Log (Dziennik systemu)	106
4.9	Lista wsparcia funkcji mobilnej sieci szerokopasmowej	

Ethernet WAN	107
5 Narzędziowych	
5.1 Device Discovery	109
5.2 Firmware Restoration	110
5.3 Konfiguracja serwera wydruku	111
5.3.1 Udostępnianie drukarki ASUS EZ	111
5.3.2 Udostępnianie drukarki za pomocą protokołu LPR.....	115
5.4 Program Download Master	120
5.4.1 Konfigurowanie ustawień pobierania BitTorrent ...	122
5.4.2 Ustawienia pobierania NZB.....	123
5.4.3 Ustawienia eMule.....	123
6 Rozwiązywanie problemów	
6.1 Rozwiązywanie podstawowych problemów	124
6.2 Często zadawane pytania (FAQ)	127
Załączniki	
Notices	136
Informacje kontaktowe producenta.....	150

1 Poznanie routera bezprzewodowego

1.1 Witamy!

Dziękujemy za zakupienie bezprzewodowego routera LTE ASUS 4G-AC86U!

Bardzo wydajny i stylowy modem/router 4G-AC86U oferuje podwójne pasmo 2,4 GHz i 5 GHz zapewniające niezrównane, jednoczesne przesyłanie strumieni HD; serwer SMB, serwer UPnP AV i serwer FTP do udostępniania plików w trybie 24/7; możliwość obsługi 300 000 sesji oraz technologię ASUS Green Network, która zapewnia do 70% oszczędności energii.

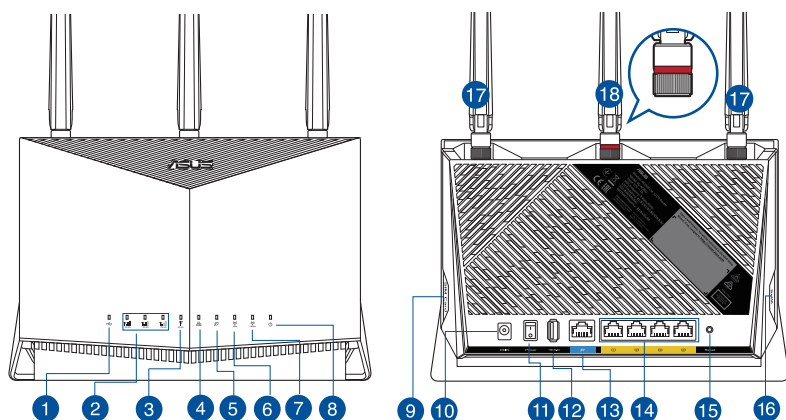
1.2 Zawartość opakowania

- | | |
|---|--|
| <input checked="" type="checkbox"/> 4G-AC86U Router bezprzewodowy | <input checked="" type="checkbox"/> Adapter zasilania |
| <input checked="" type="checkbox"/> Kabel sieciowy (RJ-45) | <input checked="" type="checkbox"/> Instrukcja szybkiego uruchomienia |
| <input checked="" type="checkbox"/> 2 x 3G/4G anteny | <input checked="" type="checkbox"/> 1x antena Wi-Fi (z czerwonym pierścieniem) |

UWAGA:

- Jeżeli którykolwiek z elementów jest uszkodzony lub brakuje go, skontaktować się z firmą ASUS celem uzyskania pomocy technicznej; patrz lista telefonów pomocy technicznej firmy ASUS 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 Dioda USB**
Wyłączona: Brak zasilania lub brak połączenia fizycznego.
Włączona: Połączenie fizyczne z urządzeniami USB.
-
- 2 Dioda siły sygnału 3G/4G**
1 zapalona dioda: Słaby sygnał
2 zapalone diody: Normlany sygnał
3 zapalone diody: Silny sygnał
-
- 3 Wskaźnik LED komórkowej sieci szerokopasmowej**
Biały: Nawiązano połączenie 4G.
Niebieski: Nawiązano połączenie 3G.
Czerwony: Brak komórkowego połączenia szerokopasmowego.
Wyłączona: Nie wykryto karty SIM.
-
- 4 LAN LED**
Wyłączona: Brak zasilania lub brak fizycznego połączenia z siecią LAN.
Włączona: Fizyczne połączenie z siecią lokalną (LAN).
-
- 5 WAN LED (Internet)**
Wyłączona: Brak zasilania lub brak fizycznego połączenia z siecią WAN.
Włączona: Fizyczne połączenie z siecią rozległą (WAN).
-
- 6 5GHz Wi-Fi LED**
Wyłączona: Brak sygnału 5 GHz.
Włączona: System bezprzewodowy jest gotowy.
Miganie: Przesyłanie lub odbieranie danych przez połączenie bezprzewodowe.
-
- 7 2.4GHz Wi-Fi LED**
Wyłączona: Brak sygnału 2.4 GHz.
Włączona: System bezprzewodowy jest gotowy.
Miganie: Przesyłanie lub odbieranie danych przez połączenie bezprzewodowe.
-

8	Dioda zasilania Wyłączona: Brak zasilania Włączona: Urządzenie jest gotowe. Powolne miganie: Tryb ratunkowy Szybkie miganie: Przetwarzanie WPS.
9	Gniazdo karty nano SIM Włóż do tego gniazda kartę nano SIM w celu nawiązania komórkowego połączenia szerokopasmowego.
10	Gniazdo zasilania (DCIN) Służy do podłączenia wtyczki zasilacza prądu przemiennego wchodzącego w skład zestawu i podłączenia routera do zasilacza.
11	Przycisk zasilania Naciśnij ten przycisk w celu włączenia lub wyłączenia zasilania systemu.
12	Gniazdo USB 2.0 Do tego gniazda można podłączyć urządzenia zgodne z USB 2.0, takie jak dyski twarde USB lub napędy flash USB.
13	Gniazdo sieci WAN (Internet) Służy do podłączania kabla sieciowego w celu ustanowienia połączenia z siecią rozległą.
14	Gniazda LAN 1 ~ 4 Służą do podłączania kabli sieciowych celem ustanowienia lokalnego połączenia sieciowego.
15	Przycisk RESET Przycisk służy do przywracania domyślnych ustawień systemu.
16	Przycisk WPS Przycisk służy do uruchamiania kreatora WPS.
17	Odlączane anteny LTE
18	Zamocowane na stałe anteny Wi-Fi

UWAGA:

- Stosować tylko zasilacz dołączony do zestawu. Zastosowanie innych zasilaczy może spowodować uszkodzenie urządzenia.
- Pamiętaj o włożeniu karty Micro SIM/USIM do gniazda karty, przed włączeniem zasilania routera.

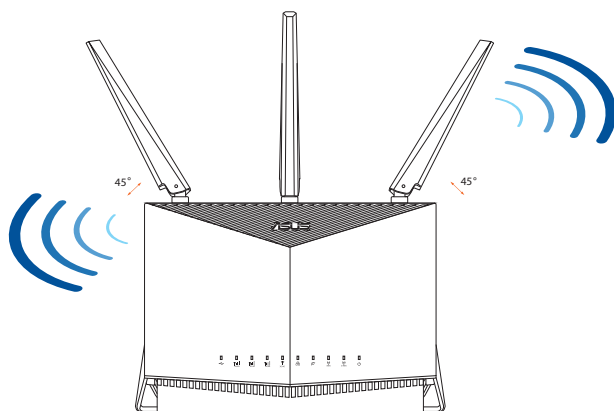
Warunki otoczenia:

Zasilacz sieciowy prądu stałego	Wyjście prądu stałego: +12 V przy prądzie maks. 3A		
Temperatura pracy	0~40°C	Przechowywanie	-40~70°C
Wilgotność działania	10 ~ 95%	Przechowywanie	5 ~ 95%

1.4 Własności urządzenia

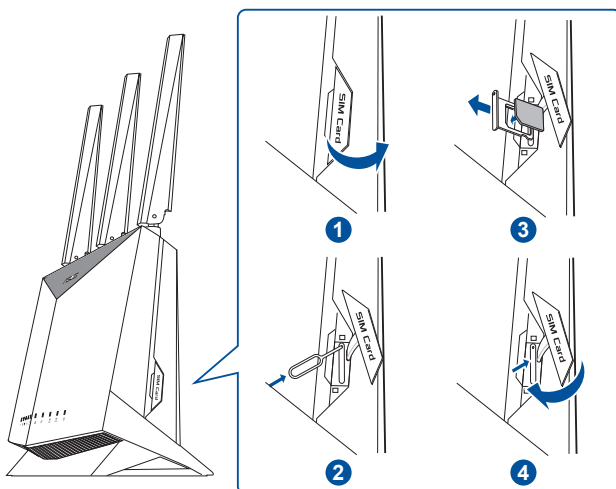
Dla zapewnienia najlepszej transmisji sygnału bezprzewodowego pomiędzy routerem bezprzewodowym a podłączonymi urządzeniami sieciowymi należy upewnić się, że:

- Router bezprzewodowy jest umieszczony centralnie, aby zapewnić maksymalny zasięg transmisji bezprzewodowej do urządzeń sieciowych.
- 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 sprzętowego można uzyskać na stronie internetowej ASUS pod adresem <http://www.asus.com>.
- Ustaw kierunek anten, tak jak na schemacie poniżej.



1.5 Instalacja karty nano SIM w routerze

1. Zdejmij pokrywę z gniazda karty nano SIM z prawej strony routera.
2. Wepchnij szpilkę do otworu tacy na kartę nano SIM, aby ją wysunąć.
3. Umieść kartę nano SIM na tacy.
4. Wciśnij tacę, aby ją zamknąć.



2 Ustawienia sprzętu

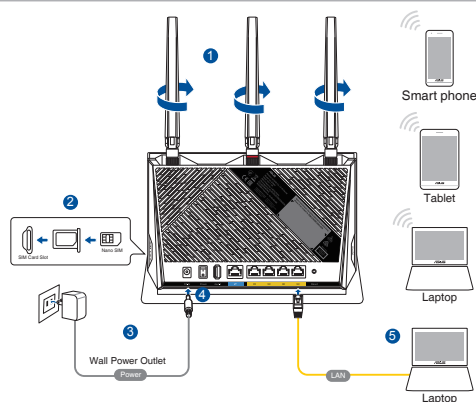
2.1 Instalacja routera

WAŻNE!

- Router bezprzewodowy należy zainstalować za pomocą połączenia przewodowego, aby uniknąć możliwych problemów z instalacją.
- Określenie lokalizacji najbliższego nadajnika sieci komórkowej może pomóc w uzyskaniu najmocniejszego sygnału.
- Domyślna nazwa użytkownika i hasło do interfejsu Web GUI to **admin** i **admin**.

UWAGI:

- Wskaźnik LED komórkowej sieci szerokopasmowej zaświeci się po włączeniu routera z zainstalowaną kartą nano SIM.
- Przed rozpoczęciem konfiguracji routera za pomocą kreatora QIS (kreator szybkiej konfiguracji połączenia z Internetem) należy upewnić się, że świeci się wskaźnik LED komórkowej sieci szerokopasmowej.
- Dostęp do Internetu można uzyskać przez komórkową sieć szerokopasmową lub Ethernet WAN.
- Automatyczne wykrywanie typu połączenia ISP jest wykonywane przy pierwszej konfiguracji routera z dostępem do komórkowej sieci szerokopasmowej lub po przywróceniu jego ustawień domyślnych. Podczas konfiguracji za pomocą kreatora QIS może być konieczne wprowadzenie kodu PIN karty SIM oraz informacji o APN (ustawienia internetowe) uzyskanych od usługodawcy internetowego (ISP).



A. Połączenie przewodowe

W celu wykonania ustawienia routera bezprzewodowego poprzez połączenie przewodowe:

1. Podłącz dwie anteny 3G/4G do złączy po lewej i prawej stronie, a antenę Wi-Fi do środkowego złącza.
2. Włóż kartę nano SIM do gniazda karty nano SIM.
3. Podłącz zasilacz do gniazda DC-IN routera i do gniazda elektrycznego.
4. Naciśnij przycisk zasilania, aby włączyć router z dostępem do komórkowej sieci szerokopasmowej i poczekaj kilka minut do momentu nawiązania połączenia z Internetem.
5. Podłącz komputer do routera przy użyciu kabla Ethernet.
6. Gdy zaświeci się wskaźnik LED ∇ komórkowej sieci szerokopasmowej, skonfiguruj router za pomocą kreatora QIS (kreator szybkiej konfiguracji połączenia z Internetem).
 - a. Otwórz przeglądarkę internetową i wpisz adres <http://router.asus.com> w celu wyświetlenia interfejsu Web GUI. Wykonaj instrukcje ekranowe, aby dokończyć konfigurację.
 - b. Konfigurację routera można także wykonać za pomocą aplikacji ASUS Router. Pobierz aplikację ASUS Router w celu konfiguracji routera przez urządzenia mobilne.
7. Ustaw hasło dla routera w celu zabezpieczenia go przed nieautoryzowanym dostępem.

Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New Password

Retype Password Show password



ASUS
Router



GET IT ON
Google Play

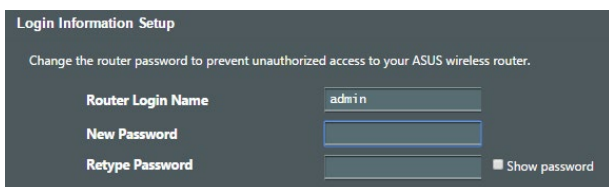


Download on the
App Store

Q | ASUS Router

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.
-



Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New Password

Retype Password Show password



ASUS
Router



ASUS Router

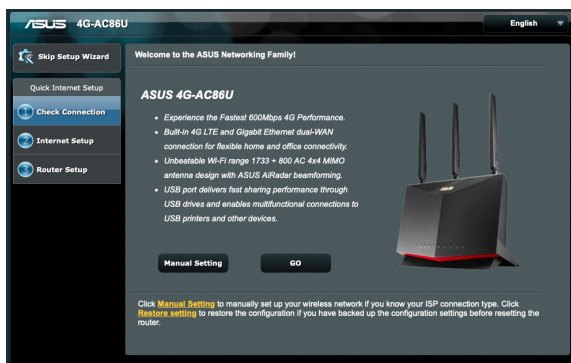
2.2 QIS (Quick Internet Setup [Szybkie ustawienia połączenia z Internetem]) z autodetekcją

Aby skonfigurować router za pomocą kreatora Quick Internet Setup (Szybka konfiguracja połączenia z Internetem):

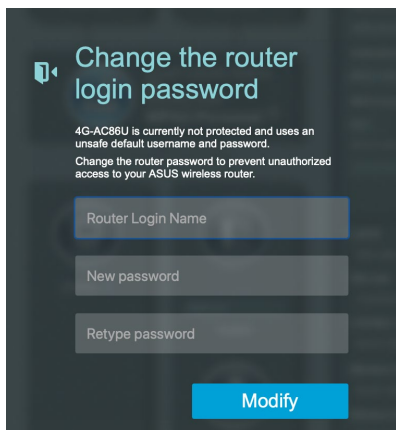
1. Naciśnij przycisk zasilania z tyłu routera. Upewnij się, że świecą następujące diody LED:
 - Dioda zasilania
 - 2.4GHz Wi-Fi LED
 - WAN or Mobile Broadband LED
 - 5GHz Wi-Fi LED
2. Uruchom przeglądarkę sieciową taką jak Internet Explorer, Google, Chrome, Firefox lub Safari.

UWAGA: Jeśli kreator QIS (Szybka konfiguracja połączenia z Internetem) nie uruchomi się automatycznie, należy wprowadzić adres <http://router.asus.com> w pasku adresu i odświeżyć przeglądarkę.

3. Zalogować się do interfejsu Web GUI. Strona QIS uruchamia się automatycznie. Domyślnie, nazwa użytkownika i hasło logowania dla interfejsu sieciowego GUI to "admin".

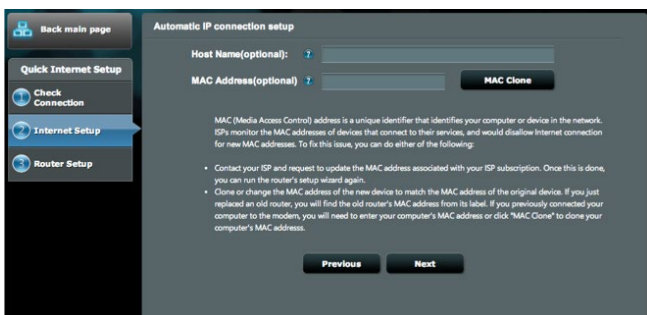


4. Przypisz nazwę logowania i hasło routera, a następnie kliknij przycisk **Next (Dalej)**. Wprowadzona nazwa logowania i hasło będą konieczne do zalogowania się do routera 4G-AC86U w celu wyświetlenia lub zmiany jego ustawień. Nazwę logowania i hasło routera można zapisać, aby móc korzystać z nich w przyszłości.



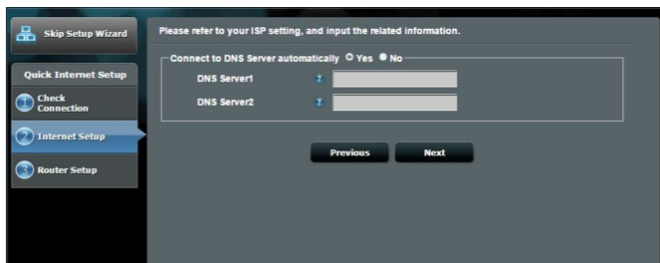
- Jeżeli podłączona jest sieć przewodowa, funkcja Quick Internet Setup (QIS - Szybkie ustawienia połączenia z Internetem) routera automatycznie wykryje czy połączenie ISP jest typu **Dynamic IP, PPPoE, PPTP, L2TP** i **Static IP**. Uzyskaj niezbędne informacje od dostawcy usług internetowych (ISP). Jeśli typem połączenia jest Dynamic IP (DHCP) [Dynamiczny adres IP (DHCP)], nastąpi automatyczne przekierowanie do następnego kroku kreatora QIS (Szybka konfiguracja połączenia z Internetem).

Typ połączenia Automatic IP (Automatyczny adres IP) (DHCP)



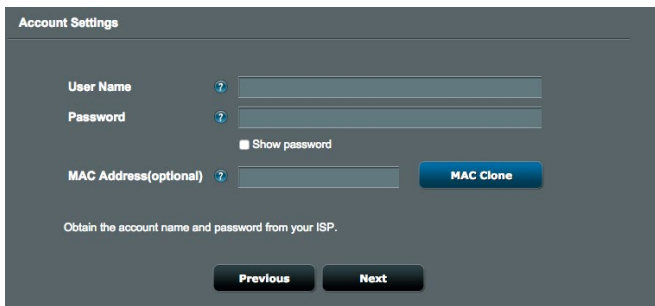
Typ połączenia PPPoE, PPTP i L2TP

Musisz wpisać nazwę konta i hasło otrzymane dla połączenia internetowego od dostawy usług.



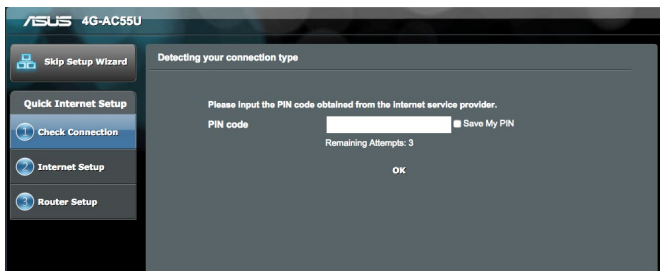
Typ połączenia Static IP (Stacyczny adres IP)

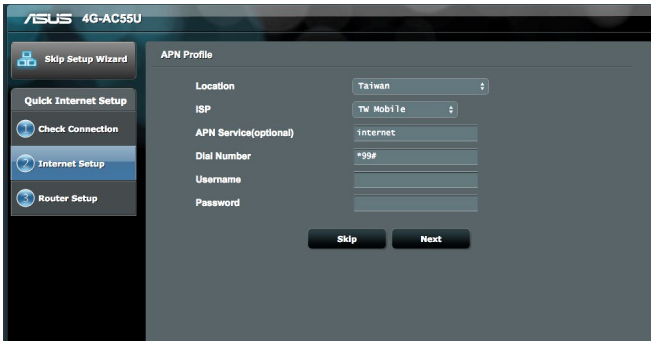
Musisz ręcznie skonfigurować adres IP.



- Jeżeli podłączona jest sieć 3G/4G, funkcja szybkiej konfiguracji połączenia z Internetem (QIS) automatycznie wykryje i zastosuje ustawienia APN w celu połączenia z bezprzewodową stacją bazową. Jeżeli kreator QIS nie zastosuje automatycznie ustawień APN, ręcznie wykonaj ustawienia APN.

UWAGA: Kod PIN różni się w zależności od dostawcy.





7. Wyświetlany jest wynik konfiguracji podwójnego połączenia WAN. Kliknij **Next (Dalej)**, aby kontynuować.

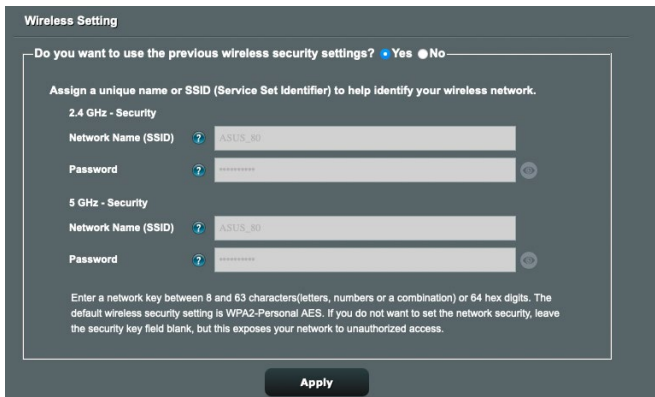
Konfiguracja szerokopasmowego połączenia mobilnego zakończyła się sukcesem



Konfiguracja połączenia Ethernet WAN zakończyła się sukcesem

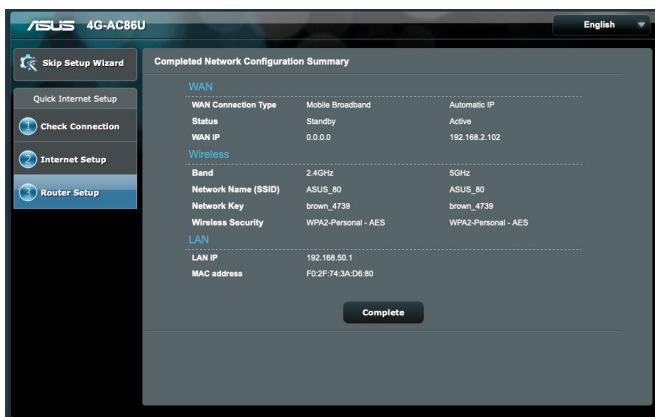


8. Jeżeli obie sieci WAN są skonfigurowane, przejdź do kolejnego kroku, aby skonfigurować ustawienia bezprzewodowej sieci LAN.



9. Przydziel nazwę sieciową (SSID) i klucz zabezpieczenia dla połączenia bezprzewodowego 2,4GHz. Po zakończeniu kliknij **Apply (Zastosuj)**.

10. Wyświetlane są ustawienia połączenia z Internetem i połączenia bezprzewodowego. Kliknij **Next (Dalej)**, aby kontynuować.

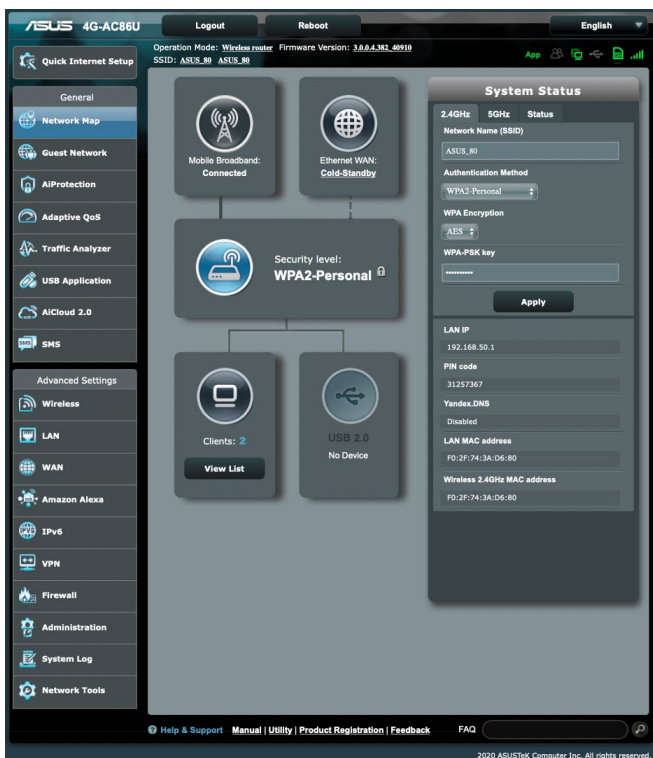


11. Dioda siły sygnału LTE zapala się i świeci w sposób ciągły po zakończeniu ustawień sieci 3G/4G przez QIS, wskazując udane połączenie z Internetem.

3 Konfiguracja ustawień ogólnych

3.1 Korzystanie z pozycji Network Map (Mapa sieci)


Pozycja **Network Map (Mapa sieci)** umożliwia sprawdzenie statusu połączenia internetowego, konfigurowanie ustawień zabezpieczeń sieci i zarządzanie klientami sieciowymi.



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. Na ekranie Mapa sieci kliknij ikonę Stan systemu . Możesz skonfigurować ustawienia bezpieczeństwa sieci bezprzewodowej takie jak **nazwa sieci bezprzewodowej (SSID), metoda uwierzytelniania i ustawienia szyfrowania**.

Ustawienia zabezpieczenia 2,4GHz Ustawienia zabezpieczenia 5GHz



System Status

2.4GHz 5GHz Status

Network Name (SSID)
ASUS_80

Authentication Method
WPA2-Personal

WPA Encryption
AES

WPA-PSK key

Apply

LAN IP
192.168.50.1

PIN code
31257367

Yandex.DNS
Disabled

LAN MAC address
F0:2F:74:3A:D6:80

Wireless 2.4GHz MAC address
F0:2F:74:3A:D6:80



System Status

2.4GHz 5GHz Status

Network Name (SSID)
ASUS_80

Authentication Method
WPA2-Personal

WPA Encryption
AES

WPA-PSK key

Apply

LAN IP
192.168.50.1

PIN code
31257367

Yandex.DNS
Disabled

LAN MAC address
F0:2F:74:3A:D6:80

Wireless 5GHz MAC address
F0:2F:74:3A:D6:84

3. W polu **Wireless name (SSID) (Nazwa sieci bezprzewodowej (SSID))**, wprowadź unikalną nazwę dla własnej sieci bezprzewodowej.
4. Na liście rozwijanej **Authentication Method (Metoda uwierzytelniania)** wybierz metodę uwierzytelniania dla sieci bezprzewodowej.


W przypadku wybrania metody uwierzytelniania WPA-Personal lub WPA-2 Personal wprowadź klucz WPA-PSK lub hasło zabezpieczeń.

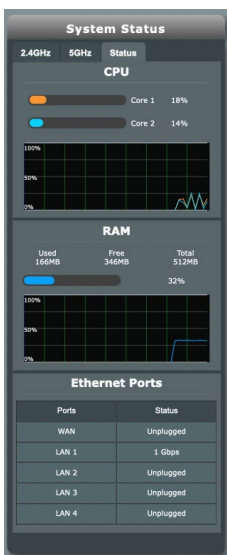
WAŻNE! Standard IEEE 802.11n/ac zakazuje używania wysokiej przepustowości z WEP lub WPA-TKP, jako pojedynczego szyfru. Jeśli używane są te metody szyfrowania, szybkość danych spadnie do szybkości połączenia 54Mbps IEEE 802.11g.

5. Po wykonaniu kliknij **Apply (Zastosuj)**.

3.1.2 System Status


To monitor the system resources:

1. W panelu nawigacji przejdź do pozycji **General > Network Map**.
2. Na ekranie Mapa sieci kliknij ikonę Stan systemu . Zawiera informacje o wykorzystaniu procesora i pamięci.





3.1.3 Zarządzanie klientami sieci


W celu zarządzania klientami sieci:

1. W panelu nawigacji przejdź do zakładki **Ogólne** > **Mapa sieci**.
2. Na ekranie **Mapa sieci** wybierz ikonę Stan klienta , w celu wyświetlenia informacji o kliencie Twojej sieci.



3. W tabeli Stan klientów, kliknij ikonę urządzenia , aby wyświetlić szczegółowy profil urządzenia.

DHCP Logged-in User 



Name	MacBook-Air-M1
IP	192.168.50.209
MAC	00:E0:4C:68:01:A2
Device	REALTEK SEMICONDUCTOR CORP.



[Default](#) [Change](#)

Block Internet Access OFF

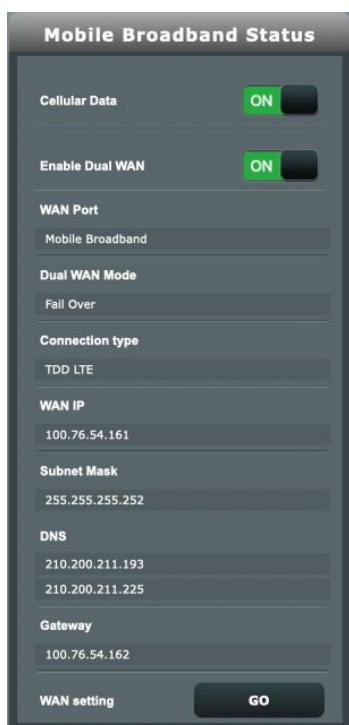
Time Scheduling OFF

3.1.4 Monitorowanie stanu Internetu

W celu monitorowania stanu Internetu:

1. W panelu nawigacji przejdź do zakładki **Ogólne > Mapa sieci**.
2. Na ekranie **Mapa sieci** wybierz ikonę Internet , w celu wyświetlenia konfiguracji Internetu. Możesz też wybrać ikonę komórkowego połączenia szerokopasmowego  w celu wyświetlenia konfiguracji tego połączenia.
3. W celu zakończenia pracy interfejsu WAN w sieci, kliknij przycisk **Switch (Przełącznika)** w opcji Wyłącz interfejs WAN.

Komórkowa sieć szerokopasmowa



Mobile Broadband Status

Cellular Data

Enable Dual WAN

WAN Port
Mobile Broadband

Dual WAN Mode
Fail Over

Connection type
TDD LTE

WAN IP
100.76.54.161

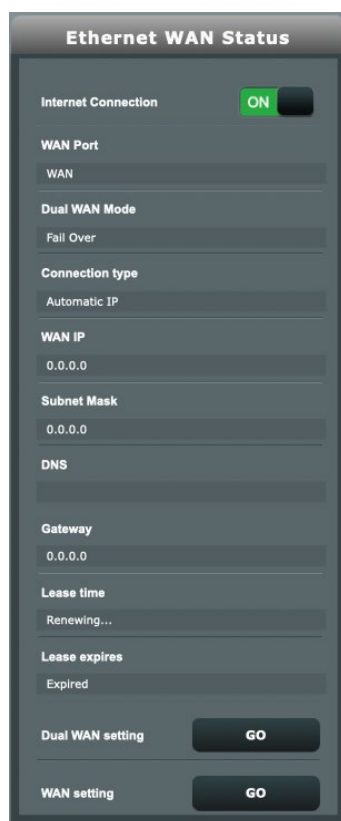
Subnet Mask
255.255.255.252

DNS
210.200.211.193
210.200.211.225

Gateway
100.76.54.162

WAN setting

Sieć Ethernet WAN



Ethernet WAN Status

Internet Connection

WAN Port
WAN

Dual WAN Mode
Fail Over

Connection type
Automatic IP

WAN IP
0.0.0.0

Subnet Mask
0.0.0.0

DNS

Gateway
0.0.0.0

Lease time
Renewing...

Lease expires
Expired


Dual WAN setting

WAN setting

3.1.5 Monitorowanie urządzenia USB

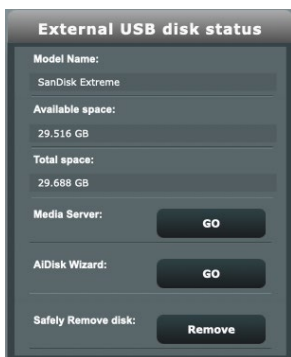
Router bezprzewodowy firmy ASUS jest wyposażony w dwa porty USB, do których można podłączyć urządzenia USB lub drukarkę USB w celu udostępnienia plików i drukarki klientom w sieci.

Aby monitorować urządzenie USB:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > Network Map (Mapa sieci)**.
2. Na ekranie **Network Map (Mapa sieci)** wybierz ikonę USB Disk Status (Stan dysku USB)  aby wyświetlić informacje o urządzeniu USB.
3. W polu **Serwer multimediiów** kliknij przycisk **PRZEJDŹ**, w celu ustawienia serwera iTunes i DLNA dla lokalnego udostępniania multimediiów.

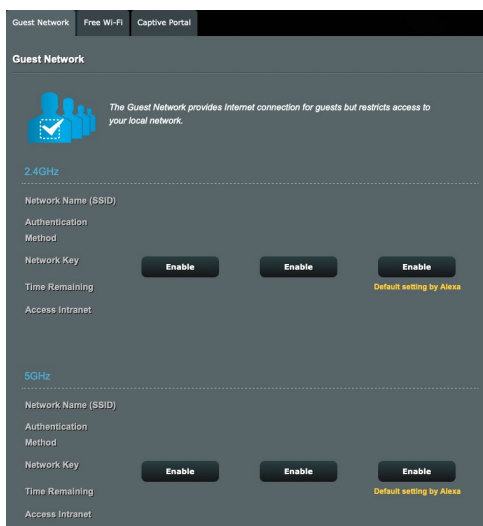
UWAGA: Router bezprzewodowy współpracuje z większością dysków twardych/dysków flash USB (wielkości do 2TB) i obsługuje dostęp odczyt-zapis w systemach FAT16, FAT32, EXT2, EXT3 i NTFS.

4. W polu **Kreator AiDisk**, kliknij przycisk **PRZEJDŹ**, aby ustawić serwer FTP dla udostępniania pliku w Internecie.
5. W celu odłączenia dysku USB od interfejsu USB, kliknij przycisk **Usuń** w polu **Bezpieczne usuwanie dysku**. Po pomyślnym wysunięciu dysku USB jego stan zostanie zmieniony na **Odłączony**.



3.2 Tworzenie 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.



W celu utworzenia sieci gości:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > Guest Network (Sieć gości)**.
2. Na ekranie Guest Network (Sieć gości) wybierz pasmo częstotliwości 2,4Ghz lub 5Ghz dla sieci gości, którą chcesz utworzyć.
3. Kliknij przycisk **Enable (Włącz)**.
4. Na rozwijalnym ekranie skonfiguruj ustawienia gości.
5. Przypisz do sieci tymczasowej nazwę sieci bezprzewodowej w polu Network Name (SSID) [Nazwa sieci (SSID)].
6. Wybierz ustawienie dla pozycji Authentication Method (Metoda uwierzytelniania).
7. W przypadku wybrania metody uwierzytelniania WPA wybierz szyfrowanie WPA.
8. Określ ustawienie pozycji **Access time (Czas dostępu)** lub wybierz opcję **Limitless (Nieograniczony)**.

- Wybierz opcję **Disable (Wyłącz)** lub **Enable (Włącz)** dla pozycji **Access Intranet (Dostęp do Intranetu)**.
- Wybierz **Disable (Wyłącz)** lub **Enable (Włącz)** dla pozycji **Enable MAC Filter (Włącz filtr adresów MAC)** dla opcji **Filtr adresów MAC** dla sieci gościnnej.

Guest Network Index	1
Hide SSID	<input checked="" type="radio"/> Yes <input type="radio"/> No
Network Name (SSID)	ASUS_80_2G_Guest
Authentication Method	WPA2: Personal
WPA Encryption	AES
WPA Pre-Shared Key	brown_4739
Access time	<input checked="" type="radio"/> 0 days <input type="radio"/> Unlimited access
Bandwidth Limiter	<input checked="" type="radio"/> Yes <input type="radio"/> No
Access Intranet	Disable
Enable MAC Filter	Disable

Cancel Apply

- Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

UWAGI:

- Przejdź na stronę <https://www.asus.com/support/FAQ/1034977/> aby dowiedzieć się, **jak skonfigurować portal uwierzytelniania**.
 - Przejdź na stronę <https://www.asus.com/support/FAQ/1034971/> aby dowiedzieć się, **jak skonfigurować bezpłatną sieć Wi-Fi**.
-

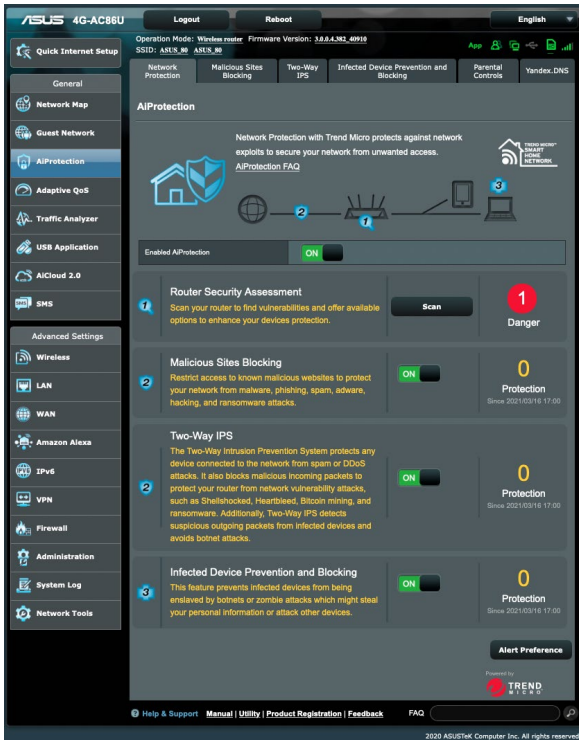
3.3 AiProtection

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.



3.3.1 Network Protection

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

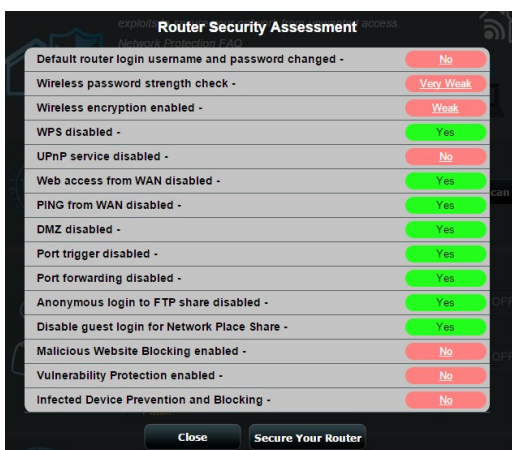


Konfiguracja funkcji Network Protection (Ochrona sieci)

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.)**.

Ochrona przed wykorzystywaniem luk

Funkcja ta rozwiązuje typowe problemy związane z wykorzystywaniem luk w konfiguracji routera.

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 **Vulnerability protection (Ochrona przed wykorzystywaniem luk)** 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):

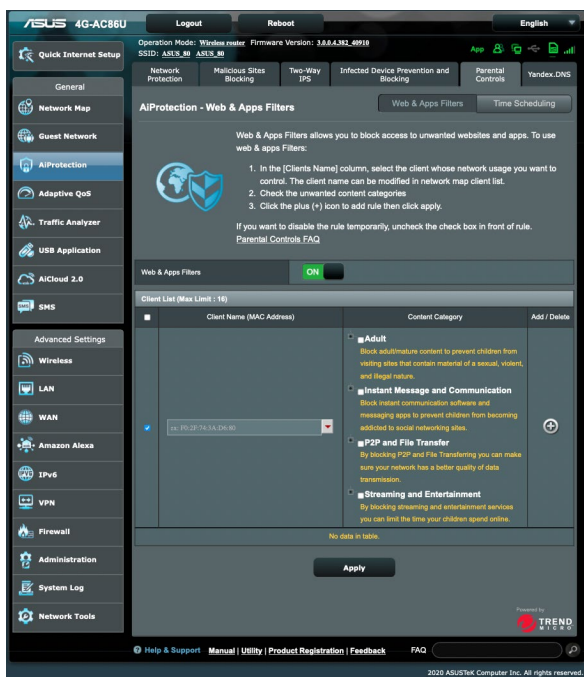
1. W panelu **Infected Device Prevention and Blocking (Wykrywanie i blokowanie zainfekowanych urządzeń)** kliknij przycisk **Alert Preference (Preferencje dotyczące alertów)**.
2. Wybierz lub wprowadź dostawcę poczty e-mail, konto e-mail oraz hasło, a następnie kliknij przycisk **Apply (Zastosuj)**.

3.3.2 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):


1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij kartę **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.

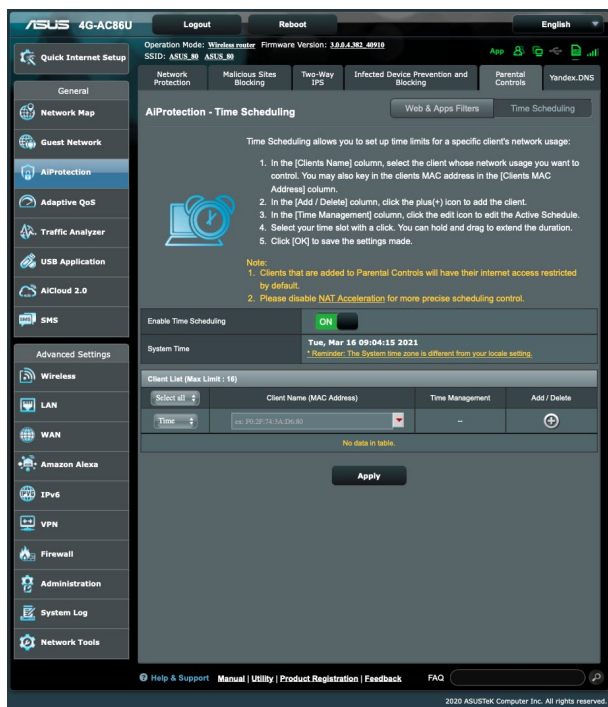
Aby skonfigurować funkcję Web & Apps Filters (Filtry sieci Web i aplikacji):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection**.
2. Na stronie głównej **AiProtection** kliknij ikonę **Parental Controls (Kontrola rodzicielska)**, aby przejść na kartę **Parental Controls (Kontrola rodzicielska)**.
3. W panelu **Web & Apps Filters (Filtry sieci Web i aplikacji)** kliknij pozycję **ON (WŁ.)**.
4. Po pojawieniu się komunikatu End Users License Agreement (EULA) [Umowa licencyjna użytkownika oprogramowania (EULA)] kliknij pozycję **I agree (Zgadzam się)**, aby kontynuować.
5. W kolumnie **Client List (Lista klientów)** wprowadź lub wybierz z listy rozwijanej nazwę klienta.
6. 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)**.
7. Kliknij ikonę  w celu dodania profilu klienta.
8. Kliknij przycisk **Apply (Zastosuj)**, aby zapisać ustawienia.

Ustawienie harmonogramu

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

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




Aby skonfigurować funkcję Time Scheduling (Ustawienie harmonogramu):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > AiProtection > Parental Controls (Kontrola rodzicielska) > Time Scheduling (Ustawienie harmonogramu)**.
2. W panelu **Enable Time Scheduling (Włącz ustawienie harmonogramu)** kliknij pozycję **ON (WŁ.)**.

3. W kolumnie **Clients Name (Nazwa klienta)(adres MAC)** wprowadź lub wybierz z listy rozwijanej nazwę klienta.

UWAGA: Można także wprowadzić adres MAC klienta w kolumnie **Client MAC Address (Adres MAC klienta)(adres MAC)**. 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.

3.4 Adaptacyjna funkcja QoS

3.4.1 Monitor przepustowości

Funkcja ta umożliwi monitorowanie przepustowości sieci WAN/LAN oraz zapewni informacje o szybkości przesyłania i pobierania.



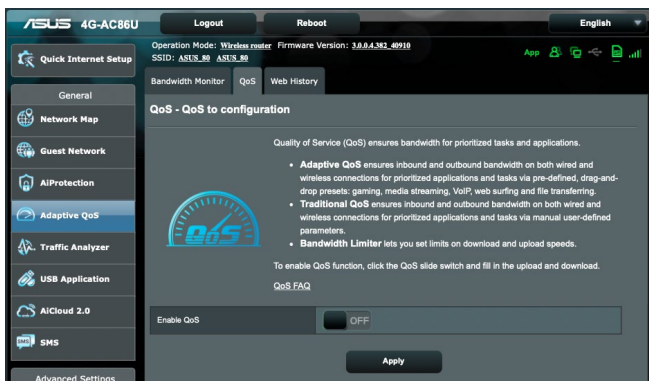
Analiza aplikacji

Aby włączyć funkcję analizy aplikacji:

1. W panelu nawigacji przejdź kolejno do pozycji General (Ogólne) > Adaptive QoS (Adaptacyjna funkcja QoS) > QoS > karta Bandwidth Monitor (Monitor przepustowości).
2. W panelu Apps Analysis (Analiza aplikacji) kliknij pozycję ON (WŁ.).

3.4.2 QoS

Funkcja ta zapewnia przepustowość dla priorytetowych zadań aplikacji.



Aby włączyć funkcję QoS:

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne)** > **Adaptive QoS (Adaptacyjna funkcja QoS)** > karta **QoS**.
2. W panelu **Enable QoS (Włącz QoS)** kliknij pozycję **ON (WŁ.)**.
3. Wypełnij pola przepustowości przesyłania i pobierania.

UWAGA: Uzyskaj informacje dotyczące pasma od ISP. Można także przejść do witryny <http://speedtest.net> w celu sprawdzenia i uzyskania informacji o przepustowości.

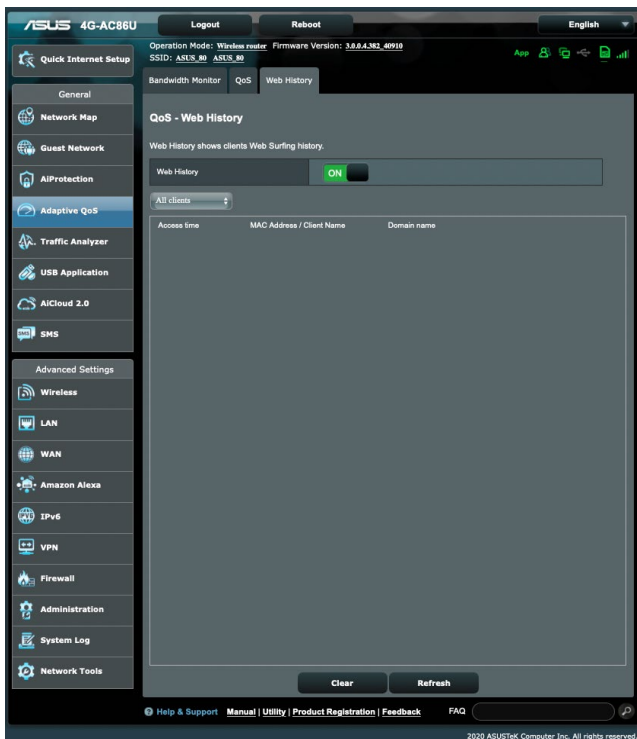
4. Wybierz typ funkcji QoS (adaptacyjny lub tradycyjny) dla danej konfiguracji.

UWAGA: Definicje typów funkcji QoS można znaleźć na karcie **QoS**.

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

3.4.3 Historia stron sieci Web

Funkcja ta umożliwia wyświetlenie historii i szczegółowych informacji o odwiedzanych przez klienta stronach internetowych lub adresach URL.

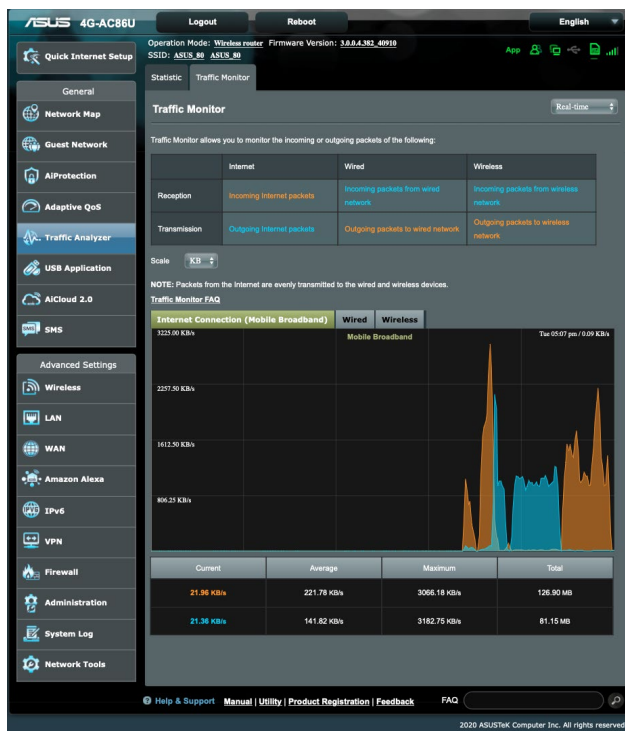


Aby wyświetlić pozycję Web History (Historia stron sieci Web):

1. W panelu nawigacji przejdź kolejno do pozycji **General (Ogólne) > Adaptive QoS (Adaptacyjna funkcja QoS) > karta Web History (Historia stron sieci Web)**.
2. (Opcjonalnie) Kliknij przycisk **Refresh (Odśwież)**, aby wyczyścić listę.

3.5 Analizator ruchu

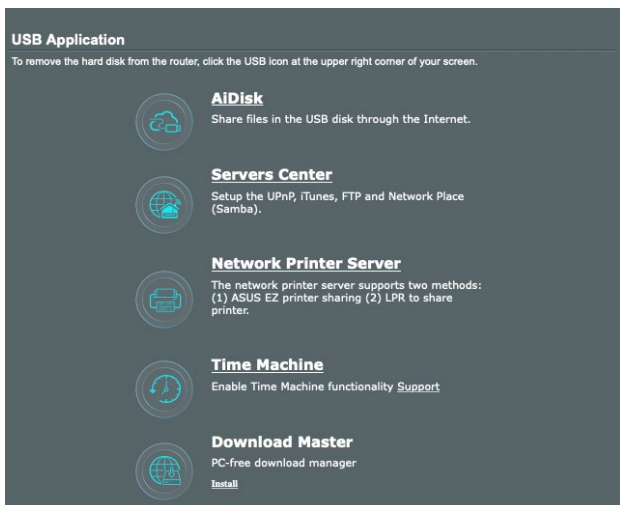
Funkcja monitorowania ruchu zapewnia informacje dotyczące przepustowości i szybkości połączenia z Internetem, siecią przewodową lub bezprzewodową. Umożliwia ona monitorowanie ruchu sieciowego w czasie rzeczywistym lub na poziomie każdego dnia. Zapewnia ponadto opcję wyświetlania informacji o ruchu sieciowym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



3.6 Używanie aplikacji USB

Funkcja USB Extension (Rozszerzenie USB) udostępnia podmenu AiDisk, Servers Center (Centrum serwerów), Network Printer Server (Serwer wydruków sieciowych) i Download Master (Zarządzanie pobieraniem).

WAŻNE! Aby móc korzystać z funkcji serwera, należy podłączyć urządzenie pamięci USB, takie jak dysk twardy USB lub pamięć flash USB, do portu USB 2.0 na panelu tylnym routera bezprzewodowego. Urządzenie pamięci USB powinno zostać odpowiednio sformatowane i podzielone na partycje. Należy zapoznać się z tabelą obsługiwanych systemów plików, która jest dostępna na stronie internetowej firmy ASUS pod adresem <http://event.asus.com/2009/networks/disksupport/>.

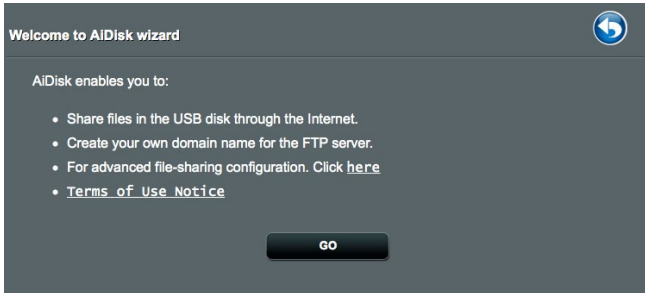


3.6.1 Korzystanie z funkcji AiDisk

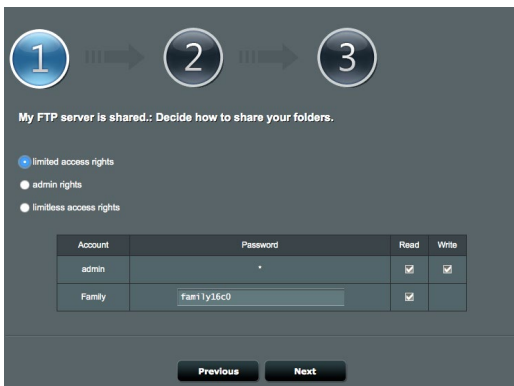
AiDisk umożliwia udostępnianie plików na dysku USB przez Internet. Funkcja AiDisk pomaga także w konfigurowaniu usługi ASUS DDNS i serwera FTP.

Aby używać AiDisk:

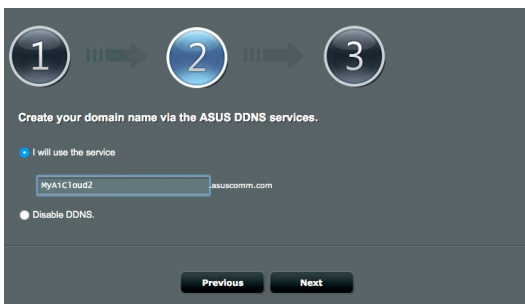
1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > USB application (Aplikacja USB)**, a następnie kliknij ikonę **AiDisk**.
2. Na ekranie **Welcome to AiDisk wizard (Witamy w kreatorze AiDisk)**, kliknij **Go (Przejdź)**.



3. Wybierz prawa dostępu, które chcesz przydzielić użytkownikom mającym dostęp do współdzielonych danych.



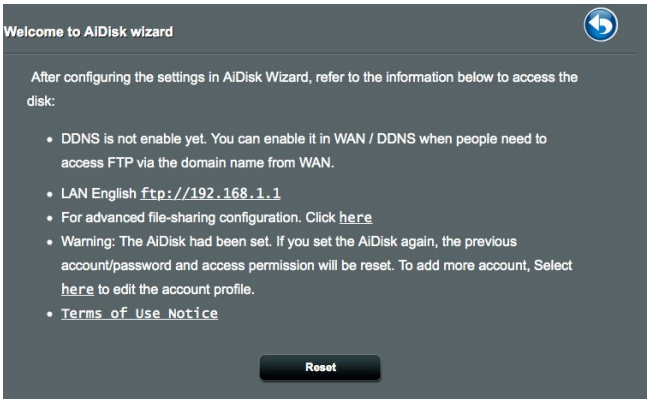
4. Utwórz nazwę domeny przez usługi DDNS ASUS, wybierz **I will use the service (Będę korzystał z tej usługi)** i wprowadź nazwę domeny. Po zakończeniu kliknij **Next (Dalej)**.





Można także wybrać pozycję **Disable DDNS (Wyłącz DDNS)** i kliknąć przycisk **Next (Dalej)** w celu pominięcia wprowadzania ustawień usługi DDNS.

5. Kliknij **Finish (Zakończ)**, aby zakończyć ustawienia.
6. Aby uzyskać dostęp do utworzonej strony FTP uruchom przeglądarkę sieci web lub program klienta FTP innej firmy i wprowadź poprzednio utworzone łącze ftp (**ftp://<domain name>.asuscomm.com**).



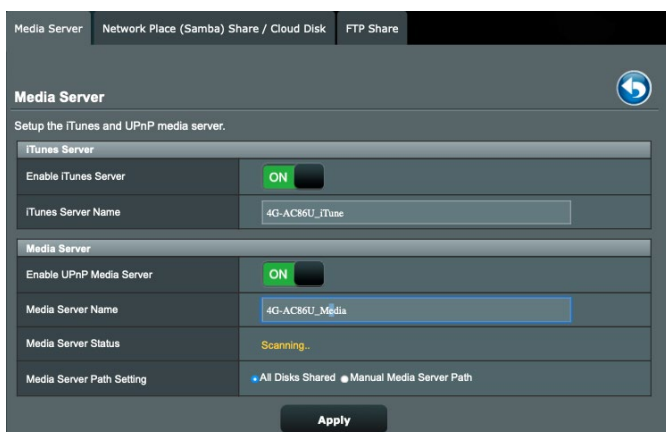
3.6.2 Korzystanie z funkcji Servers Center (Centrum serwerów)

Funkcja Servers Center (Centrum serwerów) umożliwia udostępnianie plików multimedialnych z dysku USB poprzez katalog Media Server (Serwer multimediiów), usługę udostępniania Samba lub FTP. Za pomocą funkcji Servers Center (Centrum serwerów) można także skonfigurować inne ustawienia dysku USB.

Korzystanie z pozycji Media Server (Serwer multimediiów)

Router bezprzewodowy umożliwia urządzeniom z obsługą standardu DLNA uzyskiwanie dostępu do plików multimedialnych zapisanych na dysku USB podłączonym do routera bezprzewodowego.

UWAGA: Przed rozpoczęciem korzystania z funkcji serwera multimediiów DLNA urządzenie należy połączyć z siecią routera 4G-AC86U.



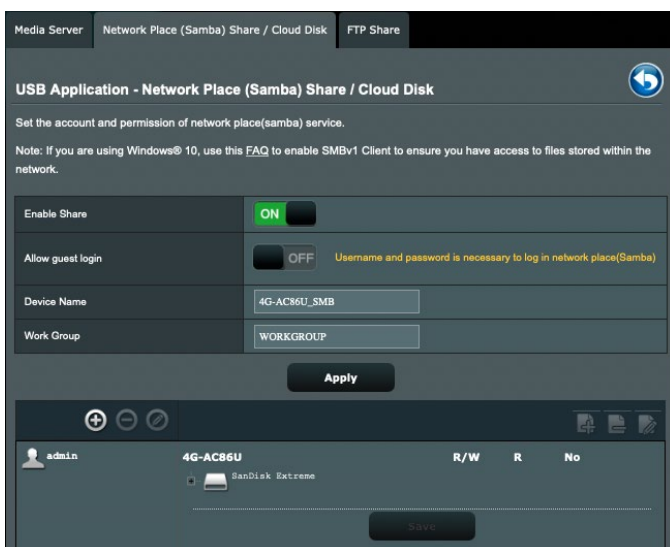
W celu wyświetlenia, przejdź kolejno do pozycji **General (Ogólne) > USB application (Aplikacja USB) > Media Services and Servers (Usługi i serwery multimedialne) > karta Media Servers (Serwery multimediiów)**. Należy zapoznać się z poniższymi opisami pól:

- **Włączyć serwer iTunes?:** Wybierz pozycję ON/OFF (WŁ./WYŁ.) w celu włączenia/wyłączenia serwera iTunes.

- **Włącz serwer multimediiów UPnP:** Wybierz pozycję ON/OFF (WŁ./WYŁ.) w celu włączenia/wyłączenia serwera multimediiów UPnP.
- **Stan serwera multimediiów:** Wyświetlanie stanu serwera multimediiów.
- **Media Server Path Setting (Ustawienia ścieżki serwera multimediiów):** Wybierz opcję **All Disks Shared (Wszystkie dyski zostały udostępnione)** lub **Manual Media Server Path (Ręczne ustawienia ścieżki serwera multimediiów)**.

3.6.3 Używanie usługi udostępniania miejsca sieciowego (Samba)

Udostępnianie miejsca sieciowego (Samba), umożliwia ustawienie konta i uprawnień dla usługi Samba.



Abby używać udostępniania Samba:

1. W panelu nawigacji, przejdź kolejno do pozycji **General (Ogólne) > USB application (Aplikacja USB) > Media Services and Servers (Usługi i serwery multimedialne)** > karta **Network Place (Samba) Share / Cloud Disk [Udostępnianie miejsca sieciowego (Samba)/Dysk w chmurze]**.

UWAGA: Funkcja Network Place (Samba) Share [Udostępnianie miejsca sieciowego (Samba)] jest domyślnie włączona.

2. Wykonaj poniższe czynności, aby dodać, usunąć lub zmodyfikować konto.


W celu utworzenia nowego konta:

- a) Kliknij ikonę , aby dodać nowe konto.

- b) W polach **Account (Konto)** i **Password (Hasło)** wpisz nazwę i hasło klienta sieciowego. Wprowadź ponownie hasło w celu potwierdzenia. Kliknij przycisk **Add (Dodaj)** w celu dodania konta do listy.



W celu usunięcia istniejącego konta:

- Wybierz konto, które chcesz usunąć.
- Kliknij ikonę .
- Po wyświetleniu monitu kliknij przycisk **Delete (Usuń)** w celu potwierdzenia usunięcia konta.

W celu dodania folderu:

- Kliknij ikonę .
- Wprowadź nazwę folderu i kliknij przycisk **Add (Dodaj)**. Utworzony folder zostanie dodany do listy folderów.



- Z listy plików/folderów wybierz typ praw dostępu, który ma zostać przydzielony określonym plikom/folderów:
 - R/W:** Wybierz tę opcję, aby przypisać dostęp do zapisu/ odczytu.

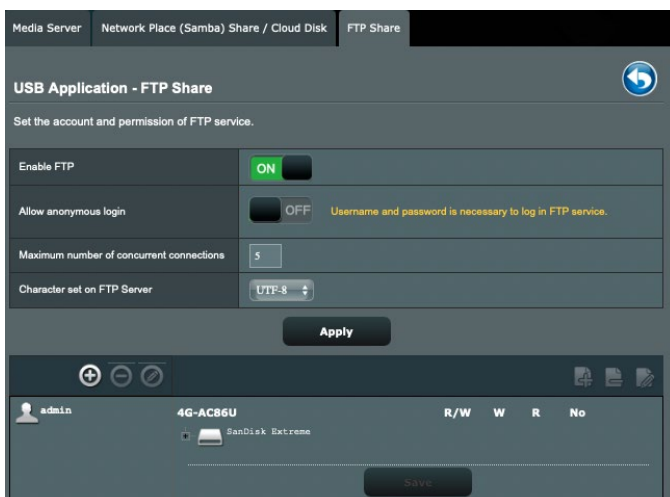
- **R:** Wybierz tę opcję, aby przypisać dostęp tylko do odczytu.
 - **Nie:** Wybierz tę opcję, aby nie udostępniać określonego foldera.
4. Kliknij **Apply (Zastosuj)**, aby zastosować zmiany.

3.6.4 Używanie usługi FTP Share (Udostępnianie FTP)

Dzięki usłudze udostępniania FTP serwer FTP udostępnia pliki z dysku USB innym urządzeniom przez sieć lokalną lub Internet.

WAŻNE!

- Upewnić się, że dysk USB został bezpiecznie wysunięty. Niewłaściwe wysunięcie dysku USB może spowodować uszkodzenie danych.
- Informacje na temat bezpiecznego usuwania dysku USB można znaleźć w części **Bezpieczne usuwanie dysku USB** w rozdziale **3.1.5 Monitorowanie urządzenia USB**.



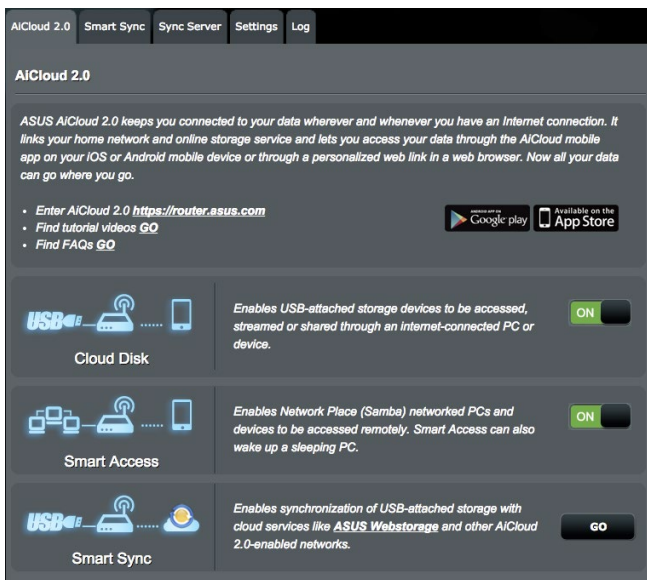
W celu korzystania z usługi udostępniania FTP:

UWAGA: Upewnij się, że serwer FTP został skonfigurowany za pomocą funkcji AiDisk. Szczegółowe informacje znajdują się w rozdziale **3.6.1 Korzystanie z funkcji AiDisk**.

1. W panelu nawigacji kliknij pozycję **General (Ogólne) > USB application (Aplikacja USB) > Media Services and Servers (Usługi i serwery multimedialne) > wybierz zakładkę FTP Share (Udostępnianie FTP)**.
2. Z listy plików/folderów wybierz typ praw dostępu, który ma zostać przydzielony określonym folderów:
 - **R/W:** Wybierz tę opcję, aby przydzielić prawo odczytu/zapisu określonych folderów.
 - **W:** Wybierz tę opcję, aby przydzielić prawo zapisu wyłącznie określonych folderów.
 - **R:** Wybierz tę opcję, aby przydzielić wyłącznie prawo odczytu określonych folderów.
 - **No:** Wybierz tę opcję, jeśli określony folderów ma nie być udostępniany.
3. Jeśli wolisz, możesz ustawić dla pola **Allow anonymous login (Zezwalaj na anonimowe logowanie)** opcję **ON (WŁ.)**.
4. W polu **Maximum number of concurrent connections (Maksymalna liczba jednoczesnych połączeń)** wprowadź liczbę urządzeń, które mogą łączyć się jednocześnie z serwerem udostępniania FTP.
5. Kliknij **Apply (Zastosuj)**, aby zastosować zmiany.
6. W celu dostępu do serwera FTP wprowadź w przeglądarce sieci web lub programie narzędziowym FTP innej firmy, łączy do ftp **ftp://<hostname>.asuscomm.com** i nazwę użytkownika oraz hasło.

3.7 Korzystanie z aplikacji AiCloud 2.0

AiCloud 2.0 to aplikacja usługi w chmurze umożliwiająca zapisywanie, synchronizowanie, udostępnianie i uzyskiwanie dostępu do plików.



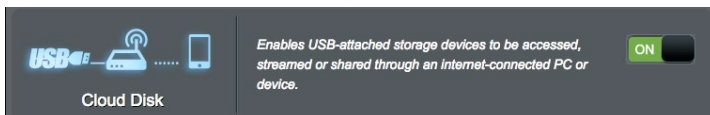
W celu korzystania z aplikacji AiCloud:

1. Pobierz aplikację ASUS AiCloud ze sklepu Google Play lub Apple Store i zainstaluj ją na urządzeniu inteligentnym.
2. Połącz urządzenie inteligentne z siecią. Wykonaj instrukcje, aby ukończyć proces konfiguracji aplikacji AiCloud.

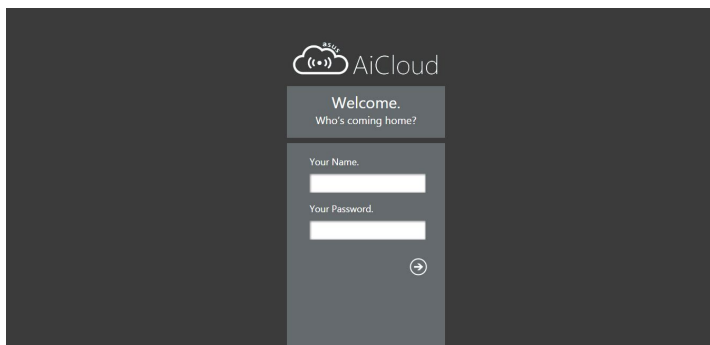
3.7.1 Funkcja Cloud Disk (Dysk w chmurze)

W celu utworzenia dysku w chmurze:

1. Podłącz urządzenie pamięci USB do routera bezprzewodowego.
2. Włącz funkcję **Cloud Disk (Dysk w chmurze)**.

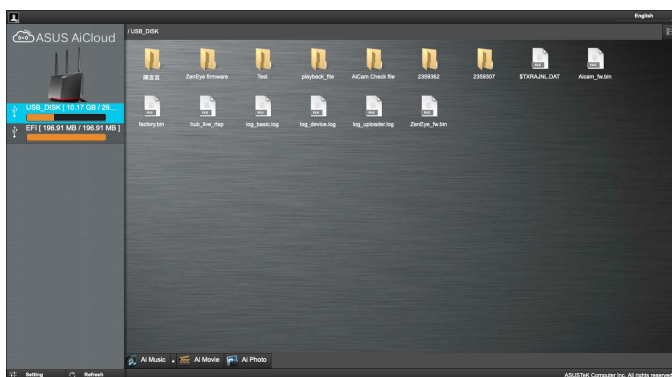


- Przejdź do witryny <https://router.asus.com> i wprowadź konto logowania i hasło routera. W celu zapewnienia lepszego działania zalecane jest używanie przeglądarki **Google Chrome** lub **Firefox**.



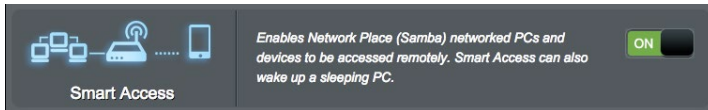
- Można już uzyskiwać dostęp do plików dostępnych w ramach funkcji Cloud Disk (Dysk w chmurze) za pomocą urządzeń połączonych z siecią.

UWAGA: Uzyskanie dostępu do urządzeń połączonych z siecią wymaga ręcznego wprowadzenia nazwy użytkownika i hasła danego urządzenia, które ze względów bezpieczeństwa nie zostaną zapisane przez aplikację AiCloud.



3.7.2 Funkcja Smart Access (Dostęp inteligentny)

Funkcja Smart Access (Dostęp inteligentny) ułatwia uzyskiwanie dostępu do sieci domowej za pomocą nazwy domeny routera.



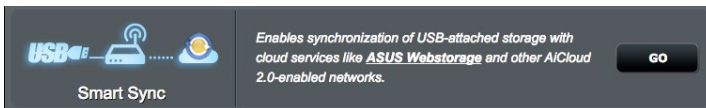
UWAGA:

- Nazwę domeny routera można utworzyć za pomocą usługi ASUS DDNS. Szczegółowe informacje zawiera rozdział **4.3.7 DDNS (Usługa DDNS)**.
- Aplikacja AiCloud zapewnia domyślnie zabezpieczone połączenie HTTPS. W celu zapewnienia bardzo bezpiecznego korzystania z funkcji Cloud Disk (Dysk w chmurze) i Smart Access (Dostęp inteligentny) należy wprowadzić adres [https://\[nazwaASUSDDNSużytkownika\].asuscomm.com](https://[nazwaASUSDDNSużytkownika].asuscomm.com).

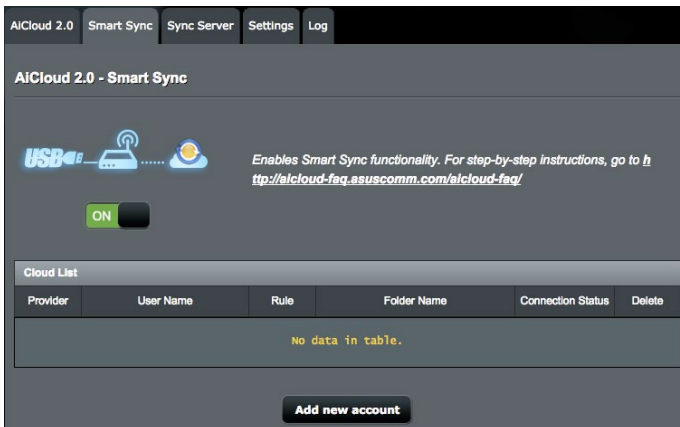
3.7.3 Smart Sync

W celu korzystania z funkcji Smart Sync (Synchronizacja inteligentna):

1. Uruchom aplikację AiCloud, kliknij pozycję **AiCloud 2.0 > AiCloud 2.0 > Smart Sync > Go**.



2. Wybierz pozycję **ON (WŁ.)** w celu włączenia funkcji Smart Sync (Synchronizacja inteligentna).
3. Kliknij przycisk **Add new account (Dodaj nowe konto)**.



4. Wprowadź hasło konta w usłudze ASUS WebStorage i wybierz katalog, który chcesz zsynchronizować z usługą WebStorage.
5. Wybierz Zasady synchronizacji dla zadania Smart Sync (Inteligentna synchronizacja).
 - **Synchronizacja:** Wybranie opcji **Synchronizacja** umożliwia synchronizację folderów między dwoma serwerami, które to zadanie synchronizacji zapewnia, że w folderach zawsze są te same pliki.
 - **Pobierz na dysk USB:** Wybranie opcji **Pobierz na dysk USB** umożliwia replikację zdalnych plików w folderze lokalnym na dysku USB.
 - **Załaduj do chmury:** Wybranie opcji **Załaduj do chmury** umożliwia replikację lokalnych plików w folderze zdalnym na **ASUS WebStorage**.

6. Kliknij przycisk **Dodaj** w celu dodania zadania synchronizacji.

3.7.4 Server synchronizaciji

AiCloud 2.0 Smart Sync Sync Server Settings Log

AiCloud 2.0 - Sync Server

Smart Sync let you to sync your cloud disk with other AiCloud 2.0 account, fill the forms below then generate an invitation to your friend.

1. Fill the invitation form as below.
2. Select a way to get a security code.
3. Click "Generate" to get an invitation.
4. Copy the contents of invitation and mail to your friends.
5. You might not use smart sync with your friends due to ISP firewall issue, please contact your ISP. For advanced users, please enter a specific "Host name" below to use smart sync with your friends.



Invitation Generator

Description

Host Name

Local sync folder

Rule

Security Code

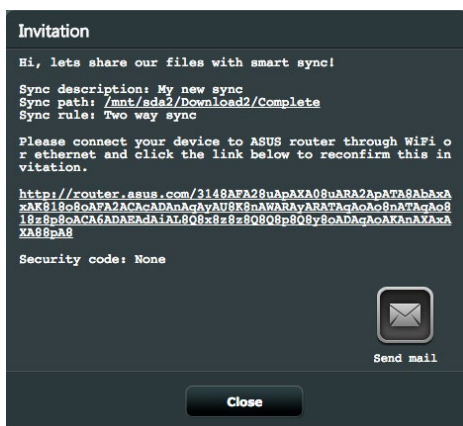


Sync List

Provider	Description	Rule	Local Sync Folder	Invitation	Delete
No data in table.					

Korzystanie z serwera synchronizacji:


1. W panelu nawigacji kliknąć opcje **AiCloud 2.0 > Server synchronizacji**.
2. Wprowadź konfigurację serwera synchronizacji w opcji **Generator zaproszeń**, w celu włączenia opcji **Synchronizacja inteligentna**.
3. Wyślij przyjacielowi zaproszenie na serwer synchronizacji.



4. Po wygenerowaniu zaproszenia możesz sprawdzić zadanie synchronizacji w tabeli **Lista synchronizacji**.

Provider	Description	Rule	Local Sync Folder	Invitation	Delete
	My new sync		/sda2/download2/complete	View	

Check log

5. Możesz kliknąć przycisk **Usuń** , aby przerwać zadanie jeżeli nie chcesz, aby więcej wykonywane było zadanie synchronizacji folderu ze zdalnym klientem synchronizacji.
6. Możesz również zaznaczyć aktywności serwera synchronizacji klikając przycisk **Sprawdź log** lub klikając zakładkę **Log**.

AICloud 2.0 Smart Sync Sync Server Settings Log

AICloud 2.0 - Settings

This page displays a log of AICloud's activities.

[Refresh](#)

3.7.5 Ustawienia

AiCloud 2.0 umożliwia zdefiniowanie polityki dostępu, w celu zapobieżenia nieautoryzowanemu dostępowi, takiemu jak atak słownikowy. Kiedy host próbuje uzyskać dostęp do AiCloud i przekroczy zdefiniowaną Maksymalną ilość nieudanych prób logowania w określonym czasie, usługa AiCloud zostanie automatycznie wyłączona.

Protokół SSL (Secure Socket Layer) jest protokołem zapewniającym szyfrowaną komunikację między serwerem sieciowym a przeglądarkami, w celu bezpiecznego transferu danych, która obejmuje hasło dostępu. Użytkownik uzyskuje dostęp do portalu sieciowego AiCloud z użyciem domyślnego portu, 443, w https. Dostarczanie treści wykorzystuje domyślny port, 8082, w https.

The screenshot shows the 'AiCloud 2.0 - Settings' page. At the top, there are navigation tabs: 'AiCloud 2.0', 'Smart Sync', 'Sync Server', 'Settings', and 'Log'. The 'Settings' tab is active. Below the title, there is a section for 'Password Protection feature' with explanatory text: 'The Password Protection feature prevents unauthorized access to AiCloud. You can set a limited number of account/password login attempts. For example, a setting of 3 times / 2 mins indicates that the user has three attempts to input the account and password in 2 minutes. Once the specified number of attempts has been exceeded, the AiCloud account will be locked and administrator access is needed to unlock it.'

The configuration options are as follows:

- 'Enable Password Protection Feature.' is turned **ON**.
- 'Maximum number of failed login attempts' is set to **3**.
- 'Duration' is set to **2** minutes.
- 'Account Status' shows a user icon and the name **admin**.
- 'AiCloud Web access port' is set to **443**.
- 'AiCloud content streaming port' is set to **8082**.

An 'Apply' button is located at the bottom of the settings area.


3.8 Obsługa wiadomości SMS

SMS (ang. Short Message Service) to usługa przesyłania wiadomości tekstowych umożliwiającą wysyłanie i odbieranie wiadomości z lub na router bezprzewodowy.

3.8.1 Wysyłanie wiadomości

Funkcja ta umożliwia wysyłanie krótkich wiadomości z routera bezprzewodowego.

Aby wysłać nową wiadomość SMS:

1. Kliknij przycisk **New (Nowa)** .
2. Wprowadź numer telefonu odbiorcy.
3. Wprowadź numer telefonu odbiorcy.
4. Kliknij przycisk **Send (Wyślij)**, aby wysłać wiadomość.





Phone Number: 0988487210

Message (Max Limit : 70): Comment est ta journée, doux robot?

Buttons: Send, Save

Aby zapisać wersję roboczą wiadomości:

1. Wersję roboczą wiadomości można zapisać, klikając przycisk **Save (Zapisz)**.
2. Wiadomość będzie widoczna na liście w tabeli **Draft (Wersje robocze)**.
3. Kliknij ikonę edycji  w celu edycji i wysłania wiadomości lub zaznacz ją i kliknij  w celu usunięcia wersji roboczej.



SMS - Send Message



Draft (Max Limit : 5) 

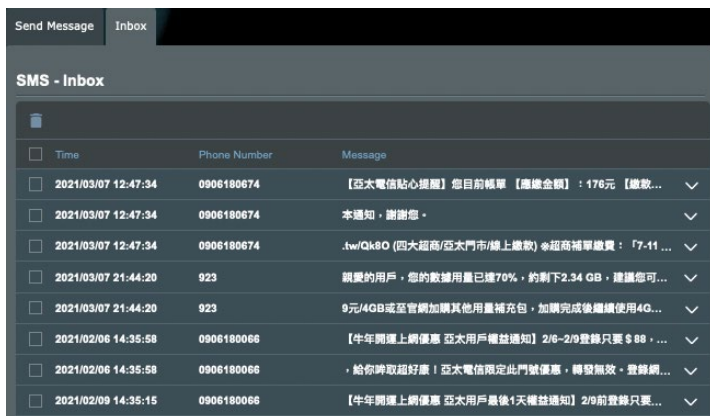
Phone Number	Message
0988487210	Comment est ta journée, doux robot?

Buttons: 

3.8.2 Inbox

Skrzynka odbiorcza umożliwia przeglądanie odebranych wiadomości SMS zapisanych na urządzeniu.

Kliknij  w celu wyświetlenia dalszych informacji lub zaznacz wiadomość i kliknij  w celu usunięcia.



<input type="checkbox"/>	Time	Phone Number	Message	
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	【亞太電信貼心提醒】您目前帳單【應繳金額】：176元【繳款...	▼
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	本週知，謝謝您。	▼
<input type="checkbox"/>	2021/03/07 12:47:34	0906180674	.tw/Qk8O (四大超商/亞太門市/線上繳款) @超商補單繳費：「7-11 ...	▼
<input type="checkbox"/>	2021/03/07 21:44:20	923	親愛的用戶，您的數據用量已達70%，約剩下2.34 GB，建議您可...	▼
<input type="checkbox"/>	2021/03/07 21:44:20	923	9元/4GB或至官網加購其他用量補充包，加購完成後繼續使用4G...	▼
<input type="checkbox"/>	2021/02/06 14:35:58	0906180066	【牛年開運上網優惠 亞太用戶權益通知】2/6-2/9登錄只要 \$ 88，...	▼
<input type="checkbox"/>	2021/02/06 14:35:58	0906180066	，給你睇取超好康！亞太電信限定此門號優惠，轉發無效，登錄網...	▼
<input type="checkbox"/>	2021/02/09 14:35:15	0906180066	【牛年開運上網優惠 亞太用戶最後4天權益通知】2/9前登錄只要...	▼

4 Konfiguracja ustawień zaawansowanych

4.1 Wireless (Sieć bezprzewodowa)

4.1.1 General (Ogólne)

Zakładka General (Ogólne) umożliwia konfigurację podstawowych ustawień sieci bezprzewodowej.

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - General					
Set up the wireless related information below.					
Band	2.4GHz				
SSID	ASUS				
Hide SSID	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Wireless Mode	Auto <input checked="" type="checkbox"/> Big Protection				
Channel bandwidth	40 MHz				
Control Channel	3				
Extension Channel	Above				
Authentication Method	WPA2-Personal				
WPA Encryption	AES				
WPA Pre-Shared Key	99999999				
Network Key Rotation Interval	3600				
Apply					

W celu skonfigurowania podstawowych ustawień sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) >** wybierz zakładkę **General (Ogólne)**.
2. Wybierz pasmo częstotliwości sieci bezprzewodowej 2,4 GHz lub 5 GHz.
3. W polu **SSID**, Przypisz unikatową nazwę identyfikatora SSID (Service Set Identifier) lub sieci zawierającą maksymalnie 32 znaki w celu identyfikacji sieci bezprzewodowej. Urządzenia Wi-Fi będą identyfikować sieć bezprzewodową i łączyć się z nią za pomocą przypisanego identyfikatora SSID. Identyfikatory SSID widoczne na pasku informacyjnym są aktualizowane po zapisaniu nowych identyfikatorów SSID w ustawieniach.

4. W polu **Hide SSID (Ukryj SSID)** wybierz opcję **Yes (Tak)**, aby nie dopuścić do wykrywania identyfikatora SSID przez urządzenia bezprzewodowe. Po włączeniu tej funkcji konieczne będzie ręczne wprowadzanie identyfikatora SSID w urządzeniu bezprzewodowym w celu zapewnienia jego dostępu do sieci bezprzewodowej.
5. W polu **Tryb bezprzewodowy**, Wybierz jedną z dostępnych opcji trybu sieci bezprzewodowej w celu określenia typów urządzeń bezprzewodowych, które będą mogły łączyć się z routerem bezprzewodowym:
 - **Automat.:** Wybierz opcję **Auto (Automat.)**, aby z routerem bezprzewodowym mogły łączyć się urządzenia 802.11AC, 802.11n, 802.11g i 802.11b.
 - **Starsze:** Wybierz opcję **Legacy (Starsze)**, aby z routerem bezprzewodowym mogły łączyć się urządzenia 802.11b/g/n. Urządzenia obsługujące natywnie tryb 802.11n będą jednak działać wyłącznie z maksymalną szybkością 54 Mb/s.
 - **Ochrona b/g:** Zaznacz pole Ochrona b/g w celu umożliwienia routerowi ochrony charakterystyki transmisji 802.11n odziedziczonych urządzeń z połączeniem 802.11g lub 802.11b.
6. W polu **Kanał kontrolny** wybierz kanał pracy routera bezprzewodowego. Wybierz opcję **Automat.**, aby router bezprzewodowy automatycznie wybierał najmniej zakłócony kanał.
7. W polu **Przepustowość kanału** wybierz jedno z dostępnych pasm kanału w celu uwzględnienia większych szybkości transmisji:
 - **20/40 MHz** (domyślnie): Wybierz to pasmo, celem automatycznego wyboru najlepszego pasma dla swojego środowiska bezprzewodowego. W paśmie 5 GHz, domyślnie wybierana jest szerokość pasma **20/40/80 MHz**.
 - **80 MHz:** Wybierz to pasmo, aby zmaksymalizować przepływność w sieci bezprzewodowej dla nadajnika 5 GHz.
 - **40 MHz:** Wybierz to pasmo, aby zmaksymalizować przepływność w sieci bezprzewodowej dla nadajnika 2,4 GHz.
 - **20 MHz:** Wybierz to pasmo w przypadku występowania problemów z połączeniem bezprzewodowym.
8. Jeżeli wybrane zostanie **20/40/80 MHz**, **20/40 MHz**, **40 MHz** lub **80 MHz**, możesz zdefiniować zastosowanie górnego lub dolnego kanału przylegającego w polu **Kanał rozszerzenia**.
9. W polu **Metoda uwierzytelniania** wybierz jedną z poniższych

metod uwierzytelniania:

- **Otwarty system:** Ta opcja nie zapewnia zabezpieczeń.
- **WPA2 Personal/WPA Auto-Personal:** Ta opcja zapewnia mocne zabezpieczenia. Można korzystać z zabezpieczenia WPA (z TKIP) lub WPA2 (z AES). Po wybraniu tej opcji konieczne jest korzystanie z szyfrowania TKIP + AES i wprowadzenie hasła WPA (klucza sieciowego).
- **WPA2 Enterprise/WPA Auto-Enterprise:** Ta opcja zapewnia bardzo mocne zabezpieczenia. Jest ona dostępna z zintegrowanym serwerem EAP lub zewnętrznym serwerem uwierzytelniania RADIUS z wewnętrzną bazą danych.

10. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

4.1.2 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.

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - WPS					
WPS (Wi-Fi 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 type="checkbox"/> OFF				
Current Frequency	2.4GHz Switch Frequency				
Connection Status	Not used				
Configured	Yes				
AP PIN Code	<input type="text" value="31257367"/>				

General	WPS	WDS	Wireless MAC Filter	RADIUS Setting	Professional
Wireless - WPS					
WPS (Wi-Fi 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 type="checkbox"/> OFF				
Current Frequency	5GHz Switch Frequency				
Connection Status	Not used				
Configured	Yes				
AP PIN Code	<input type="text" value="31257367"/>				

W celu włączenia funkcji WPS w sieci bezprzewodowej:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) >** wybierz zakładkę **WPS**.
2. W polu **Enable WPS (Włącz funkcję WPS)** przesun suwak do opcji **ON (WŁ.)**.
3. WPS wykorzystuje równocześnie kanały radiowe 2,4 GHz i 5 GHz.
4. Możesz zastosować dowolną z następujących metod WPS do parowania połączenia bezprzewodowego:
 - **Tryb PBC (Konfiguracja przyciskiem):**
 - Sprzętowa PBC na routerze: Naciśnij fizyczny przycisk WPS na routerze bezprzewodowym, a następnie naciśnij na trzy (3) minuty przycisk WPS na kliencie bezprzewodowym.
 - Programowa PBC na routerze: Zaznacz <Przycisk> w polu **Metoda WPS**, kliknij **Start**, a następnie naciśnij na trzy (3) minuty przycisk WPS na kliencie bezprzewodowym.
 - **Tryb Kod PIN:**
 - Parowanie z klienta bezprzewodowego: Naciśnij przycisk WPS na routerze bezprzewodowym, a następnie wykonaj proces połączenia WPS w trybie kodu PIN i wpisz **Kod PIN AP** na urządzeniu klienckim.
 - Parowanie z routera bezprzewodowego: Naciśnij przycisk WPS na kliencie bezprzewodowym, a następnie wykonaj proces połączenia WPS w trybie kodu PIN i wpisz **Kod PIN klienta** w polu **Metoda WPS > Kod PIN klienta**. Sprawdź, czy kod PIN jest prawidłowy, a następnie kliknij przycisk **Start**, aby sparować z klientem bezprzewodowym.

UWAGA:

- Funkcja WPS obsługuje uwierzytelnianie za pomocą metod Open System (Otwarty system) i WPA2-Personal. Funkcja WPS nie obsługuje sieci bezprzewodowych korzystających z metody szyfrowania Shared Key (Klucz wspólny), WPA-Personal, WPA-Enterprise, WPA2-Enterprise ani RADIUS.
 - Należy poszukać przycisku WPS na urządzeniu bezprzewodowym lub sprawdzić jego lokalizację w podręczniku użytkownika.
 - W czasie procesu WPS router bezprzewodowy wyszukuje wszystkie dostępne urządzenia WPS. Jeśli router bezprzewodowy nie znajdzie żadnych urządzeń WPS, przełączy się do trybu wstrzymania.
 - Diody zasilania routera będą migać szybko przez trzy minuty, do momentu ukończenia konfiguracji WPS.
-

4.1.3 WDS

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.

W celu skonfigurowania mostka bezprzewodowego:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz zakładkę Bridge (Mostek).**

General WPS WDS Wireless MAC Filter RADIUS Setting Professional

Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your 4G-AC55U to connect to an access point wirelessly. WDS may also be considered a repeater mode. But with this method, the devices connected to the access point will only be able to use half of the access point's original wireless speed.

Note: The function only support [Open System/NONE, Open System/WEP] security authentication method.

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.

Basic Config

2.4GHz MAC	AC:9E:17:56:6F:48
5GHz MAC	AC:9E:17:56:6F:4C
Band	2.4GHz ▾
AP Mode	AP Only ▾
Connect to APs in list	<input checked="" 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.	

Apply

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.
4. W polu **Connect to APs in list (Nawiązuj 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 obszarze **Remote AP List (Lista zdalnych punktów dostępu)** wpisz adres MAC i kliknij przycisk **Add (Dodaj)** w celu wprowadzenia adresu MAC innego dostępnego punktu dostępu.
6. Kliknij przycisk **Apply (Zastosuj)**.

UWAGA:

- W trybie Hybrid (Hybrydowy) urządzenia bezprzewodowe połączone z routerem bezprzewodowym firmy ASUS będą miały zapewnioną tylko połowę szybkości połączenia punktu dostępowego.
 - Ustawienie Kanał kontrolny oraz stała Szerokość kanału każdego dodanego do listy punktu dostępowego powinny być takie same jak w przypadku lokalnego routera bezprzewodowego firmy ASUS. Pozycję Kanał kontrolny można zmodyfikować, wybierając kolejno **Ustawienia zaawansowane > Sieć bezprzewodowa > zakładka Ogólne**.
-

4.1.4 Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych)

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.

The screenshot shows the 'Wireless - Wireless MAC Filter' configuration page. At the top, there are tabs for 'General', 'WPS', 'WDS', 'Wireless MAC Filter', 'RADIUS Setting', and 'Professional'. The 'Wireless MAC Filter' tab is selected. Below the tabs, the page title is 'Wireless - Wireless MAC Filter'. A descriptive text states: 'Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.' Under the 'Basic Config' section, there are three settings: 'Band' set to '2.4GHz', 'Enable MAC Filter' with 'Yes' selected, and 'MAC Filter Mode' set to 'Accept'. Below this is a table titled 'MAC filter list (Max. Limit : 64)'. The table has two columns: 'MAC filter list' and 'Add / Delete'. The table is currently empty, with the text 'No data in table.' displayed below it. An 'Apply' button is located at the bottom of the page.

W celu skonfigurowania filtra adresów MAC urządzeń bezprzewodowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Wireless (Sieć bezprzewodowa) > wybierz zakładkę Wireless MAC Filter (Filtr adresów MAC urządzeń bezprzewodowych).**
2. Zaznacz opcję **Yes (Tak)** w polu **Enable Mac Filter (Włącz filtr adresów MAC).**
3. Z listy rozwijanej **MAC Filter Mode (Tryb filtra 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.
4. W obszarze **MAC filter list (Lista filtrowanych adresów MAC)** kliknij przycisk **Add (Dodaj)** i wprowadź adres MAC urządzenia bezprzewodowego.
5. Kliknij przycisk **Apply (Zastosuj).**

4.1.5 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).

The screenshot shows the 'RADIUS Setting' tab in a router's configuration menu. The page title is 'Wireless - RADIUS Setting'. Below the title, there is a descriptive paragraph: '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/ Radius with 802.1x".' The configuration fields are: 'Band' set to '2.4GHz', 'Server IP Address' (empty), 'Server Port' set to '1812', and 'Connection Secret' (empty). An 'Apply' button is located at the bottom center.

W celu skonfigurowania ustawień serwera RADIUS w sieci bezprzewodowej:

1. Upewnij się, że wybrana metoda uwierzytelniania routera bezprzewodowego to **WPA-Enterprise** lub **WPA2-Enterprise**.

UWAGA: W celu skonfigurowania metody uwierzytelniania routera bezprzewodowego należy zapoznać się z rozdziałem **4.1.1 General (Ogólne)**.

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 **Server Port (Port serwera)** wprowadź port serwera.
6. W polu **Connection Secret (Tajne połączenie)** przypisz hasło zapewniające dostęp do serwera RADIUS.
7. Kliknij przycisk **Apply (Zastosuj)**.

4.1.6 Professional (Profesjonalne)

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

UWAGA: Zalecane jest zachowanie wartości domyślnych tego ekranu.

General WPS WDS Wireless MAC Filter RADIUS Setting Professional

Wireless - Professional

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

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

Band	5GHz
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
Enable IGMP Snooping	Disable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Disable
Enable Packet Aggregation	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Enable WMM DLS	Disable
Airtime Fairness	Disable
Multi-User MIMO	Enable
802.11ac Beamforming	Enable
Universal Beamforming	Disable
Tx power adjustment	<input type="range"/> Performance

Apply

Na ekranie **Professional Settings (Ustawienia profesjonalne)** można skonfigurować następujące pozycje:

- **Band (Pasmo):** 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.

- **Włącz harmonogram sieci bezprzewodowej:** Wybierz opcję **Tak**, aby włączyć sieć bezprzewodową działającą zgodnie z ustalonym harmonogramem. Wybierz opcję **Nie**, aby wyłączyć ustalony harmonogram.
- **Data włączania łączności radiowej (dni robocze):** Można określić, w które dni tygodnia sieć bezprzewodowa ma być włączona.
- **Pora dnia, w której łączność radiowa ma być włączona:** Można określić przedział czasu, w którym sieć bezprzewodowa ma być w ciągu tygodniu włączona.
- **Data włączania łączności radiowej (weekend):** Można określić, w które dni weekendu sieć bezprzewodowa ma być włączona.
- **Pora dnia, w której łączność radiowa ma być włączona:** Można określić przedział czasu, w którym sieć bezprzewodowa ma być włączona podczas weekendu.
- **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.
- **Asystent roamingu:** Kiedy środowisko bezprzewodowe zapewnia szereg punktów dostępowych (AP) lub powtarzaczy bezprzewodowych dla pokrycia wszystkich stref martwych sieci bezprzewodowej. Kiedy klient połączony z AP1 przechodzi z miejsca o lepszym sygnale do miejsca o słabym sygnale, ale jest kolejny sygnał z AP2. W celu zapobieżenia stałemu łączeniu klienta z AP1, możesz włączyć opcję Asystent roamingu i ustawić minimalną wartość RSSI jako wartość progową. Kiedy jakość połączenia jest gorsza niż wartość progowa, AP1 odłącza klienta bezprzewodowego tak, że może on dognać ponownej oceny środowiska bezprzewodowego, aby wybrać AP z najlepszą jakością sygnału, jak np. AP2.
- **Włącz Śledzenie IGMP:** Kiedy włączone jest śledzenie IGMP, ruch multimijsji jest tylko przekazywany do klienta bezprzewodowego, który jest członkiem określonej grupy multimijsji.
- **Szybkość multimijsji (Mb/s):** Wybierz szybkość przesyłania w ramach multimijsji 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.
- **AMPDU RTS:** W trybie 802.11n lub 802.11ac wykorzystuje metodę A-MPDU, do łączenia krótszych pakietów w dłuższy pakiet dla tego samego adresu MAC. Kiedy urządzenie bezprzewodowe gotowe do transmisji wysyła RTS (Request to Send - Żądanie wysłania). Po włączeniu AMPDU RTS, każda ramka AMPDU wysyłana z procesem RTS.
- **Próg RTS:** Wybierz niższą wartość dla pozycji RTS (Request to Send) Threshold (Próg RTS) w celu usprawnienia komunikacji bezprzewodowej w przypadku zajętej lub zakłóconej 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) umożliwi zwiększenie szybkości transmisji między routerem bezprzewodowym a urządzeniami 802.11g.
- **Enable WMM APSD:** Tryb WMM APSD (Automatic Power Save Delivery) służy poprawie oszczędzania energii urządzeń starszych wersji. Włącz WMM APSD - bezprzewodowy punkt dostępowy zarządzania wykorzystaniem transmisji radiowej w celu wydłużenia trwałości baterii w przypadku bateryjnych klientów bezprzewodowych takich jak smartfony i laptopy. APSD automatycznie przełącza na wykorzystanie dłuższego odstępu wiązki, kiedy ruch nie wymaga krótkiego czasu wymiany pakietów.

4.2 LAN (Sieć LAN)

4.2.1 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 IP	DHCP Server	Route	IPTV	Switch Control
LAN - LAN IP				
Configure the LAN setting of RT-AC3200.				
IP Address	192.168.1.1			
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) >** wybierz zakładkę **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)**.

4.2.2 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. At the top, there are navigation tabs: LAN IP, DHCP Server (selected), Route, IPTV, and Switch Control. Below the tabs, the page title is 'LAN - DHCP Server'. A descriptive paragraph explains that DHCP is a protocol for automatic configuration on IP networks, used by the 4G-AC55U router to assign IP addresses and inform clients of DNS server and default gateway IP. A link for 'Manually Assigned IP around the DHCP list FAQ' is provided. The configuration is divided into several sections: 'Basic Config' with fields for 'Enable the DHCP Server' (radio buttons for Yes/No), '4G-AC55U's Domain Name', 'IP Pool Starting Address' (192.168.1.2), 'IP Pool Ending Address' (192.168.1.254), 'Lease time' (86400), and 'Default Gateway'. 'DNS and WINS Server Setting' includes fields for 'DNS Server' and 'WINS Server'. 'Enable Manual Assignment' has radio buttons for Yes/No. Below this is a table for 'Manually Assigned IP around the DHCP list (Max Limit : 64)' with columns for 'MAC address', 'IP Address', and 'Add / Delete'. The table is currently empty, showing 'No data in table.' and an 'Apply' button at the bottom.

W celu wykonania ustawień serwera DHCP:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > LAN (Sieć LAN) >** wybierz zakładkę **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.

UWAGA:

- Podczas określania zakresu adresów IP zalecane jest stosowanie formatu adresów IP: 192.168.1.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.



4.2.3 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.

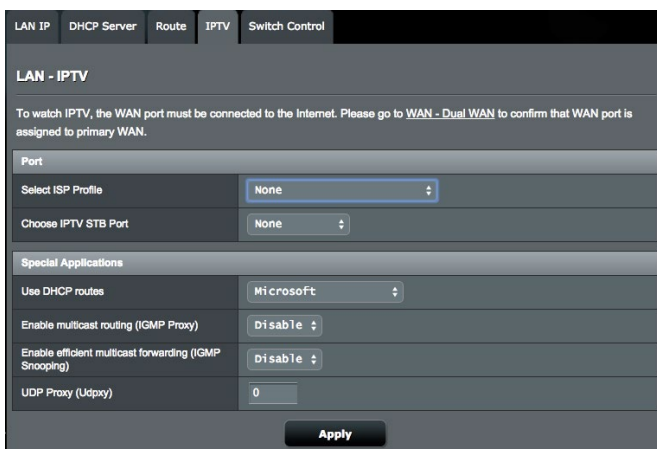
Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
No data in table.					

W celu skonfigurowania tabeli routingu sieci LAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane)** > **LAN (Sieć LAN)** > wybierz zakładkę **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)**.

4.2.4 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.



The screenshot shows the 'LAN - IPTV' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. The 'IPTV' tab is selected. Below the tabs, the page title is 'LAN - IPTV'. A note states: '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.' The configuration options are as follows:


Port	
Select ISP Profile	None
Choose IPTV STB Port	None

Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing (IGMP Proxy)	Disable
Enable efficient multicast forwarding (IGMP Snooping)	Disable
UDP Proxy (Udpxy)	0

An 'Apply' button is located at the bottom of the configuration area.

4.2.5 Sterowanie przełączaniem

Zakładka Sterowanie przełączaniem umożliwia skonfigurowanie Przyspieszenia NAT i Ramki Jumbo w celu poprawy wydajności sieci. Jeśli użytkownik nie posiada specjalistycznej wiedzy, zalecane jest pozostawienie domyślnych ustawień trasy.



The screenshot shows the 'LAN - Switch Control' configuration page. At the top, there are tabs for 'LAN IP', 'DHCP Server', 'Route', 'IPTV', and 'Switch Control'. The 'Switch Control' tab is selected. Below the tabs, the page title is 'LAN - Switch Control'. A note states: 'Setting 4G-AC55U switch control.' The configuration options are as follows:

NAT Acceleration(IPv4 Only)	Enable
Enable Jumbo Frame	Disable

An 'Apply' button is located at the bottom of the configuration area.

4.3 WAN (Sieć WAN)

4.3.1 Internet Connection (Połączenie internetowe)

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

The screenshot shows the 'WAN - Internet Connection' configuration page. At the top, there are tabs for 'Internet Connection', 'Dual WAN', 'Port Trigger', 'Virtual Server / Port Forwarding', 'DMZ', 'DDNS', and 'NAT Passthrough'. The 'Internet Connection' tab is active. Below the tabs, there is a title 'WAN - Internet Connection' and a descriptive paragraph: '4G-AC55U 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.' The configuration is organized into several sections: 'WAN Index' with a 'WAN Type' dropdown set to 'WAN'; 'Basic Config' with 'WAN Connection Type' set to 'Automatic IP', and three radio buttons for 'Enable WAN', 'Enable NAT', and 'Enable UPnP' (with 'UPnP_FAQ' link), all set to 'Yes'; 'WAN DNS Setting' with 'Connect to DNS Server automatically' set to 'Yes'; 'Account Settings' with 'Authentication' set to 'None'; 'Special Requirement from ISP' with 'Host Name' and 'MAC Address' input fields (the latter has a 'MAC Clone' button) and 'DHCP query frequency' set to 'Aggressive Mode'. An 'Apply' button is at the bottom.

4.3.1.1 WAN

W celu skonfigurowania ustawień połączenia WAN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN)** > wybierz zakładkę **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.
- **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.

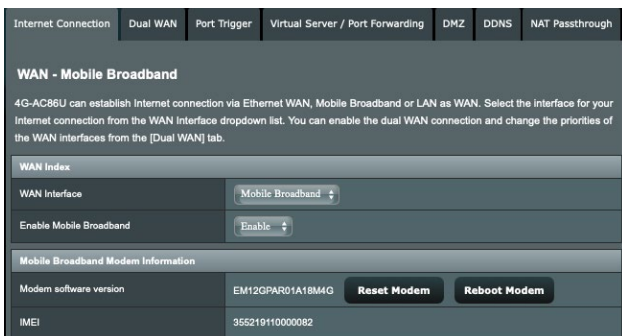
- **Adres MAC:** Pozycja MAC (Media Access Control) address (Adres MAC) to unikatowy identyfikator urządzenia sieciowego. Niektórzy usługodawcy internetowi monitorują adresy MAC urządzeń sieciowych, które łączą się z ich usługą i odrzucają wszelkie próby połączeń urządzeń nierozpoznanych. Aby uniknąć 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.
- **DHCP query frequency (Częstotliwość zapytań DHCP):** Zmiana ustawień interwału odnajdowania serwerów DHCP w celu uniknięcia przeciążenia serwera DHCP.

4.3.1.2 Mobilna sieć szerokopasmowa


4G-AC86U ma wbudowany modem 3G/4G, który umożliwia użycie połączenia Mobilna sieć szerokopasmowa w celu uzyskania połączenia z Internetem.

W celu skonfigurowania mobilnego szerokopasmowego dostępu do Internetu:

1. W panelu nawigacji przejdź do pozycji **Ustawienia zaawansowane > Sieć WAN**, zakładka **Połączenie internetowe**, wybierz **Mobilna sieć szerokopasmowa** w polu **WAN Interface (Interfejs WAN)**.



2. W polu **Włącz mobilną sieć szerokopasmową** wybierz pozycję **Włącz**.
3. Sprawdź, czy karta SIM została prawidłowo włożona, a następnie skonfiguruj w routerze ustawienia sieci komórkowej.

WAN Index	
WAN Interface	Mobile Broadband ▾
Enable Mobile Broadband	Enable ▾
Mobile Broadband Modem Information	
Modem software version	EM12GPAR01A21M4G Reset Modem Reboot Modem
IMEI	355219110000084
Configure the Mobile Broadband settings of 4G-AC96U.	
Internet Connection	
Connection status	Connected 
Network Type	Auto ▾
PDP Type	IPv4 ▾
LTE Band	Auto ▾
Roaming	Disable ▾

4. Konfiguracja połączenia z Internetem:

- 1) W polu **Typ sieci**, wybierz preferowaną sieć:
 - **Automat.** (Domyślna): Wybierz opcję **Automat.**, aby router bezprzewodowy automatycznie wybierał kanał, który ma dostępne połączenie z sieci 4G i 3G.
 - **Tylko 4G:** Wybierz tę opcję, aby router bezprzewodowy łączył się automatycznie tylko z siecią 4G.
 - **Tylko 3G:** Wybierz tę opcję, aby router bezprzewodowy łączył się automatycznie tylko z siecią 3G.
- 2) **Typ PDP:** Router bezprzewodowy obsługuje szereg typów PDP: PPP, IPv4, IPv6, IPv4toIPv6.
- 3) **Pasmo LTE:** Pole to umożliwia wybranie pasma LTE.
- 4) **Roaming:** W przypadku podróży do innego kraju możesz korzystać z oryginalnej karty SIM w celu uzyskania dostępu do sieci lokalnej, jeżeli Twój dostawca usług internetowych zapewnia usługę roamingu w danym kraju. Włączenie tej funkcji umożliwia dostęp do sieci lokalnej.
 - Kliknij przycisk **Skanuj**, aby pokazać wszystkie dostępne sieci komórkowe.
 - Wybierz dostępną sieć komórkową i kliknij przycisk **Zastosuj**, w celu nawiązania połączenia.

UWAGI:

- Router LTE może wykrywać Twojego dostawcę usług internetowych w oparciu o informacje IMSI karty SIM. Jeżeli sieć komórkowa twojego dostawcy usług internetowych nie zostanie znaleziona, podłącz się do sieci roamingowej innego dostawcy usług.
 - Korzystanie z usługi roamingu spowoduje naliczenie dodatkowych opłat. Uzyskaj informacje u swojego operatora sieci komórkowej przed skorzystaniem z usługi roamingu.
-

Data Usage Limitation	
Data Usage	9.84 MBytes (Starting Day : 1) Clear
Cycle Start Day	1 + -
Data Usage Limit	0 GBytes + (Disable : 0)
Data Usage Alert	0 GBytes + (Disable : 0)
Send SMS Notification	Disable + -

5. Limit zużycia danych

- **Wykorzystanie danych:** Pokazuje wykorzystanie danych.
- **Cycle Start Day (Pierwszy dzień cyklu):** Wybierz dzień, w którym zaczynać się będzie obliczanie zużycia danych. Użycie danych będzie zerowane na końcu każdego cyklu.
- **Limit wykorzystania danych:** Umożliwia ustawienie górnego miesięcznego limitu wykorzystania połączenia z Internetem. Kiedy wykorzystanie danych dojdzie do limitu, dostęp do Internetu zostanie zablokowany.
- **Data Usage Alert (Alert o użyciu danych):** Ustaw maksymalny limit korzystania z Internetu, przy którym wysyłany będzie alert. Po osiągnięciu tego limitu korzystania z Internetu dostęp do niego zostanie zablokowany.
- **Send SMS notification (Wyślij powiadomienie SMS):** Włącz tę funkcję, aby otrzymywać powiadomienia SMS po osiągnięciu maksymalnego limitu korzystania z Internetu.

APN Profile	
APN Configuration	Auto
APN Service(optional)	Gent
Dial Number	*99#
Username	
Password	
Authentication	None

APN Profile	
APN Configuration	Manual Setting
Location	Taiwan
ISP	Far EastOne
APN Service(optional)	internet
Dial Number	*99#
Username	
Password	
Authentication	None

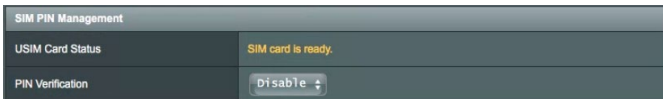
6. Konfiguracja punktu dostępu

- 1) **Automat.** (Domyślna): System domyślnie wybiera automatyczne ustawienia punktu dostępu.
- 2) **Ręczna:** Jeśli automatyczne połączenie telefoniczne nie powiedzie się, wybierz opcję Ręczna w celu ręcznej konfiguracji ustawień punktu dostępu.
 - A. **Lokalizacja:** Wybierz lokalizację dostawcy usług 3G/4G z listy rozwijanej.
 - B. **Usługodawca internetowy:** Wybierz usługodawcę internetowego (ISP) z listy rozwijanej.
 - C. **Usługa APN (nazwa punktu dostępowego)** (opcjonalnie): W celu uzyskania szczegółowych informacji skontaktuj się z dostawcą usług 3G/4G.
 - D. **Wybierz numer:** Numer dostępowy dostawcy 3G/4G.
 - E. **Nazwa użytkownika/Hasło:** Wpisz nazwę użytkownika i hasło zapewniane przez operatora sieci 3G/4G.


7. Ustawianie kodu PIN

Kod PIN: Jeśli wymagana jest karta SIM, wprowadź w pozycji SIM PIN Management (Zarządzanie kodem PIN karty SIM) kod PIN od dostawcy Internetu 3G/4G.

- Domyślny kod PIN może być różny w zależności od dostawcy Internetu. Jeśli weryfikacja kodem PIN została wyłączona domyślnie przez usługodawcę internetowego, ustawienie to można pominąć.



SIM PIN Management	
USIM Card Status	SIM card is ready.
PIN Verification	Disable ▾

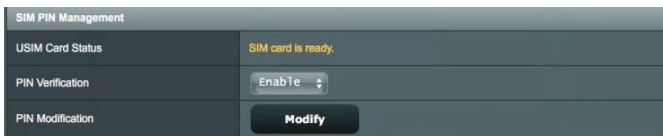
- Jeśli weryfikacja kodem PIN została włączona domyślnie przez usługodawcę internetowego, w obszarze ikony stanu widoczna będzie ikona blokady karty SIM  i wymagane będzie wprowadzenie kodu PIN.



Configure the Mobile Broadband settings of 4G-AC86U.

SIM PIN Management	
USIM Card Status	PIN code is required.
PIN code	1234 <input checked="" type="checkbox"/> Save My PIN <input type="button" value="OK"/>
	Remaining Attempts: 3

- Weryfikację kodem PIN można także włączyć ręcznie za pomocą interfejsu Web GUI routera lub telefonu komórkowego. Konieczne jest także wprowadzenie kodu PIN.



SIM PIN Management	
USIM Card Status	SIM card is ready.
PIN Verification	Enable ▾
PIN Modification	<input type="button" value="Modify"/>




SIM PIN Management - PIN Verification

Please input the PIN code obtained from the internet service provider.

PIN code	<input type="text"/>
PIN Remaining Attempts	2

Stan połączenia mobilnego

Wyszukiwanie informacji o mobilnej sieci szerokopasmowej:

1. Kliknij , aby uzyskać szczegółowe informacje

Internet Connection	
Connection status	Connected 
Network Type	Auto
PDP Type	IPv4
LTE Band	Auto
Roaming	Disable

2. Ekran **Stan połączenia mobilnego** wyświetla szczegółowe informacje o stanie szerokopasmowego połączenia mobilnego.

WAN - Mobile Connection Status	
This page displays basic device information, internet connection status and internet usage.	
Product Information	
Model Name	4G-AC86U
IMSI	466056008449
ICCID	8988605101902049
Phone Number	+88690697
Wireless Status	
Cell ID	1B60134
Connection Type	TDD LTE
Band	LTE BAND 38
RSSI	-58 dBm
SINR	11 dB
RSRP	-94 dBm
RSRQ	-13 dBm
Internet Usage	
Connection Status	 Connected
SIM Provider	KGT-Online
Network Provider	LTE GT
Data Usage	212.514 MBytes
Data Sent	8.841 MBytes
Data Received	203.673 MBytes
Data Sent/Sec	
Data Received/Sec	
Connection Time	0 days 0 hour(s) 28 minute(s) 22 seconds
Close	

4.3.2 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.

The screenshot shows the IPv6 configuration interface. At the top, it says 'Configure the IPv6 Internet setting of 4G-AC86U.' Below that is a 'Basic Config' section with 'Connection type' set to 'Static IPv6'. The 'IPv6 WAN Setting' section includes fields for 'WAN IPv6 Address', 'WAN Prefix Length', and 'WAN IPv6 Gateway'. The 'IPv6 LAN Setting' section includes fields for 'LAN IPv6 Address', 'LAN Prefix Length', and 'LAN IPv6 Prefix', with 'Auto Configuration Setting' set to 'Stateless'. The 'IPv6 DNS Setting' section has three fields for 'IPv6 DNS Server 1', 'IPv6 DNS Server 2', and 'IPv6 DNS Server 3'. The 'Auto Configuration Setting' section at the bottom has 'Enable Router Advertisement' set to 'Enable'. An 'Apply' button is at the bottom right.

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.

4.3.3 Dwie sieci WAN

Router bezprzewodowy firmy ASUS zapewnia obsługę dwóch sieci WAN. Dla funkcji dwóch sieci WAN można ustawić dowolny z poniższych dwóch trybów:

- **Tryb pracy awaryjnej:** Wybierz ten tryb w celu używania dodatkowej sieci WAN jako awaryjnego dostępu do sieci.
- **Zrównoważone obciążenie:** Wybierz ten tryb, aby zezwolić na jednoczesne używanie dwóch połączeń WAN w celu poprawy przepustowości i niezawodności.
- **Włącz powrót:** Zaznacz pole wyboru, aby umożliwić automatyczne przełączenie połączenia z Internetem z powrotem na podstawową sieć WAN, kiedy podstawowa sieć WAN będzie dostępna.

The screenshot shows the 'WAN - Dual WAN' configuration page. At the top, there are tabs for 'Internet Connection', 'Dual WAN', 'Port Trigger', 'Virtual Server / Port Forwarding', 'DMZ', 'DDNS', and 'NAT Passthrough'. The 'Dual WAN' tab is selected. Below the tabs, there is a section titled 'WAN - Dual WAN' with a description: '4G-AC86U 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](#)'. The 'Basic Config' section includes: 'Enable Dual WAN' (ON), 'Primary WAN' (Mobile Broadband), 'Secondary WAN' (WAN), 'Dual WAN Mode' (Fail Over selected, with Load Balance and Allow fallback options), and 'Hot-Standby' (Disable). The 'Auto Network Detection' section includes: 'Detect Interval' (Every 3 seconds), 'Fallback Trigger Condition' (When the current WAN fails 12 continuous times, fallback to Secondary WAN), and 'Network Monitoring' (DNS Query and Ping checkboxes). An 'Apply' button is at the bottom.


- **Detect interval (Interwał wykrywania):** Ustaw interwał (w sekundach) między dwoma pakietami ping.
- **Failover Trigger Condition (Warunek wyzwalania pracy awaryjnej):** Ustaw liczbę przypadków, po upływie którego system uaktywni pracę awaryjną lub wykona czynność powrotu po awarii po wykonaniu określonej liczby testów ping i niezyskaniu odpowiedzi z docelowego adresu IP.

- **Monitorowanie sieci**

- 1) **Zapytanie DNS:** Wybierz tę opcję w celu okresowego rozpoznawania nazwy FQDN (ang. Fully Qualified Domain Name).

Network Monitoring	<input checked="" type="checkbox"/> DNS Query <input type="checkbox"/> Ping
Resolve Hostname	<input type="text" value="dns.asftncs1.com"/>
Resolved IP Addresses	<input type="text" value="131.107.255.255 112.4.20.71 fd3e:4f5a:5b81::1"/>

- 2) **Ping:** Wybierz tę opcję w celu okresowego wykonywania testu ping domeny lub adresu IP.

Network Monitoring	<input type="checkbox"/> DNS Query <input checked="" type="checkbox"/> Ping
Ping Target	<input type="text" value="www.facebook.com"/> 

Jeśli wystąpi błąd połączenia internetowego spowodowany problemem z dzierżawą DHCP, takim jak wygaśnięcie adresu IP, można włączyć opcję DNS Query (Zapytanie DNS) lub Ping w celu zaradzenia problemowi.

4.3.4 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.

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

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	Add / Delete
<input type="text"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="text"/>	<input type="text" value="TCP"/>	<input type="button" value="⊕"/>

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 zakładkę Port Trigger (Wyzwalanie portów).**

2. W polu **Enable Port Trigger (Włącz wyzwalanie portów)** zaznacz opcję **Yes (Tak)**.
3. W polu **Well-Known Applications (Dobrze znane aplikacje)** wybierz popularne gry i usługi sieci Web w celu ich dodania do pozycji Port Trigger List (Lista portów wyzwalania).
4. W tabeli **Trigger Port List (Lista portów wyzwalania)** wprowadź następujące informacje:
 - **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.
5. Kliknij przycisk **Add (Dodaj)**  w celu dodania do listy informacji o wyzwalaniu portów. Kliknij przycisk **Delete (Usuń)**  w celu usunięcia z listy wpisu dotyczącego wyzwalania portów.
6. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

UWAGA:

- 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 wyzwalania portów umożliwi 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 wyzwalania do routera.
-

4.3.5 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.

Internet Connection | Dual WAN | Port Trigger | **Virtual Server / Port Forwarding** | DMZ | DDNS | NAT Passthrough

WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network. If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with 4G-AC55U's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with 4G-AC55U's native FTP server.

Virtual_Server / Port_Forwarding_FAQ

Basic Config

Enable Port Forwarding: Yes No

Famous Server List: Please select ↓

Famous Game List: Please select ↓

FTP Server Port: 2021

Port Forwarding List (Max Limit : 32)

Service Name	Port Range	Local IP	Local Port	Protocol	Add / Delete
				TCP ↓	+

No data in table.

Apply

W celu skonfigurowania pozycji Port Forwarding (Przekierowanie portów):



1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) >** wybierz zakładkę **Virtual Server / Port Forwarding (Serwer wirtualny/Przekierowanie portów)**.
2. W polu **Enable Port Forwarding (Włącz przekierowanie portów)** zaznacz opcję **Yes (Tak)**.

3. W polu **Famous Server List (Lista znanych serwerów)** wybierz typ usługi, do której chcesz uzyskać dostęp.
4. W polu **Famous Game List (Lista znanych gier)** wybierz popularną grę, do której chcesz uzyskać dostęp. Pozycja ta zawiera informacje o porcie wymaganym do prawidłowego działania wybranej popularnej gry online.
5. W tabeli **Port Forwarding List (Lista przekierowania portów)** wprowadź następujące informacje:
 - **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).

UWAGA:

- Jeśli zaporę 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 **4.2 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)**.
6. Kliknij przycisk **Add (Dodaj)**  w celu dodania do listy informacji o wyzwalaniu portów. Kliknij przycisk **Delete (Usuń)**  w celu usunięcia z listy wpisu dotyczącego wyzwalania portów.
7. Po zakończeniu kliknij przycisk **Apply (Zastosuj)**.

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.

Różnica 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.

4.3.6 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 wyzwalanie 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.

Przeostroga: 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.

Internet Connection Dual WAN Port Trigger Virtual Server / Port Forwarding DMZ DDNS NAT Passthrough

WAN - DMZ

Virtual DMZ allows you to expose one computer to the Internet, so that all the inbounds packets will be redirected to the computer you set. It is useful while you run some applications that use uncertained incoming ports. Please use it carefully.

Special Applications: Some applications require special handler against NAT. These special handlers are disabled in default.

[DMZ FAQ](#)

Enable DMZ Yes No

IP Address of Exposed Station

Apply

W celu skonfigurowania strefy DMZ:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) >** wybierz zakładkę **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)**.

4.3.7 DDNS (Usługa DDNS)

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

Internet Connection	Dual WAN	Port Trigger	Virtual Server / Port Forwarding	DMZ	DDNS	NAT Passthrough
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.						
The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x).						
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.						
Enable the DDNS Client	<input checked="" type="radio"/> Yes <input type="radio"/> No					
Server	www.asus.com					
Host Name	key in the name .asuscomm.com					
Apply						

W celu skonfigurowania usługi DDNS:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN)** > wybierz zakładkę **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.

UWAGA:

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.

4.3.8 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)

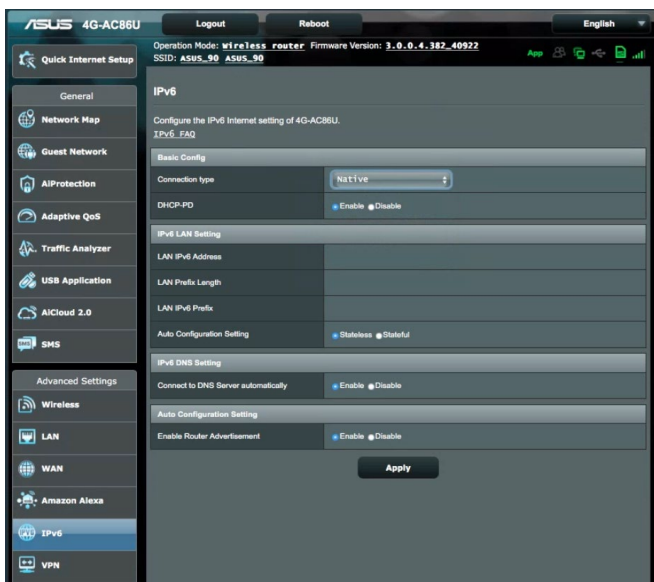
1. Przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > wybierz zakładkę NAT Passthrough (Przekazywanie NAT).**
2. Wybierz opcję **Włącz** lub **Wyłącz** dla przechodzenia określonych typów ruchu przez zaporę NAT.
3. Po zakończeniu kliknij przycisk **Apply (Zastosuj).**

Option	Status
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

4.4 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:

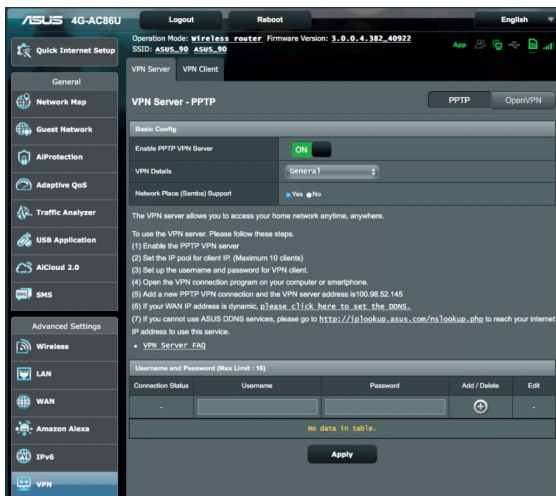
1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > IPv6 (Protokół IPv6)**.
2. Wybierz opcję dla pozycji **Connection type (Typ połączenia)**. Opcje konfiguracji różnią się w zależności od wybranego typu połączenia.
3. Wprowadź ustawienia sieci LAN i DNS dla protokołu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


4.5 Serwer sieci VPN

Wirtualna sieć prywatna VPN (Virtual Private Network) zapewnia bezpieczną komunikację z komputerem zdalnym lub siecią zdalną przy użyciu sieci publicznej, np. Internetu.

UWAGA: Do skonfigurowania połączenia sieci VPN konieczny jest adres IP lub nazwa domeny serwera sieci VPN, do którego dostęp ma zostać uzyskany.



W celu skonfigurowania dostępu do serwera sieci VPN:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > VPN Server (Serwer sieci VPN)**.
2. W pozycji **Enable PPTP VPN Server (Włącz serwer PPTP VPN)** wybierz opcję **ON (Wł.)**, aby włączyć serwer PPTP VPN.
3. Na liście rozwijanej **VPN Details (Szczegóły sieci VPN)** wybierz pozycję **Advanced Settings (Ustawienia zaawansowane)**, jeśli chcesz skonfigurować zaawansowane ustawienia sieci VPN, takie jak obsługa emisji, uwierzytelnianie, szyfrowanie MPPE i zakres adresów IP klienta.
4. W polu **Network Place (Samba) Support [Obsługa miejsca sieciowego (Samba)]** zaznacz opcję **Yes (Tak)**.
5. Wprowadź nazwę użytkownika i hasło w celu uzyskania dostępu do serwera sieci VPN. Kliknij przycisk .
6. Kliknij przycisk **Apply (Zastosuj)**.

4.6 Zapora

Router bezprzewodowy może pełnić funkcję zapory sprzętowej w sieci.

UWAGA: Funkcja Firewall (Zapora) jest domyślnie włączona.

4.6.1 Ogólne

W celu skonfigurowania podstawowych ustawień pozycji Firewall (Zapora):


1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) >** wybierz zakładkę **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)**.

4.6.2 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) >** wybierz zakładkę **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)**.

4.6.3 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) >** wybierz zakładkę **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)**.


UWAGA:

- 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.

4.6.4 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.

W celu skonfigurowania filtra usług sieciowych:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Firewall (Zapora) >** wybierz zakładkę **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 **Black List (Czarna lista)** umożliwia blokowanie określonych usług sieciowych. Pozycja **White List (Biała lista)** 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)**.

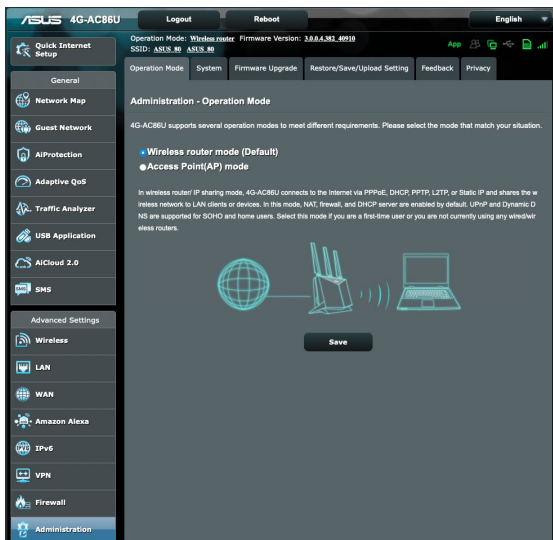
4.6.5 Zapora IPv6

Router bezprzewodowy firmy ASUS blokuje domyślnie cały niechciany ruch przychodzący. Funkcja IPv6 Firewall (Zapora IPv6) umożliwia dopuszczenie do sieci ruchu przychodzącego z określonych usług.

4.7 Administration (Administracja)

4.7.1 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 zakładkę 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 (AP):** W tym trybie router tworzy nową sieć bezprzewodową w sieci już istniejącej.
3. Kliknij przycisk **Apply (Zastosuj)**.

UWAGA: Po zmianie trybu nastąpi ponowne uruchomienie routera.

4.7.2 System

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

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - System					
Change the router login password, time zone, and NTP server settings.					
Change the router login password					
Router Login Name	<input type="text" value="admin"/>				
New password	<input type="password"/>				
Retype Password	<input type="password"/>				<input type="checkbox"/> Show password
Enable Login Captcha	<input checked="" type="radio"/> Yes <input type="radio"/> No				
Basic Config					
Time Zone	<input type="text" value="(GMT) Greenwich Mean Time"/> *Reminder: The System time zone is different from your locale setting.				
NTP Server	<input type="text" value="pool.ntp.org"/>				NTP Link
Network Monitoring	<input checked="" type="checkbox"/> DNS Query <input checked="" type="checkbox"/> Ping				
Auto Logout	<input type="text" value="30"/> minute(s) (Disable - 0)				
Enable WAN down browser redirect notice	<input checked="" type="radio"/> Yes <input type="radio"/> No				
WPS Button behavior	<input checked="" type="radio"/> Activate WPS <input type="radio"/> Toggle Radio <input type="radio"/> Turn LED On/Off				
Enable Reboot Scheduler	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Service					
Enable Telnet	<input checked="" type="radio"/> Yes <input type="radio"/> No * Due to security concerns, we suggest using SSH instead of Telnet. SSH provides an encrypted network communication.				
Enable SSH	<input type="text" value="No"/>				
Idle Timeout	<input type="text" value="20"/> minute(s) (Disable - 0)				
Local Access Config					
Authentication Method	<input type="text" value="HTTP"/>				
Remote Access Config					
Enable Web Access from WAN	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Enable Access Restrictions	<input type="radio"/> Yes <input checked="" type="radio"/> No				
Apply					

W celu skonfigurowania ustawień System:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > wybierz zakładkę System.**
2. Można skonfigurować następujące ustawienia:
 - **Zmień hasło logowania do routera:** YHasło i nazwę logowania routera bezprzewodowego można zmienić, wprowadzając nową nazwę i hasło.
 - **Strefa czasowa:** Wybierz strefę czasową sieci.
 - **Serwer NTP:** Router bezprzewodowy może uzyskiwać dostęp do serwera NTP (Network time Protocol) w celu synchronizacji godziny.
 - **Automatyczne wylogowanie:** System wyloguje się automatycznie ze strony administracyjnej po okresie bezczynności. W celu wyłączenia opcji automatyczne wylogowanie, ustaw wartość na 0.
 - **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.
 - **Włącz ograniczenia dostępu:** Wybierz opcję Yes (Tak), aby ustawić białą listę, która umożliwi administratorowi kontrolę i ograniczenie dostępu wyłącznie do zaufanych adresów IP.
 - a). **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.
 - b). **Określony adres IP:** Wprowadź adresy IP sieci WAN urządzeń sieciowych, które mogą uzyskiwać dostęp do ustawień routera bezprzewodowego. Ta **Lista klientów** umożliwia dodanie maks. liczby adresów IP 4.
3. Kliknij przycisk **Apply (Zastosuj).**

4.7.3 Aktualizacja firmware

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

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - Firmware Upgrade					
Note:					
1. The latest firmware version includes updates from the previous version.					
2. Configuration parameters will keep their settings during the firmware update process.					
3. In case the upgrade process fails, 4G-AC86U enters the emergency mode automatically. The LED signals at the front of 4G-AC86U will indicate such a situation. Please visit ASUS Download Center to download ASUS Device Discovery utility.					
4. Get the latest firmware version from the ASUS Support site: https://www.asus.com/support/					
Firmware Version					
Product ID	4G-AC86U				
Signature version	2.220 Updated : 2021/03/16 17:01			Check	
Firmware Version	3.0.0.4.382_40910-g755bc74			Check	
New Firmware File	<input type="button" value="選擇檔案"/> 尚未選取檔案		Upload		
4G Modem Firmware					
Modem Firmware version	EM12GPAR01A18M4G				
New Modem Firmware	<input type="button" value="選擇檔案"/> 尚未選取檔案		Upload		

Aktualizacja firmware:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) > wybierz zakładkę Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)**.
2. W polu **New Firmware File (Nowy plik oprogramowania sprzętowego) New Modem Firmware (Nowe oprogramowanie sprzętowe modemu)** kliknij pozycję **Browse (Przeglądaj)**, aby zlokalizować pobrany plik.
3. Kliknij **Upload (Prześlij)**.

UWAGA:

- Po ukończeniu procesu uaktualniania należy poczekać, aż system uruchomi się ponownie.
- Jeśli aktualizacja nie powiedzie się, router bezprzewodowy automatycznie przejdzie do trybu awaryjnego, lub zacznie wolno migać wskaźnik LED zasilania na panelu przednim. Aby przywrócić system, zapoznaj się z sekcją **5.2 Odtwarzanie oprogramowania sprzętowego**.

4.7.4 Przywracanie/zapisywanie/przesyłanie ustawień

Operation Mode	System	Firmware Upgrade	Restore/Save/Upload Setting	Feedback	Privacy
Administration - Restore/Save/Upload Setting					
This function allows you to save current settings of 4G-AC86U to a file, or load settings from a file.					
Factory default	Restore	<input type="checkbox"/> Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.			
Save setting	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	Upload				

Aby przywrócić/zapisać/przesłać ustawienia:

1. W panelu nawigacji przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > Administration (Administracja) >** wybierz zakładkę **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 ustawienia)**, przejdź do folderu, w którym chcesz zapisać plik i kliknij pozycję **Save (Zapisz)**.
 - Aby przywrócić poprzednie ustawienia systemu, kliknij **Browse (Przełóżaj)**, zlokalizuj plik systemowy do przywrócenia, a następnie kliknij **Upload (Prześlij)**.

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

4.8 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
 - IPv6 (informacje o sieci WAN i LAN)
 - Dzierżawy DHCP
 - Tabela routingu
 - Przekierowanie portów
 - Połączenie

General Log Wireless Log DHCP leases IPv6 Routing Table Port Forwarding Connections

System Log - General Log

This page shows the detailed system's activities.

System Time **Tue, Mar 16 10:59:11 2021**

Uptime **0 days 0 hour(s) 49 minute(s) 58 seconds**

Remote Log Server

Remote Log Server Port * The default port is 514. If you reconfigured the port number, please make sure that the remote log server or IoT devices' settings match your current configuration.

Apply

```
Mar 16 10:24:29 kernel: [ 916.086997] sw = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:29 kernel: [ 916.551820] MlCmdChannelSwitch: control_ch1 = 9, control_ch2=0, central_ch1 = 9 DBDCId
Mar 16 10:24:29 kernel: [ 916.560873] SW = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:29 kernel: [ 916.707763] MlCmdChannelSwitch: control_ch1 = 10, control_ch2=0, central_ch1 = 10 DBDCI
Mar 16 10:24:29 kernel: [ 916.718283] SW = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:29 kernel: [ 916.867173] MlCmdChannelSwitch: control_ch1 = 11, control_ch2=0, central_ch1 = 11 DBDCI
Mar 16 10:24:29 kernel: [ 916.876909] SW = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.023715] MlCmdChannelSwitch: control_ch1 = 12, control_ch2=0, central_ch1 = 12 DBDCI
Mar 16 10:24:30 kernel: [ 917.032865] SW = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.179716] MlCmdChannelSwitch: control_ch1 = 13, control_ch2=0, central_ch1 = 13 DBDCI
Mar 16 10:24:30 kernel: [ 917.188880] SW = 0, TXStream = 4, RXStream = 4, scan(1)
Mar 16 10:24:30 kernel: [ 917.135788] scan_ch_restore: restore channel done in non-offchannel scan path
Mar 16 10:24:30 kernel: [ 917.344890] MlCmdChannelSwitch: control_ch1 = 8, control_ch2=0, central_ch1 = 10 DBDCI
Mar 16 10:24:30 kernel: [ 917.353992] SW = 1, TXStream = 4, RXStream = 4, scan(0)
Mar 16 10:24:30 kernel: [ 917.362366] [DfCacNormalStart] Normal start. Enable MAC TX
Mar 16 10:32:30 rc_services: httpd 2101: modify_rc_start_lockpin 0 0000
Mar 16 10:41:10 kernel: [ 917.437055] scan_ch_restore: control_ch1=0, bw=1
Mar 16 10:41:10 kernel: [ 917.437055] *M
Mar 16 10:43:28 kernel: [ 2055.628779] entry_wcid 1 QosMapSupport=0
Mar 16 10:43:28 kernel: [ 2055.764733] AP SETKEYS DONE - AKMMap=WPA2-Personal, FairwiseCipher=AE3, GroupCipher=AE3
Mar 16 10:43:28 kernel: [ 2055.764733]
Mar 16 10:43:28 kernel: [ 2055.778081] PTK: 871acc461967ae6ca12bda5d2c7683ac7193ca184401fcdf5dd3238109b77d0Def
Mar 16 10:43:28 kernel: [ 2055.857106] Rcv Wcid(1) AddrAReq
Mar 16 10:43:28 kernel: [ 2055.860358] Start Req = 00000000
Mar 16 10:43:32 dnsmasq[2091]: failed to execute /sbin/dhccp_lease: No such file or directory
Mar 16 10:43:43 kernel: [ 2070.455806] Rcv Wcid(1) AddrAReq
Mar 16 10:43:43 kernel: [ 2070.459309] Start Req = 00000002
```

Clear **Save**

4.9 Lista wsparcia funkcji mobilnej sieci szerokopasmowej Ethernet WAN

Router bezprzewodowy obsługuje przewodową sieć WAN oraz mobilną szerokopasmową sieć WAN w trybach pracy awaryjnej i powrotu. Mobilna szerokopasmowa sieć WAN służy zarówno do dostępu do Internetu jak i jako interfejs zapasowy sieci WAN. LAN, WAN, VPN i Zapora obsługują różne funkcje. Informacje porównawcze znajdują się w tabeli poniżej.

	Sieć kablowa WAN	Sieć LAN jako sieć WAN	Mobilna sieć szerokopasmowa
Sieć LAN			
IPTV	V	Nd.	Nd.
Sterowanie przełączaniem >>Przyspieszenie NAT (tylko IPv4)	V	Nd.	Nd.
Sterowanie przełączaniem >>Ramka Jumbo	V	Nd.	Nd.
Sieć WAN			
IPv6 (Protokół IPv6)	V	V	V (1)
Wyzwalanie portów	V	V	V (2)
Serwer wirtualny/Przekierowanie portów	V	V	V (2)
DMZ (Strefa DMZ)	V	V	V (2)
Usługa DDNS	V	V	V (2)
Przekazywanie NAT	V	V	V (2)
Menedżer ruchu			
QoS	V	V	V
Zapora			
Ogólne	V	V	V
Filtr adresów URL	V	V	V
Filtr słów kluczowych	V	V	V
Filtr usług sieciowych	V	V	V
Zapora IPv6	V	V	Nd.
Administracja			
System >>Włącz dostęp do sieci z sieci WAN	V	V	V (2)

Aplikacje			
AiCloud Dostęp z sieci WAN	V	V	V (2)
Serwer sieci VPN	V	V	V (2)
Serwer FTP	V	V	V (2)

UWAGA:

V (1): Mobilna sieć WAN ma oddzielną konfigurację na swojej stronie konfiguracji

V (2): W większości przypadków zastosowania, usługa Internetu zapewnia wysyłanie mobilnej sieci szerokopasmowej prywatnego adresu IP, co spowoduje uniemożliwienie usłudze sieci WAN dostępu ze strony sieci WAN.

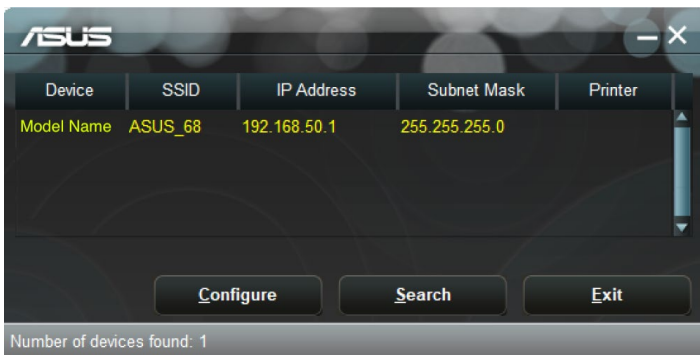
5 Narzędziowych

UWAGA: Pobierz i zainstaluj programy narzędziowe routera bezprzewodowego z witryny firmy ASUS <https://www.asus.com/support/Download-Center/>.

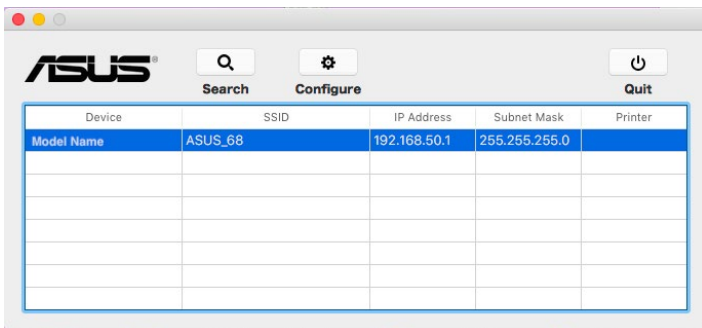
5.1 Device Discovery

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

Windows:



Mac OS:

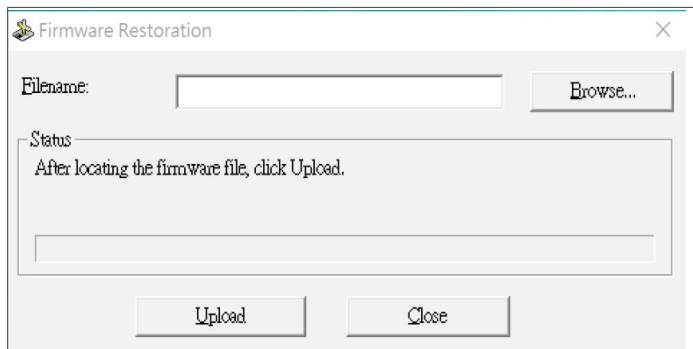


UWAGA: W przypadku ustawienia routera w trybie punktu dostępowego w celu uzyskania adresu IP routera należy skorzystać z narzędzia Device Discovery (Wykrywanie urządzeń).

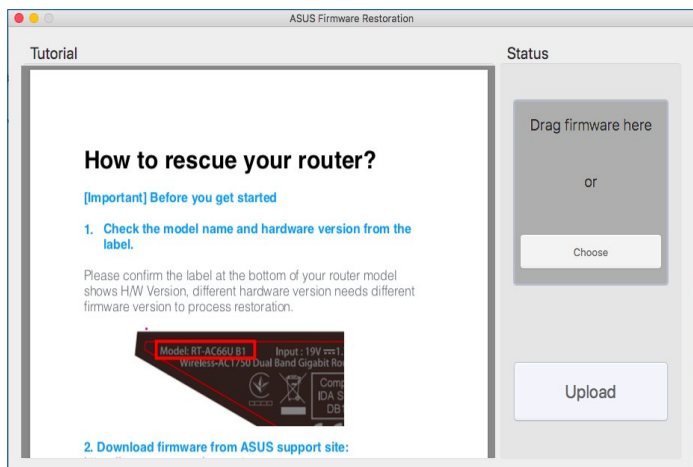
5.2 Firmware Restoration

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.

Windows:



Mac OS:



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

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 (Bezprzewodowego routera) > 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 **Konfiguracja ustawień zaawansowanych**.

5.3 Konfiguracja serwera wydruku

5.3.1 Udostępnianie drukarki ASUS EZ

Program narzędziowy ASUS EZ Printing Sharing umożliwia konfigurację serwera wydruku po podłączeniu drukarki USB do portu USB routera bezprzewodowego. Zapewnia to bezprzewodowe drukowanie i skanowanie plików przez klientów sieciowych.



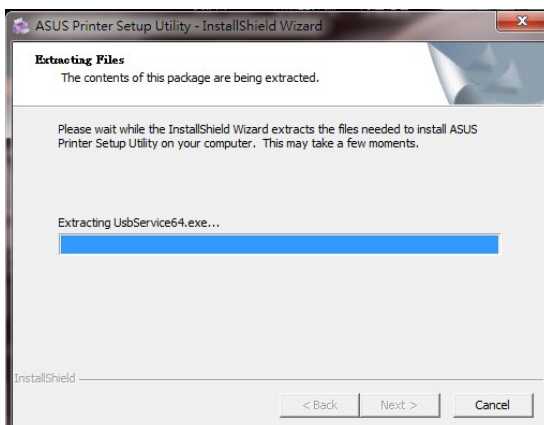
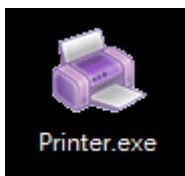
W celu skonfigurowania trybu udostępniania drukarki EZ:

1. W panelu nawigacji przejdź do pozycji **General (Ogólne) > USB Application (Aplikacja USB) > Network Printer Server (Sieciowy serwer wydruku)**.
2. Kliknij pozycję **Download Now! (Pobierz teraz!)**, aby pobrać program narzędziowy drukarki sieciowej.

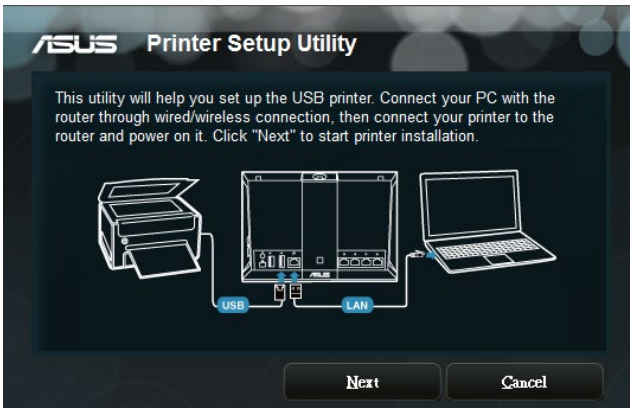


UWAGA: Program narzędziowy drukarki sieciowej jest obsługiwany tylko w systemie Windows® XP, Windows® Vista i Windows® 7. Aby zainstalować program narzędziowy w systemie Mac OS, należy wybrać pozycję **Use LPR protocol for sharing printer (Udostępniaj drukarkę za pomocą protokołu LPR)**.

3. Rozpakuj pobrany plik i kliknij ikonę drukarki w celu uruchomienia programu ustawień drukarki sieciowej.



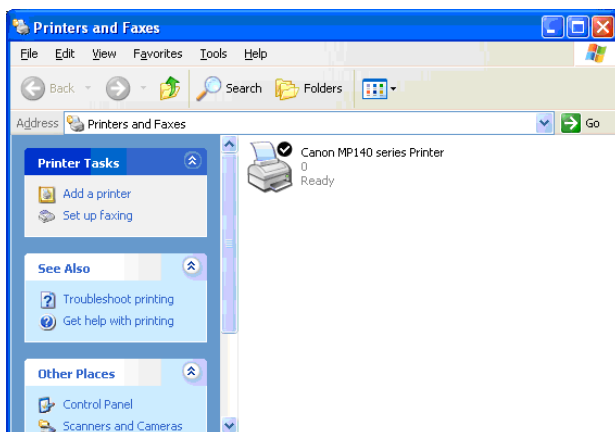
4. Wykonaj instrukcje ekranowe w celu przeprowadzenia ustawień sprzętu, a następnie kliknij **Next (Dalej)**.



5. Zaczekaj kilka minut na zakończenie początkowych ustawień. Kliknij **Next (Dalej)**.
6. Kliknij **Finish (Zakończ)** w celu dokończenia instalacji.
7. Wykonaj instrukcje systemu operacyjnego Windows® w celu instalacji sterownika drukarki.



8. Po zakończeniu instalacji sterownika drukarki klienci sieciowi będą mogli korzystać z drukarki.



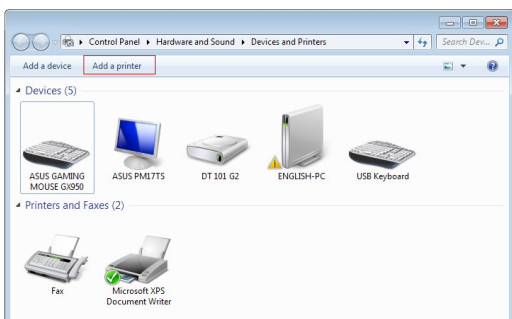
5.3.2 Udostępnianie drukarki za pomocą protokołu LPR

Za pomocą protokołu LPR/LPD (Line Printer Remote/Line Printer Daemon) drukarkę można udostępnić komputerom z systemem operacyjnym Windows® i MAC.

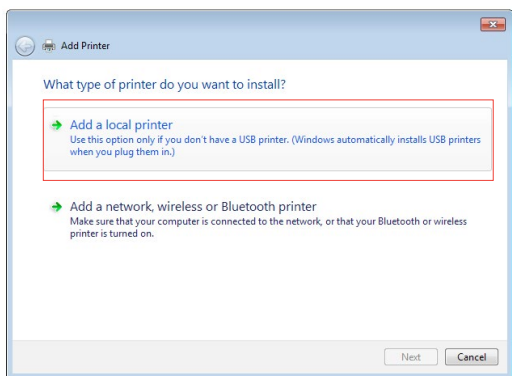
Udostępnianie drukarki LPR

W celu udostępnienia drukarki LPR:

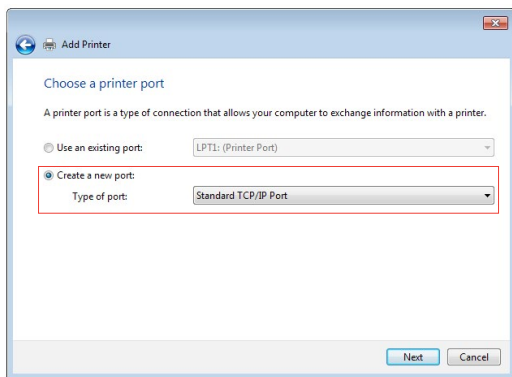
1. Na pulpicie systemu Windows® kliknij kolejno pozycje **Start > Devices and Printers (Urządzenia i drukarki) > Add a printer (Dodaj drukarkę)** w celu uruchomienia pozycji **Add Printer Wizard (Kreator dodawania drukarki)**.



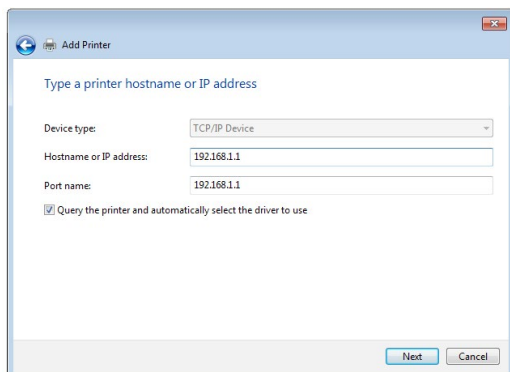
2. Wybierz pozycję **Add a local printer (Dodaj drukarkę lokalną)**, a następnie kliknij przycisk **Next (Dalej)**.



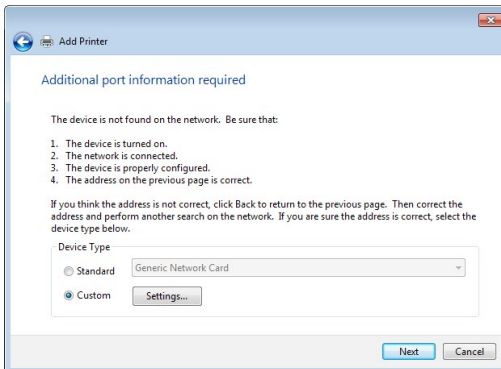
3. Zaznacz pozycję **Create a new port (Utwórz nowy port)**, a następnie ustaw dla pozycji **Type of Port (Typ portu)** opcję **Standard TCP/IP Port (Standardowy port TCP/IP)**. Kliknij przycisk **New Port (Nowy port)**.



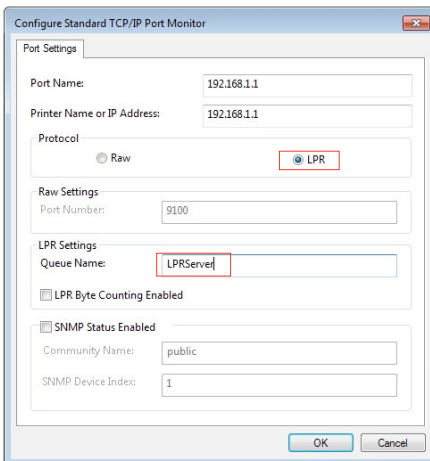
4. W polu **Hostname or IP address (Nazwa hosta drukarki lub adres IP)** wprowadź adres IP routera bezprzewodowego, a następnie kliknij przycisk **Next (Dalej)**.



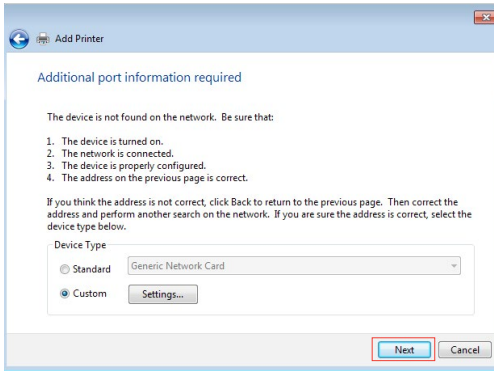
5. Zaznacz pozycję **Custom (Niestandardowy)**, a następnie kliknij przycisk **Settings (Ustawienia)**.



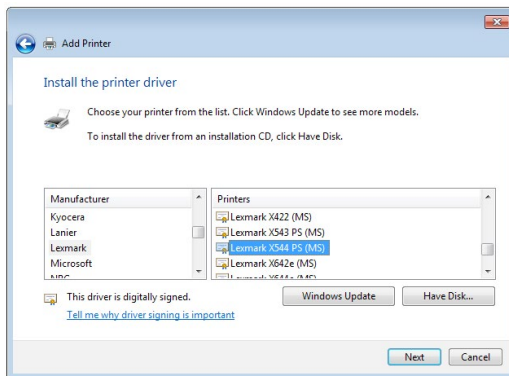
6. Ustaw dla pozycji **Protocol (Protokół)** opcję **LPR**. W polu **Queue Name (Nazwa kolejki)** wprowadź wartość **LPRServer**, a następnie kliknij przycisk **OK**, aby kontynuować.



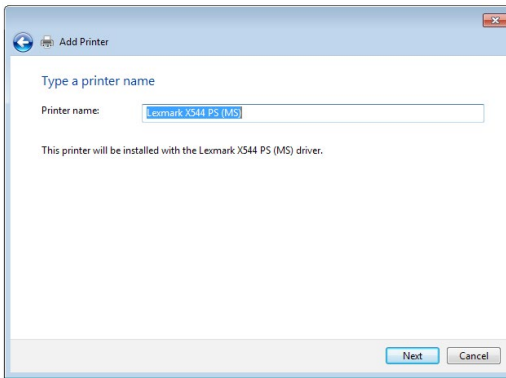
7. Kliknij przycisk **Next (Dalej)**, aby zakończyć konfigurację standardowego portu TCP/IP.



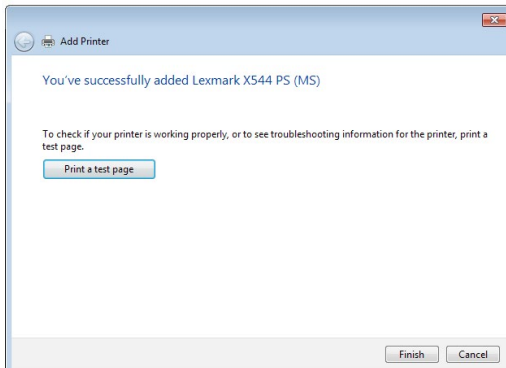
8. Zainstaluj sterownik drukarki podany na liście dostawców. Jeśli danej drukarki nie ma na liście, kliknij przycisk **Have Disk (Z dysku)**, aby ręcznie zainstalować sterowniki drukarki z dysku CD-ROM lub pliku.



9. Kliknij przycisk **Next (Dalej)**, aby zaakceptować domyślną nazwę drukarki.



10. Kliknij przycisk **Finish (Zakończ)**, aby zakończyć instalację.



5.4 Program Download Master

Download Master to program narzędziowy umożliwiający pobieranie plików nawet wtedy, gdy laptop lub inne urządzenia są wyłączone.

UWAGA: Aby móc korzystać z programu Download Master, do routera bezprzewodowego należy podłączyć urządzenie USB.

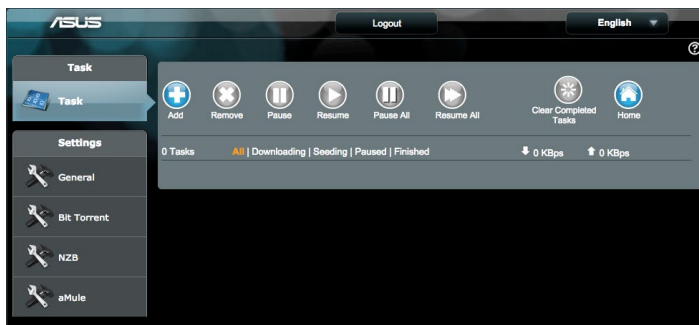
W celu korzystania z programu Download Master:

1. Kliknij kolejno pozycje **General (Ogólne) > USB application (Aplikacja USB) > Download Master**, aby automatycznie pobrać i zainstalować program narzędziowy.

UWAGA: Jeśli dostępnych jest więcej niż jedno urządzenie USB, należy wybrać urządzenie USB, na które pliki mają zostać pobrane.



2. Po ukończeniu procesu pobierania kliknij ikonę programu Download Master, aby rozpocząć korzystanie z programu narzędziowego.
3. Kliknij pozycję **Add (Dodaj)**, aby dodać zadanie pobierania.



- Wybierz typ pobierania, np. BitTorrent, HTTP lub FTP. Wprowadź plik torrent lub adres URL, aby rozpocząć pobieranie.

UWAGA: Szczegółowe informacje na temat pobierania BitTorrent można znaleźć w części **5.4.1 Konfigurowanie ustawień pobierania BitTorrent**.

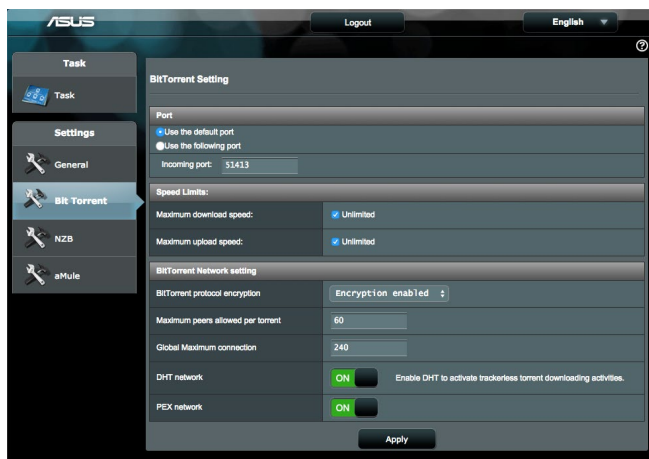
- Skonfiguruj **Ustawienia ogólne** za pomocą panelu nawigacji.
 - Możesz zdefiniować harmonogram pobierania przez wybranie pobierania **Natychmiast** lub **W zaplanowanym czasie**.

<input type="radio"/> Immediately <input checked="" type="radio"/> At Scheduled Time	
Date to Enable Download (week days)	<input checked="" type="checkbox"/> Mon <input checked="" type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input checked="" type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri
Time of Day to Enable Download	00 : 00 - 23 : 59
Date to Enable Download (weekend)	<input checked="" type="checkbox"/> Sat <input checked="" type="checkbox"/> Sun
Time of Day to Enable Download	00 : 00 - 23 : 59

- Informacja o zadaniach pobierania jest domyślnie aktualizowana co 5 sekund. Opcje, **Częstotliwość odświeżania**, umożliwiają zmianę okresu aktualizacji informacji.
- Jako repozytorium pobieranych plików można wybrać ścieżkę folderu w polu **Pobieraj do**.
- Domyślnym numerem portu dla strony administracji **DownloadMaster** jest 8081. Jeżeli numer portu jest w konflikcie z innymi aplikacjami, można go tutaj zmienić.
- Aby zarządzać **DownloadMaster** z Internetu, można przesunąć suwak **Sieć WAN** do położenia **WŁ**.
- Jeżeli zasoby sieciowe są ograniczone, zalecamy wyłączenie opcji Keep seeding (Rozsiewaj) po zakończeniu zadania, przez przesunięcie suwaka do położenia **WYŁ**.

ASUS		Logout	English
Task	General Setting		
Task	Download Schedule		
Settings	<input checked="" type="radio"/> Immediately <input type="radio"/> At Scheduled Time		
General	Download to	/tmp/mnt/sda2/download2/comp1 etc <input type="button" value="Browse"/>	
Bit Torrent	Refresh rate	5 Seconds	
NZB	DownloadMaster Port	8081	
aMule	WAN network	<input type="checkbox"/> OFF Enable/disable the WAN connection.	
	Keep seeding after task completed	<input checked="" type="checkbox"/> ON	
	<input type="button" value="Apply"/>		

5.4.1 Konfigurowanie ustawień pobierania BitTorrent

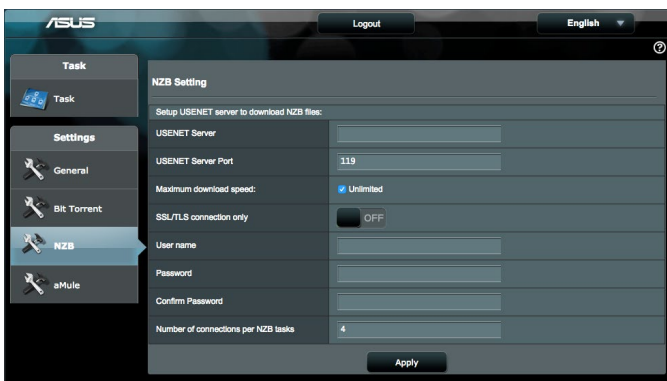


W celu skonfigurowania ustawień pobierania BitTorrent:

1. W panelu nawigacji programu Download Master kliknij pozycję **Bit Torrent (Pobieranie BitTorrent)**, aby wyświetlić stronę **Bit Torrent Setting (Ustawienia pobierania BitTorrent)**.
2. Wybierz określony port dla zadania pobierania.
3. Aby zapobiec przeciążeniu sieci, w obszarze **Speed Limits (Limity szybkości)** można ograniczyć maksymalne szybkości przekazywania i pobierania.
4. Można ograniczyć maksymalną liczbę dozwolonych peerów i włączyć lub wyłączyć szyfrowanie plików podczas pobierania.
5. Włączenie sieci DHT (Distributed Hash Table) może poprawić prędkości pobierania i szybkość transferu przez połączenie domeny udostępniania informacji. Aby korzystać z sieci DHT, router bezprzewodowy musi również udostępniać niektóre informacje innym użytkownikom sieci,
6. Włącz sieć PEX (Peer Exchange), aby wymienić informacje partnerów między dwoma podłączonymi partnerami, pomagając zgromadzić więcej partnerów w sieci.

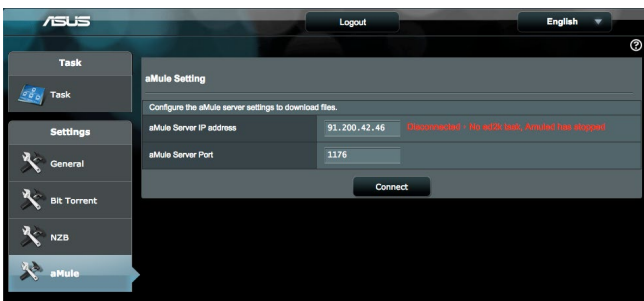
5.4.2 Ustawienia pobierania NZB

Można skonfigurować serwer USENET w celu pobierania plików NZB. Po wprowadzeniu ustawień serwera USENET kliknij przycisk **Apply (Zastosuj)**.



5.4.3 Ustawienia eMule

Można skonfigurować serwer eMule w celu pobierania plików z eMule. Po wprowadzeniu ustawień serwera eMule, kliknij przycisk **Zastosuj**.



6 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: <http://support.asus.com/> w celu uzyskania dalszych informacji o produkcie oraz szczegółowych danych kontaktowych działu pomocy technicznej firmy ASUS.

6.1 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) > wybierz zakładkę 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 <http://www.asus.com/support> i pobierz najnowszą wersję oprogramowania sprzętowego.

3. Na stronie **Firmware Upgrade (Uaktualnienie oprogramowania sprzętowego)** kliknij przycisk **Browse (Przełączaj)**, 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 kable Ethernet są prawidłowo podłączone.

- Jeśli kabel Ethernet łączący router z modemem jest podłączony w prawidłowy sposób, świecić się będzie dioda LED sieci WAN.
- Jeśli kabel Ethernet łączący uruchomiony komputer z routerem jest podłączony w prawidłowy sposób, świecić się będzie odpowiednia dioda LED sieci LAN.

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.

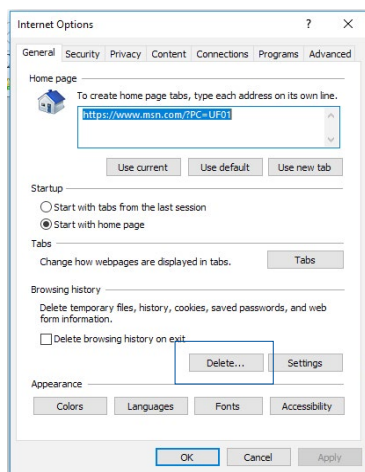
- W przypadku niektórych dostawców usług internetowych zapewnianych przez modem kablowy wymagane jest używanie adresu MAC komputera, dla którego zarejestrowano wstępnie konto. Adres MAC można sprawdzić za pomocą sieciowego interfejsu graficznego, na stronie **Network Map (Mapa sieci)** > **Clients (Klienci)**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



6.2 Często zadawane pytania (FAQ)

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. Domyślna fabryczna nazwa logowania i hasło to „admin/admin”. 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 8 należy wykonać poniższe czynności:
 1. Uruchom program Internet Explorer 8, 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 **Tymczasowe pliki internetowe i pliki witryn internetowych i Pliki cookie i dane witryn internetowych**, a następnie kliknij przycisk **Delete (Usuń)**.



UWAGA:

- 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 funkcję podwójnego pasma.

- **Poza zakresem:**
 - Przesuń router bliżej klienta bezprzewodowego.
 - Ustaw anteny routera w najlepszym położeniu zgodnie z opisem w części **1.4 Ustawianie pozycji routera.**
- **Wyłączono serwer DHCP:**
 1. Uruchoom 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)**.
- 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 **No (Nie)** dla pozycji **Hide SSID (Ukryj SSID)** i zaznacz opcję **Auto (Automat.)** dla pozycji **Control Channel (Kanał kontrolny)**.
- 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)**.

Przewodowe połączenie z Internetem nie jest dostępne.

- 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 **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 Control (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.
- Sprawdź wskaźniki stanu modemu ADSL i routera bezprzewodowego. Jeśli nie świeci się dioda LED sieci WAN routera bezprzewodowego, sprawdź, czy wszystkie kable są prawidłowo podłączone.

Komórkowe połączenie szerokopasmowe z Internetem nie jest dostępne.

- Włóż do gniazda karty USIM kartę SIM z planem taryfowym obejmującym transmisję danych. Zaświeci się wskaźnik LED komórkowej sieci szerokopasmowej 3G/4G, co oznacza, że karta SIM została prawidłowo zainstalowana.
- Ustawienia punktu dostępu nie są stosowane automatycznie. Uzyskaj ustawienia usługi punktu dostępu od usługodawcy internetowego, a następnie wykonaj poniższe czynności, aby ręcznie skonfigurować ustawienia punktu dostępu.
 - Przejdź do pozycji **Advanced Settings (Ustawienia zaawansowane) > WAN (Sieć WAN) > Internet Connection (Połączenie internetowe)**.
 - W polu **WAN Type (Typ sieci WAN)** wybierz opcję **Mobile broadband (Komórkowa sieć szerokopasmowa)**.

- Jeśli punkt dostępu został prawidłowo skonfigurowany, ale nadal nie będzie można nawiązać połączenia z Internetem, upewnij się, że:
 - Pasma częstotliwości jest zgodne z używanym przez usługodawcę internetowego.
 - Router bezprzewodowy znajduje się blisko okna w celu zapewnienia mocnego sygnału 3G/4G.
- Funkcje wyzwalania portów, przekierowania portów, usługi DDNS i DMZ nie mogą działać. Większość usługodawców internetowych zapewnia prywatny adres IP dla urządzenia z dostępem do komórkowej sieci szerokopasmowej. Z tego powodu niektóre usługi, takie jak iCloud, nie są dostępne. Skontaktuj się z usługodawcą internetowym w celu uzyskania pomocy.

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)**. Domyślne konto logowania i hasło to „admin”.

Jak przywrócić domyślne ustawienia systemu?

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

Następujące ustawienia są fabrycznymi ustawieniami domyślnymi:

Nazwa użytkownika: admin

Hasło: admin

Adres IP sieci LAN routera: 192.168.50.1 / router.asus.com

Ustawienia sieci Wi-Fi:

SSID (2.4GHz): ASUS_XX

SSID (5GHz): ASUS_XX

Domyślny klucz sieci Wi-Fi: Na etykiecie z tyłu routera.

UWAGA: XX to dwie ostatnie cyfry adresu MAC 2,4 GHz. Można go znaleźć na etykiecie z tyłu routera 4G-AC86U.

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 **5.2 Odtwarzanie oprogramowania sprzętowego**.

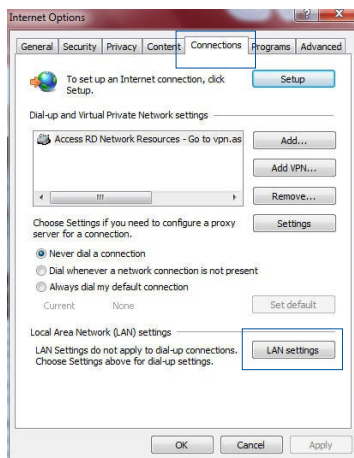
Nie można uzyskać dostępu do sieciowego interfejsu graficznego

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)** > zakładkę **Connections (Połączenia)** > **LAN settings (Ustawienia sieci LAN)**.

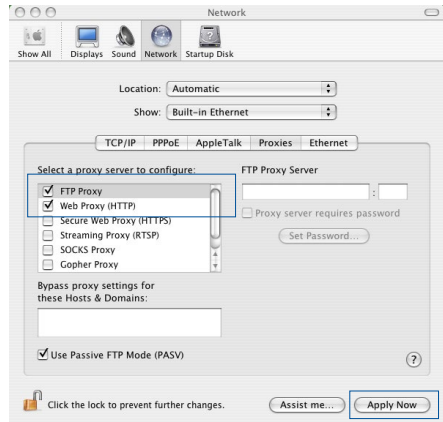


3. Na ekranie Local Area Network (LAN) Settings (Ustawienia sieci lokalnej (LAN)) odznacz opcję **Use a proxy server for your LAN (Użyj serwera proxy dla sieci LAN)**.
4. Po zakończeniu kliknij przycisk **OK**.



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)**.

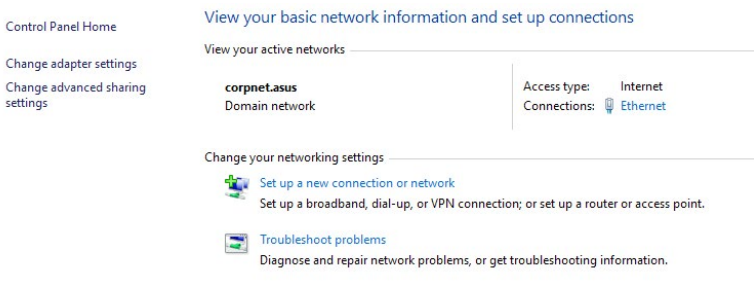


UWAGA: Szczegółowe informacje dotyczące wyłączenia serwera proxy, patrz funkcja pomocy danej przeglądarki.

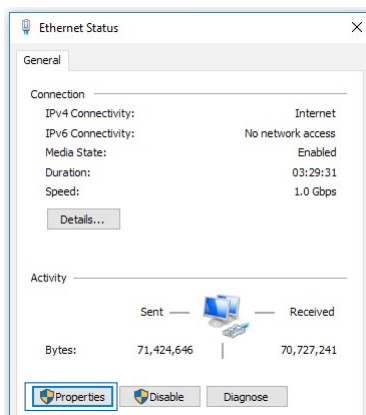
B. Skonfigurować ustawienia TCP/IP do automatycznego uzyskiwania adresu IP.

Windows®

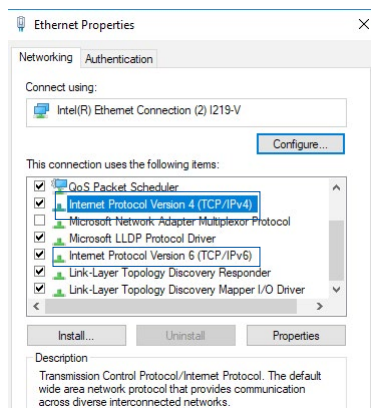
1. Kliknij przycisk **Start > Control Panel (Panel Sterowania) > Network and Sharing Center (Centrum sieci i udostępniania)**, następnie kliknij połączenie sieciowe, aby wyświetlić okno stanu.



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



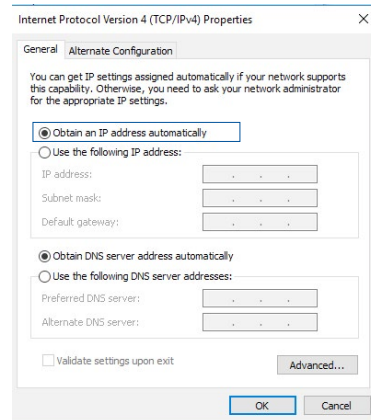
3. Zaznacz opcję **Internet Protocol Version 4 (TCP/IPv4)** (Protokół internetowy w wersji 4 (TCP/IPv4)) lub **Internet Protocol Version 6 (TCP/IPv6)** (Protokół internetowy w wersji 6 (TCP/IPv6)), a następnie kliknij przycisk **Properties** (**Właściwości**).




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

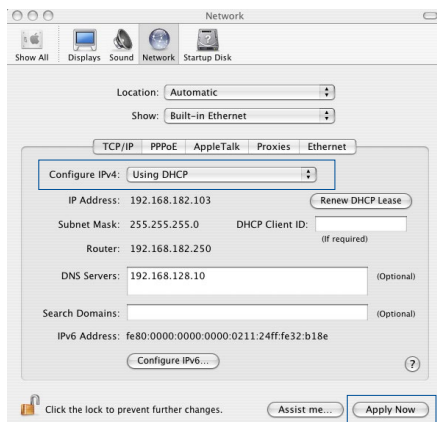
W celu automatycznego uzyskania ustawień IPv6 IP, zaznacz opcję **Obtain an IPv6 address automatically** (**Automatycznie uzyskaj adres IPv6**).

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)**.

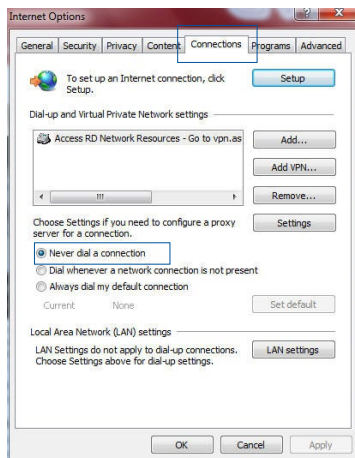


UWAGA: Informacje dotyczące konfiguracji ustawień połączenia TCP/IP komputera patrz pomoc systemu operacyjnego i funkcje wsparcia.

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) > zakładkę 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

Notices

ASUS Recycling/Takeback Services

ASUS recycling and takeback programs come from our commitment to the highest standards for protecting our environment. We believe in providing solutions for you to be able to responsibly recycle our products, batteries, other components, as well as the packaging materials. Please go to <http://csr.asus.com/english/Takeback.htm> for the detailed recycling information in different regions.

REACH

Complying with the REACH (Registration, Evaluation, Authorisation, and Restriction of Chemicals) regulatory framework, we published the chemical substances in our products at ASUS REACH website at

<http://csr.asus.com/english/index.aspx>

Federal Communications Commission Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

IMPORTANT! This device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

WARNING!

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
 - Users must not modify this device. Modifications by anyone other than the party responsible for compliance with the rules of the Federal Communications Commission (FCC) may void the authority granted under FCC regulations to operate this device.
 - For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
-

CE statement

Simplified EU Declaration of Conformity

ASUSTek Computer Inc. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. Full text of EU declaration of conformity is available at <https://www.asus.com/support/>

Declaration of Conformity for Ecodesign directive 2009/125/EC

Testing for eco-design requirements according to (EC) No 1275/2008 and (EU) No 801/2013 has been conducted. When the device is in Networked Standby Mode, its I/O and network interface are in sleep mode and may not work properly. To wake up the device, press the Wi-Fi on/off, LED on/off, reset, or WPS button.

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

All operational modes:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40) , 802.11n (HT80)

The frequency, mode and the maximum transmitted power in EU are listed below:


2412-2472MHz (802.11n HT40 MCS 8): 19.97 dBm

5180-5240MHz (802.11n HT40 MCS 8): 22.43 dBm

5260-5320MHz (802.11n HT40 MCS 8): 22.81 dBm

5500-5700MHz (802.11n HT20 MCS 8): 29.75 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range.

	AT	BE	BG	CZ	DK	EE	FR
	DE	IS	IE	IT	EL	ES	CY
	LV	LI	LT	LU	HU	MT	NL
	NO	PL	PT	RO	SI	SK	TR
	FI	SE	CH	UK	HR		

Safety Notices

- Use this product in environments with ambient temperatures between 0°C(32°F) and 40°C(104°F).
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- DO NOT place on uneven or unstable work surfaces. Seek servicing if the casing has been damaged.
- DO NOT place or drop objects on top and do not shove any foreign objects into the product.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the modem during electrical storms.
- DO NOT cover the vents on the product to prevent the system from getting overheated.
- DO NOT use damaged power cords, accessories, or other peripherals.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.

CE Mark Warning

This is a Class B product, in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

This equipment may be operated in AT, BE, CY, CZ, DK, EE, FI, FR, DE, GR, HU, IE, IT, LU, MT, NL, PL, PT, SK, SL, ES, SE, GB, IS, LI, NO, CH, BG, RO, RT.

Radio Frequency (RF) Exposure Information

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 31 cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 31 cm de distance entre la source de rayonnement et votre corps.

Canada, avis d'Industry Canada (IC)

Le présent appareil est conforme aux normes CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

Son utilisation est sujette aux deux conditions suivantes : (1) cet appareil ne doit pas créer d'interférences et (2) cet appareil doit tolérer tout type d'interférences, y compris celles susceptibles de provoquer un fonctionnement non souhaité de l'appareil.

NCC 警語

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

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. We include a copy of the GPL with every CD shipped with our product. 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

For Turkey only

Authorised distributors in Turkey:

BOGAZICI BİL GİSAYAR SAN. VE TİC. A.S.

Tel. No.: +90 212 3311000

Address: AYAZAGA MAH. KEMERBURGAZ CAD. NO.10
AYAZAGA/İSTANBUL

CIZGI Elektronik San. Tic. Ltd. Sti.

Tel. No.: +90 212 3567070

Address: CEMAL SURURI CD. HALİM MERİC İS MERKEZİ
No: 15/C D:5-6 34394 MECİDİYEKOY/İSTANBUL

KOYUNCU ELEKTRONİK BİLGİ İSLEM SİST. SAN. VE DİŞ TİC. A.S.

Tel. No.: +90 216 5288888

Address: EMEK MAH.ORDU CAD. NO:18, SARİGAZİ,
SANCAKTEPE İSTANBUL

ENDEKS BİLİŞİM SAN VE DİŞ TİC LTD ŞTİ

Tel. No.: +90 216 523 35 70 (pbx)

Address: Bulgurlu Mahallesi Alemdağ Caddesi No:56 /
B-1 34696 Üsküdar/ İSTANBUL

AEEE Yönetmeliğine Uygundur.

Informacje kontaktowe producenta

ASUSTeK COMPUTER INC. (Asia Pacific)

Adres 1F., No. 15, Lide Rd., Beitou Dist., Taipei City 112,
Taiwan
Telefon +886-2-2894-3447
Faks +886-2-2893-1687
Strona internetowa <https://www.asus.com>

Pomoc techniczna

Telefon +86-21-38429911
Wsparcie online <https://qr.asus.com/techserv>

ASUS COMPUTER INTERNATIONAL (Ameryka)

Adres 48720 Kato Rd., Fremont, CA 94538, USA
Telefon +1-510-739-3777
Faks +1-510-608-4555
Strona internetowa <https://www.asus.com/us/>

Pomoc techniczna

Fax (wsparcie) +1-812-284-0883
Telefon +1-812-282-2787
Wsparcie online <https://qr.asus.com/techserv>

ASUS COMPUTER GmbH (Niemcy i Austria)

Adres Harkortstrasse 21-23, 40880 Ratingen, Germany
Web site <https://www.asus.com/de>
Kontakt online <https://www.asus.com/support/Product/ContactUs/Services/questionform/?lang=de-de>

Pomoc techniczna

Telefon (DE) +49-2102-5789557
Telefon (AT) +43-1360-2775461
Wsparcie online <https://www.asus.com/de/support>