Instrukcja obsługi

Asmax BR615N Wireless

Nowości, dane techniczne – http://www.asmax.pl
Sterowniki, firmware – ftp://ftp.asmax.pl/pub/sterowniki
Instrukcje, konfiguracje – ftp://ftp.asmax.pl/pub/instrukcje

Copyright (c) 2009, Asmax International. All Rights Reserved.

Ta instrukcja jest przeznaczona dla użycia z urządzeniem Asmax BR615N Wireless. Informacje zawarte w tym dokumencie zostały sprawdzone dla danego urządzenia; jednakże nie ma żadnej gwarancji na jej poprawną zawartość. Producent nie daje żadnej gwarancji i nie przyjmuje zażaleń dotyczących dokładności, kompletności tego dokumentu i nie będzie w żadnym wypadku odpowiedzialny za jakąkolwiek stratę albo szkodę.

Ten produkt jest chroniony prawami autorskimi. Treść niniejszej publikacji nie może być powielana w jakiejkolwiek części lub w całości, przechowywana, zapisana w systemie wyszukiwania informacji, tłumaczona na jakikolwiek język lub przesyłana w jakiejkolwiek formie lub w jakikolwiek sposób, mechaniczne, magnetyczne, elektroniczne, optycznie, ksero, instrukcja obsługi lub w inny sposób, bez uprzedniej pisemnej zgody właściciela. Marka i nazwa produktu są znakami fabrycznymi poszczególnych przedsiębiorstw. Są one używane do celów identyfikacji. Specyfikacje mogą ulec zmianie bez uprzedniego powiadomienia.

Zawartość

Świadectwo zgodności FCC

Niniejsze urządzenie spełnia wymogi części 15 przepisów Federalnej Komisji Komunikacji (FCC klasa B, część 15).

UWAGA: Wszelkie przeróbki tego urządzenia, na które nie uzyskano wyraźnej zgody instytucji odpowiedzialnej za przestrzeganie zgodności z normami, mogą skutkować utratą prawa do korzystania z urządzenia. To urządzenie przeszło pomyślnie testy na zgodność z normą dla urządzeń cyfrowych klasy B w rozumieniu części 15 przepisów FCC. Normy te mają zapewnić należytą ochronę przed szkodliwą interferencją z innymi urządzeniami w budynkach mieszkalnych. To urządzenie generuje, używa i może emitować fale o częstotliwości radiowej, a jeśli nie zostało zainstalowane zgodnie z instrukcjami, może powodować zakłócenia w łączności radiowej. Nie można jednak zagwarantować, że w konkretnej konfiguracji interferencja nie będzie miała miejsca. Jeśli urządzenie stwarza interferencję zakłócającą pracę odbiorników radiowych i telewizyjnych, co da się stwierdzić przez jego wyłączenie i ponowne włączenie, można zastosować poniższe zabiegi, by zmniejszyć intensywność zakłóceń:

• Zmienić ukierunkowanie anteny odbiorczej lub przenieść ją w inne miejsce.
• Zwiększyć dystans między odbiornikiem a miejscem eksploatacji urządzenia.
• Podłączyć urządzenie do gniazda należącego do odrębnego obwodu niż ten, do którego przyłączony jest odbiornik.
• Zasięgnąć porady sprzedawcy.

Stanowisko FCC dotyczące promieniowania radiowego

Niniejsze urządzenie pozostaje w zgodności z ograniczeniami i limitami ustalonymi przez FCC, dotyczącymi stopnia emisji fal radiowych w środowisku niekontrolowanym.
Urządzenie oraz jego antena nie powinny być umieszczane w bezpośrednim sąsiedztwie innej działającej anteny, bądź nadajnika/odbiornika.
„By spełniać wymagania FCC dotyczące emisji fal radiowych, antena używana wraz z niniejszym urządzeniem musi być zainstalowana z zachowaniem przynajmniej dwudziestocentymetrowego odstępu od ludzi oraz nie może znajdować się w bezpośrednim sąsiedztwie innej działającej anteny, bądź nadajnika/odbiornika”.

Urządzenie zostało zaprojektowane i wyprodukowane z najwyższą starannością o bezpieczeństwo osób instalujących i użytkujących. Dla zapewnienia bezpieczeństwa pracy należy stosować się do wszelkich wskazań zawartych w tej instrukcji jak i instrukcjach obsługi urządzeń towarzyszących (np. komputera PC). Nie powinno się przebywać w odległości mniejszej niż 20cm od pracującego urządzenia.

Deklaracja zgodności CE

Niniejsze urządzenie spełnia ograniczenia emisji szumu radiowego określone dla urządzeń klasy B zgodnie z normą dla sprzętu wytwarzającego zakłócenia sygnałów radiowych.

Zawartość opakowania

W opakowaniu powinny znajdować się następujące elementy:

- Wireless Router Asmax BR615N
- Zasilacz (12V DC 500mA)
- Płyta CD-ROM z instrukcją obsługi
- Kabel sieciowy (RJ-45)
- Instrukcja instalacji

W przypadku braku któregokolwiek z elementów proszę o kontakt ze sprzedawcą. Instrukcje obsługi oraz sterowniki można pobrać bezpłatnie z serwera ftp://ftp.asmax.pl/pub z katalogu sterowniki oraz instrukcje.

Wprowadzenie

Router Asmax BR615N jest wydajnym szerokopasmowym urządzeniem dostępowym z rozbudowaną funkcjonalnością, umożliwiającym podzielenie jednego łącza Internetowego dla wielu użytkowników sieci lokalnej LAN i WLAN chronionych poprzez wbudowany wydajny firewall, NAT i funkcje blokowania i wykrywania ataków hakerskich. Urządzenie posiada wbudowany bardzo szybki punkt dostępowy w standardzie 802.11 b/g/n mogący pracować z prędkościami do 150Mbps, także jako klient sieci bezprzewodowej. Wbudowany punkt dostępowy posiada możliwość utworzenia pięciu sieci bezprzewodowych i izolację klientów sieci bezprzewodowej, regulację mocy punktu bezprzewodowego. Asmax BR615N jest routerem umożliwiającym proste utworzenie dwóch podsieci i rozbudowanie sieci LAN (adresacja dla 506 komputerów). Urządzenie posiada rozbudowany serwer DHCP pozwalający przypisanie komputerowi, czy innemu urządzeniu w naszej sieci lokalnej stały, zawsze taki sam adres IP. Dzięki takiemu rozwiązaniu nie musimy za każdym razem szukać danego urządzenia w sieci lokalnej. Urządzenie posiada trzy tryby pracy, może być zwykłym routerem xDSL, klientem sieci bezprzewodowej lub mostem sieciowym. Urządzenie posiada możliwość klonowania adresu MAC na porcie WAN. Urządzenie posiada też funkcję TTL, dzięki czemu nawet, jeśli nasz ISP stosuje filtrację TTL będziemy mogli łatwo rozdzielić Internet. Bez problemów zapanujemy też nad naszym łączem internetowym dzięki zaawansowanej, ale prostej w obsłudze funkcji zarządzania pasmem QoS. Asmax BR615N jest urządzeniem klasy SOHO (ang. Small Office and Home Office), przeznaczonym dla sieci domowych oraz małych firm. Asmax BR615N jest w pełni konfigurowalny w prosty sposób z poziomu przeglądarki internetowej. Umożliwia bezpieczne podłączenie wielu

użytkowników sieci lokalnej LAN, wyposażonych zarówno w karty Ethernet, jak i bezprzewodowe w standardzie 802.11b/g/n do Internetu przez dowolne łącze xDSL, modem kablowy lub sieć Ethernet. Urządzenie stanowi idealne połączenie wszystkich potrzebnych funkcji, jakie są potrzebne, by móc wygodnie stworzyć wydajną, stabilną, prostą w zarządzaniu i co najważniejsze bezpieczną sieć z dostępem do Internetu. Połącz się z punktem dostępowym i uzyskaj dostęp do szybkiego łącza w standardzie 802.11n, kiedy udostępniasz bądź pobierasz zdjęcia, pliki, muzykę, wideo, drukarki, oraz gdy korzystasz z dysków sieciowych i zgromadzonych na nich danych. Dzięki szybkiemu połączeniu z siecią bezprzewodową możesz cieszyć się płynnymi rozmowami telefonicznymi, grami sieciowymi, transmisją wideo, zwiększonym zasięgiem. Dzięki technologii 802.11n, zwiększono przepustowość do maksymalnej wartości 150Mbps. Dzięki dodaniu przycisku WPS teraz możesz w szybki i bezpieczny sposób połączyć bezprzewodowo z routerem Asmax BR615N inne urządzenia bezprzewodowe wpierające funkcję WPS.

Zastosowanie

- Sieć bezprzewodowa w domu / biurze
- TV over IP (IPTV)
- Voice over IP (VoIP)
- Bardzo szybka wymiana danych (plików, aplikacji) pomiędzy urządzeniami
- Udostępnianie Internetu szerokopasmowego
- Transmisja audio i video
- Gry sieciowe i internetowe
- Obsługuje do 506 użytkowników
- Dostęp do Prywatnych Serwerów LAN z Sieci Publicznej
- Zastosowania Specjalne, DMZ, Serwery Wirtualne, Kontrola Dostępu, Firewall, QoS

Właściwości urządzenia

- Zgodność ze standardami IEEE802.11b, IEEE802.11g, IEEE802.11n, IEEE802.3, IEEE802.3u, IEEE802.11i, IEEE802.11e.
- Port WAN (RJ45) 10/100M z auto-negocjacją, 4 porty LAN (RJ45) 10/100M z auto-negocjacją i wykrywaniem przeplotu (Auto MDI/MDIX).
- Możliwość pracy na dwóch podsieciach jednocześnie.
- Wsparcie dla prędkości transmisji 150/54/48/36/24/18/12/9/6Mbps.
- Udostępnia uwierzytelnianie WPA/WPA2, WPA-PSK/WPA2-PSK z szyfrowaniem TKIP/AES.
- Umożliwia dostęp do Internetu korzystając z protokołów PPPoE, Dynamic IP, Static IP, L2TP, PPTP.
- Obsługuje funkcje Virtual Server, DMZ, DNS proxy, filtrowania treści po adresach URL/IP/MAC, portach.
- Obsługuje UPnP, dynamiczny DNS, statyczny oraz dynamiczny routing, VPN Pass-through
- Odłączana antena na złączu RP-SMA.

- Podłączanie na żądanie i odłączanie po określonym czasie bezczynności dla PPPoE.
- Wbudowane serwery NAT i DHCP umożliwiające przydzielanie stałych adresów IP.
- Wbudowany zaawansowany firewall.
- Umożliwia łączenie/rozłączenie połączenia internetowego w określonych godzinach.
- Wspiera kontrolę dostępu, umożliwiając rodzicom lub administratorom na ograniczenie dostępu dzieciom lub pracownikom w określonych godzinach.
- Udostępnia 64/128/152-bitowe szyfrowanie WEP i LAN ACL (Access Control List – lista kontroli dostępu).
- Wsparcie dla funkcji zdalnego dostępu do urządzenia.
- Wsparcie dla logowania zdarzeń i wprowadzenia komend bezpośrednio z panelu web.
- Udostępnia statystyki.
- Funkcja zapisywania kopii i przywracania pliku konfiguracyjnego.
- Obsługuje zaawansowaną ochronę przed atakami z Internetu.
- Umożliwia ignorowanie pakietów ping z portów WAN i LAN.
- Umożliwia aktualizację oprogramowania za pomocą przeglądarki internetowej.
- Wsparcie dla zaawansowanego zarządzania pasmem QoS i zasady tworzenia reguł w oparciu o protokół, port, adres IP, DSCP lub aplikacje.

Kraje przeznaczenia

Urządzenie jest przystosowane do pracy na terenie Polski. Urządzenie pracujące w trybie ETSI jest przeznaczone do pracy w warunkach domowych i biurowych w krajach Unii Europejskiej, a także w Norwegii i Szwajcarii – krajach członkowskich EFTA. Francja dopuszcza pracę tego urządzenia wyłącznie na kanałach: 10, 11, 12, 13.

Bezpieczeństwo urządzenia i gwarancja

Zapoznaj się z punktami poniżej, by chronić urządzenie przed wszelkiego rodzaju przepięciami występujących w sieci energetycznej i podczas wyładowań atmosferycznych.

- Proszę używać tylko zasilaczy zalecanych przez producenta urządzenia i dostarczonych wraz z urządzeniem.
- Chroń urządzenie przed przepięciami zwłaszcza w czasie wyładowań atmosferycznych.
- Przeciążone gniazdo sieciowe albo uszkodzone linie i wtyczki mogą spowodować porażenie prądem albo nieszczęśliwy wypadek.
- Właściwa przestrzeń pozostawiona dla wentylacji urządzenia jest konieczna, aby uniknąć przegrzania się urządzenia. Otwory w urządzeniu zaprojektowane w celu odprowadzania nadmiaru gorącego powietrza. Nie zakrywaj otworów wentylacyjnych urządzenia.
- Nie umieszczaj urządzenia blisko źródeł ciepła albo tam, gdzie jest wysoka temperatura.
- Nie kładź tego urządzenia w miejscu wilgotnym bądź wodnistym. Nie rozlewaj żadnego płynu na to urządzenie.

- Nie umieszczaj tego urządzenia na niestabilnej powierzchni albo podparciu.

Uszkodzenia powstałe z winy użytkownika, takie jak:

- Mechaniczne uszkodzenie urządzenia.
- Zalanie urządzenia, niewłaściwe jego zamontowanie (zbyt duża wilgoć, wysoka temperatura pracy, wysokie zapylenie, brak obiegu powietrza).
- Wgranie firmware od innego urządzenia.
- Zastosowanie innego zasilacza niż dołączonego w zestawie.
- Wad instalacji elektrycznej i Ethernet.
- Przepięć z instalacji elektrycznej i Ethernet (w tym przepięć generowanych podczas wyładowań atmosferycznych).

Nie podlegają gwarancji.

Urządzenia rozkręcone, z uszkodzonymi plombami gwarancyjnymi i/lub etykietami producenta, z uszkodzonymi numerami seryjnymi nie podlegają gwarancji.

Miejsce zamontowania urządzenia

Aby zapewnić jak najlepszą pracę urządzenia, powinno ono zostać zamontowane w miejscu o małej wilgotności powietrza, z dala od słońca i innych źródeł ciepła, umożliwiających swobodny przepływ powierza chłodzącego jego elementy. Chroń urządzenie przed zalaniem.

Wybieranie najlepszej lokalizacji dla pracy sieci bezprzewodowej

Wiele czynników środowiskowych może oddziaływać na pracę sieci bezprzewodowej. Jeśli jest to Twoja pierwsza konfiguracja urządzenia bezprzewodowego to przeczytaj i rozważ punkty umieszczone poniżej. Asmax BR615N zaprojektowano, by pokrył zasięgiem obszar do 100 metrów wewnątrz i do 300 metrów na zewnątrz, dzięki czemu możesz pozbyć się kabli i cieszyć się dostępem do Internetu w obrębie zasięgu routera. Jednakże liczba ścian, strop albo inne przedmioty, które przepuszczają sygnał sieci bezprzewodowej mogą ograniczyć sygnał pasma. Dla uzyskania optymalnego zasięgu uwzględnij podstawowe wskazówki:

- **Pamiętaj, że liczba ścian i sufitów ma wpływ na moc sygnału:**

Sygnał sieci bezprzewodowej LAN może przebić się przez ściany i sufit. Jednakże każda ściana lub sufit może zmniejszyć zasięg urządzenia bezprzewodowego LAN od 1 do 30 metrów.

- **Przeszkody:**

Pozycja urządzenia bezprzewodowego musi być taka, żeby sygnał miał na przeszkodzie jak najmniej ścian żelbetonowych oraz metalicznych materiałów.

- **Pozycja anteny dla najlepszego odbioru:**

Poruszaj anteną dookoła, żeby zobaczyć, czy amplituda sygnału się poprawia. Pozostaw antenę w takiej pozycji, w jakiej uzyskasz najlepszy sygnał.

- **Trzymaj urządzenie w odległości co najmniej 1-2 metry od urządzeń elektrycznych**

Lokalizacja urządzenia bezprzewodowego musi być oddalona od elektrycznych urządzeń, które generują duże zaszumienie sygnału radiowego, takie jak kuchenki mikrofalowe, monitory, silniki elektryczne, itd.

Wskaźniki i złącza urządzenia

Przedni panel

Na przednim panelu znajdują się diody LED sygnalizujące status operacji wykonywanych przez router.

Funkcje wskaźników LED:

Dioda LED	Kolor	Status	Opis
Power	Czerwona	Włączona	Zasilanie zostało włączone
	Zielona	Włączona	Urządzenie uruchomione prawidłowo
	-	Wyłączona	Zasilanie urządzenia jest wyłączone
WLAN	Zielona	Włączona	WiFi zostało włączone
	Zielona	Miga	Dane są przesyłane przez sieć bezprzewodową
	-	Wyłącozna	WiFi zostało wyłączone
WPS	Zielona	Włączona	Nawiązano połączenie z Wi-Fi Protected Setup (WPS).
	Zielona	Miga	Negocjacja z klientem bezprzewodowym w trybie Wi-Fi Protected Setup (WPS).
	-	Wyłączona	Wi-Fi Protected Setup (WPS) jest wyłączone.
WAN	Zielona	Włączona	Aktywny port WAN, nawiązano połączenie z ISP
	Zielona	Miga	Dane za pomocą portu WAN są transmitowane.
	-	Wyłączona	Brak połączenia na porcie WAN.
LAN 1/2/3/4	Zielona	Włączona	Aktywny dany port LAN (1-4), nawiązano połączenie z podłączonym urządzeniem.
	Zielona	Miga	Dane na konkretnych portach (1-4) są transmitowane.
	-	Wyłączona	Brak połączenia na danym pocie (1-4)

Tylni panel

Na tylnim panelu znajdują się wszystkie gniazda złącz sieciowych i zasilania, przycisk włączenia/wyłączenia zasilania oraz przycisk RESTART umożliwiający przywrócenie ustawień fabrycznych (przytrzymany przez 6 sekund).

Interface/Button	Description
Reset	Przycisk służący do przywracania ustawień fabrycznych.
Power	Złącze zasilania służące do podłączenia zasilacza (12VDC 500mA).
WAN	Gniazdo Ethernet RJ45 interfejsu WAN
LAN1~LAN4	Gniazda Ethernet RJ45 interfejsu LAN
WPS	Przycisk nawiązywania połączenia ze stacją bezprzewodową za pomocą WPS. Należy przytrzymać wciśnięty przycisk WPS przez około 2-3 sekundy, gdy stacja bezprzewodowa obsługująca WPS próbuje się połączyć (funkcja WPS PBC musi być włączona).

Uwaga: Nie naciskaj przycisku „Reset”, chyba że chcesz wyczyścić bieżące ustawienia. Przycisk resetowania znajduje się w małym otworze na tylnym panelu. Jeśli chcesz przywrócić domyślne ustawienia, proszę nacisnąć przycisk „Reset” delikatnie przez 6 sekund cienką igłą wprowadzoną w otwór, a następnie zwolnić przycisk. Nastąpi ponowne uruchomienie urządzenia i powrót do ustawień fabrycznych. W domyślnej konfiguracji urządzenie posiada adres IP 192.168.1.1, login: **admin**, hasło: **admin**. Domyślnie włączony jest serwer DHCP, dzięki czemu po podłączeniu komputera otrzymamy automatycznie adres IP z właściwego zakresu. Hasło domyślne należy zmienić na własne, a gdy zapomnimy podane nowe hasło, możemy przywrócić ustawienia fabryczne urządzenia. Gdy posiadasz dostęp do interfejsu użytkownika możesz przywrócić ustawienia domyślne klikając na zakładkę: **Administration-->Configuration-->Load Factory Defaults** i kliknąć **Load Default.**

Przygotowanie do konfiguracji urządzenia Asmax BR615N

1) Komputer należy podłączyć do urządzenia Asmax BR615N za pomocą kabla sieciowego RJ45. W celu pierwszej konfiguracji podłączamy komputer kablowo bezpośrednio do portu LAN. Wszystkie porty LAN routera wykonane są w technologii umożliwiającej automatyczne włączenie autoprzeplotu. Urządzenie automatycznie dobiera maksymalną dostępną prędkość połączenia dzięki funkcji autonegocjacji prędkości. Transmisja z prędkością 10/100 Mb/s wymaga użycia kabla kategorii 5 z wtykami RJ-45. W przypadku kabla prostego obie wtyczki muszą być zaciśnięte w standardzie EIA/TIA 568B. W przypadku kabla z przeplotem, jedna wtyczka powinna być w standardzie EIA/TIA 568A, a druga w EIA/TIA 568B. Po podłączenia urządzenia do jednego z portów odpowiednia dioda zacznie migać sygnalizując proces autodiagnostyki portu oraz negocjację prędkości połączenia. Następnie, aby uzyskać połączenie z routerem należy ustawić automatyczne pobieranie adresu sieciowego (serwer DHCP w routerze jest domyślnie włączony) lub przypisać adres IP i inne parametry naszego połączenia lokalnego ręcznie. Zalecana jest opcja automatycznego pobierania parametrów sieciowych z serwera DHCP urządzenia Asmax BR615N, umożliwi to automatyczne przydzielenie adresu IP, maski podsieci, bramy domyślnej oraz adresów serwerów DNS dla urządzeń w sieci LAN. Jak ustawić komputer w celu automatycznego pobrania danych z serwera DHCP opiszemy poniżej w kolejnych krokach. Proszę pamiętać, iż w standardzie Ethernet długość kabla sieciowego nie może przekraczać 100m. Po skonfigurowaniu urządzenia można również podłączyć komputery wyposażone w karty bezprzewodowe standardu 802.11b/g/n.

2) Podłącz urządzenie do sieci Internet, wpinając kabel od naszego dostawcy usług internetowych (ISP) do portu WAN.

3) Podłącz zasilacz do sieci elektrycznej oraz do gniazda POWER.
Podłącz zasilacz do sieci elektrycznej 230V/50Hz, a następnie do gniazda POWER w routerze 12V DC 500mA.

Uwaga!

Proszę używać tylko zasilaczy zalecanych przez producenta urządzenia i dostarczonych wraz z urządzeniem. Chroń urządzenie przed przepięciami zwłaszcza w czasie wyładowań atmosferycznych. Korzystanie z zasilacza o innym napięciu znamionowym niż w zasilaczu dołączonym do urządzenia Asmax BR615N spowoduje uszkodzenie routera i utratę praw gwarancyjnych.

Konfiguracja protokołu TCP/IP do współpracy z serwerem DHCP urządzenia Asmax BR615N

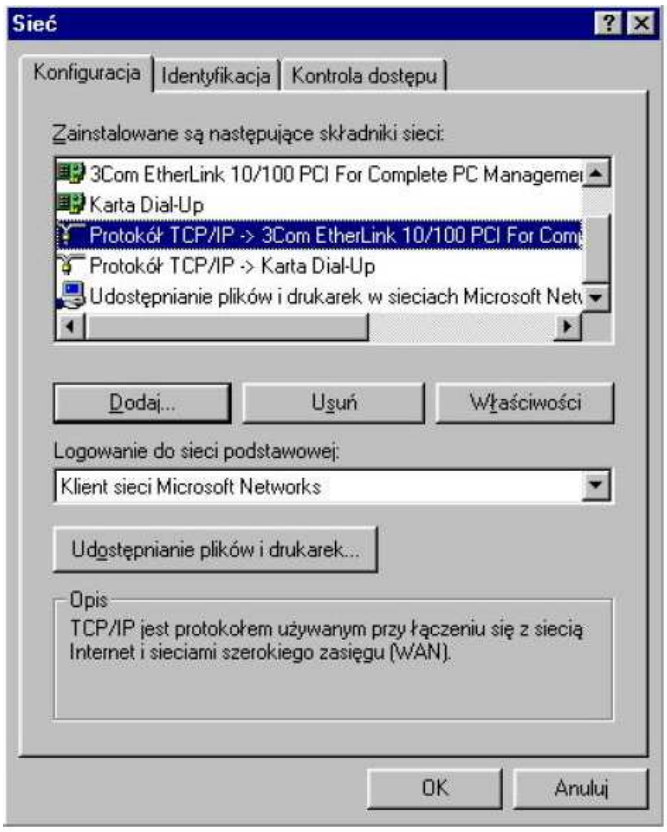
Wszystkie komputery w sieci LAN muszą należeć do podsieci interfejsu LAN routera. W tym celu najłatwiej skorzystać z serwera DHCP wbudowanego w routerze , który domyślnie jest włączony. Wystarczy na każdym z hostów w sieci LAN ustawić klienta DHCP kierując się następującymi krokami:

(dla Windows 98, 98SE, ME)

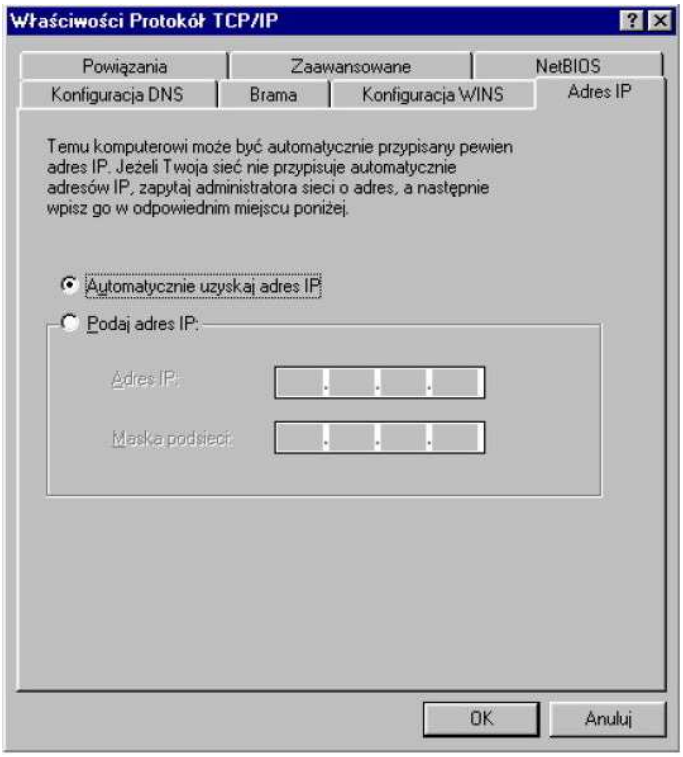
Krok 1: Wybierz z Menu Start – Ustawienia – Panel Sterownia.

Krok 2: Zaznacz ikonkę Sieć i podwójnie kliknij na niej lub kliknij prawym przyciskiem myszy i wybierz opcję „Otwórz”.

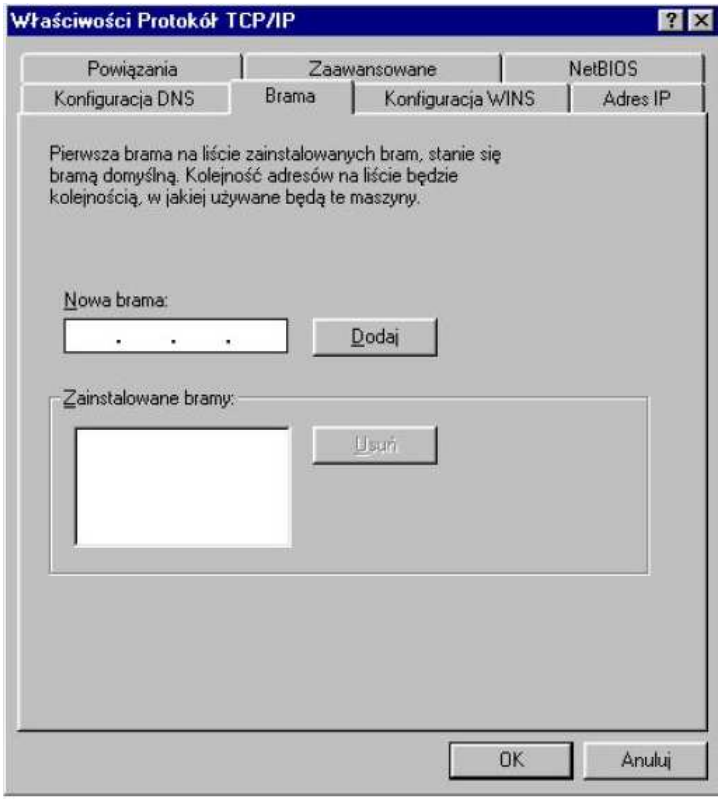
Krok 3: W zakładce Konfiguracja wybierz Protokół TCP/IP dla danej karty sieciowej i kliknij przycisk „Właściwości”.



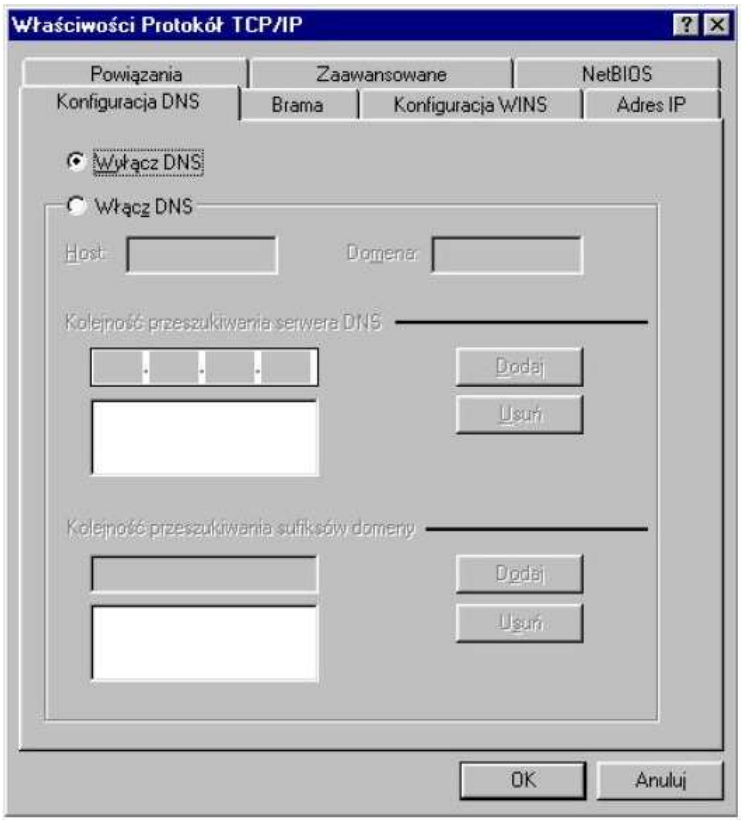
Krok 4: W zakładce Adres IP wybierz opcję Automatycznie uzyskaj adres IP.



Krok 5: W zakładce Brama wyczyść wszystkie wpisy przyciskiem Usuń. Lista „Zainstalowane bramy” musi być pusta.

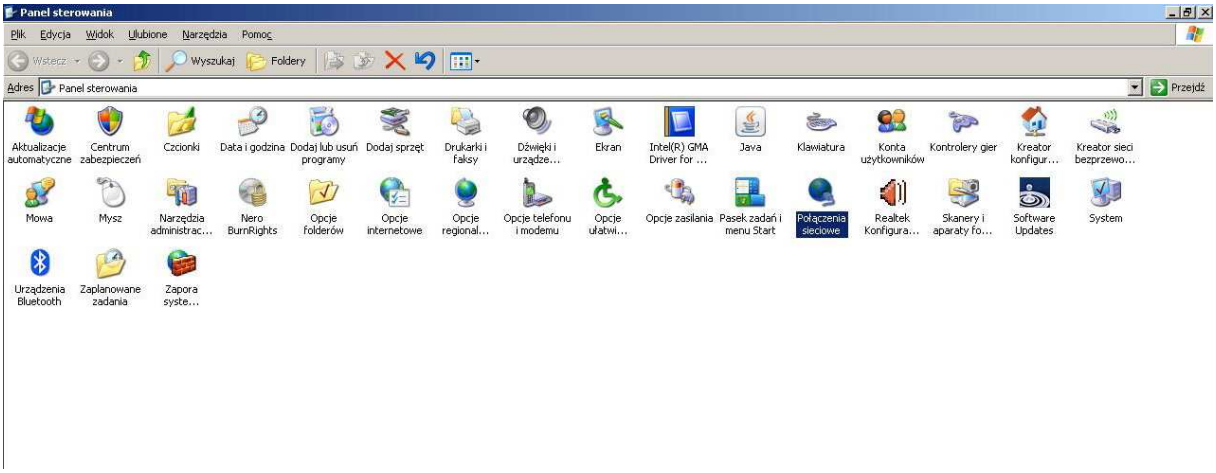


Krok 6: W zakładce Konfiguracja DNS zaznacz opcję Wyłącz DNS, a następnie kliknij przycisk OK.

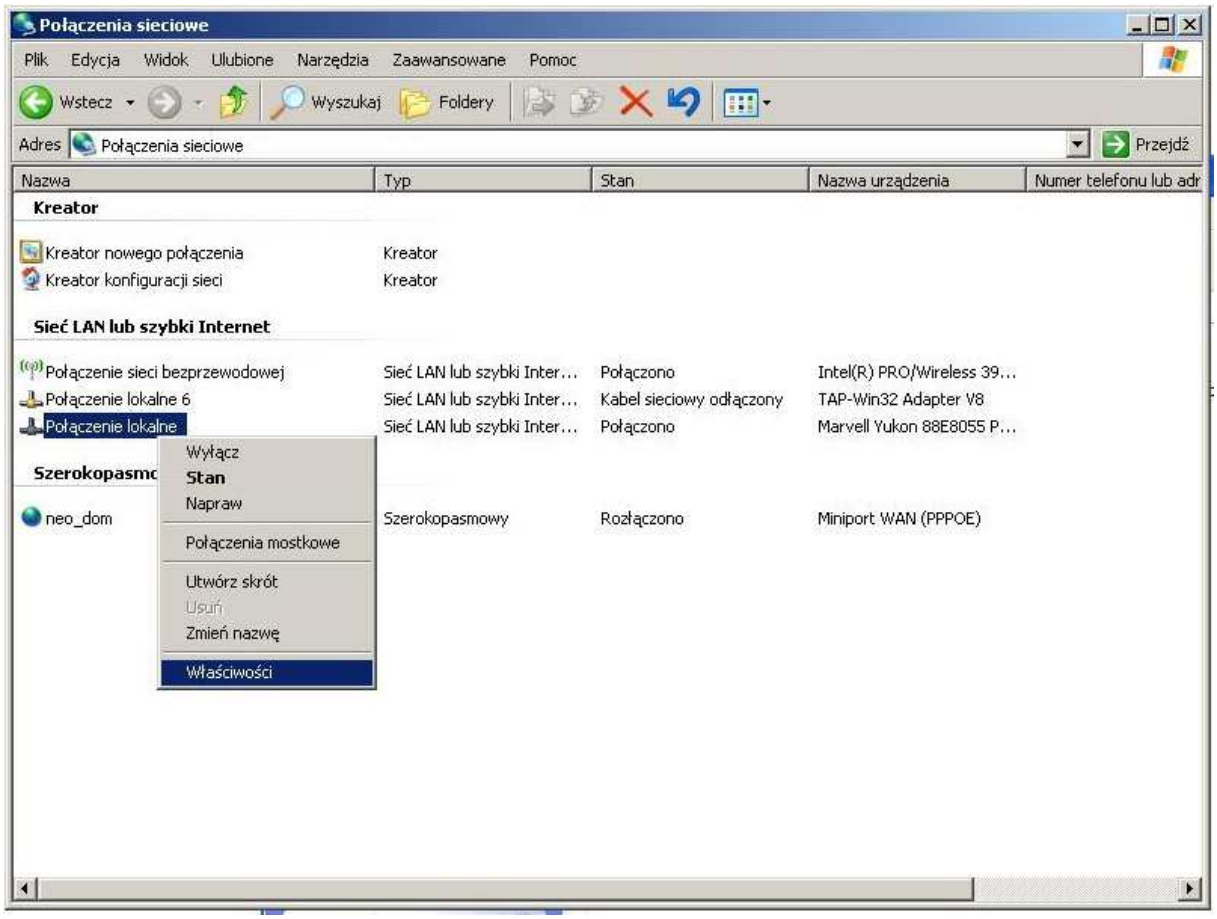


(Dla Windows 2000, XP, 2003)

Krok 1: Wybierz z menu Start „Panel sterownia”, a następnie opcję „Połączenia sieciowe i internetowe”.

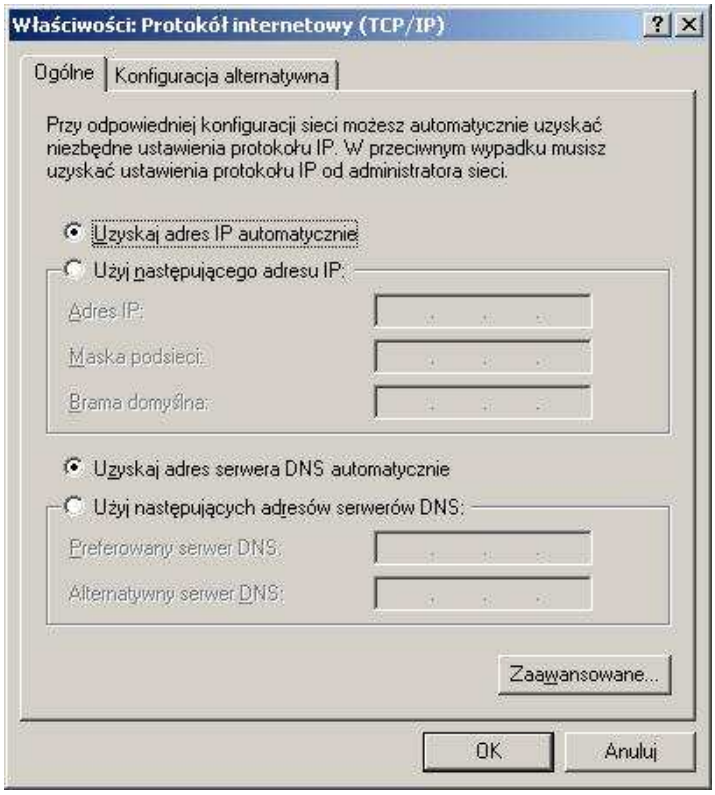


Krok 2: Po wejściu w „Połączenia sieciowe” zaznacz połączenie lokalne, z którego będziesz korzystał prawym przyciskiem myszy i wybierz „Właściwości”.



Krok 3: Wybierz z listy opcję „Protokół internetowy (TCP/IP)” i kliknij przycisk Właściwości.

Krok 4: Zaznacz opcję „Uzyskaj adres IP automatycznie” oraz „Uzyskaj adres serwera DNS automatycznie”, a następnie kliknij przycisk OK.

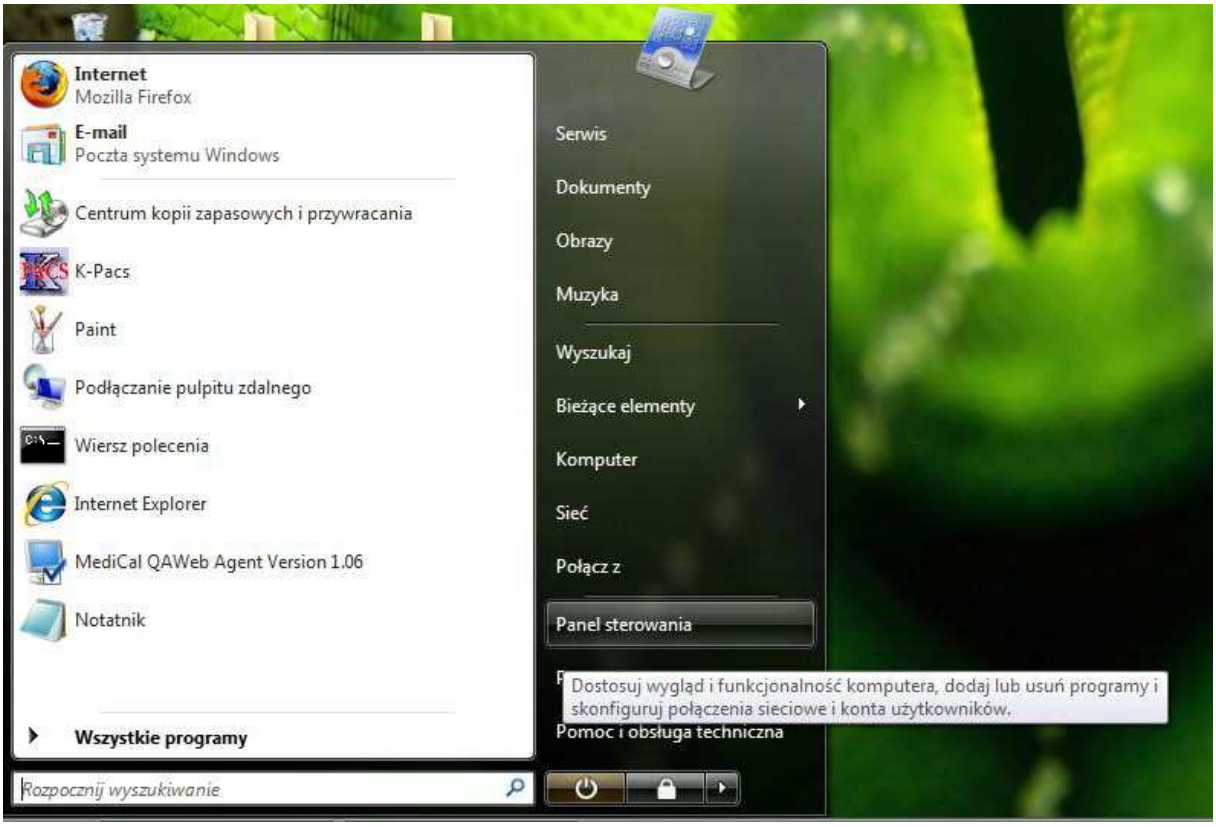


Uwaga! Połączenie sieciowe może posiadać również stały adres IP. Należy jednak zachować szczególną ostrożność przy konfiguracji protokołu TCP/IP. Adres IP komputera lub innego urządzenia musi być zgodny z podsiecią routera. Komputery w sieci LAN muszą mieć różne adresy IP. Należy również pamiętać, że przy statycznej adresacji hostów w sieci LAN każdy host musi mieć wpisany: swój adres IP z maską podsieci, domyślną bramę i adresy serwerów DNS.

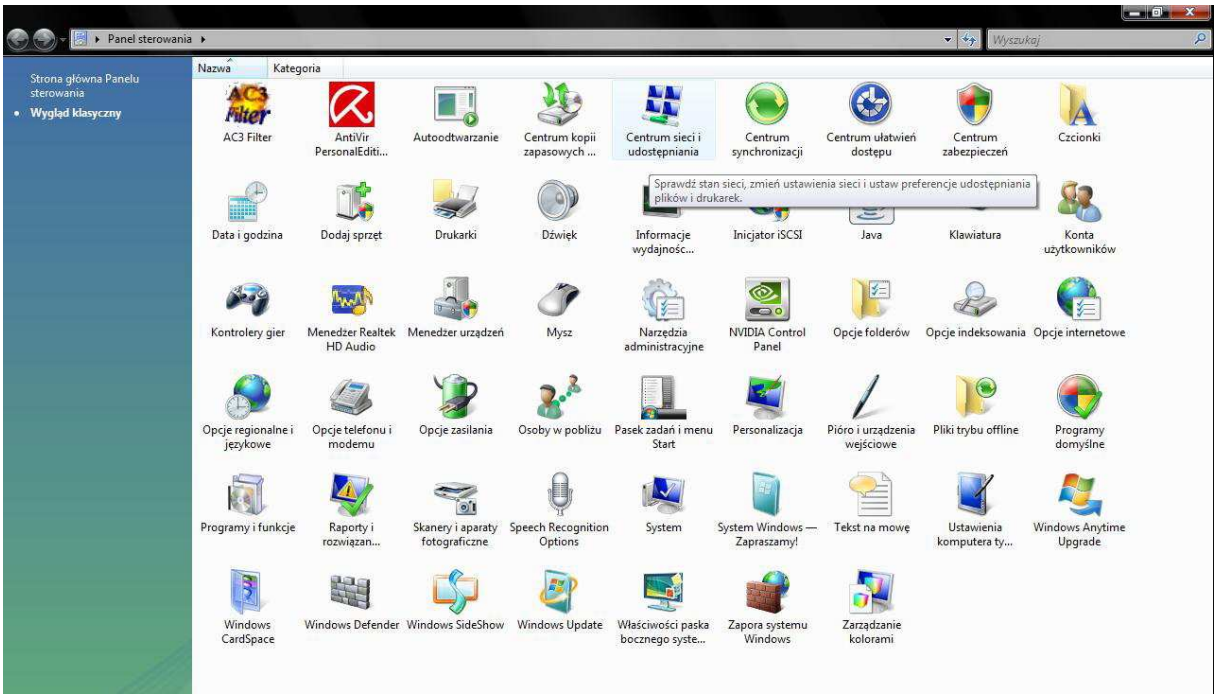
(Dla Windows Vista)

Uwaga: W przypadku, gdy system operacyjny MS Vista nie może uzyskać adresu IP z serwera DHCP routera, proszę postępować zgodnie z instrukcjami wymienionymi na stronie pomocy technicznej firmy Microsoft (http://support.microsoft.com/kb/928233/en-us (strona ta może być niedostępna w języku użytkownika urządzenia).

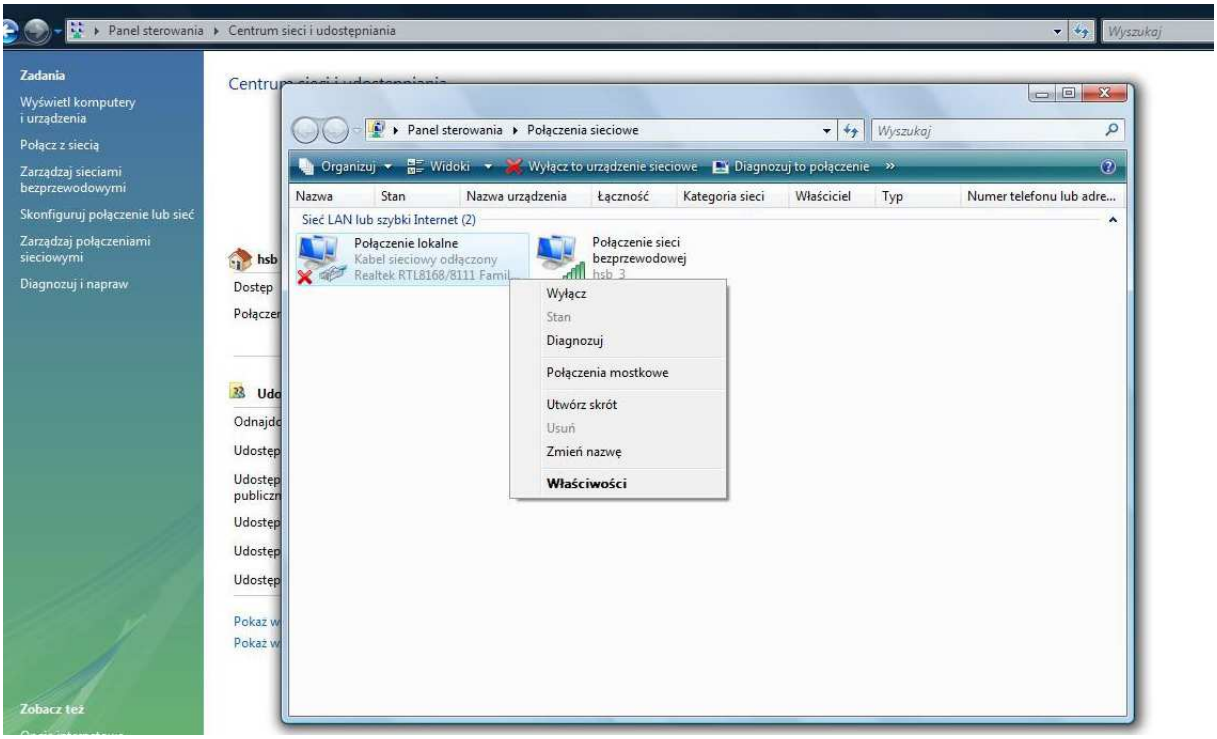
Krok 1: Wybierz z menu Start „Panel Sterownia” .



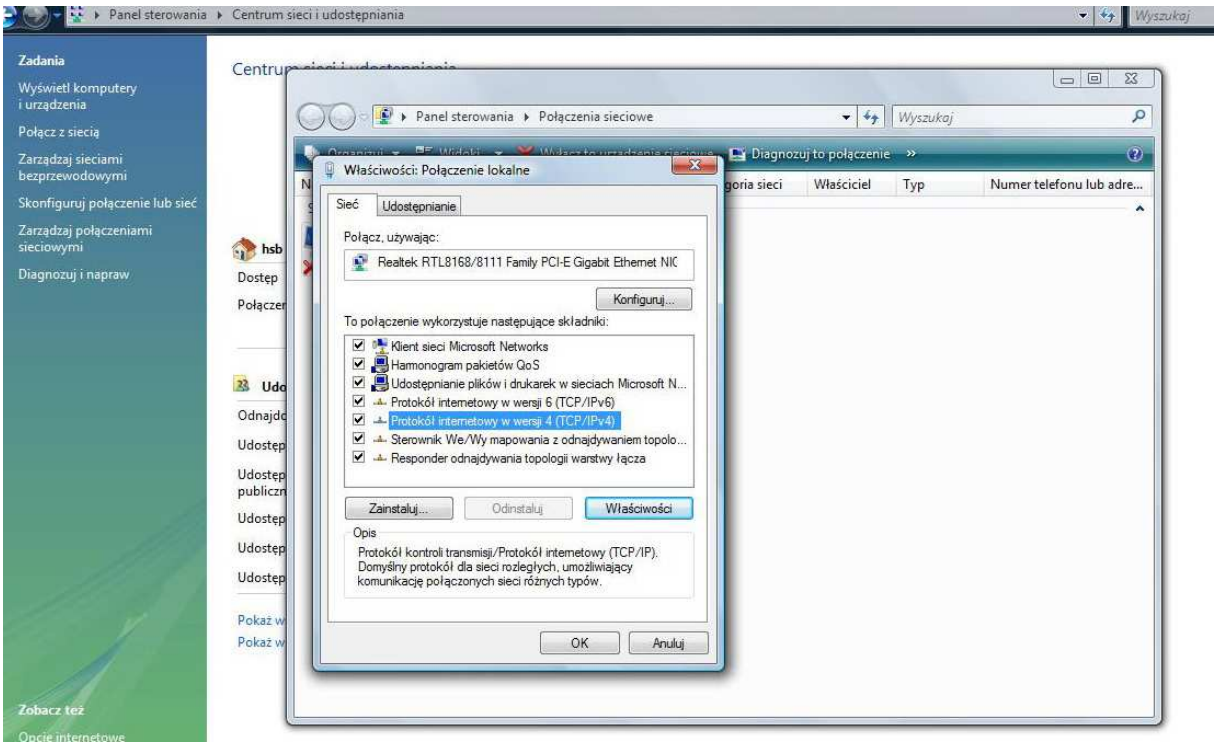
Krok 2: W „Panelu sterownia” wybierz „Centrum sieci i udostępniania”.



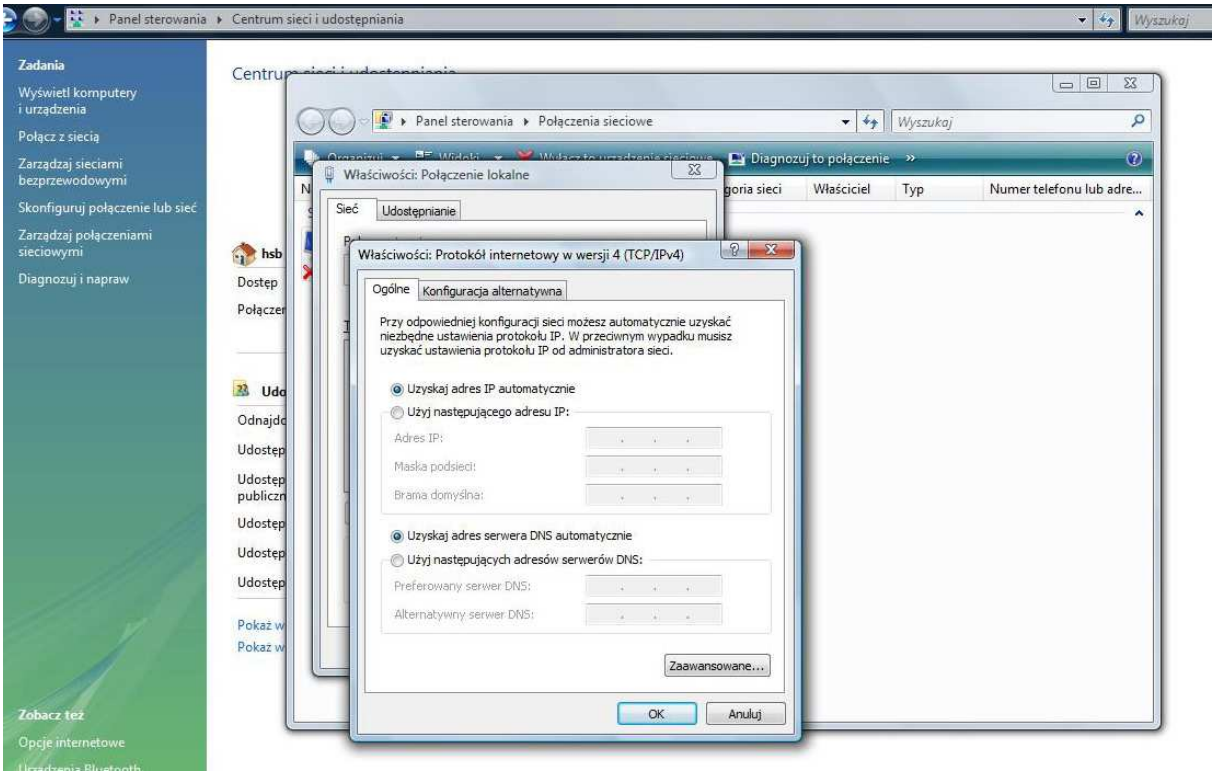
Krok 3: W „Centrum sieci i udostępniania” kliknij na „Zarządzaj połączeniami sieciowymi”, a następnie „Właściwości”.



Krok 4: Wyświetlone zostaną właściwości połączenia lokalnego, kliknij na „Protokół internetowy w wersji 4 (TCP/IPv4)", a następnie „Właściwości".

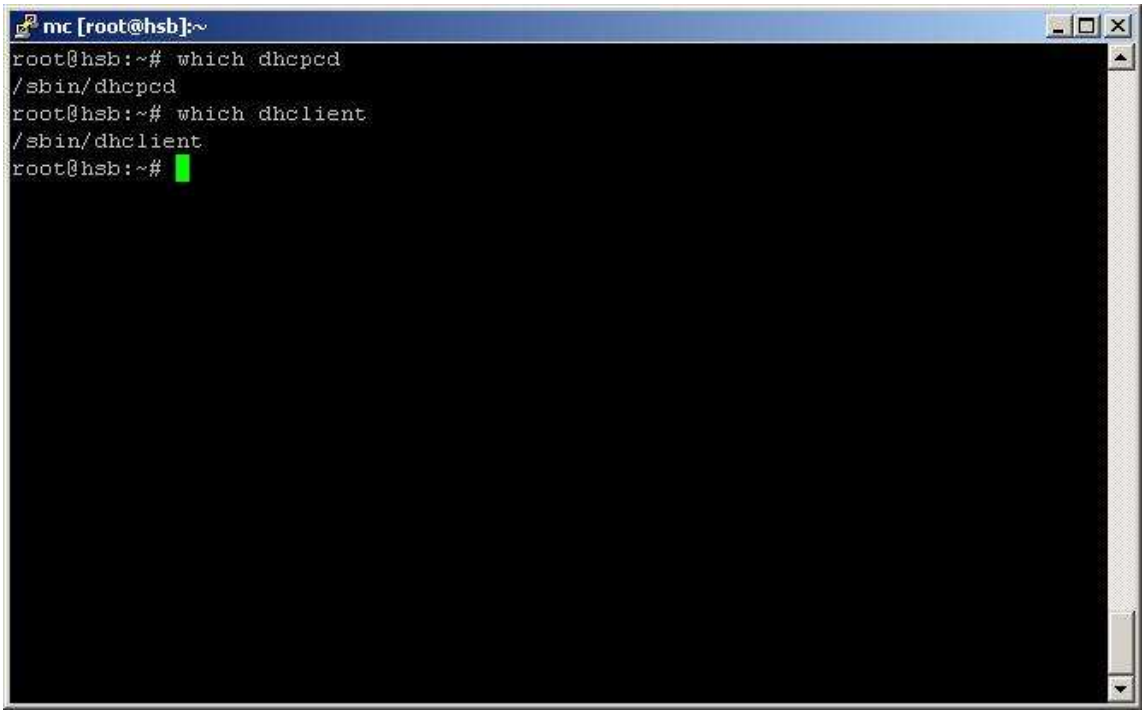


Krok 5: W zakładce „Ogólne" zaznacz Uzyskaj adres IP automatycznie" i „Uzyskaj adres serwera DNS automatycznie", a następnie kliknij OK.



(Dla systemu Linux)

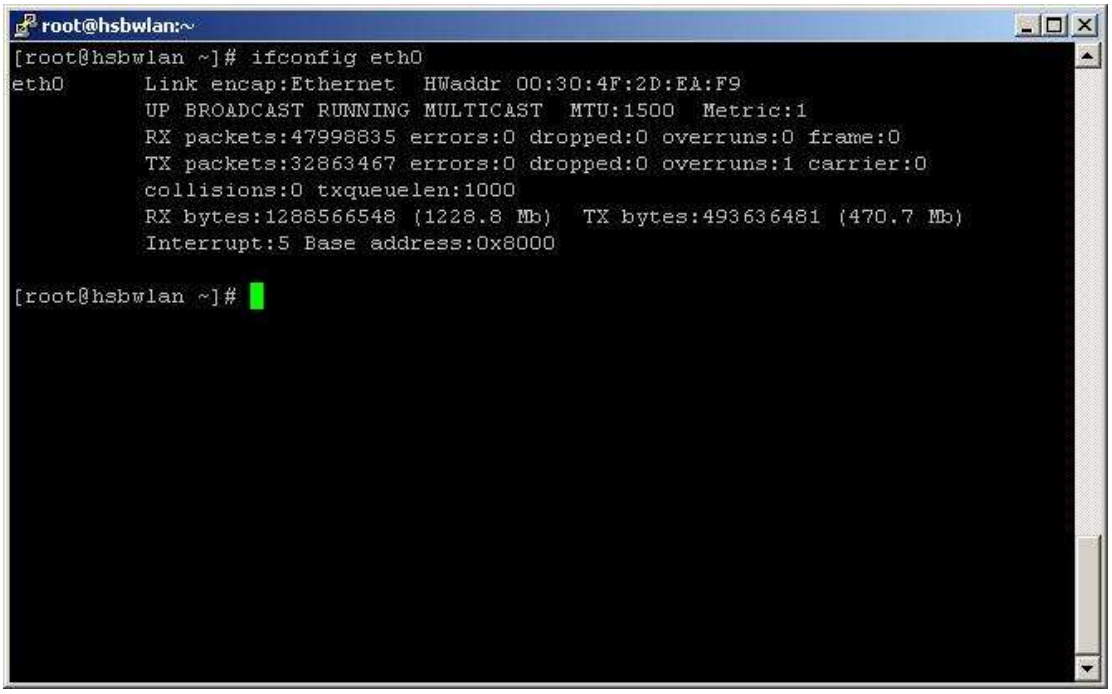
Krok 1: Sprawdzamy, jaki moduł klienta serwera DHCP posiadamy w naszym systemie, wydajemy komendę **„which dhcpcd”** lub **„which dhclient”**



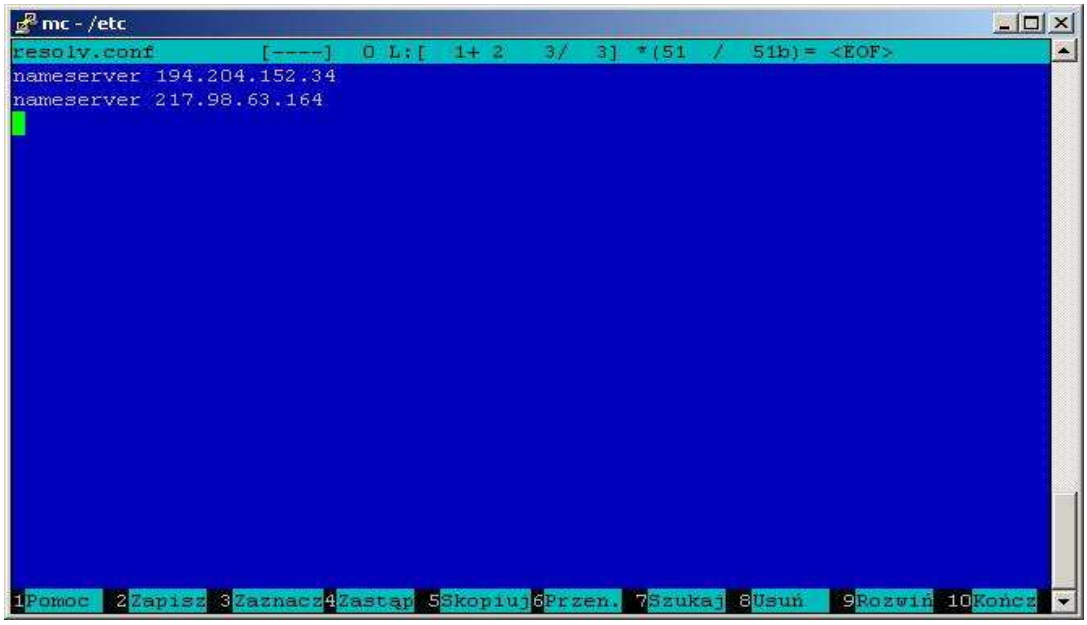
Krok 2: Jeśli nie mamy „dhcpcd” lub „dhclient” sprawdzamy, czy mamy „pump’a” wpisując komendę **„which pump”**. Jeżeli nie mamy żadnego z nich to należy zainstalować wybranego klienta serwera

DHCP lub wpisać statycznie parametry połączenia, takie jak: adres IP, maska podsieci, brama domyślna, serwery DNS.

Krok 3: Zakładając, że będziemy używać jako klienta serwera DHCP „dhcpcd", upewnijmy się, że nasz interfejs lokalny, np. eth0 działa poprawnie, w tym celu wydając komendę „ifconfig eth0"



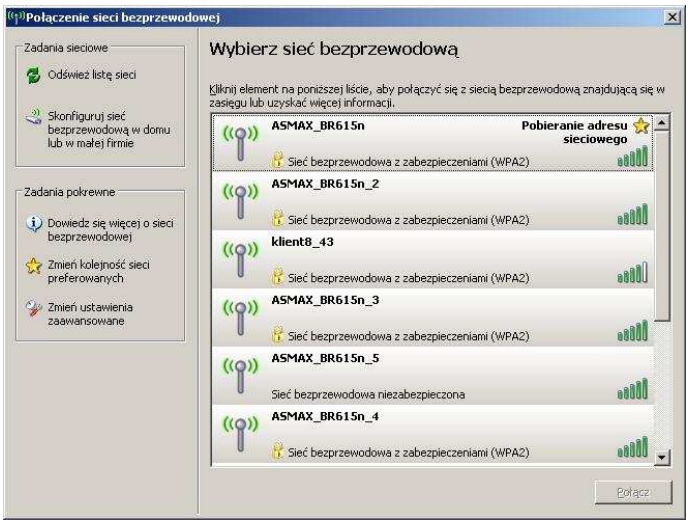
Krok 4: Jeśli nasz interfejs lokalny działa, mamy zainstalowanego klienta „dhcpcd", wydajemy komendę **„dhcpcd eth0"** (eth0 to nasz interfejs sieciowy). Nasz klient serwera DHCP pobierze teraz potrzebne parametry z serwera DHCP. Komunikację z routerem sprawdzamy wydając polecenie „**ping 192.168.1.1**", a komunikację z Internetem wydając polecenie „**ping www.google.pl**". Gdy uzyskamy odpowiedź z routera, a Internetu nie to możemy użyć komendy definiującej naszą bramę do Internetu, czyli nasz router „**route add default gw 192.168.1.1 dev eth0**". W celu dodania/edycji serwerów DNS edytujemy plik **/etc/resolv.conf** definiując adresy IP serwerów DNS. Plik z adresami serwerów DNS /etc/resolv.conf jest przy każdym uruchomieniu klienta nadpisywany. Jeśli tego nie chcemy należy zaznaczyć to w konfiguracji naszego klienta DHCP. Aby przy starcie naszego systemu operacyjnego konfiguracja sieci była ładowana automatycznie należy dodać odpowiedni wpis do jednego ze skryptów startowych, np. w systemach uniksopodobnych jest to plik **rc.local**. Najczęściej występuje on w katalogu /etc/, bądź /etc/rc.d/.



Uwaga! Możemy statycznie podać adres IP wpisując komendę „ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up", gdzie eth0 to nazwa interfejsu lokalnego, 192.168.1.2 to adres IP naszego komputera. Większość dystrybucji systemu Linux zawiera gotowe kreatory połączeń w środowisku tekstowym bądź graficznym, umożliwiające proste skonfigurowanie połączenia podobnie, jak w MS Windows.

Podłączenie karty bezprzewodowej

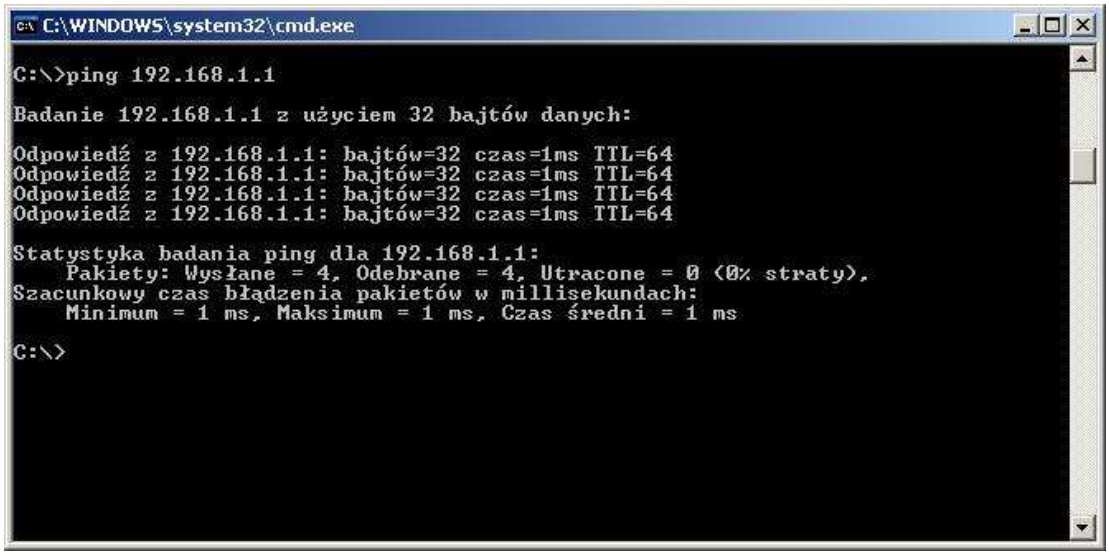
Po skonfigurowaniu urządzenia można również podłączyć komputery wyposażone w karty bezprzewodowe standardu 802.11b/g/n. W tym celu uruchom aplikację do zarządzania kartą bezprzewodową i połącz się z punktem dostępowym wbudowanym w nasz router jego nazwa SSID domyślna to „ASMAX_BR615n".



Uwaga! Aby bezprzewodowa karta sieciowa mogła zobaczyć SSID urządzenia, musi być włączone rozgłaszanie SSID w tym urządzeniu. Domyślnie opcja jest zawsze włączona i nie zaleca się jej wyłączać niezaawansowanym użytkownikom.

Testowanie połączenia z routerem, sprawdzenie adresu fizycznego (MAC) karty sieciowej, klonowanie adresu MAC i odświeżanie adresu dla klienta DHCP

Poprawność konfiguracji protokołu TCP/IP połączenia sieciowego można sprawdzić za pomocą polecenia: **ping adres_IP_routera**. Poprawne połączenie prezentuje poniższy rysunek:

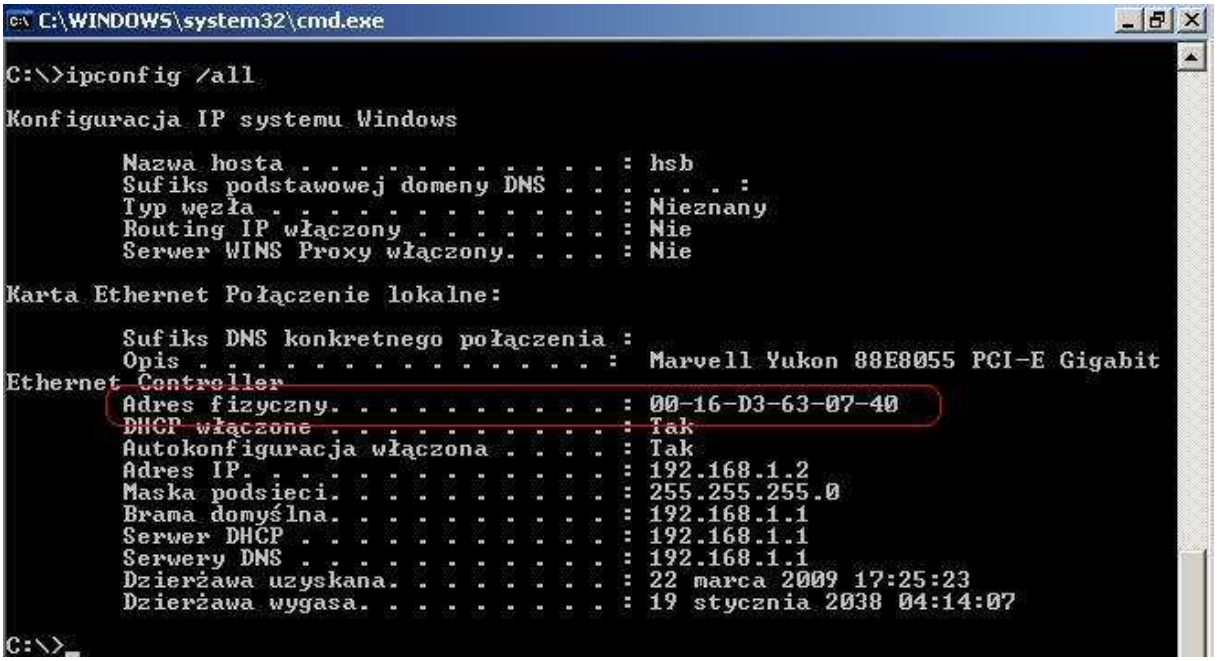


Kliknij w menu „Start" na „Uruchom" lub skorzystaj ze skrótu naciskając (klawisz Win+R), wpisz „**cmd**", uruchomiony zostanie wiersz poleceń, tu wpisz „**ping 192.168.1.1**". Efektem tego powinien być podobny wynik do tego z rysunku powyżej. Świadczy to o poprawnej komunikacji pomiędzy routerem a komputerem. W przypadku innego rezultatu sprawdź ustawienia protokołu TCP/IP lub, czy kabel sieciowy jest wpięty do odpowiedniego portu LAN 1-4, a nie np. do portu WAN. Dla połączenia niepoprawnego, źle skonfigurowanego lub źle podłączonego otrzymamy:

- Upłynął limit czasu żądania.
- Host docelowy jest nieosiągalny.
- Błąd ogólny.

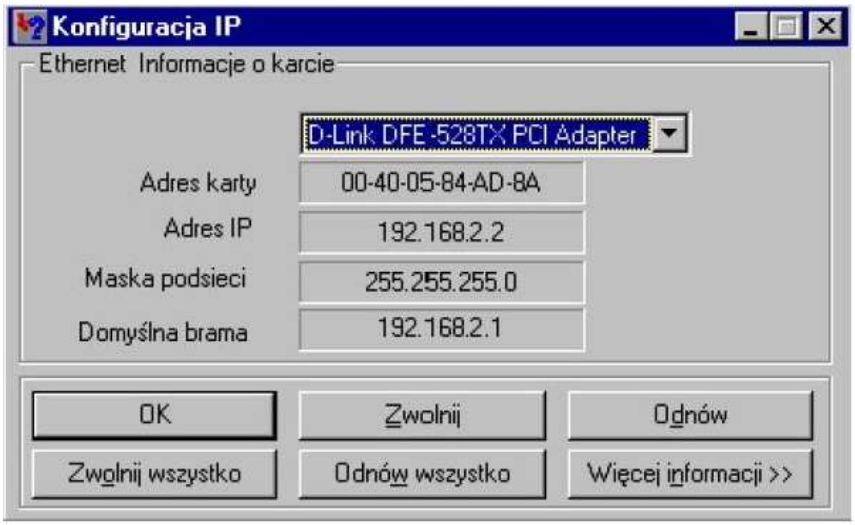
Sprawdzenie adresu fizycznego będzie nam potrzebne później przy konfiguracji połączenia z naszym dostawcą Internetu (ISP). Część ISP identyfikuje swoich klientów po adresie fizycznym karty sieciowej (MAC). W momencie podłączenia routera Asmax BR615N, to on będzie otrzymywał sygnał internetowy od naszego dostawcy, a nie karta sieciowa i dlatego nie chcąc czekać na zmianę adresu MAC na nowy, możemy użyć funkcji w routerze Asmax BR615N w zakładce **Internet Settings → WAN → MAC Clone (Enable)** i w polu „**MAC Address"** podajemy adres MAC naszej karty sieciowej, której wcześniej używaliśmy do łączenia się z Internetem w postaci np. 00:16:d3:63:07:40. Aby sprawdzić adres MAC kliknij w menu „Start" na „Uruchom" lub skorzystaj ze skrótu naciskając (klawisz

Win+R), wpisz „cmd”, uruchomiony zostanie wiersz poleceń, tu wpisz „ipconfig /all”, otrzymasz następujący wynik:



Adres fizyczny to nasz adres MAC i jego podajemy w polu **„WAN MAC Address”.** W polu **„Your PC's MAC Address”** widzimy adres MAC naszej karty sieciowej, z której konfigurujemy router.

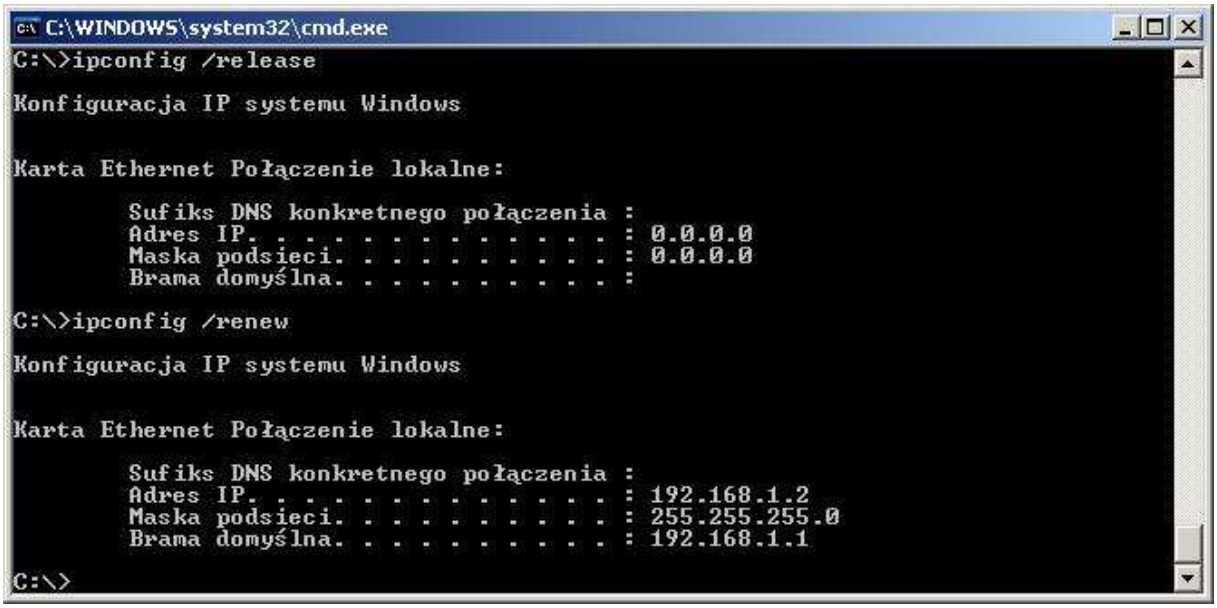
- Aby odświeżyć adres w przypadku klienta DHCP dla Windows 9x należy wybrać z menu Start opcję Uruchom i wpisać polecenie „winipcfg” i kliknąć przycisk OK. Za pomocą przycisku „Zwolnij” oraz „Odnów” można odpowiednio zwolnić i odświeżyć adres IP.



Dla Windows 2000/XP/2003/Vista

Wybieramy z menu Start opcję „Uruchom” lub możemy użyć skrótu naciskając klawisze (Win+R), wpisujemy „cmd” i klikamy OK. Zostanie uruchomiony wiersz poleceń. Następnie za pomocą

polecenia „**ipconfig /release**” oraz „**ipconfig /renew**” można odpowiednio zwolnić i odświeżyć adres IP.



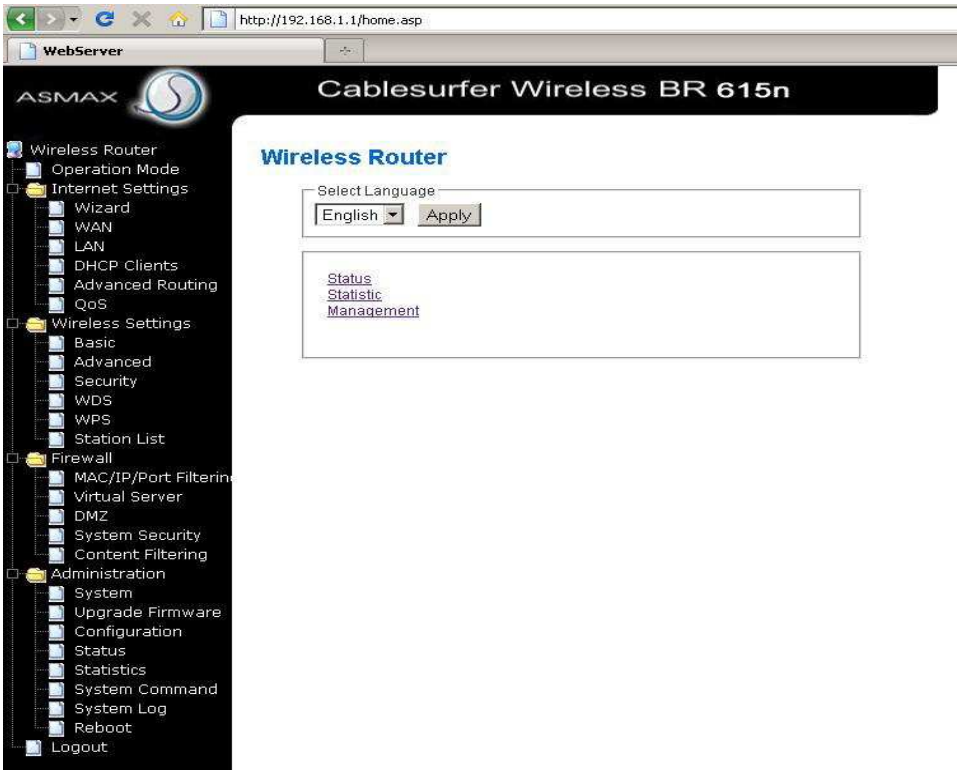
Konfiguracja routera Asmax BR615N za pomocą przeglądarki internetowej

Router Asmax BR615N jest w pełni konfigurowalny przez przeglądarkę internetową. Strona konfiguracyjna urządzenia umożliwia pełną jego konfigurację oraz prezentację statusu urządzenia. Okno strony konfiguracyjnej składa się z dwóch ramek. W lewej ramce znajduje się menu umożliwiające wybór funkcji konfiguracji lub statusu urządzenia pogrupowanych w zakładki. Prawa ramka stanowi okno wywołanej funkcji.

Logowanie do urządzenia

Krok 1: Włącz przeglądarkę internetową, np. Opera, Mozilla, Internet Explorer.
Krok 2: W polu adres wpisz adres interfejsu LAN routera – http://192.168.1.1 .
Krok 3: Na ekranie wyświetli się monit autoryzacji. Wprowadź nazwę użytkownika i hasło. Domyślna nazwa użytkownika to „**admin**” oraz hasło „**admin**”.

Krok 4: Po poprawnym wpisaniu nazwy użytkownika i hasła na ekranie zostanie wyświetlona strona konfiguracji urządzenia, jak poniżej.

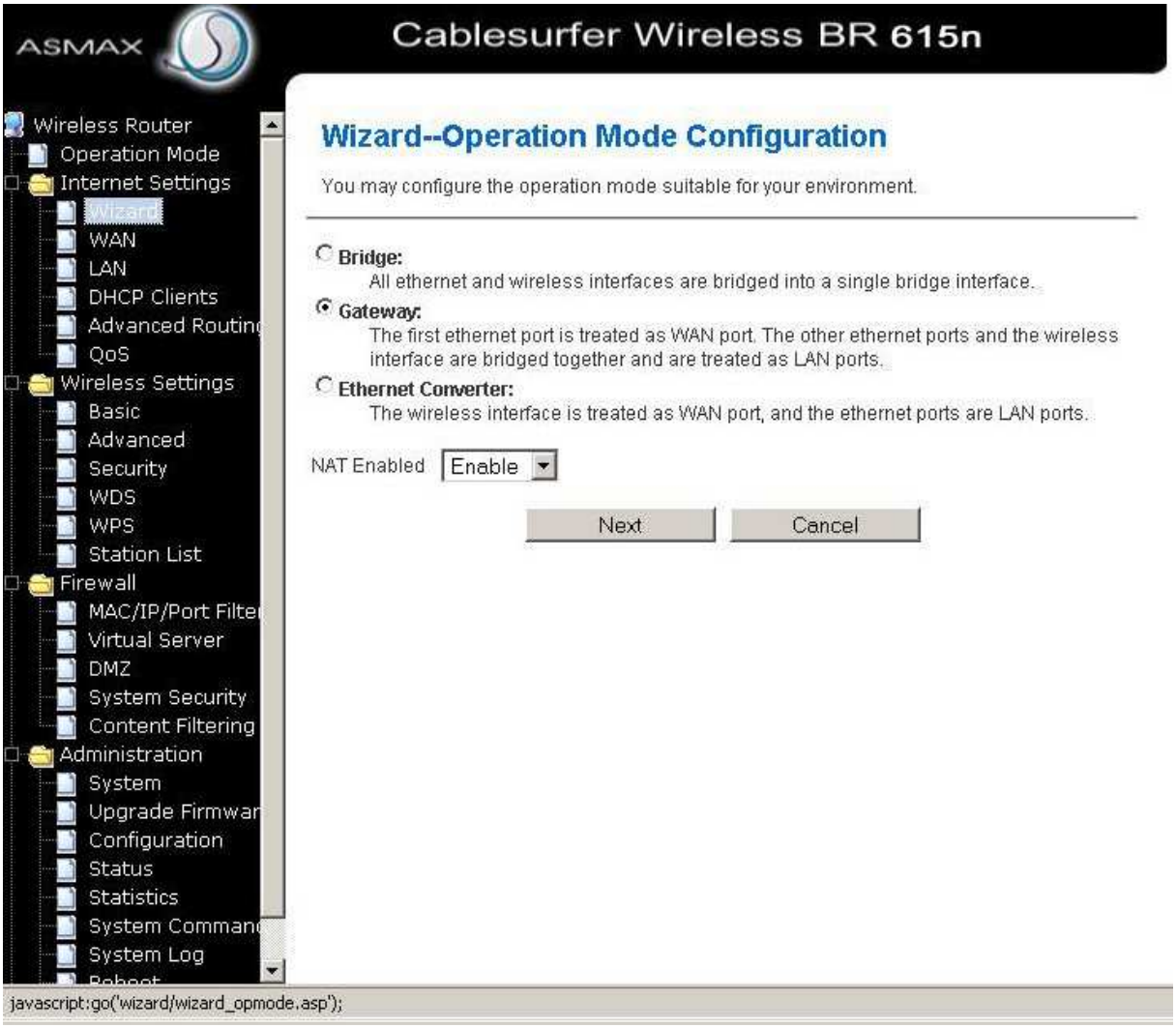


Lewe okno – Menu nawigacyjne.

Prawe okno – Zawartość elementu wybranego w menu nawigacyjnym.

Wizard

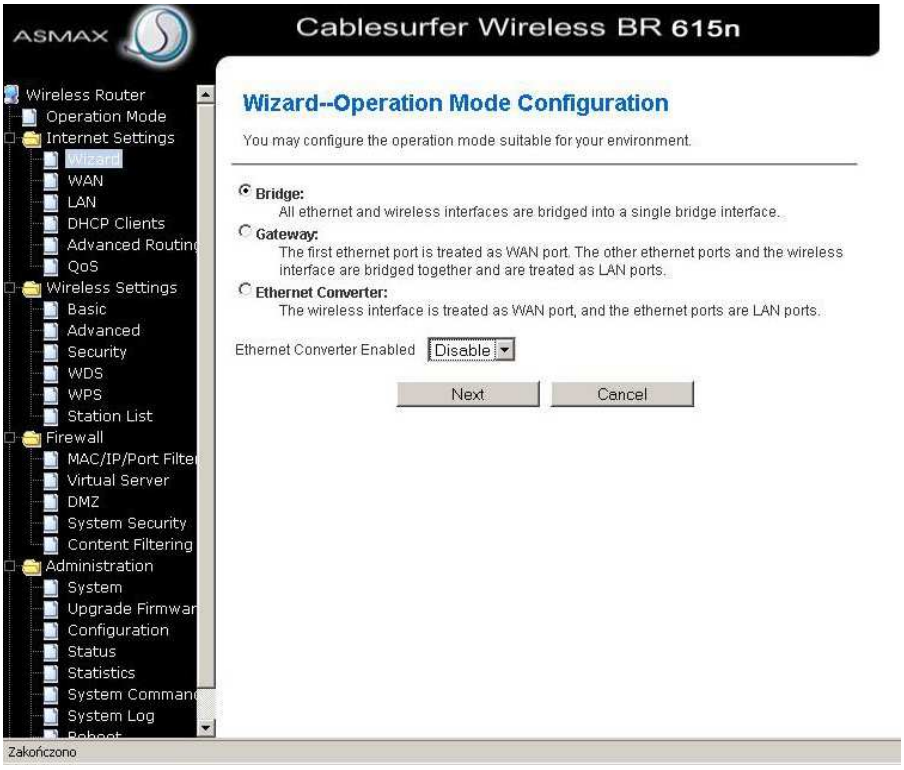
Funkcja „Wizard” umożliwia prostą, podstawową konfigurację urządzenia krok po kroku w celu zapewnienia dostępu do sieci Internet.



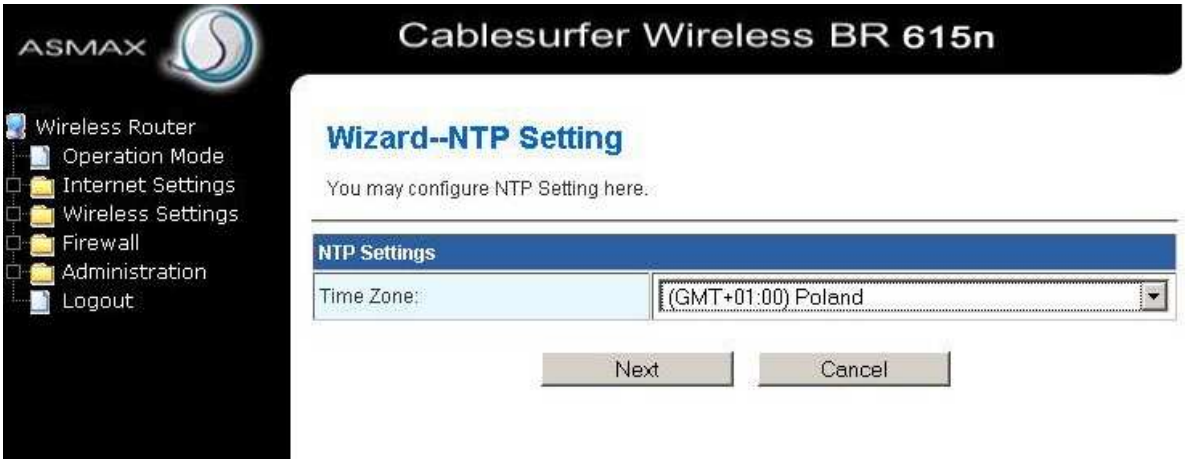
W przypadku modułu „Setup Wizard” użytkownik przechodzi kolejno poprzez wszystkie funkcje menu za pomocą przycisków „Next” i „Back”.

Aby rozpocząć konfigurację urządzenia, przeczytaj poniżej o wyborze trybu pracy naszego urządzenia, a następnie kliknij przycisk „Next”.

Funkcja „Operation Mode” umożliwia wybór trybu pracy urządzenia. W celu uzyskania dostępu do sieci Internet za pomocą połączenia przewodowego (gniazdo WAN: stałe łącze, modem kablowy, modem ADSL) wybierz opcję „Gateway” i kliknij „Next”. W przypadku bezprzewodowego dostępu do sieci Internet za pomocą modułu bezprzewodowego wbudowanego w urządzenie i mogącego pracować jako klient punktu dostępowego (WISP) wybierz „Ethernet Converter” i kliknij „Next”. Gdy potrzebujesz z urządzenia utworzyć most sieciowy i połączyć, np. dwie lokalizacje w sieci bezprzewodowo, wybierz tryb „Bridge”, w tym trybie wszystkie porty LAN oraz interfejs bezprzewodowy są połączone, a mechanizmy NAT i Firewall są wyłączone. Aby ustawić tryb mostu ustaw w zakładce „Operation Mode” tryb „Bridge”. W zdecydowanej większości będzie to domyślny tryb „Gateway” . Wybieramy i klikamy „Next”.

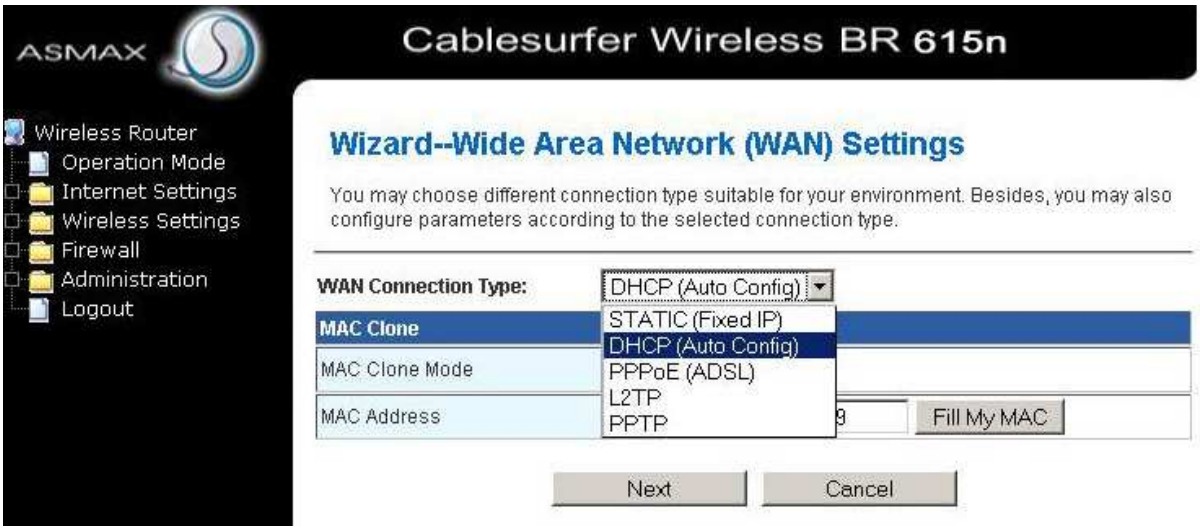


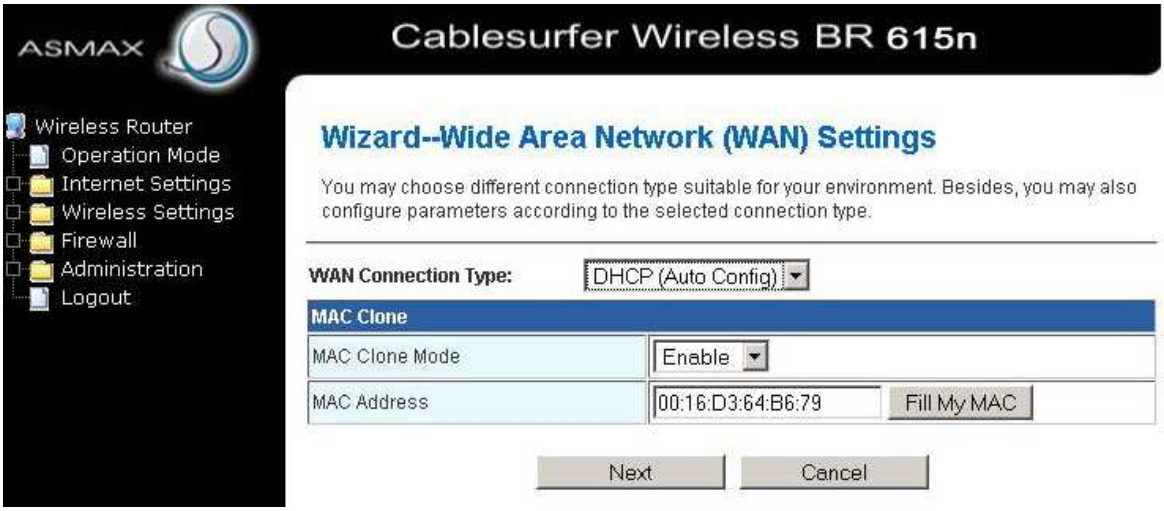
Funkcja „NTP Setting” umożliwia wybranie strefy czasowej dla protokołu NTP. Wybierz strefę czasową w polu „NTP Setting” oraz opcjonalnie serwer NTP w polu „NTP Server”, a następnie kliknij przycisk „Next”. Domyślną strefą jest „Poland”.



Wide Area Network (WAN) Settings

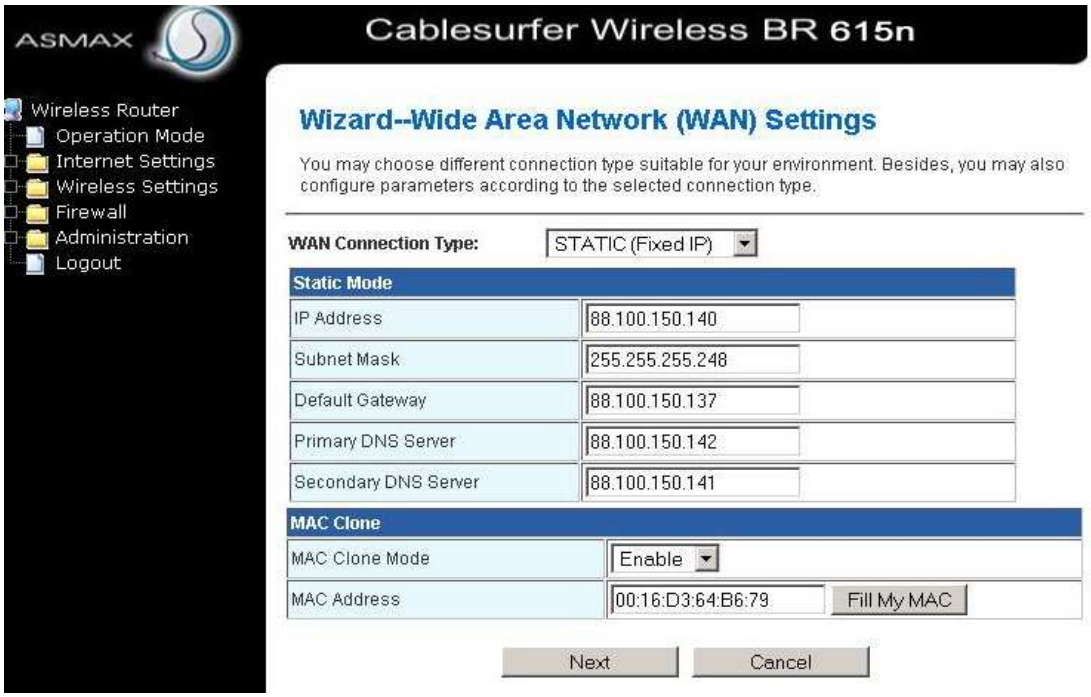
Zakładka „Wide Area Network (WAN) Settings" umożliwia określenie parametrów interfejsu WAN. Za pomocą opcji „WAN Connection Type" wybierz tryb pracy interfejsu WAN (dostępne tryby widzimy na rysunku poniżej). Jednocześnie mamy możliwość podania adresu MAC, który jest zarejestrowany u naszego dostawcy (ISP). Funkcje te były szczegółowo opisywane już na stronie 22.





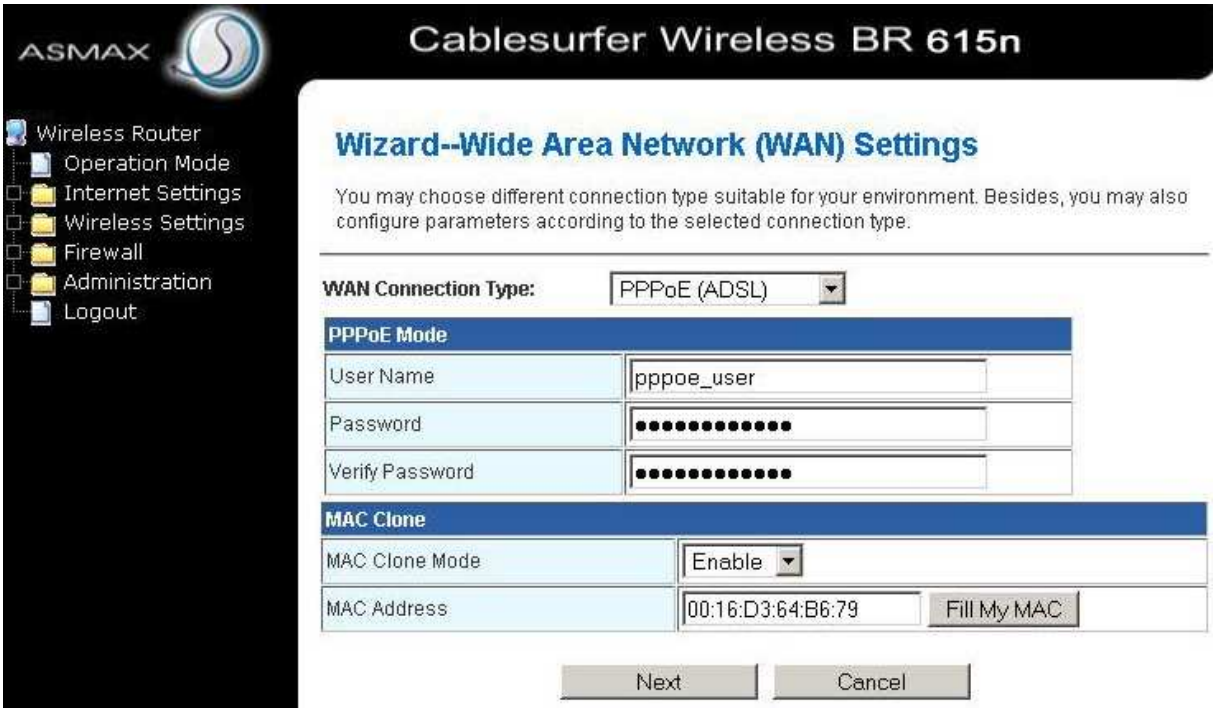
DHCP (Auto Config): W przypadku pracy urządzenia jako klient serwera DHCP wybierz tryb „DHCP (Auto Config)", poniżej możesz podać zarejestrowany adres MAC i kliknąć „Next". Większość ISP używa właśnie serwera DHCP do przypisywania swoim klientom właściwych parametrów połączenia. Pole „Mac Clone Mode" wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC i w polu „MAC Address" podać zarejestrowany adres MAC w postaci, np. 00:16:D3:64:B6:79, jak widać na rysunku powyżej. Możemy też kliknąć przycisk „Fill My MAC", aby automatycznie został pobrany adres MAC karty, z której właśnie konfigurujemy nasz router.

Static (Fixed IP): w przypadku statycznego, stałego adresu IP (np. usługa Internet DSL TPSA) należy określić adres IP interfejsu WAN (IP Address), maskę podsieci (Subnet Mask), bramę domyślną (Default Gateway) oraz adres serwera DNS, a następnie kliknij przycisk „Next".



W polu „IP Address” podajemy adres IP uzyskany od naszego ISP, w polu „Subnet Mask” podajemy uzyskaną maskę podsieci, w polu „Default Gateway” podajemy bramę główną uzyskaną od ISP, w polu „Primary/Secondary DNS Server” podajemy preferowany i alternatywny serwer nazw, także uzyskane od ISP. Poniżej możesz podać zarejestrowany adres MAC i kliknąć „Next”. Pole „Mac Clone Mode” wybieramy „Enable”, aby uaktywnić funkcję klonowania adresu MAC i w polu „MAC Address” podać zarejestrowany adres MAC w postaci, np. 00:16:D3:64:B6:79, jak widać na rysunku powyżej. Możemy też kliknąć przycisk „Fill My MAC”, aby automatycznie został pobrany adres MAC karty, z której właśnie konfigurujemy nasz router.

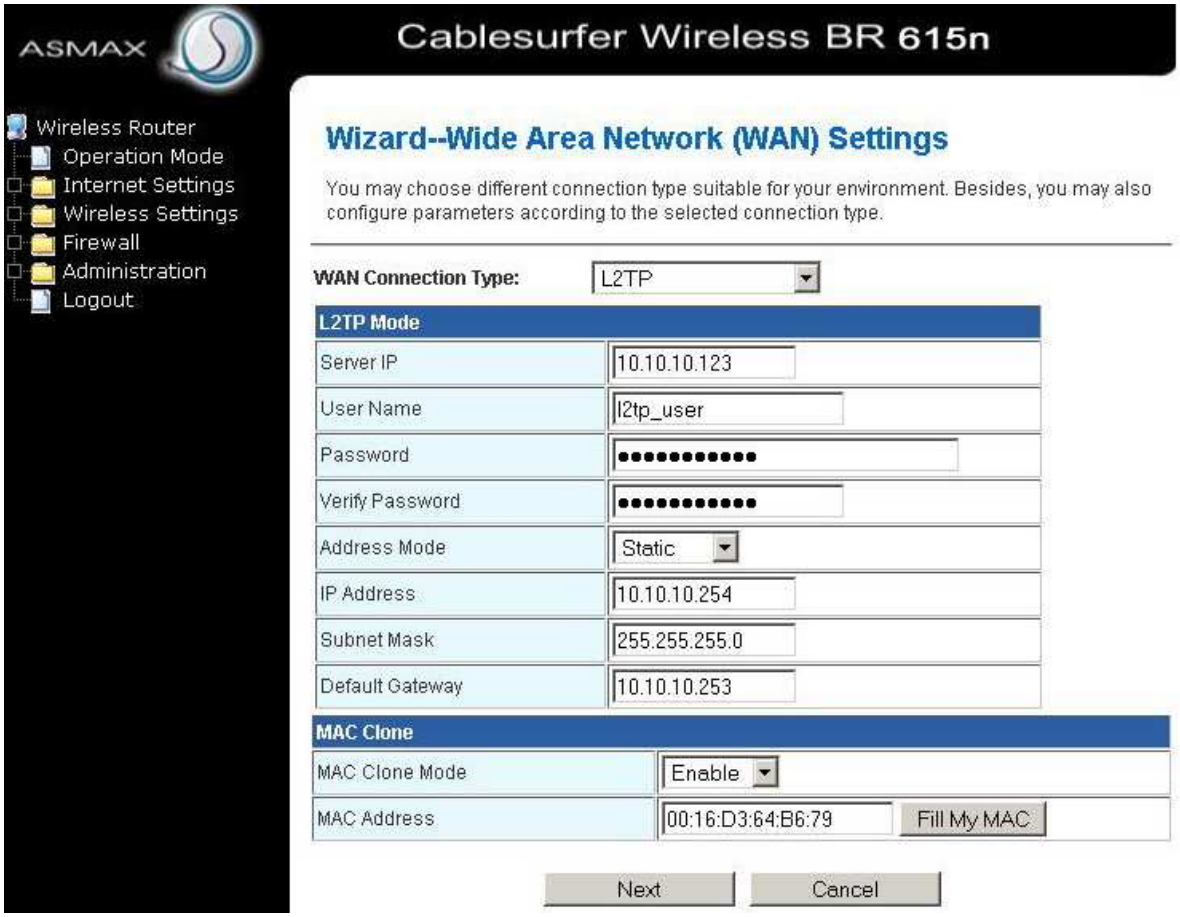
PPPoE: W przypadku pracy jako klient serwera PPPoE wpisz nazwę użytkownika potrzebną do autoryzacji połączenia w polu „User Name” oraz hasło w polu „Password”, potwierdź hasło w polu „Verify Password” i kliknij „Next”. Poniżej możesz podać zarejestrowany adres MAC i kliknąć „Next”. Pole „Mac Clone Mode” wybieramy „Enable”, aby uaktywnić funkcję klonowania adresu MAC i w polu „MAC Address” podać zarejestrowany adres MAC w postaci, np. 00:16:D3:64:B6:79, jak widać na rysunku poniżej. Możemy też kliknąć przycisk „Fill My MAC”, aby automatycznie został pobrany adres MAC karty, z której właśnie konfigurujemy nasz router.



PPTP: W przypadku klienta PPTP wpisz nazwę użytkownika potrzebną do autoryzacji połączenia w polu „User Name” oraz hasło w polu „Password”. Następnie w polu „IP Address” określ adres urządzenia, w polu „Subnet Mask” maskę podsieci, a w polu „Serwer IP Address” adres IP serwera PPTP. Po ustawieniu parametrów połączenia PPTP kliknij przycisk „Next”. Poniżej możesz podać zarejestrowany adres MAC i kliknąć „Next”. Pole „Mac Clone Mode” wybieramy „Enable”, aby uaktywnić funkcję klonowania adresu MAC i w polu „MAC Address” podać zarejestrowany adres MAC w postaci, np. 00:16:D3:64:B6:79, jak widać na rysunku poniżej. Możemy też kliknąć przycisk „Fill My

MAC", aby automatycznie został pobrany adres MAC karty, z której właśnie konfigurujemy nasz router.

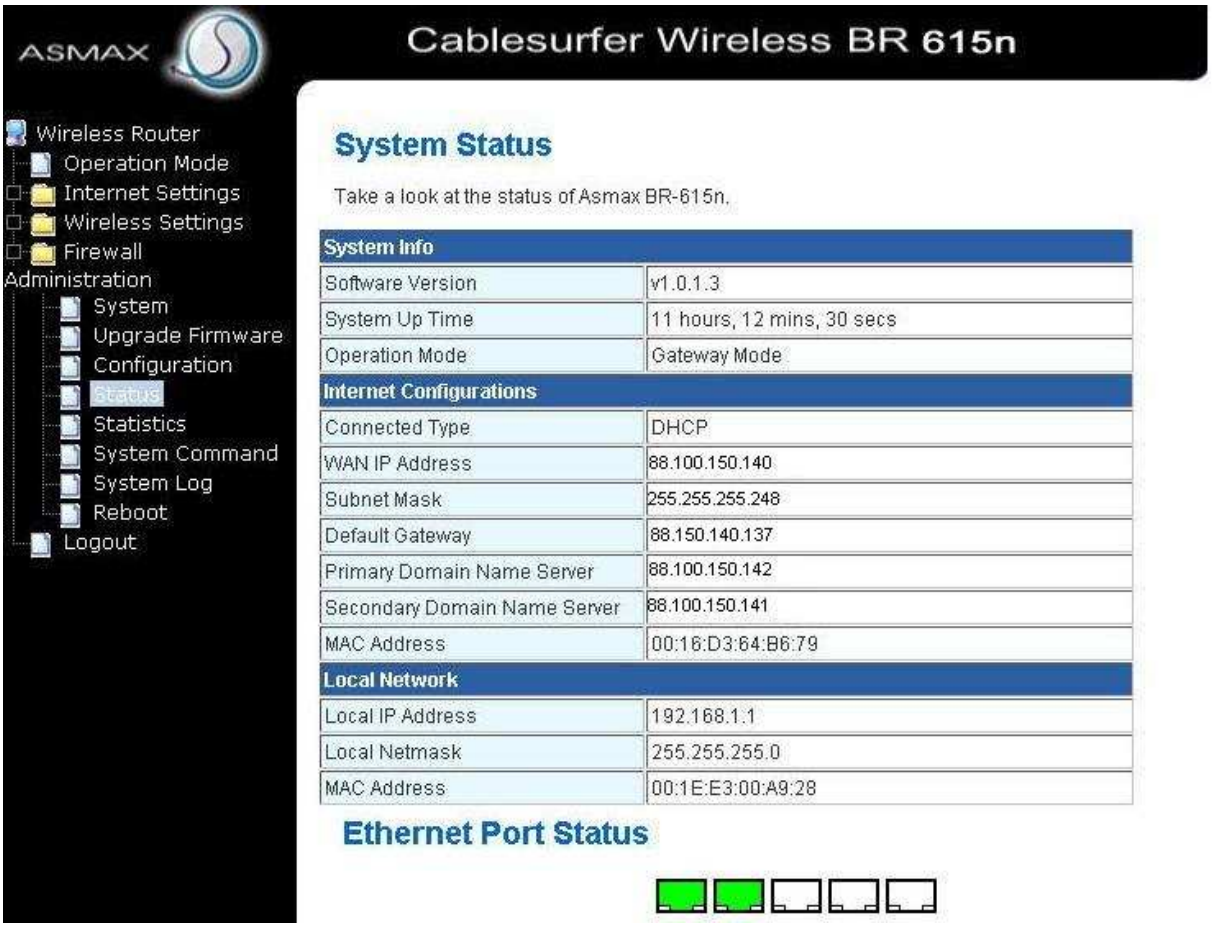
L2TP: W przypadku klienta L2TP wpisz nazwę użytkownika potrzebną do autoryzacji połączenia w polu „User Name" oraz hasło w polu „Password". Następnie w polu „IP Address" określ adres urządzenia, w polu „Subnet Mask" maskę podsieci, a w polu „Serwer IP Address" adres IP serwera L2TP. Po ustawieniu parametrów połączenia L2TP kliknij przycisk „Next". Poniżej możesz podać zarejestrowany adres MAC i kliknąć „Next". Pole „Mac Clone Mode" wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC i w polu „MAC Address" podać zarejestrowany adres MAC w postaci, np. 00:16:D3:64:B6:79, jak widać na rysunku poniżej. Możemy też kliknąć przycisk „Fill My MAC", aby automatycznie został pobrany adres MAC karty, z której właśnie konfigurujemy nasz router.



Podstawowa konfiguracja sieci bezprzewodowej

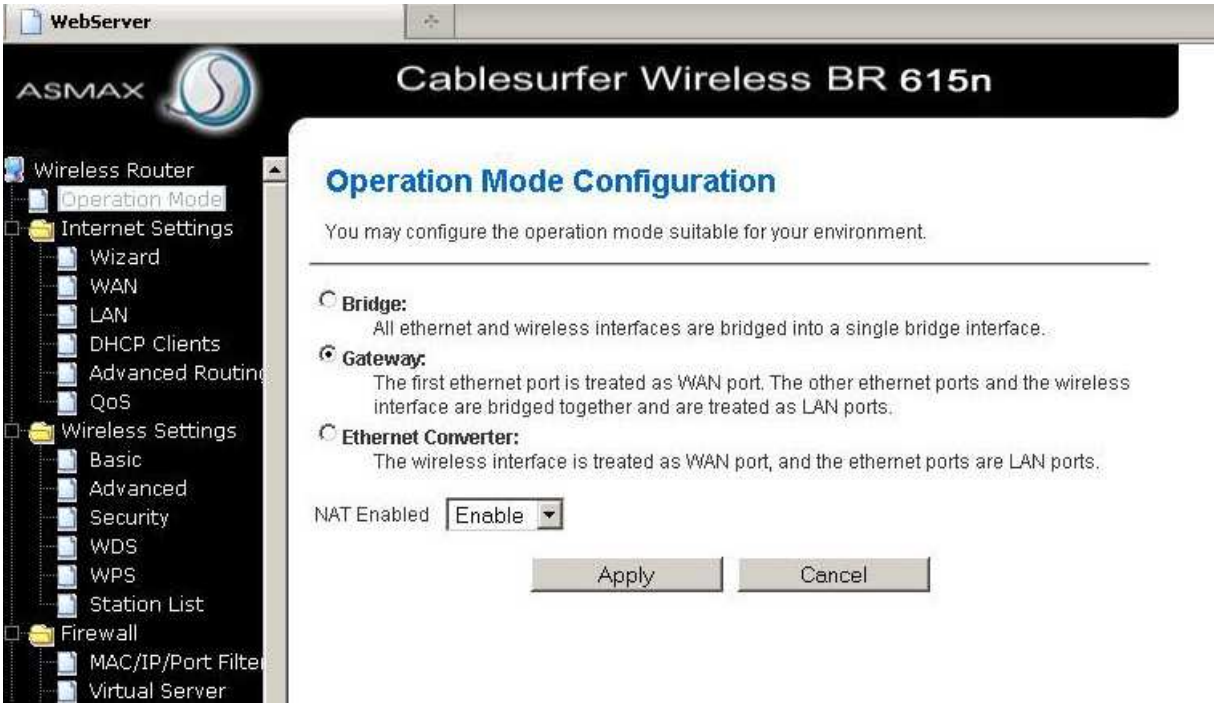
Funkcja „Basic Wireless Settings” umożliwia określenie podstawowych parametrów wbudowanego interfejsu bezprzewodowego. W polu „Network Name (SSID)” podajemy nazwę, z jaką będzie rozgłaszany sygnał wbudowanego punktu dostępowego – domyślnie jest to „ASMAX_BR615n”. W polu „Security Policy” wybieramy metodę zabezpieczenia naszej sieci bezprzewodowej, zalecamy wybranie WPA2-PSK. Poniżej wybieramy algorytm szyfrowania, np. AES i w polu „Pass Phrase” podajemy nasz klucz, który będziemy wpisywać w komputerach chcących podłączyć się do naszej sieci. Po wybraniu odpowiednich parametrów klikamy „Apply”. Urządzenie zostanie uruchomione ponownie i po chwili zostanie wyświetlony komunikat, jak poniżej.

Następnie kliknij na zakładkę **Administration** → **Status**, aby sprawdzić stan połączenia z ISP, poniżej widok z trybu „DHCP (Auto Config)”.



Wybór trybu pracy urządzenia – funkcja „Operation Mode”

Funkcja „Operation Mode” umożliwia wybór trybu pracy urządzenia.



- Gateway

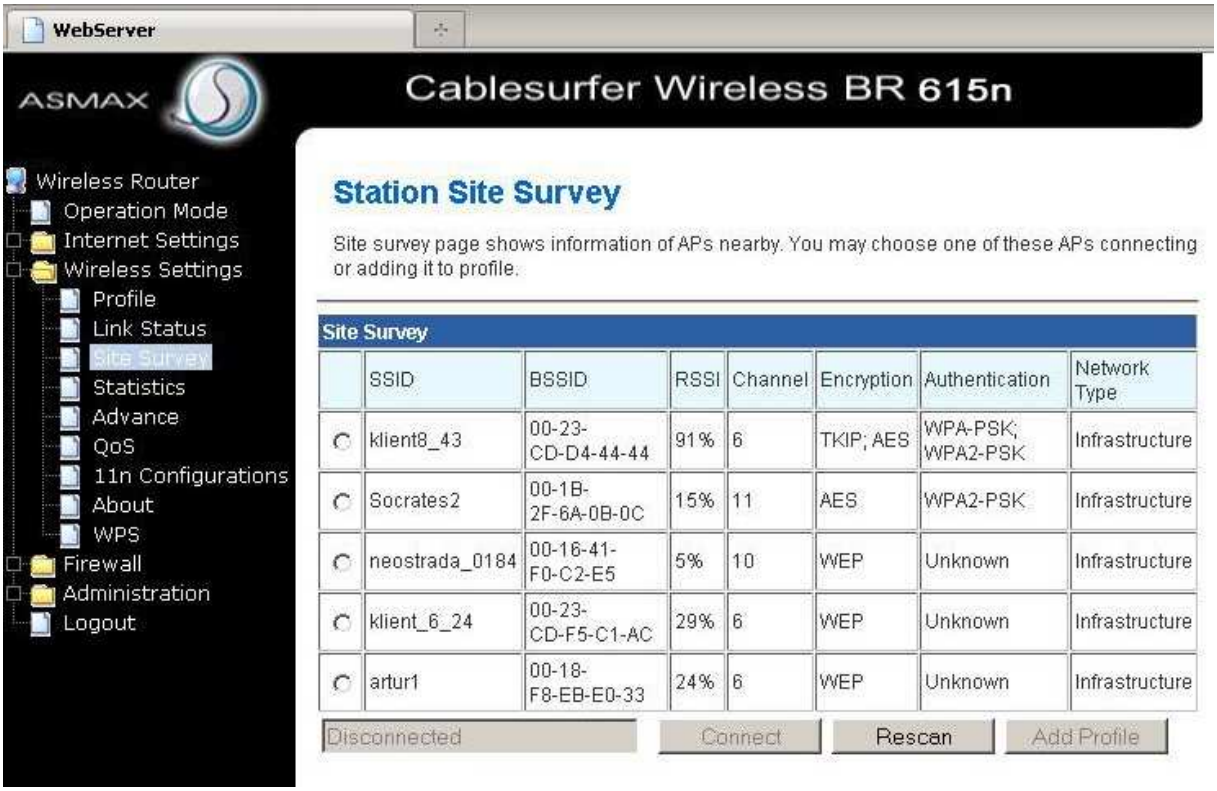
W trybie „Gateway”, w celu dostępu do Internetu używany jest interfejs WAN, do którego może być podłączony dodatkowo modem kablowy lub ADSL. Użytkownicy sieci LAN dzielą jeden adres IP otrzymany od dostawcy ISP (adres IP interfejsu WAN) i używają NAT w celu dostępu do sieci Internet.

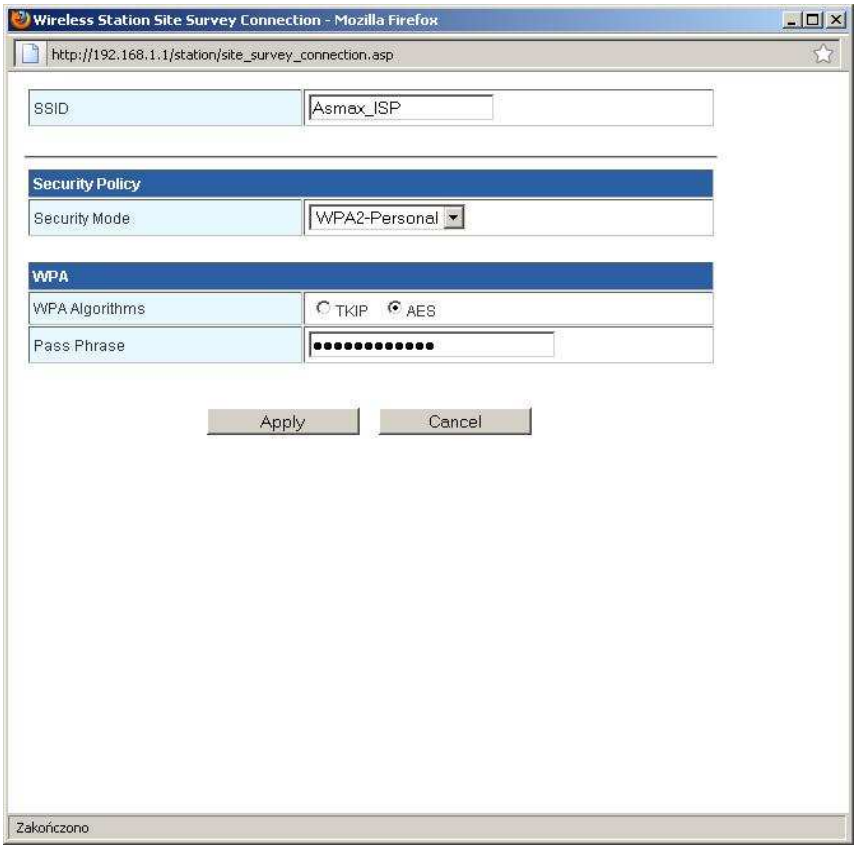
- Bridge

W trybie „Bridge” wszystkie porty LAN i interfejs bezprzewodowy są połączone. Funkcja NAT jest wyłączona, podobnie funkcje zapory sieciowej. Aby urządzenie działało w trybie mostu sieciowego zaznaczamy tryb „Bridge”.

- Ethernet Converter (WISP)

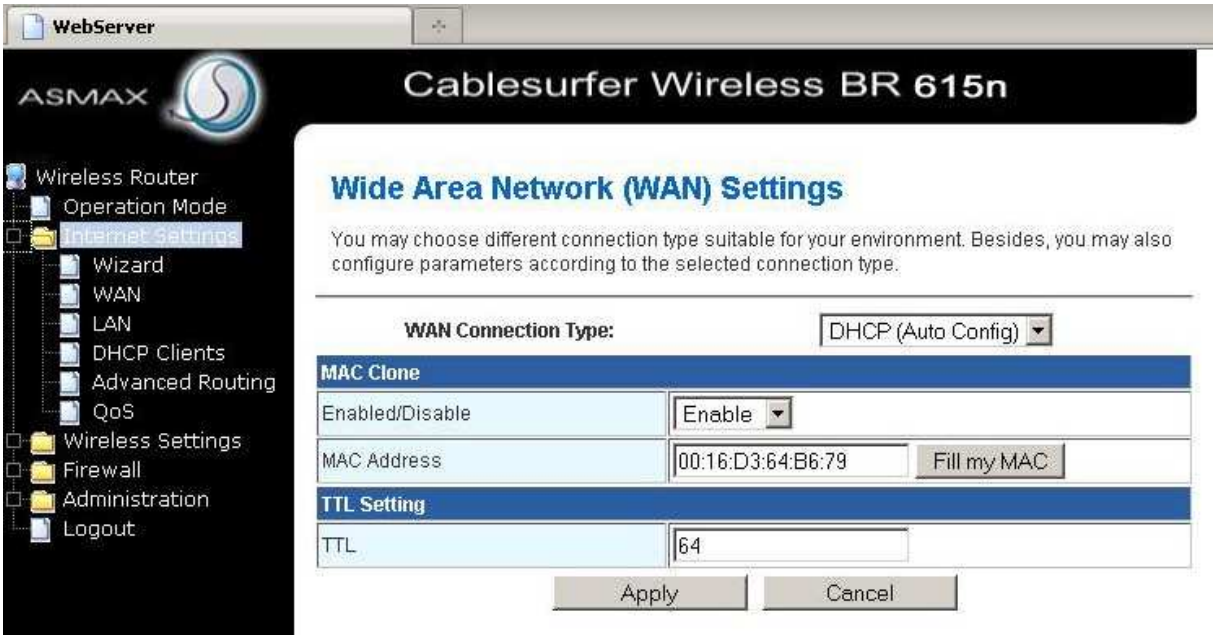
W trybie „Ethernet Converter” wbudowany interfejs bezprzewodowy pracuje jako klient punktu dostępowego w celu połączenia z punktem dostępowym AP dostawcy ISP. Za pomocą modułu „Wireless Settings → Site Survey” należy wybrać sieć bezprzewodową, do której chcemy się podłączyć i kliknąć „Connect”. Jeśli wybrana sieć bezprzewodowa jest zabezpieczona i wymaga podania klucza dostępowego to zostanie wyświetlone okienko, jak poniżej, gdzie ten klucz należy podać. Użytkownicy sieci LAN dzielą jeden adres IP otrzymany od dostawcy ISP i używają translacji adresów sieciowych NAT w celu dostępu do sieci Internet. Możemy zdefiniować klika profili dla połączenia bezprzewodowo z naszym ISP.


WebServer
ASMAX
Cablesurfer Wireless BR 615n
Wireless Router
Operation Mode
Internet Settings
Wireless Settings
Profile
Link Status
Site Survey
Statistics
Advance
QoS
11n Configurations
About
WPS
Firewall
Administration
Logout
Station Site Survey
Site survey page shows information of APs nearby. You may choose one of these APs connecting or adding it to profile.
Site Survey
SSID
BSSID
RSSI
Channel
Encryption
Authentication
Network Type
klient8_43
00-23-CD-D4-44-44
91%
6
TKIP; AES
WPA-PSK; WPA2-PSK
Infrastructure
Socrates2
00-1B-2F-6A-0B-0C
15%
11
AES
WPA2-PSK
Infrastructure
neostrada_0184
00-16-41-F0-C2-E5
5%
10
WEP
Unknown
Infrastructure
klient_6_24
00-23-CD-F5-C1-AC
29%
6
WEP
Unknown
Infrastructure
artur1
00-18-F8-EB-E0-33
24%
6
WEP
Unknown
Infrastructure
Disconnected
Connect
Rescan
Add Profile


Wireless Station Site Survey Connection - Mozilla Firefox
http://192.168.1.1/station/site_survey_connection.asp
SSID
Asmax_ISP
Security Policy
Security Mode
WPA2-Personal
WPA
WPA Algorithms
TKIP
AES
Pass Phrase
Apply
Cancel
Zakończono

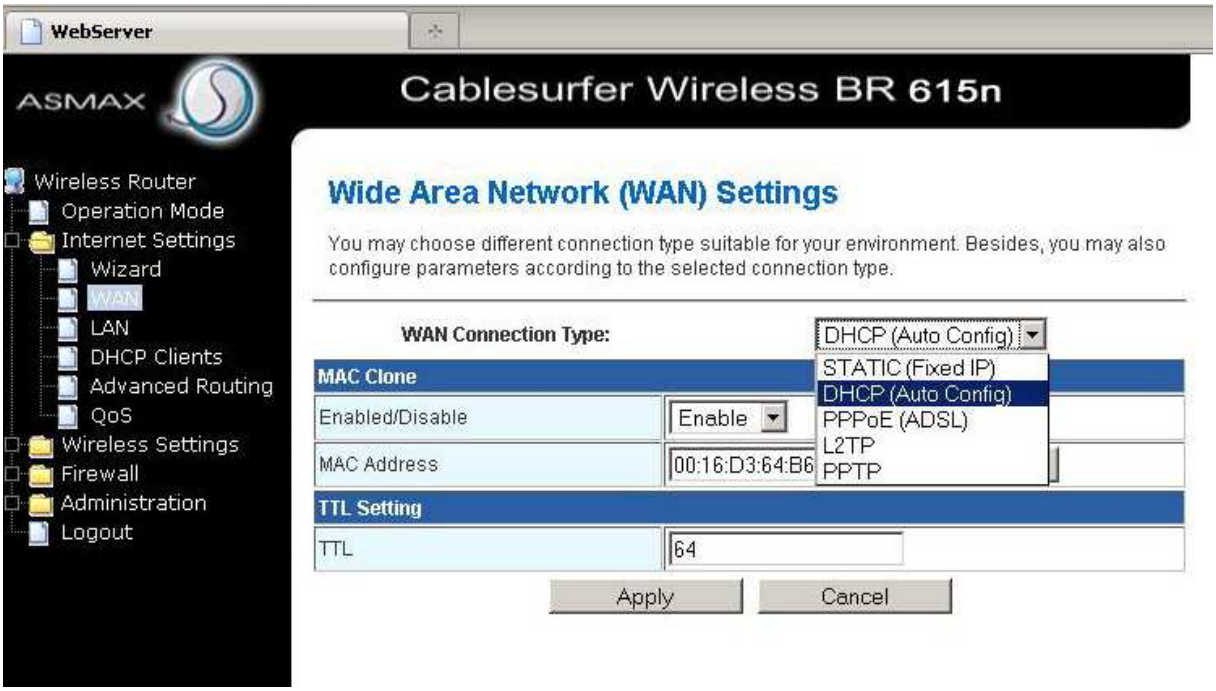
Zakładka „Internet Settings”

W tej zakładce możemy konfigurować/modyfikować parametry interfejsu LAN, WAN, trasowania, serwera DHCP i określić politykę zarządzania dostępnym pasmem.



Konfiguracja zakładki „WAN”

Zakładka „WAN” umożliwia konfigurację głównego interfejsu urządzenia, interfejsu za pomocą, którego nasz dostawca usług internetowych (ISP) dostarcza nam usługę.



Parametry:

WAN Connection Type – Rodzaj połączenia z Internetem poprzez port WAN („Static IP" – stały adres IP, „DHCP Klient" – klient serwera DHCP, „PPPoE" – klient serwera PPPoE, „PPTP" – klient serwera PPTP, „L2TP"- klient serwera L2TP.

Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.

MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.

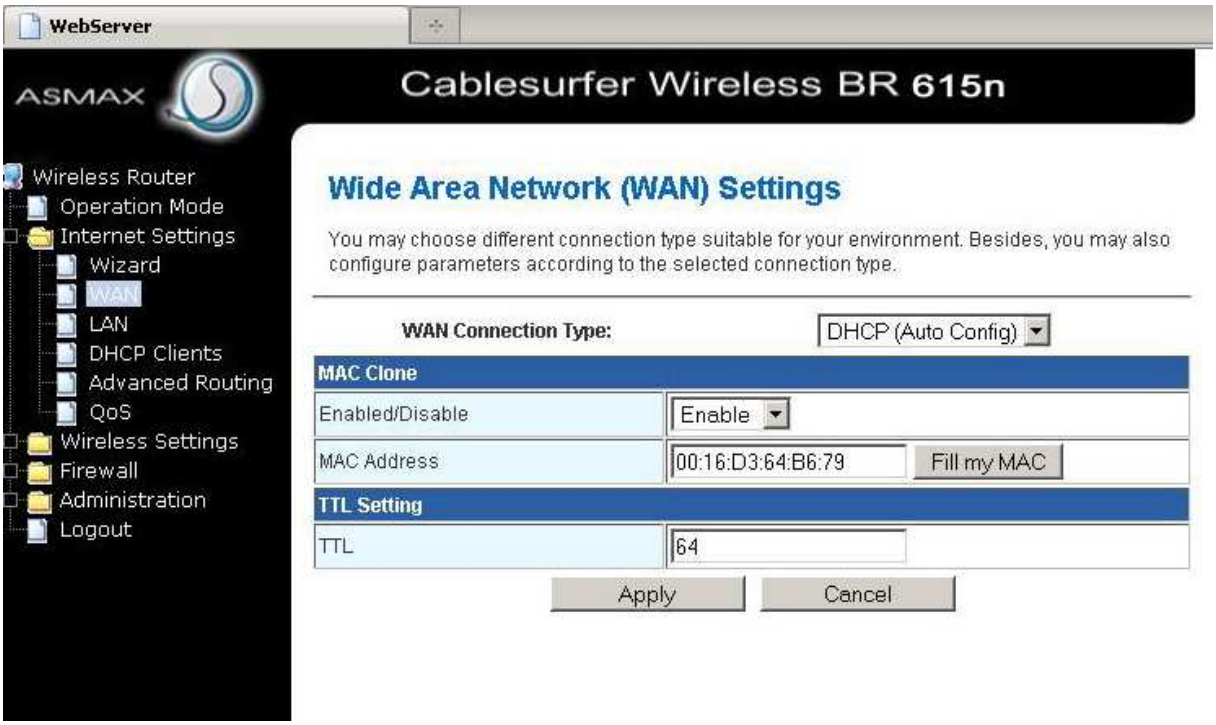
Fill My MAC – Klikając na ten przycisk w polu „MAC Address" zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.

TTL - (time-to-live), możliwość statycznego określenia „czasu życia" pakietu danych (zalecane jest pozostawienie domyślnej wartość), urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

DHCP (Auto Config)

Opcja klienta serwera DHCP umożliwia pracę urządzenia jako klienta DHCP na interfejsie WAN. Urządzenie automatycznie otrzyma adres IP, maskę podsieci, bramę domyślną oraz adresy serwerów DNS z serwera DHCP umieszczonego u dostawcy usług Internetowych ISP.



Parametry:

WAN Connection Type – Rodzaj połączenia z Internetem poprzez port WAN („Static IP" – stały adres IP, „DHCP Klient" – klient serwera DHCP, „PPPoE" – klient serwera PPPoE, „PPTP" – klient serwera PPTP, „L2TP"- klient serwera L2TP.

Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.

MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.

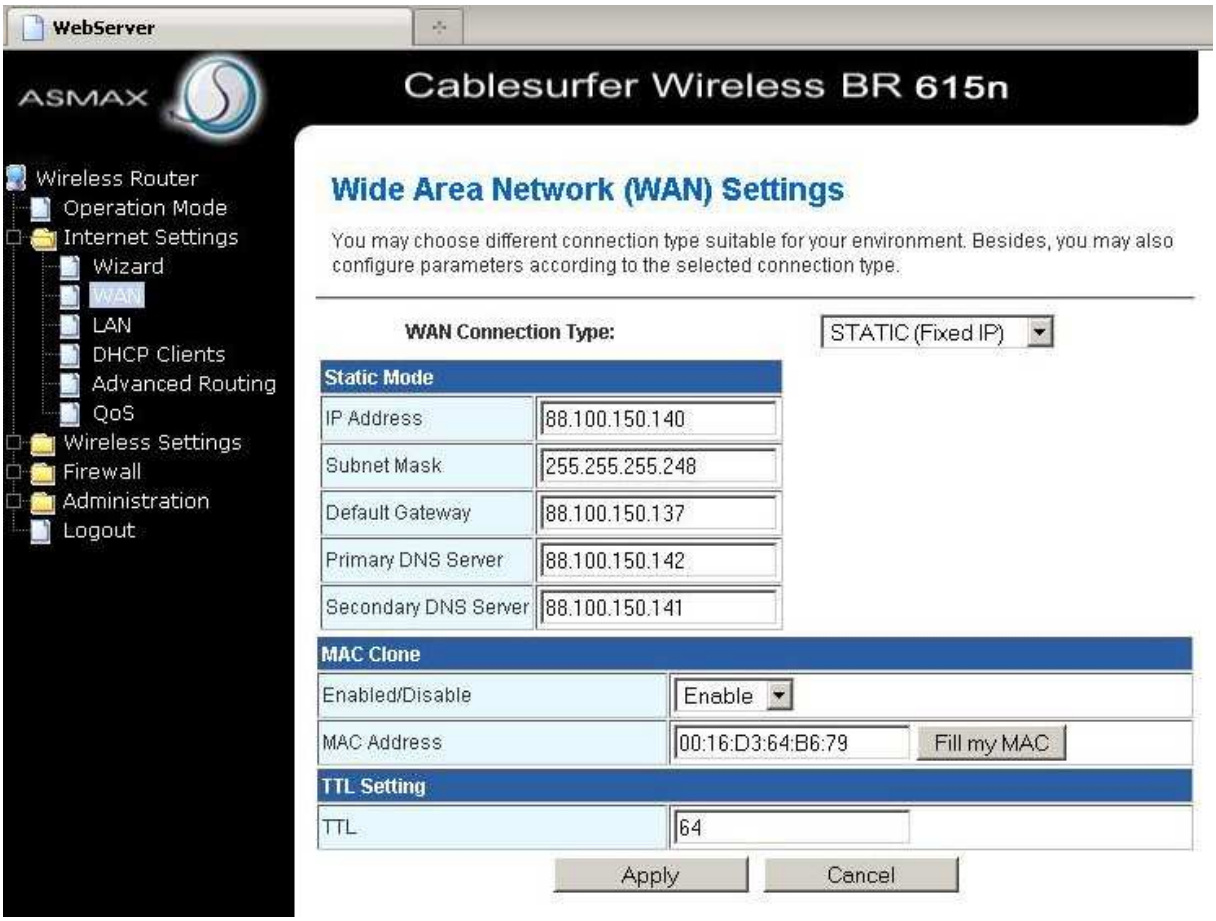
Fill My MAC – Klikając na ten przycisk w polu „MAC Address" zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.

TTL - (time-to-live), możliwość statycznego określenia „czasu życia" pakietu danych (zalecane jest pozostawienie domyślnej wartość), urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

Static (Fixe IP)

Opcja „Static IP" umożliwia przypisanie urządzeniu stałego adresu IP od strony interfejsu WAN (Internetu). Użytkownik musi samodzielnie przypisać adres IP, maskę podsieci, bramę domyślną (Default Gateway) oraz adresy serwerów DNS.



Parametry:

IP Address – Podaj adres IP uzyskany od usługodawcy.

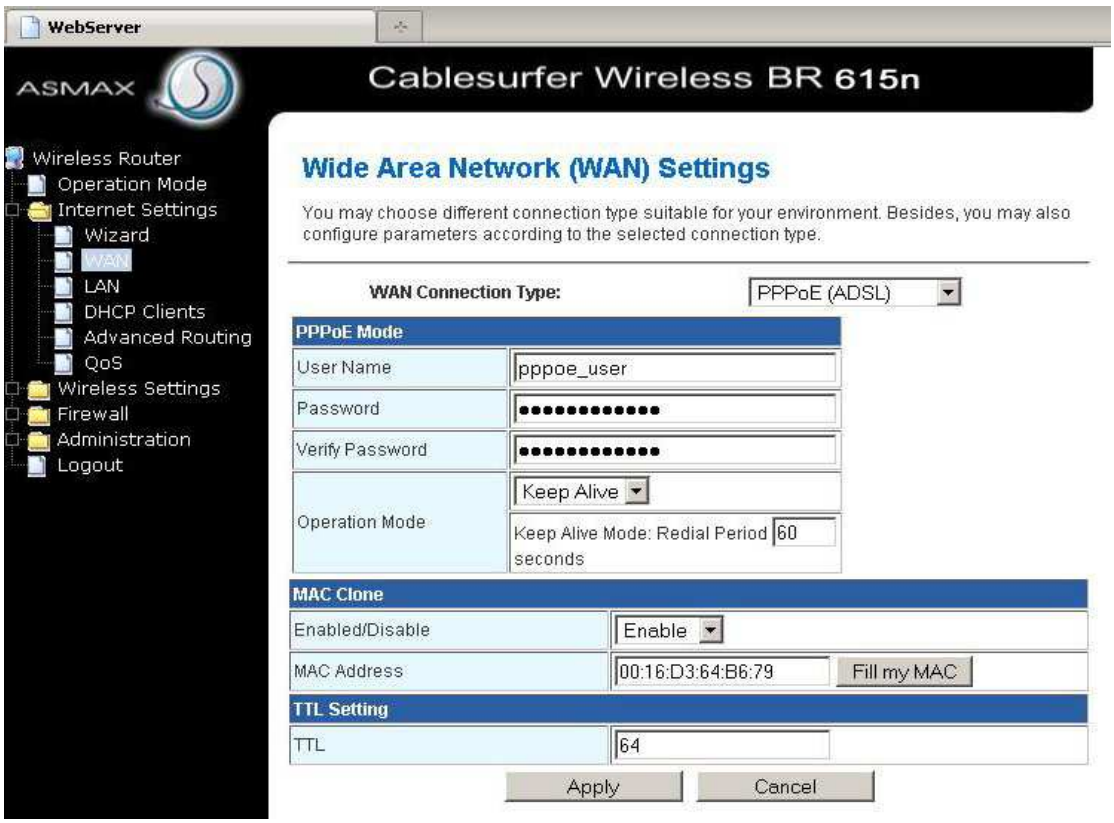
Subnet Mask – Podaj maskę podsieci uzyskaną od usługodawcy.

Default Gateway – Parametr opcjonalny. Wpisz adres IP bramy domyślnej uzyskany od usługodawcy.
Primary DNS/Secondary DNS – Parametr opcjonalny. Wpisz adresy IP serwerów DNS uzyskane od usługodawcy.
Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.
MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.
Fill My MAC – Klikając na ten przycisk w polu „MAC Address" zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.
TTL - (time-to-live), możliwość statycznego określenia „czasu życia" pakietu danych (zalecane jest pozostawienie domyślnej wartość) urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

PPPoE (ADSL)

Opcja klienta serwera PPPoE umożliwia skonfigurowania urządzenia do pracy jako klient serwera PPPoE. Połączenie PPPoE często wykorzystywane jest w bezprzewodowym dostępie do Internetu lub w sieciach ADSL z wykorzystaniem modemu ADSL z interfejsem Ethernet RJ-45 podłączonego do interfejsu WAN routera.



Parametry:

User Name/Password – Wpisz nazwę użytkownika i hasło uzyskane od usługodawcy. W tych polach ważna jest wielkość znaków.

Verify Password – Dla potwierdzenia wcześniej podanego hasła w polu „Password" wprowadź ponownie to samo hasło.

Operation Mode - Keep Alive – funkcja ta odpowiada za podtrzymywanie aktywnej sesji połączenia z serwerem naszego dostawcy usług internetowych (ISP) w czasie, gdy ani nasz komputer, ani serwer nie zgłaszają zapotrzebowań na kolejne bity danych. Przykładowo, gdy oglądamy stronę www nasze połączenie z serwerem, mimo że pozostaje aktywne, nie generuje żadnego ruchu, a to może doprowadzić do automatycznego zerwania naszego połączenia PPPoE. Aby zapobiec takim sytuacjom stworzono opcję „Keep Alive", która pozwala określić, co jaki czas nasz router Asmax BR615N ma wysyłać do serwera naszego ISP kontrolny pakiet podtrzymujący aktywne połączenie. Nasz router domyślnie wysyła do serwera potwierdzenie aktywności co 60 sekund. Możemy modyfikować wprowadzając odpowiednią wartość w polu „Keep Alive Mode: Redial Period seconds", co w wyjątkowych sytuacjach może nam pomóc. Zalecamy pozostawić wartość domyślną.

Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.

MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.

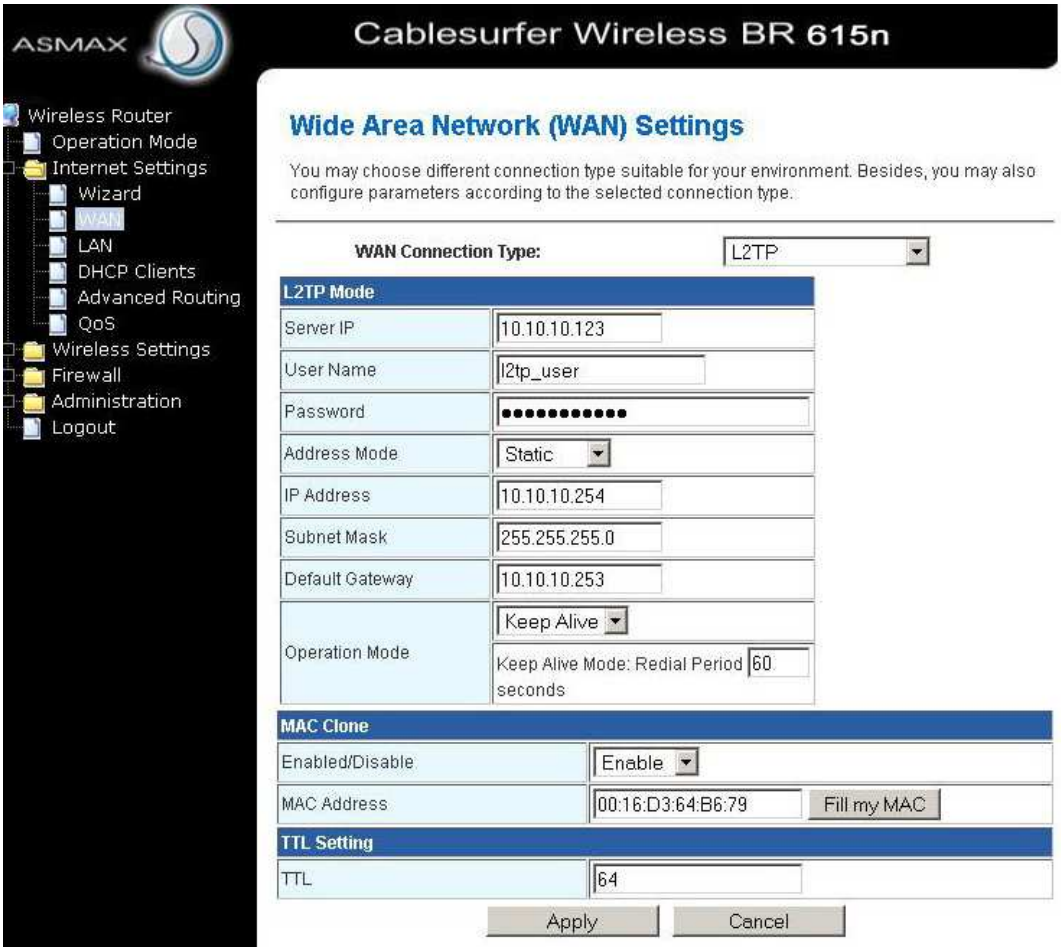
Fill My MAC – Klikając na ten przycisk w polu „MAC Address" zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.

TTL - (time-to-live), możliwość statycznego określenia „czasu życia" pakietu danych (zalecane jest pozostawienie domyślnej wartość), urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

L2TP

W przypadku konfiguracji połączenia L2TP dane, takie jak: adres IP serwera, login i hasło użytkownika uzyskujemy od naszego ISP i wprowadzamy w pola opisane poniżej.



Parametry:

Server IP – Wpisz adres IP serwera lub jego nazwę uzyskaną od usługodawcy.

User Name/Password – Wpisz nazwę użytkownika i hasło uzyskane od usługodawcy. W tych polach rozróżniana jest wielkość znaków.

Address Mode – Wybór metody przypisania parametrów dla połączenia L2TP, możemy wybrać ręczne przypisanie adresu (Static) lub automatyczne (Dynamic).

Operation Mode - Keep Alive – funkcja ta odpowiada za podtrzymywanie aktywnej sesji połączenia z serwerem naszego dostawcy usług internetowych (ISP) w czasie, gdy ani nasz komputer, ani serwer nie zgłaszają zapotrzebowań na kolejne bity danych. Przykładowo, gdy oglądamy stronę www nasze połączenie z serwerem, mimo że pozostaje aktywne, nie generuje żadnego ruchu, a to może doprowadzić do automatycznego zerwania naszego połączenia L2TP. Aby zapobiec takim sytuacjom stworzono opcję „Keep Alive", która pozwala określić, co jaki czas nasz router Asmax BR615N ma wysyłać do serwera naszego ISP kontrolny pakiet podtrzymujący aktywne połączenie. Nasz router domyślnie wysyła do serwera potwierdzenie aktywności co 60 sekund. Możemy modyfikować wprowadzając odpowiednią wartość w polu „Keep Alive Mode: Redial Period seconds", co w wyjątkowych sytuacjach może nam pomóc. Zalecamy pozostawić wartość domyślną.

Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.

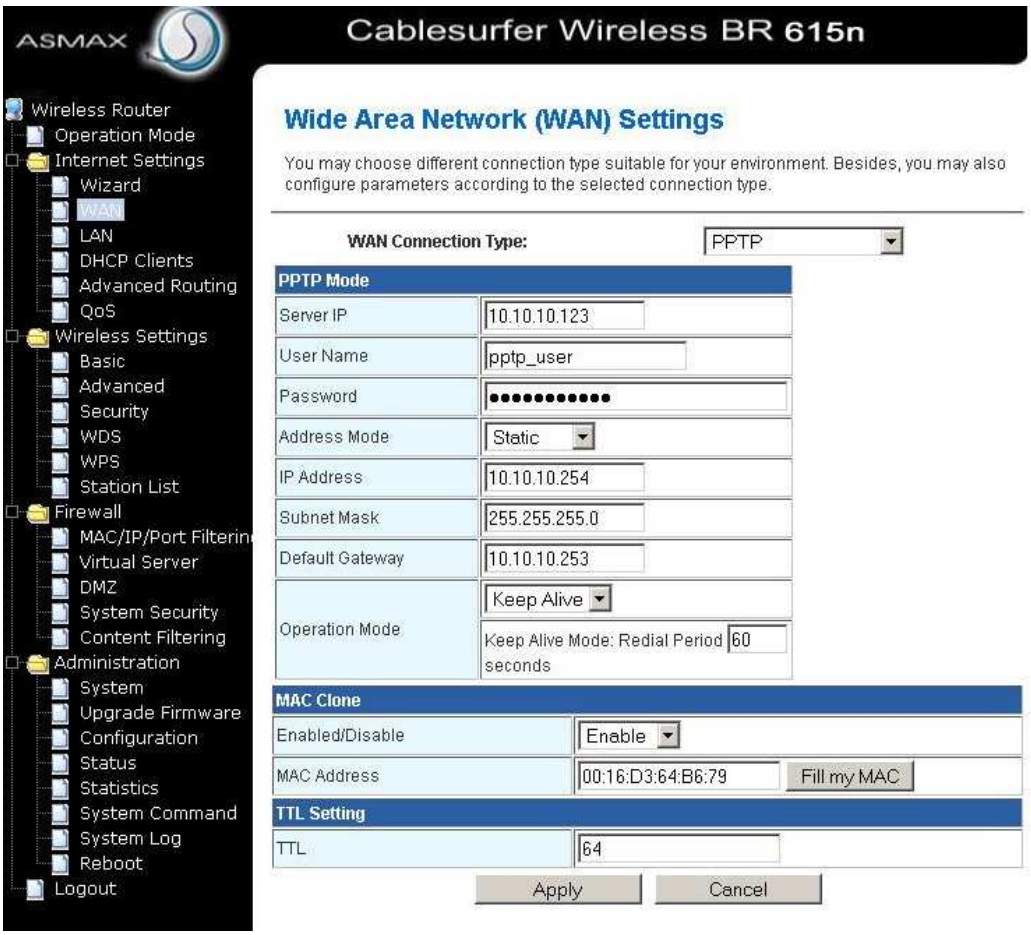
MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.

Fill My MAC – Klikając na ten przycisk w polu „MAC Address” zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.
TTL - (time-to-live), możliwość statycznego określenia „czasu życia” pakietu danych (zalecane jest pozostawienie domyślnej wartość) urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

PPTP

Opcja PPTP umożliwia skonfigurowanie urządzenia do pracy jako klient PPTP. Urządzenie zostanie połączone z serwerem ISP bezpiecznym tunelem PPTP. Dane umożliwiające autoryzację połączenia PPTP otrzymasz od swojego ISP.



Parametry:

Server IP – Wpisz adres IP serwera lub jego nazwę uzyskaną od usługodawcy.

User Name/Password – Wpisz nazwę użytkownika i hasło uzyskane od usługodawcy. W tych polach rozróżniana jest wielkość znaków.

Address Mode – Wybór metody przypisania parametrów dla połączenia PPTP, możemy wybrać ręczne przypisanie adresu (Static) lub automatyczne (Dynamic).

Operation Mode - Keep Alive – funkcja ta odpowiada za podtrzymywanie aktywnej sesji połączenia z serwerem naszego dostawcy usług internetowych (ISP) w czasie, gdy ani nasz komputer, ani serwer nie zgłaszają zapotrzebowań na kolejne bity danych. Przykładowo, gdy oglądamy stronę www nasze połączenie z serwerem, mimo że pozostaje aktywne, nie generuje żadnego ruchu, a to może doprowadzić do automatycznego zerwania naszego połączenia PPTP. Aby zapobiec takim sytuacjom stworzono opcję „Keep Alive", która pozwala określić, co jaki czas nasz router Asmax BR615N ma wysyłać do serwera naszego ISP kontrolny pakiet podtrzymujący aktywne połączenie. Nasz router domyślnie wysyła do serwera potwierdzenie aktywności co 60 sekund. Możemy modyfikować wprowadzając odpowiednią wartość w polu „Keep Alive Mode: Redial Period seconds", co w wyjątkowych sytuacjach może nam pomóc. Zalecamy pozostawić wartość domyślną.

Mac Clone Mode - wybieramy „Enable", aby uaktywnić funkcję klonowania adresu MAC lub „Diable", aby wyłączyć funkcję klonowania adresu MAC.

MAC Address – Tu należy podać adres MAC, jaki będzie posiadał nasz interfejs WAN w routerze w postaci 00:XX:XX:XX:XX:XX lub możemy użyć funkcji opisanej poniżej.

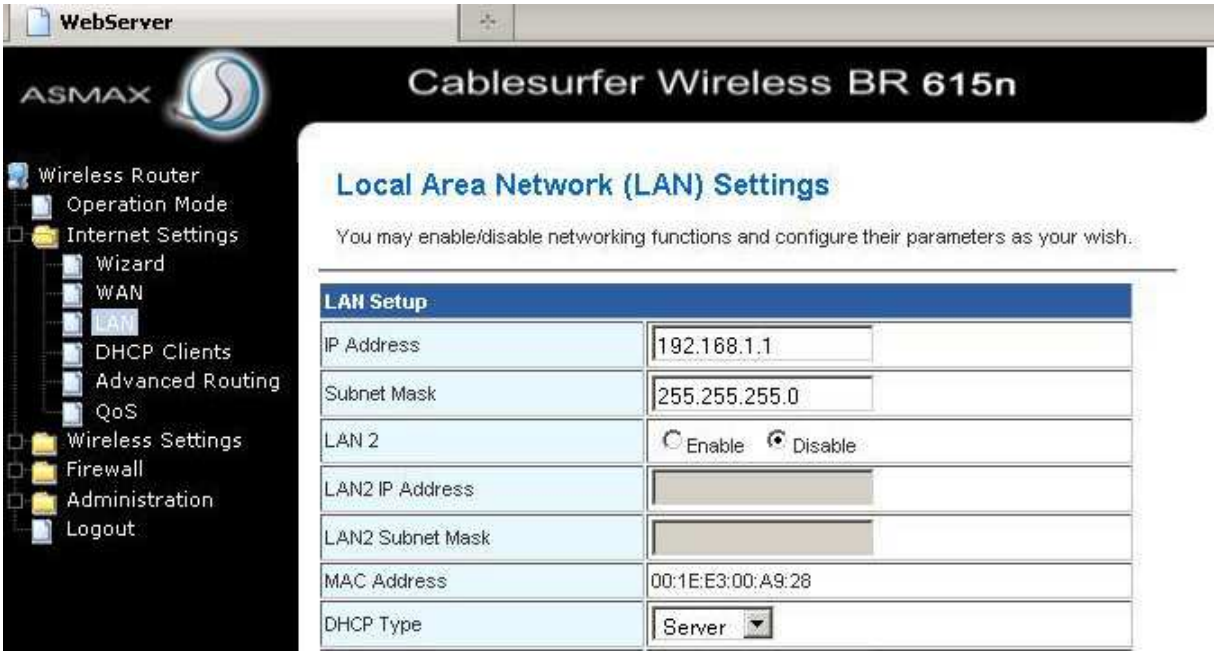
Fill My MAC – Klikając na ten przycisk w polu „MAC Address" zostanie podany adres MAC karty sieciowej, z której właśnie konfigurujemy nasze urządzenie.

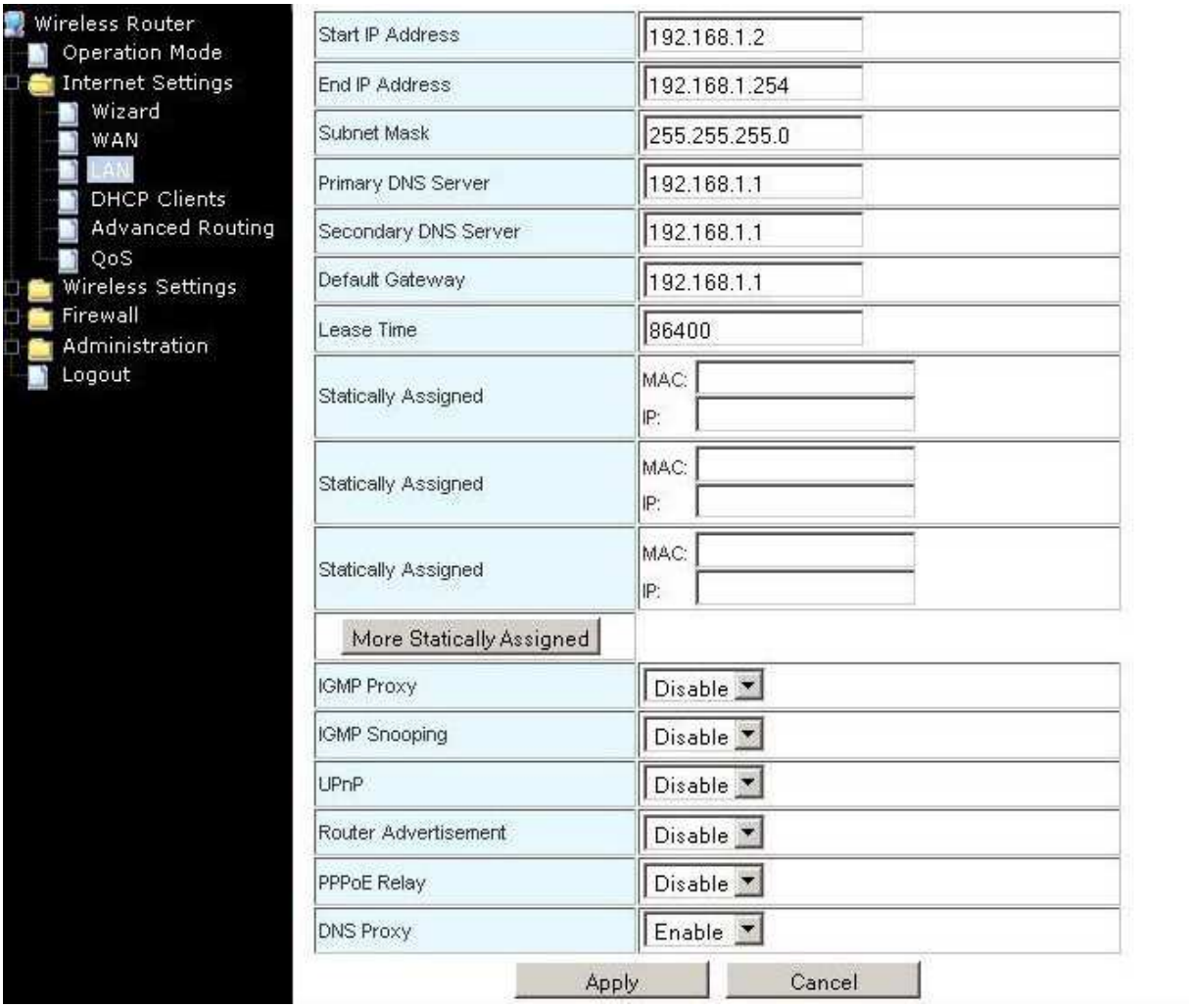
TTL - (time-to-live), możliwość statycznego określenia „czasu życia" pakietu danych (zalecane jest pozostawienie domyślnej wartość), urządzenie posiada automatyczne wbudowaną funkcję TTL+1.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

Zakładka konfiguracyjna podsieci LAN

Umożliwia konfigurację interfejsu LAN urządzenia, rozbudowanego serwera DHCP i usług usprawniających pracę wewnętrznych podsieci LAN.

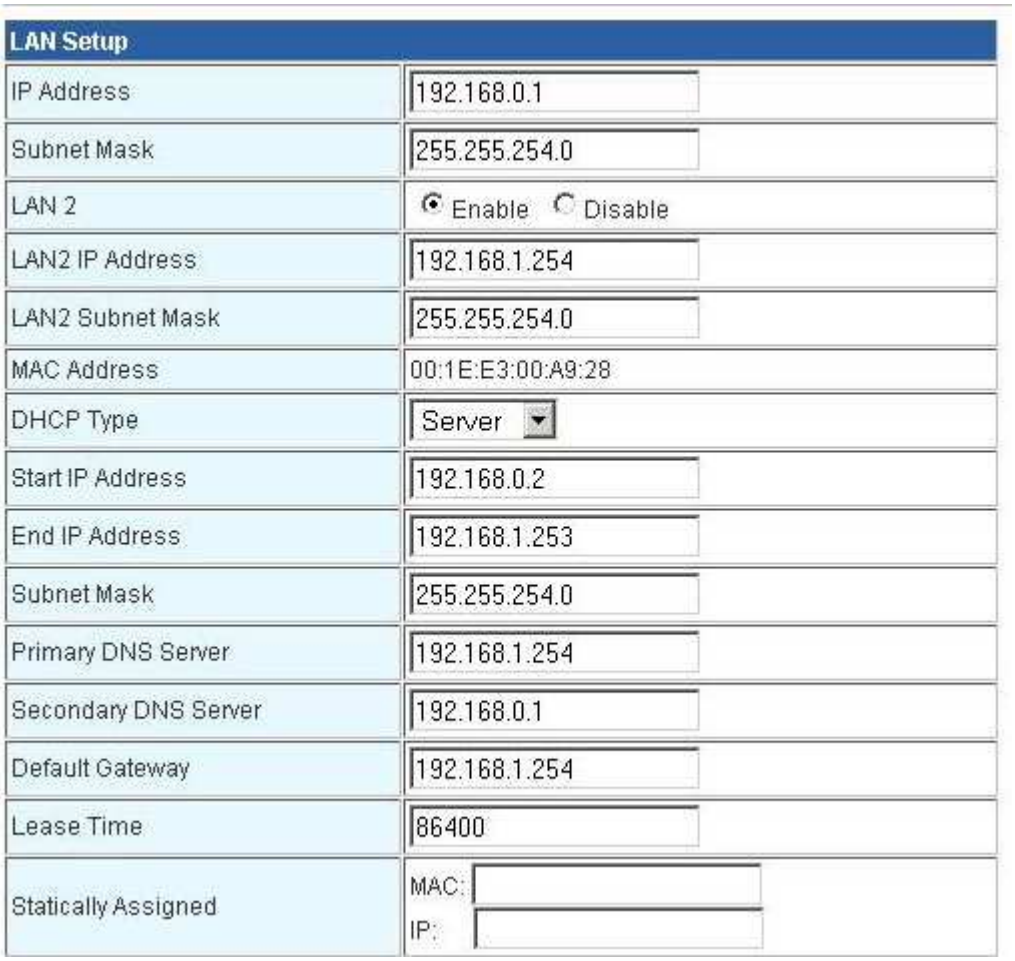




Parametry:

IP Address - Adres IP podstawowego interfejsu LAN (na ten adres logujemy się w celu konfiguracji urządzenia, w przypadku jego zmiany na inny należy o tym pamiętać i go zapisać). Domyślnie jest to 192.168.1.1.

Subnet Mask - Maska podsieci podstawowego interfejsu LAN. Domyślnie jest to 255.255.255.0, co oznacza, że w głównej (pierwszej) podsieci mamy dostępne adresy IP z zakresu od 192.168.1.2 do 192.168.1.254. W przypadku wykorzystania drugiej podsieci opisanej poniżej możemy stworzyć drugą osobną podsieć bez komunikacji między nimi, np. 192.168.2.0/255.255.255.0 lub możemy umożliwić komunikację dzięki podaniu odpowiedniej maski podsieci, którą możemy wyliczyć za pomocą dostępnych w Internecie kalkulatorów IP, np. http://42.pl/ipcalc/. Przykład konfiguracji dla 506 klienckich adresów IP na rysunku poniżej. Przykład pokazuje wykorzystanie i połączenie podsieci 192.168.0.0/255.255.254.0 i 192.168.1.0/255.255.254.0, gdzie adresy IP interfejsu LAN to 192.168.0.1 i 192.168.1.254, a zakres od 192.168.0.2 do 192.168.1.253 to adresy użytkowników.



LAN 2 – Drugi interfejs sieci LAN, domyślnie jest wyłączony „Disable", aby go uaktywnić zaznacz „Enable".

LAN2 IP Address – Po uaktywnieniu w polu „LAN 2" drugiego interfejsu sieci LAN w tym polu wpisujemy jego adres IP.

LAN2 Subnet Mask - Po uaktywnieniu w polu „LAN 2" drugiego interfejsu sieci LAN w tym polu wpisujemy jego maskę podsieci.

MAC Address – Adres MAC interfejsu LAN

DHCP Type – Możliwe opcje to tryb serwera DHCP (domyślnie zaznaczona opcja to „Server") lub wyłączenie serwera DHCP w urządzeniu po wybraniu opcji „Disable".

Start IP Address – Początkowy zakres adresów IP serwera DHCP.

End IP Address – Końcowy zakres adresów IP serwera DHCP.

Subnet Mask – Maska podsieci serwera DHCP.

Primary DNS Server – Adres IP podstawowego serwera DNS (zwykle będzie to adres IP interfejsu LAN, Asmax BR615N posiada własny prosty serwer DNS).

Secondary DNS Server – Adres IP alternatywnego serwera DNS.

Default Gateway – Brama domyślna dla klientów naszego routera.

Lease Time – Czas dzierżawy adresu IP przyznanego przez nasz serwer DHCP.

Statically Assigned – Pole powiązania danego adresu MAC z konkretnym adresem IP. W polu MAC podaj adres MAC, a w polu IP podaj adres IP, jaki ma otrzymywać dane urządzenie.

More Statically Assigned – Kliknięcie na przycisk rozwinie dodatkową listę powiązać MAC + IP

IGMP Proxy – Włączenie „Enable” lub wyłączenie „Disable” funkcji IGMP Proxy.

IGMP Snooping - Włączenie „Enable" lub wyłączenie „Disable" filtracji pakietów multicast. Po włączeniu tej funkcji, pakiety broadcast IGMP, nie będą wysyłane do interfejsu LAN, który nie należy do danej grupy.

UPnP - (Universal Plug-and-Play) - protokół typu P2P (połączenie bezpośrednie) dla komputerów osobistych oraz urządzeń inteligentnych i bezprzewodowych. Usługa UPnP minimalizuje konieczność konfiguracji komputera lub oprogramowania do pracy w sieci. Komputer obsługujący UPnP automatycznie konfiguruje swoją kartę sieciową oraz wyświetla informacje o stanie bramy sieciowej, dzięki czemu kompatybilne z tą technologią aplikacje sieciowe mogą zostać natychmiast uruchomione i nie wymagają dodatkowej konfiguracji zapory sieciowej, np. otwierania portów.

Router Advertisement - Funkcja umożliwia wyłączenie „Disable” lub włączenie „Enable” wysyłania w regularnych odstępach czasu komunikatów „Router Advertisement" w celu poinformowania o swojej obecności w podsieci. Dodatkowo komunikat „Router Advertisement" jest wysyłany jako odpowiedź na zapytanie komunikatu „Router Solicitation".

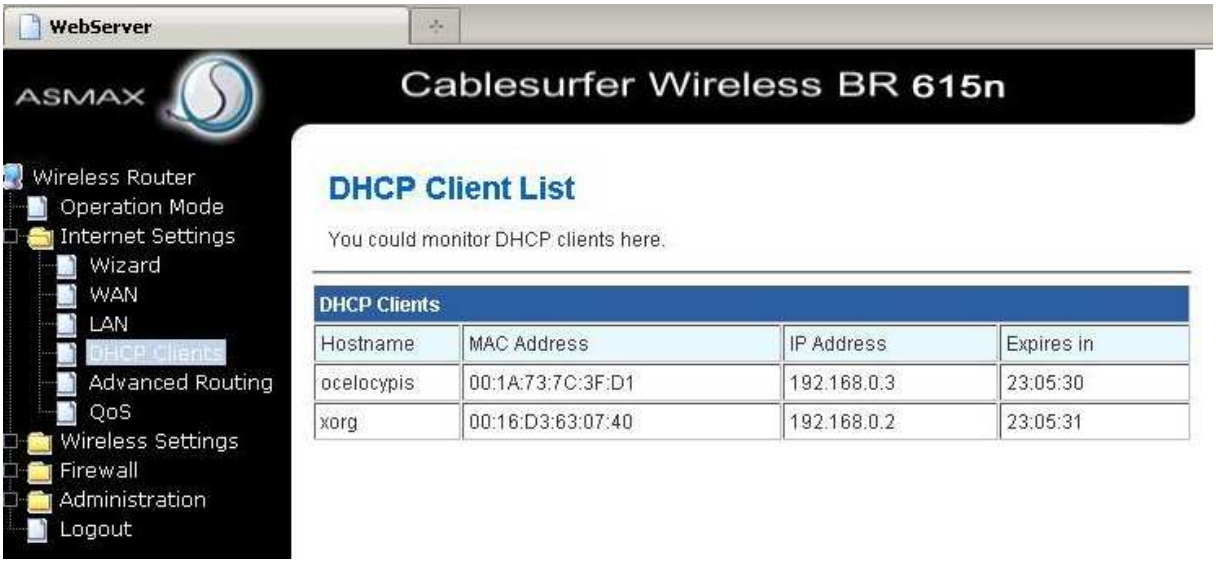
PPPoE Relay – Włącz „Enable” lub wyłącz „Disable” funkcję PPPoE Relay. Po włączeniu tej funkcji z lokalnego komputera można dokonać bezpośrednio połączenia PPPoE w trybie bramki.

DNS Proxy - Włącz lub wyłącz funkcję serwera proxy DNS, przyspiesza ładowanie stron, ponieważ router Asmax BR615N posiada własną pamięć, gdzie zapisuje zapytania DNS.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

DHCP Clients

Zakładka pokazuje nam podłączonych klientów, którzy otrzymali adres IP z serwera DHCP.



Parametry:

Hostname – Nazwa podłączonego urządzenia/komputera.

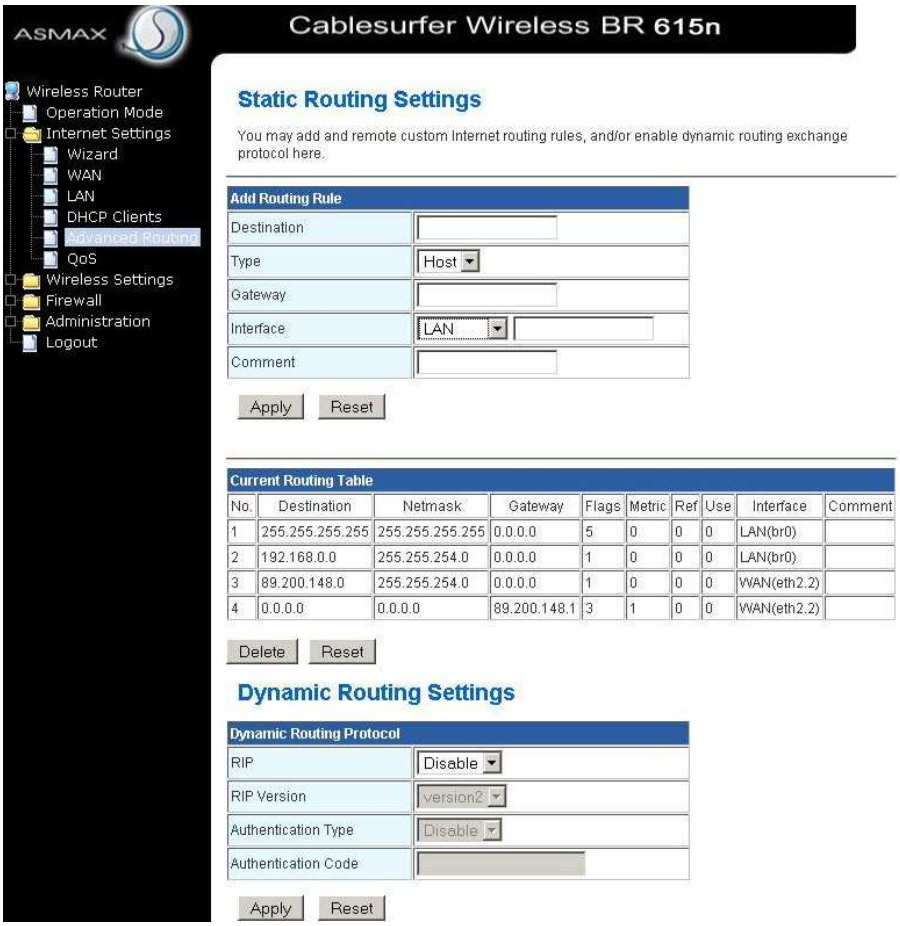
MAC Address – Adres MAC podłączonego urządzenia/komputera.

IP Address – Adres IP podłączonego urządzenia/komputera.

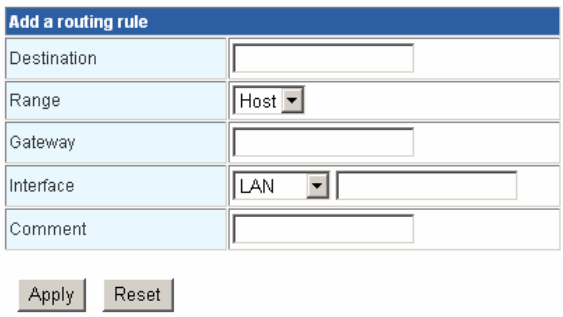
Expres In – Wygaśnięcie dzierżawy.

Zaawansowany routing

W zakładce „Advanced Routing" możemy dodawać własne reguły trasowania pakietów. Wyświetlić aktualny widok tras i skonfigurować statyczny i dynamiczny routing.



Dodawanie reguł trasowania



Parametry:

Destination – Adres docelowy reguły routingu.

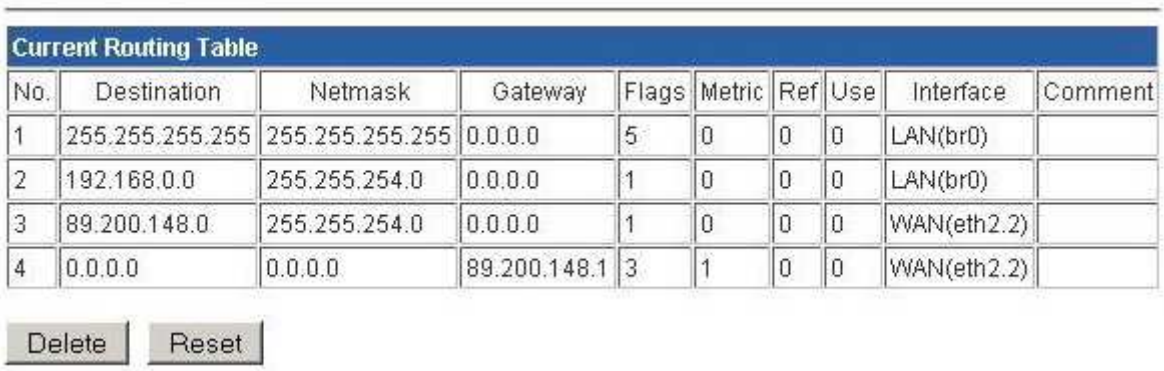
Range - Możliwość wyboru hosta lub podsieci.

Gateway – Adres IP bramy dla reguły.

Netmask – W przypadku wybrania opcji „Net" należy podać maskę podsieci.

Comment – Komentarz do dodanej reguły.

Aktualna tablica tras wygląda, jak na rysunku poniżej.

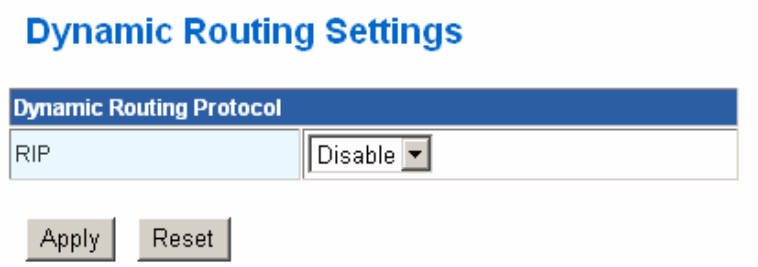


Current Routing Table

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface	Comment
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)	
2	192.168.0.0	255.255.254.0	0.0.0.0	1	0	0	0	LAN(br0)	
3	89.200.148.0	255.255.254.0	0.0.0.0	1	0	0	0	WAN(eth2.2)	
4	0.0.0.0	0.0.0.0	89.200.148.1	3	1	0	0	WAN(eth2.2)	

Delete Reset

Funkcja dynamicznego routingu



Można włączyć „Enable" lub wyłączyć „Disable" funkcję RIP (Routing Information Protocol) w tej części zakładki. Po włączeniu funkcji RIP, można odświeżyć swoje informacje routingu RIP i wysłać informacje do innych urządzeń.

Zarządzanie pasmem - QoS

W tej zakładce możesz zagwarantować pasmo dla poszczególnych usług, jak telefonia internetowa, gry, aplikacje. Dzięki tej funkcji możesz wygodnie pracować, nawet jeśli kilka komputerów korzysta w tym samym czasie z programów typu p2p i innych powodujących przeciążenie naszego łącza do Internetu. Funkcja Quality of Service umożliwia nam pełną kontrolę nad naszym łączem do Internetu. Dane mogą otrzymywać odpowiedni priorytet gwarantujący, że ruch dla nas ważny, np. gry internetowe, aplikacje wymagające niskich opóźnień (głos, obraz) lub ważne pliki są przesyłane z maksymalną szybkością nawet przy dużym obciążeniu naszego łącza. Posiadamy możliwość regulacji szybkości, z jaką poszczególne typy danych są przesyłane przez nasz router. Posiadamy możliwość prostego ich klasyfikowania i przydzielania do odpowiednich grup. Możemy też skorzystać

z możliwości szybkiej konfiguracji za pomocą gotowych reguł. Wystarczy kliknąć na jeden przycisk i utworzony zostanie zaawansowany podział pasma.

Zakładka z rysunku powyżej służy do konfiguracji zarządzania przepustowością pobierania i wysyłania danych przez interfejs WAN oraz definiowania reguł zarządzania pasmem QoS.

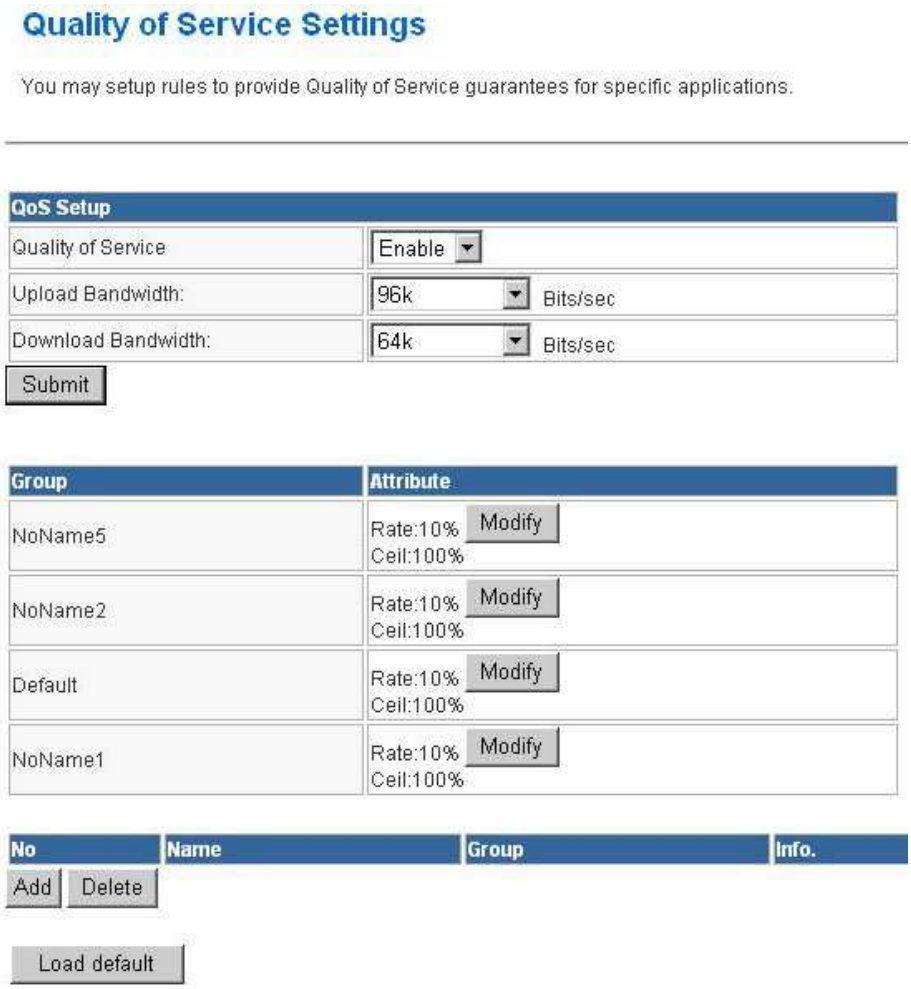
Parametry:

Quality of Service – Włącz „Enable" lub wyłącz „Disable" funkcję QoS. Domyślnie funkcja QoS jest wyłączona. Po włączeniu funkcji QoS, możemy ustawić przepustowość wysyłania i pobierania przez interfejs WAN.

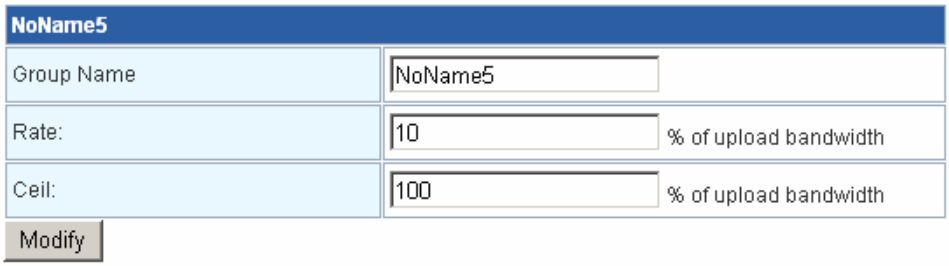
Upload Bandwidth - Możesz samodzielnie zdefiniować szybkość swojego pasma lub wybierz odpowiednią wartość łącza z rozwijanej listy.

Download Bandwidth - Możesz samodzielnie zdefiniować szybkość swojego pasma lub wybierz odpowiednią wartość łącza z rozwijanej listy.

Po włączeniu funkcji QoS i określeniu przepustowości pasma (np. przepustowość pobierania to 128kb/s, a wysyłania to 64kb/s), kliknij przycisk „Add", a na następnej stronie pojawi się okno, jak na rysunku poniżej.



Na wyświetlonej stronie mamy 4 grupy z zagwarantowanym pasmem. Nową regułę możemy dołączyć do którejś grupy. Po dołączeniu nowej reguły do grupy, minimum i maksimum dostępnego pasma są taki same, jak grupy. Grupy możemy modyfikować. Aby zmodyfikować grupę kliknij na przycisk „Modify" , po kliknięciu pojawi się okno, jak na rysunku poniżej.



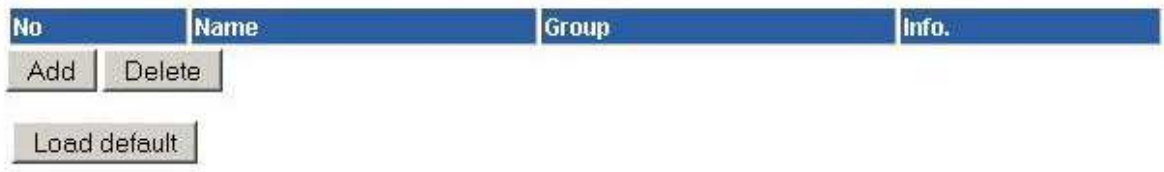
Parametry:

Group Name – Wyświetla nazwę danej grupy, możesz ją zmienić, jeśli uznasz to za konieczne.

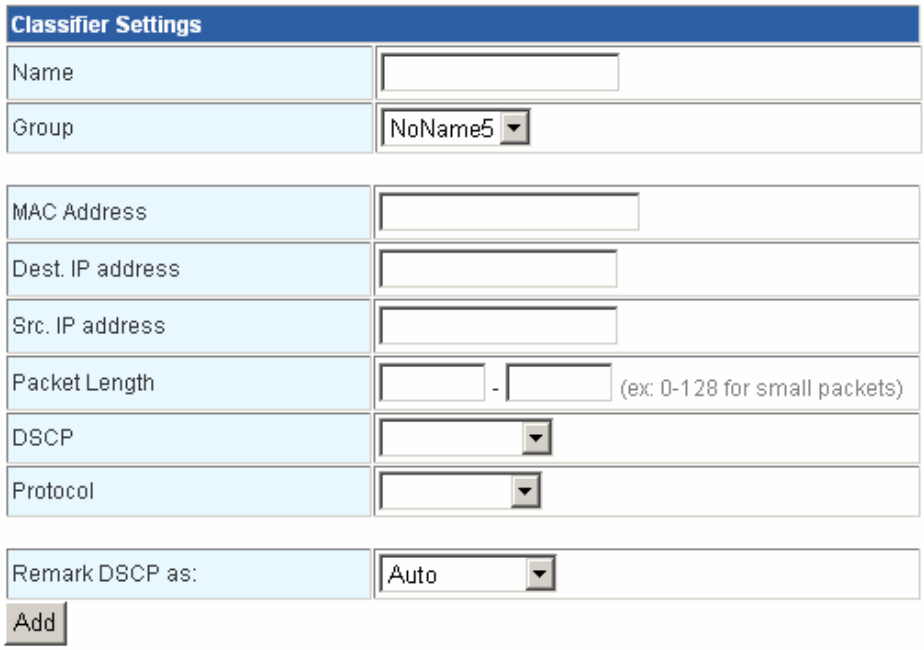
Rate - Gdy przepływ danych jest osiąga założoną granicę, wartość ta przedstawia minimalną przepustowość dla grupy. Jej zakres wartości może wynosić od 1 do wartości podanej w polu „Ceil".

Ceil – Wartość określająca maksymalną przepustowość dla grupy. Możemy podać wartości od 1 do 100.

Aby dodać regułę, kliknij przycisk „Add”.



Zostanie wyświetlona strona dodawania reguły, jak na rysunku poniżej.



Parametry:

Name – Wprowadź nazwę reguły.

Group – Wybierz z listy grupę przynależności dla tworzonej reguły.

MAC Address - Źródłowy adres MAC reguły. Jeśli pakiety danych zawierają podany adres MAC, pakiety danych są wprowadzane do odpowiedniej grupy.

Dest. IP address - Docelowy adres IP reguły. Jeśli pakiety danych zawiera podany adres IP, pakiety danych są wprowadzane do odpowiedniej grupy.

Src. IP address - Źródłowy adres IP reguły. Jeśli pakiety danych zawiera podany adres IP, pakiety danych są wprowadzane do odpowiedniej grupy.

Packet Length - Długość pakietu reguły. Jeśli pakiety danych jest określonej długości, pakiet danych zostaje wprowadzony do odpowiedniej grupy.

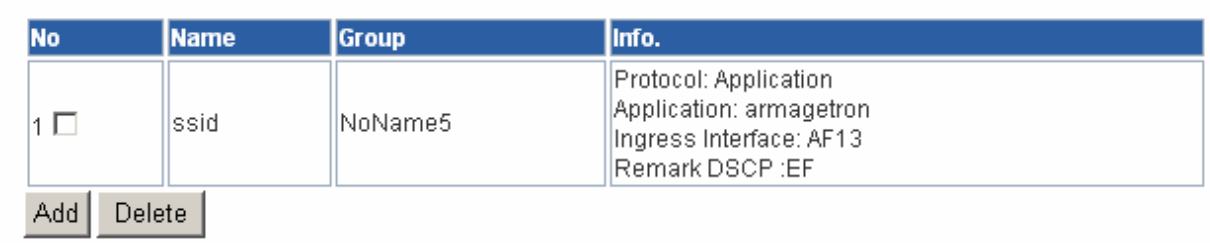
DSCP - Znak DSCP. Jeśli pakiety danych zawierają odpowiednie znaki DSCP, pakiety danych są wprowadzane do odpowiedniej grupy.

Protocol - Typy protokołów to: TCP, UDP, ICMP i aplikacje. Jeśli pakiety danych są zgodne z danym protokołem, pakiety danych są wprowadzane do odpowiedniej grupy. Przy wyborze TCP lub UDP,

musisz ustawić port źródłowy i zakres portów źródłowych. Po wybraniu aplikacji, możesz wybrać właściwy protokół z rozwijanej listy.

Remark DSCP as - Ustawienie domyślne to „Auto”.

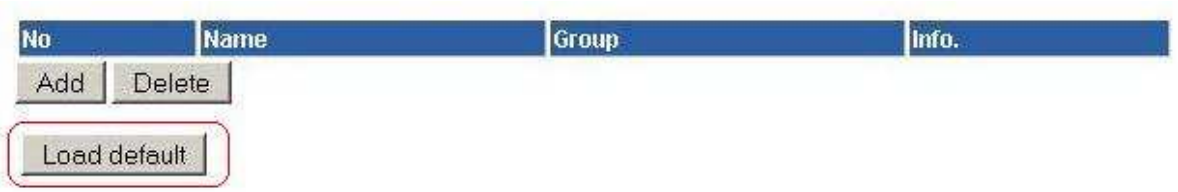
Kasowanie wprowadzonych reguł



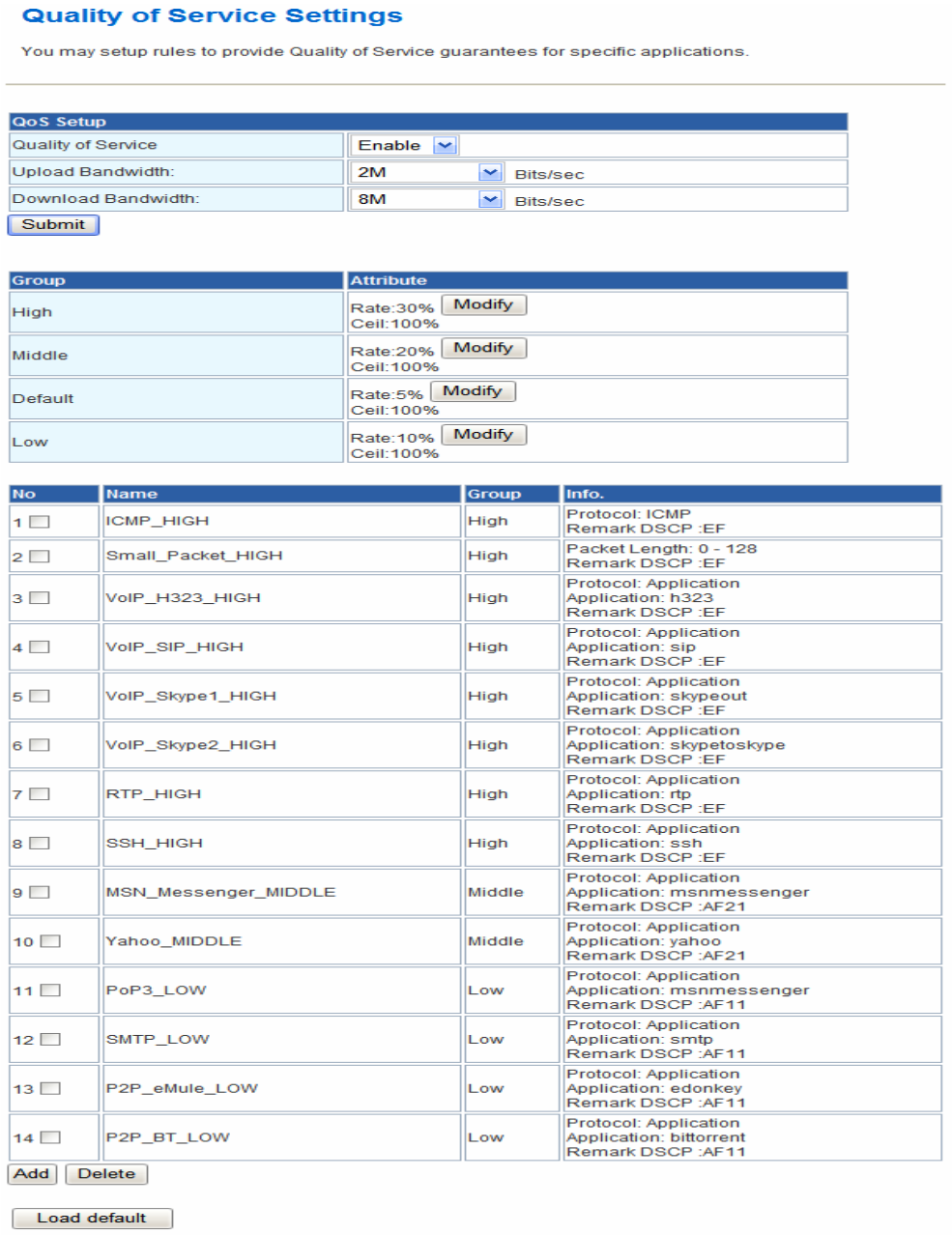
Jeśli istnieją reguły QoS w tabeli, a chcesz usunąć regułę QoS, możesz wybrać daną regułę, zaznaczając ją w polu „No", a następnie kliknąć przycisk „Delete”, aby usunąć wybraną regułę.

Szybka konfiguracja domyślnej polityki zarządzania pasmem

Router Asmax BR615N posiada możliwość automatycznego utworzenia domyślnej polityki dla zarządzania pasmem, aby to skorzystać z gotowego rozwiązania wystarczy kliknąć przycisk „Load default”.



Po kliknięciu na przycisk „Load default” utworzone zostaną gotowe reguły zarządzania pasmem dla podstawowych usług jak na rysunku poniżej.



Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Enable
Upload Bandwidth:	2M Bits/sec
Download Bandwidth:	8M Bits/sec

Submit

Group	Attribute
High	Rate:30% Modify Ceil:100%
Middle	Rate:20% Modify Ceil:100%
Default	Rate:5% Modify Ceil:100%
Low	Rate:10% Modify Ceil:100%

No	Name	Group	Info.
1	ICMP_HIGH	High	Protocol: ICMP Remark DSCP :EF
2	Small_Packet_HIGH	High	Packet Length: 0 - 128 Remark DSCP :EF
3	VoIP_H323_HIGH	High	Protocol: Application Application: h323 Remark DSCP :EF
4	VoIP_SIP_HIGH	High	Protocol: Application Application: sip Remark DSCP :EF
5	VoIP_Skype1_HIGH	High	Protocol: Application Application: skypeout Remark DSCP :EF
6	VoIP_Skype2_HIGH	High	Protocol: Application Application: skypetoskype Remark DSCP :EF
7	RTP_HIGH	High	Protocol: Application Application: rtp Remark DSCP :EF
8	SSH_HIGH	High	Protocol: Application Application: ssh Remark DSCP :EF
9	MSN_Messenger_MIDDLE	Middle	Protocol: Application Application: msnmessenger Remark DSCP :AF21
10	Yahoo_MIDDLE	Middle	Protocol: Application Application: yahoo Remark DSCP :AF21
11	PoP3_LOW	Low	Protocol: Application Application: msnmessenger Remark DSCP :AF11
12	SMTP_LOW	Low	Protocol: Application Application: smtp Remark DSCP :AF11
13	P2P_eMule_LOW	Low	Protocol: Application Application: edonkey Remark DSCP :AF11
14	P2P_BT_LOW	Low	Protocol: Application Application: bittorrent Remark DSCP :AF11

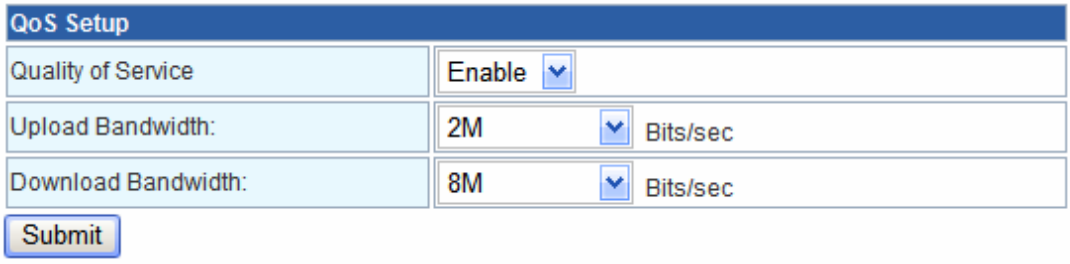
Add Delete

Load default

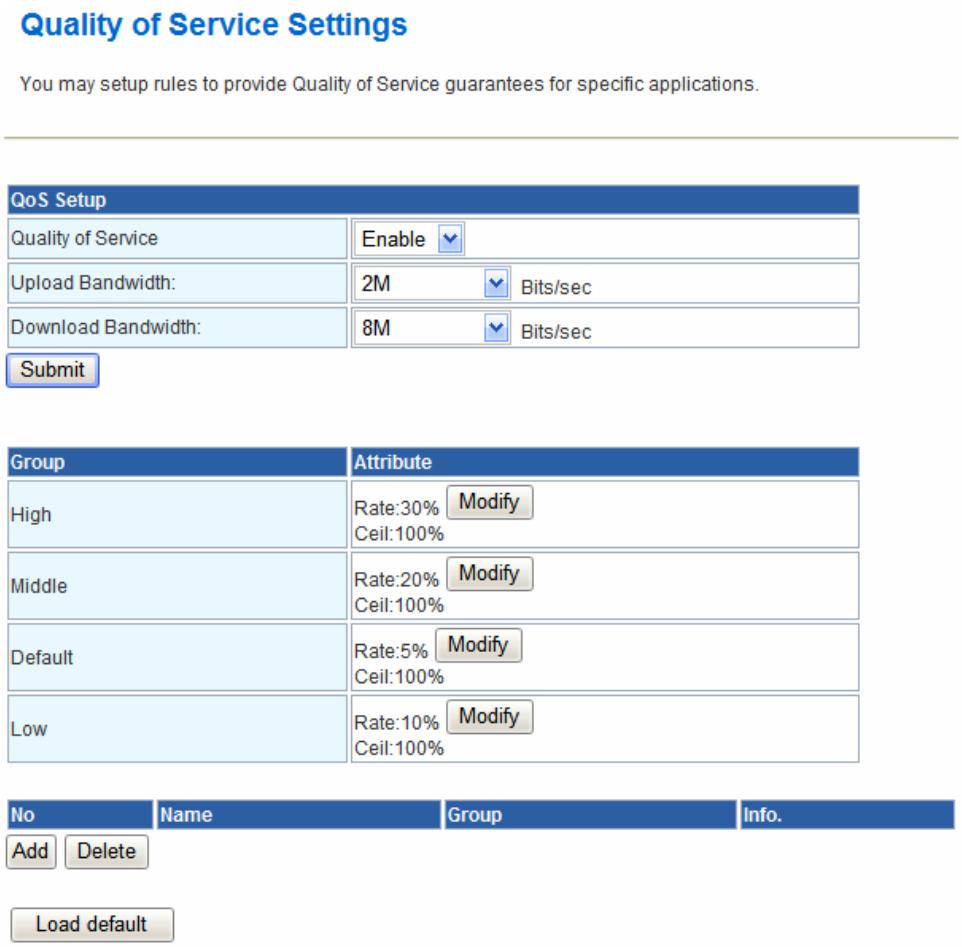
Po załadowaniu domyślnych reguł, cztery grupy zostaną ponownie zdefiniowane jako „High”, „Middle”, „Default”, „Low”, a minimalna przepustowość wartości odpowiednich grup zmieniły się na 30%, 20%, 5% i 10%. Można również usunąć domyślne reguły w razie potrzeby i modyfikować wszystkie grupy.

Przykładowe ustawienia QoS

Ustawiamy prędkość wysyłania i pobierania, jak na rysunku poniżej.

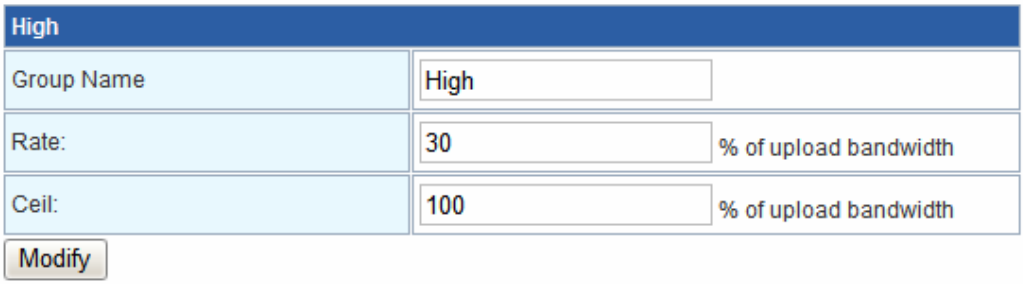


W zakładce „Quality of Service Settings” włącz obsługę QoS, wartość pola „Quality of Sernice” na „Enable” i ustaw przepustowość wysyłania i pobrania. Na przykład dla wartości wysyłania ustawiamy przepustowość do 2Mbps i odpowiednio dla pobierania 8Mbps. Po zakończeniu wprowadzania ustawień kliknij przycisk „Submit”, aby zapisać wprowadzone ustawienia.



Modyfikacja atrybutów wybranej grupy

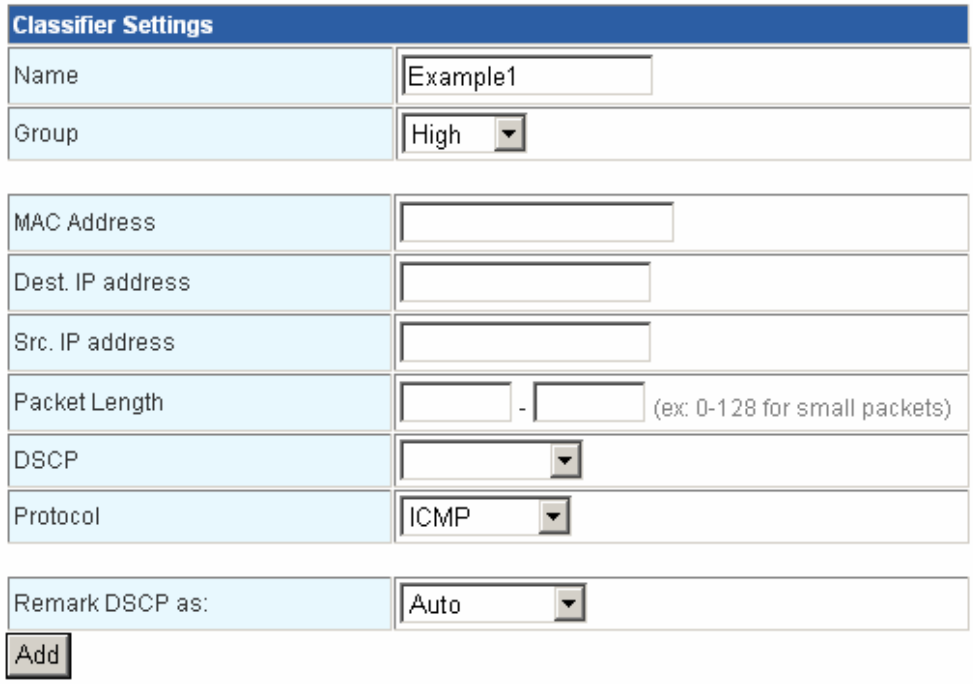
Po włączeniu funkcji QoS, system ustanawia domyślnie 4 grupy. Kliknij przycisk „Modify” dla odpowiedniej grupy.



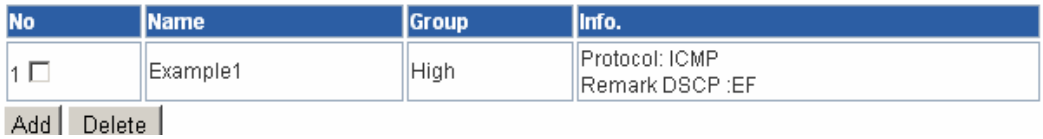
Na tej stronie, należy ustawić wartość „Rate” do 30% maksymalnej wartości. Jeśli przepustowość wysyłania wynosi 2Mbps, w momencie obciążenia, kiedy przepływ danych jest duży, oznacza to, że minimalna przepustowość tej grupy wynosi 30% całkowitej szerokości pasma, czyli około 0,6 Mbps. Gdy przepływ danych jest mały, maksymalna przepustowość wysyłania tej grupy wynosi 100% łącznej przepustowości, czyli 2 Mbps.

Dodawanie reguły QoS

Aby dodać regułę kliknij „Add”, wyświetlona zostanie strona, jak poniżej.

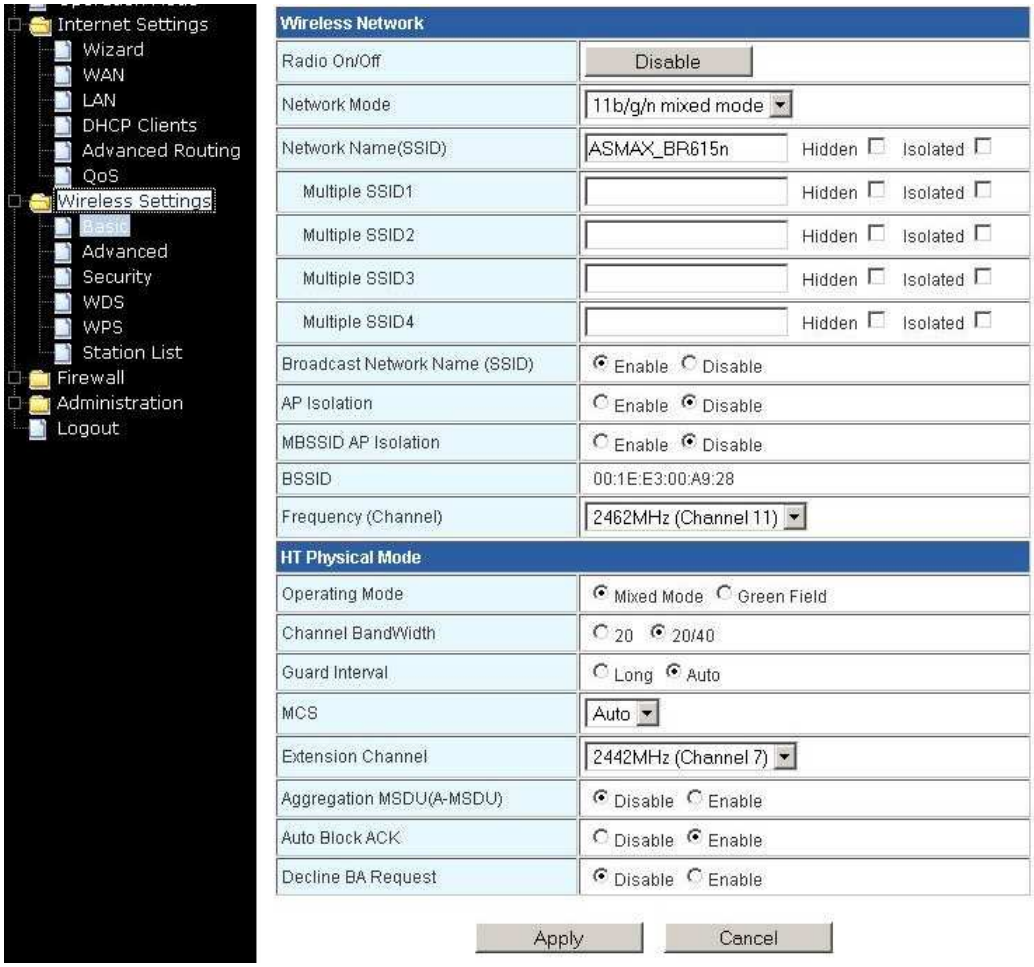


Na tej stronie można dodać reguły QoS. Na przykład, ustawimy nazwę reguły „Example1”, dodamy regułę go do grupy „High” i wybierzemy protokół ICMP.
Po zakończeniu wprowadzania ustawień, kliknij przycisk „Add” .



Sieć bezprzewodowa – Wireless Settings

Zakładka „Wireless Settings → Basic" umożliwia konfigurację wbudowanego modułu bezprzewodowego oraz bezpieczeństwa transmisji bezprzewodowej.



Parametry:

Radio On/Off – Włączony lub wyłączony moduł sieci bezprzewodowej. Domyślnie jest włączony, aby wyłączyć kliknij „Disable".

Network Mode – Tryb pracy sieci bezprzewodowej, domyślnie jest to 802.11b/g/n. Jest to tryb mieszany umożliwiający wsteczną kompatybilność z urządzeniami starej generacji 802.11b/g.

- 11b mode: Umożliwia klientom bezprzewodowym łączenie się z routerem w trybie 11b z maksymalną szybkością 11 Mb/s.
- 11g mode: Umożliwia urządzeniom klienckim zgodnym ze standardem 11g/11n łączenie się z punktem dostępowym z maksymalną szybkością 54 Mb/s.
- 11b/g mixed mode: Umożliwia urządzeniom klienckim zgodnym ze standardem 11b/g łączenie się z punktem dostępowym z szybkością negocjowaną automatycznie, a klientom bezprzewodowym zgodnym ze standardem 11n — z szybkością przewidzianą w ramach standardu 11g.
- 11b/g/n mixed mode: Umożliwia urządzeniom klienckim zgodnym ze standardami
- 11n łączenie się z punktem dostępowym z szybkością negocjowaną automatycznie .

Network Name (SSID) - (Service Set IDentifier), unikalny identyfikator (nazwa sieci bezprzewodowej), który muszą dzielić wszyscy klienci bezprzewodowi w ramach sieci bezprzewodowej. SSID musi być identyczny we wszystkich urządzeniach klienckich oraz węzłach bezprzewodowych. Dowolna wartość alfanumeryczna do 32 znaków używana dla zapobiegania przecięcia komunikacji pomiędzy dwoma (lub więcej) sieciami WLAN w jednej przestrzeni. Wielkość wprowadzonych liter ma znaczenie.

Multiple SSID1~4 – Asmax BR615N umożliwia utworzenie do czterech wirtualnych punktów dostępowych. W pola „Multiple SSID" podajemy SSID każdego z nich Każdy wirtualny punkt dostępowy umożliwia nam osobną konfigurację, zaznaczając opcję „Hidden" wyłączymy rozgłaszanie identyfikatora SSID. Opcja „Isolated" włącza izolację klientów sieci bezprzewodowej.

Broadcast Network Name (SSID) – Funkcja rozgłaszania identyfikatora SSID, nie zalecamy wyłączenia tego parametru.

AP Isolation – Blokada komunikacji pomiędzy użytkownikami sieci bezprzewodowej.

MBSSID AP Isolation - Włącz lub wyłącz izolację pomiędzy różnymi SSID. Po włączeniu tej funkcji, terminale klientów z różnych SSID nie będą mogli komunikować się ze sobą.

BSSID – Adres MAC interfejsu bezprzewodowego.

Frequency (Channel) – Częstotliwość (kanał) pracy interfejsu bezprzewodowego, domyślnie jest to kanał 11.

Operation Mode – Wybór trybu pracy, domyślnie jest to tryb mieszany „Mixed Mode".

Channel BandWidth - W tym miejscu należy wybrać przepustowość kanału, aby zwiększyć wydajność sieci bezprzewodowej. Jeśli w sieci działają urządzenia klienckie zgodne ze standardami 11b/g oraz 11n, można wybrać wartość 20. W przypadku sieci typu 11n można wybrać wartość 20/40, aby zwiększyć przepustowość.

Guard Interval – Okres ochronny domyślnie powinien być ustawiony na „AUTO".

MCS - Można wybrać wartość MCS od 0 do 32. Domyślnie MCS to „Auto".

Reverse Direction Grant (RDG) – Możesz wyłączyć „Disable" lub włączyć „Enable". Wartość domyślna to „Enable".

Extension Chanel - W tym miejscu wybiera się kanał rozszerzenia, który służy do zwiększenia szybkości transmisji danych w sieci bezprzewodowej w trybie 11n.

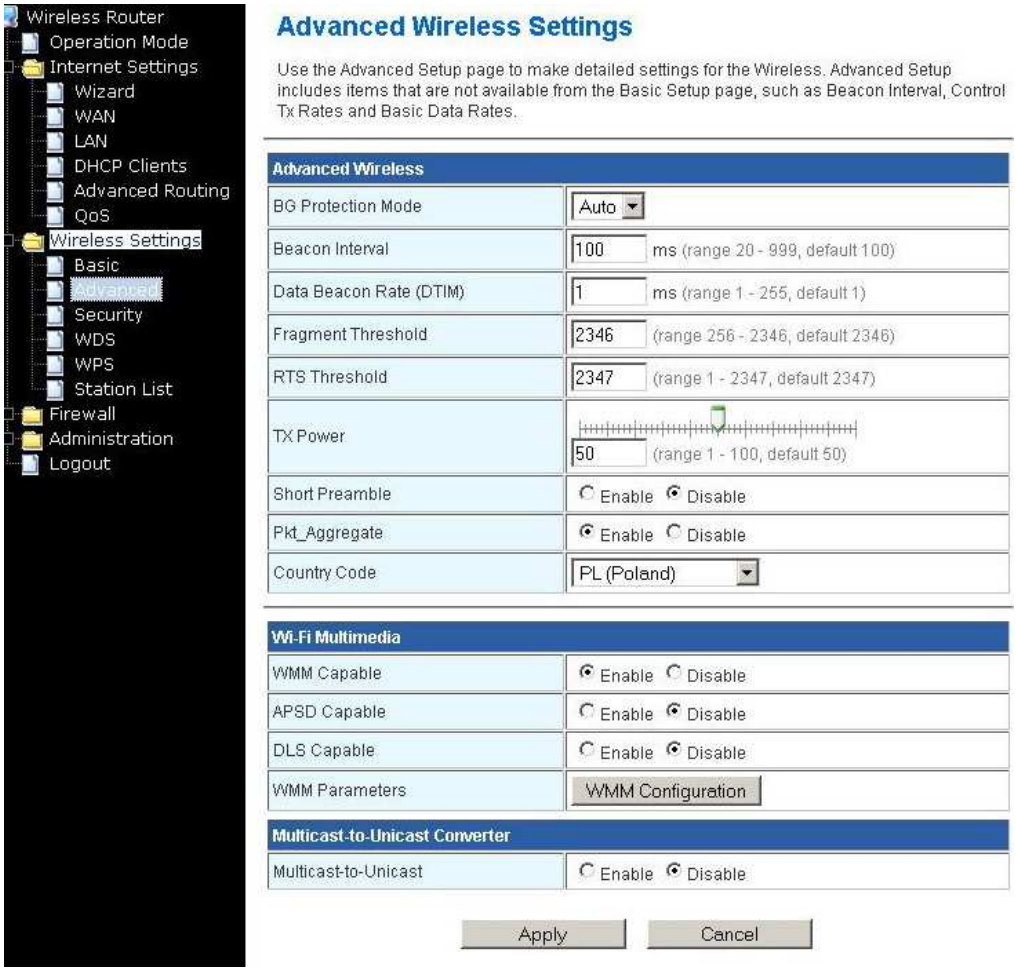
Aggregation MSDU (A-MSDU) - MAC Service Data Unit Aggregation (A-MSDU) – grupuje paczki kontrolne logicznego połączenia (MSDU) z takimi samymi ramkami 802.11e QoS, które są niezależne od źródła i celu. Otrzymana ramka MAC zawiera tylko jeden nagłówek MAC, który jest „przyczepiony" do 7935 bajtów MSDU (parę ramek spiętych w jedną).

Auto Block ACK – Funkcja redukuje liczbę paczek ACP, które odbiorca musi wysłać do adresata, by potwierdzić przybycie paczki. Typowe urządzenia 802.11g oczekują prawie natychmiastowej odpowiedzi ACK na każdą nie multicastową/broadcastową ramkę. Z kolei urządzenia 802.11n akceptują Bloki ACK, które potwierdzają odebranie wielu ramek unicast.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

Zakładka Advanced

Zakładka „Advanced” umożliwia zaawansowane konfigurowanie opcji sieci bezprzewodowej.



Parametry:

BG Protection Mode - Możesz wybrać „ON”, „OFF” lub „Auto”. Domyślny tryb ochrony to „Auto”, który umożliwia klientom bezprzewodowym zgodnym ze standardem 11b/g bezproblemowe łączenie się z sieciami w standardzie 802.11n w skomplikowanych konfiguracjach.

Beacon Interval - (20-999) - Sygnały identyfikacji są pakietami wysłanymi przez punkt dostępu, by zsynchronizować sieć bezprzewodową. Parametr ten określa przedział czasowy pomiędzy transmisjami sygnału identyfikacji. Sygnał identyfikacji to wysyłanie sygnału o jego aktywności w sieci przez urządzenie bezprzewodowe. Możliwe ustawienie to wartość pomiędzy 20 a 1000 milisekund. Domyślny czas pomiędzy sygnałami identyfikacji to 100 milisekund.

Data Beacon Rate (DTIM) - Częstotliwość pakietów DTIM to odstęp czasu, w którym pakiety DTIM są rozsyłane do komputerów klienckich w sieci. DTIM (Delivery Traffic Indication Message - Informacja o zaistnieniu ruchu). DTIM to wiadomość rozsyłana do komputerów klienckich, dla których uaktywniono obsługę zarządzania energią, informująca je, że pojawiły się dane, które mają zostać do nich przesłane i że w związku z tym muszą przejść w tryb aktywności, aby je otrzymać. Mniejsza wartość DTIM oznacza, że komputery klienckie nie mogą zbyt długo pracować w trybie oszczędzania energii.

Wyższa wartość oznacza, że mogą przejść w tryb oszczędzania energii, ale równocześnie muszą dłużej pracować w trybie aktywności, ponieważ przesyłanych będzie więcej danych.

Fragment Threshold – (256-2346) - Próg fragmentacji określa maksymalny poziom osiągany przez urządzenie podczas przesyłania informacji, zanim pakiety zostaną podzielone na mniejsze fragmenty. Problemy podczas wysyłania informacji pojawiają się, gdy w sieci transmitowany jest inny ruch i transmisje danych kolidują ze sobą. Dzieląc informacje na fragmenty możemy zapobiec temu zjawisku. Im niższa wartość, tym mniejszy musi być pakiet zanim zostanie podzielony na fragmenty. Wartość domyślna to 2346, wtedy fragmentacja jest całkowicie wyłączona. Zalecane jest pozostawienie tej opcji w postaci domyślnej.

RTS Threshold - (1-2347) - Parametr ustalający górny próg, przy którym będą wysyłane pakiety RTS (Request To Send) używane w celu unikania kolizji danych w sieciach bezprzewodowych. Ustawienie niskiej wartości parametru powoduje, że częściej będą wysyłane pakiety RTS zajmując więcej dostępnego pasma, co widocznie zmniejszy wydajność sieci. Jednakże szybsze systemy mogą odbierać częściej pakiety RTS z interfejsu lub kolizji. Ta wartość powinna pozostać w ustawieniu standardowym 2347.

TX Power - Określ moc sygnału bezprzewodowego emitowanego przez urządzenie. Gdy na danym obszarze znajdują się inne sieci bezprzewodowe i sygnały mogą zachodzić na siebie można obniżyć poziom mocy sygnału, aby zredukować zakłócenia.

Short Preamble – Krótka sekwencja wstępna.

Short Slot - Pracująca w technologii krótkich szczelin czasowych, zdefiniowana w standardzie 802.11g.

Tx Burst - Włączenie lub wyłączenie trybu przyśpieszenia ramek. Tryb ten może nie być kompatybilny ze wszystkimi urządzeniami sieciowymi.

Pkt_Aggregate - Pkt_Aggregate może łączyć wiele pakietów danych na rzecz poprawy efektywności nadawania.

Country Code - Wybieramy kraj, w którym działa nasze urządzenie, by udostępnić pule kanałów radiowych właściwych dla danego państwa.

WMM Capable - Funkcja umożliwiająca działanie mechanizmu Quality of Service (QoS), wykorzystywanego przez aplikacje multimedialne, takie jak Voice-over-IP (VoIP) oraz wideo. Mechanizm ten umożliwia pakietom sieciowym tych aplikacji uzyskanie priorytetu większego niż zwykłe pakiety sieciowe.

APSD Capable - Parametr APSD (Automatic Power Save Delivery) zarządza użyciem akumulatorów urządzeń zasilanych bateryjnie, aby w pewnych warunkach maksymalnie wydłużyć czas ich pracy. Funkcja APSD umożliwia stosowanie dłuższych czasów pomiędzy sygnałami identyfikacyjnymi, dopóki nie zostanie uruchomiona aplikacja wymagająca krótkiego czasu wymiany pakietów, np. protokół Voice Over Internet Protocol (VoIP) jest aplikacją wymagającą krótkiego czasu wymiany pakietów. Funkcja APSD może wydłużyć czas korzystania z komunikacji radiowej i czas pracy akumulatora tylko wtedy, gdy klient bezprzewodowy również obsługuje tę funkcję.

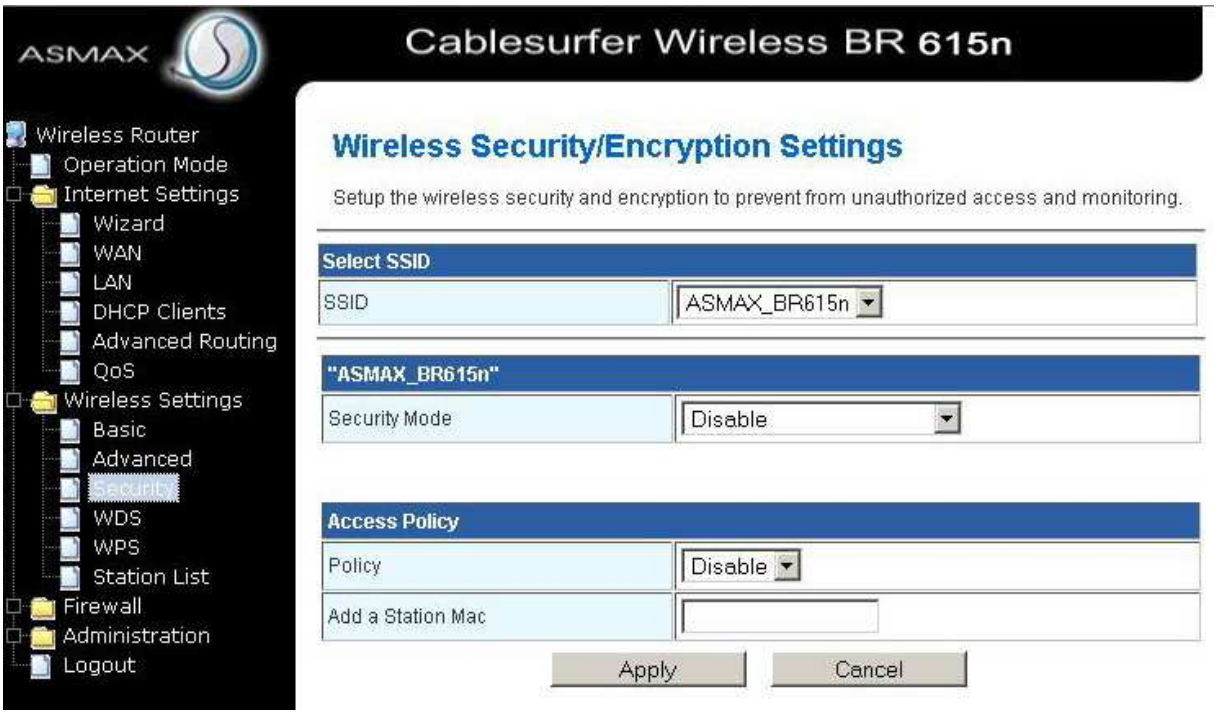
DLS Capable – Włączenie „Enable” lub wyłączenie „Disable” DLS.

WMM Parameters – Kliknij przycisk, aby wyświetlić stronę konfiguracji parametrów WMM.

Multicast-to-Unicast Converter – Włącz „Enable” lub wyłącz „Disable” Multicast-to-Unicast. Po włączeniu tej funkcji, jakości transmisji bezprzewodowej strumienia multicast można poprawić.
Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

Wireless Security - Encryption Settings

Ta zakładka pozwala skonfigurować funkcje bezpieczeństwa sieci bezprzewodowej. Możesz ustawić metodę identyfikacji sieci, wybierając szyfrowanie danych, wyszczególnić, czy klucz sieci jest wymagany, aby podłączyć się do sieci bezprzewodowej i wybrać siłę szyfrowania. Asmax BR615N posiada wsparcie dla: 802.1X, WPA/WPA2 (Wi-Fi Protected Access). Najnowsze standardy bezpieczeństwa sieci bezprzewodowej, które w połączeniu z wirtualnymi punktami dostępowymi, pozwalają na uruchomienie czterech wirtualnych punktów dostępowych. Każdy z takich punktów dostępu może mieć inne ustawienia bezpieczeństwa, autoryzacji użytkowników, na jednym można uruchomić izolowanie od siebie klientów, a na kolejnym ukryć wyświetlanie SSID i wiele innych kombinacji, które dodatkowo w połączeniu z zewnętrznym serwerem RADIUS tworzą bardzo dobrze zabezpieczoną sieć bezprzewodową. Ale Asmax BR615N wspiera także starsze metody zabezpieczenia przesyłanych danych w sieci bezprzewodowej, jak WEP (Wired Equivalent Privacy), WPA, co pozwala bez żadnych problemów bezpiecznie łączyć się użytkownikom, którzy posiadają starsze urządzenia klienckie. Domyślnie funkcje zabezpieczenia sieci są wyłączone i dostęp do punktu dostępowego jest otwarty. Przed ustaleniem polityki bezpieczeństwa w Twojej sieci rozważ jej wielkość, położenie, posiadany sprzęt kliencki i wtedy określ metodę zabezpieczenia sieci bezprzewodowej. Poniżej przedstawiono opis opcji konfiguracyjnych.



Parametry:

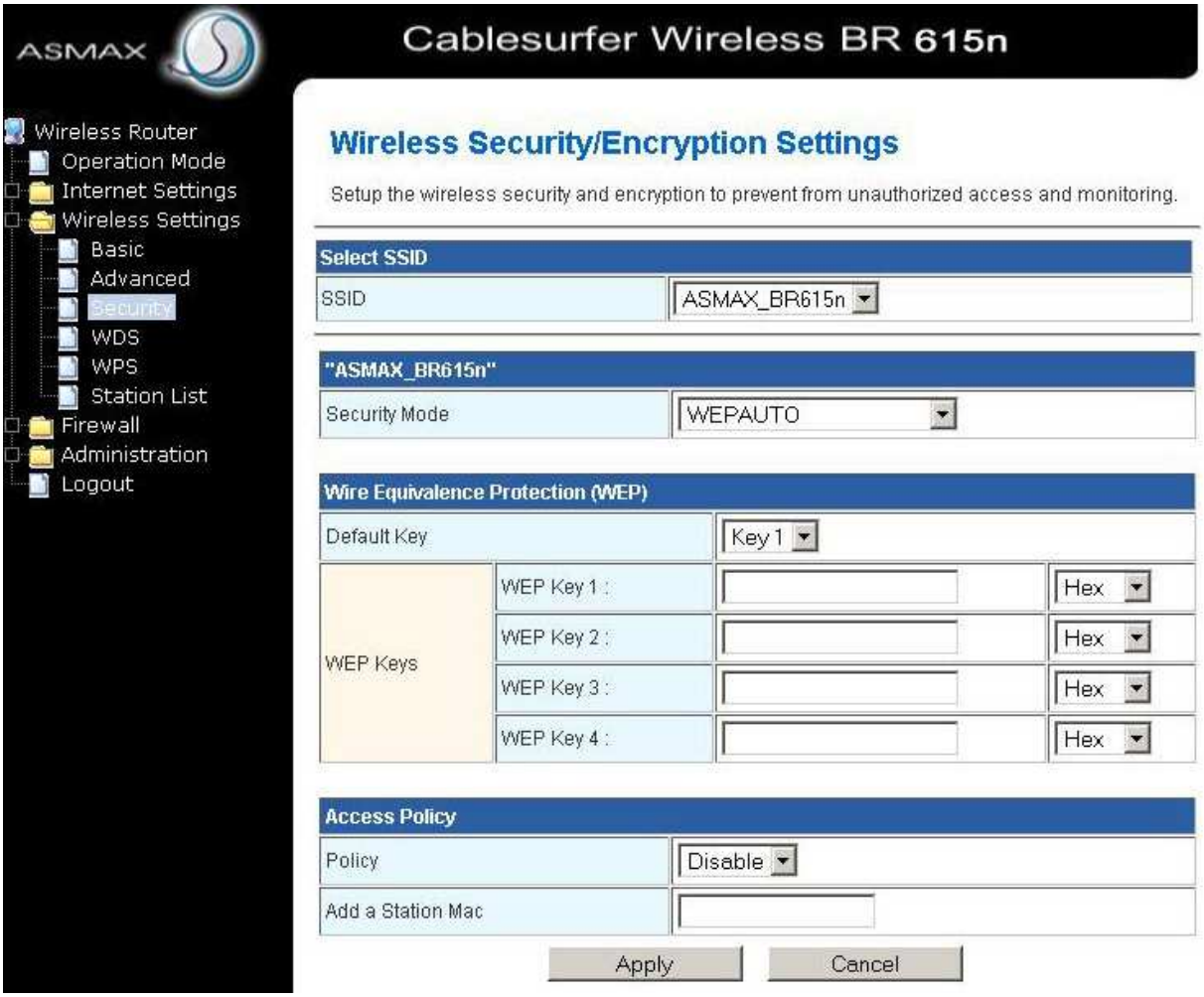
Select SSID – Wybierz SSID sieci, którą chcesz zabezpieczyć.

Security Mode – Wybierz metodę zabezpieczenia, zalecana to WPA2PSK/AES.

Access Policy – Dodatkowa kontrola poza szyfrowaniem, po włączeniu „Enable" tylko zdefiniowane adresy MAC będą mogły uzyskać połączenie z naszą siecią bezprzewodową.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

WEP (Wired Equivalent Privacy) to podstawowa metoda szyfrowania, która jest zazwyczaj wykorzystywana do szyfrowania danych w sieciach bezprzewodowych przy użyciu szeregu kluczy cyfrowych (o długości 64 lub 128 bitów). Zastosowanie tych samych kluczy we wszystkich urządzeniach podłączonych do sieci bezprzewodowej uniemożliwia monitorowanie transmisji lub wykorzystywanie zasobów sieci przez urządzenia nieautoryzowane. Po wybraniu opcji „WEPAUTO" zostanie wyświetlone poniższe okno.



Parametry:

Security Mode - W tym polu znajduje się menu rozwijane służące do wybierania odpowiednich trybów szyfrowania.

Default Key – W tym miejscu określamy, który z czterech skonfigurowanych kluczy ma być aktualnie dostępny.

WEP Keys 1–4 - Pola te służą do ustawiania kluczy szyfrowania WEP i wyboru formatu (ASCII lub Hex). Można w nich wpisać kod w formacie ASCII (złożony z 5 lub 13 znaków ASCII, przy czym niedozwolone jest stosowanie znaku „/") lub 10-/26-znakową wartość szesnastkową.

Access Policy – Dodatkowa kontrola poza szyfrowaniem, po włączeniu „Enable" tylko zdefiniowane adresy MAC będą mogły uzyskać połączenie z naszą siecią bezprzewodową.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

WPA (WiFi Protected Access) oraz WPA2 jest zaawansowanym mechanizmem zabezpieczania sieci bezprzewodowej opartym na współdzielonym kluczu (Pre-shared key) lub autentykacji za pomocą serwera RADIUS (802.1x). Tryb „WPA 2 Mixed" umożliwia wspólne użytkowanie sieci o tym samym SSID dla użytkowników zarówno WPA, jak też WPA2. AES WPA2 korzysta z 256-bitowego szyfrowania danych, co zapewnia bardzo wysoki poziom bezpieczeństwa przesyłu danych przez sieć bezprzewodową. WPA/WPA2 pozwala zastosować bardziej zaawansowane typy szyfrowania, takie jak TKIP (Temporal Key Integrity Protocol) i AES (Advanced Encryption Standard) oraz umożliwia dynamiczną zmianę kluczy we wszystkich autoryzowanych urządzeniach bezprzewodowych.

Parametry:

WPA Algorithms - W tym polu można wybrać algorytm TKIP (Temporal Key Integrity Protocol) lub AES (Advanced Encryption Standard). Domyślny algorytm dla WPA to TKIP.

Pass Phrase - W tym miejscu należy wpisać klucz szyfrowania złożony z 8–63 znaków ASCII.

Key Renewal Interwal - W tym miejscu należy wskazać, jak często ma być odnawiany klucz.

Access Policy – Dodatkowa kontrola poza szyfrowaniem, po włączeniu „Enable" tylko zdefiniowane adresy MAC będą mogły uzyskać połączenie z naszą siecią bezprzewodową.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

WPA2-PSK

Parametry:

WPA Algorithms - W tym polu można wybrać algorytm TKIP (Temporal Key Integrity Protocol) lub AES (Advanced Encryption Standard). Domyślny algorytm dla WPA2 to AES.

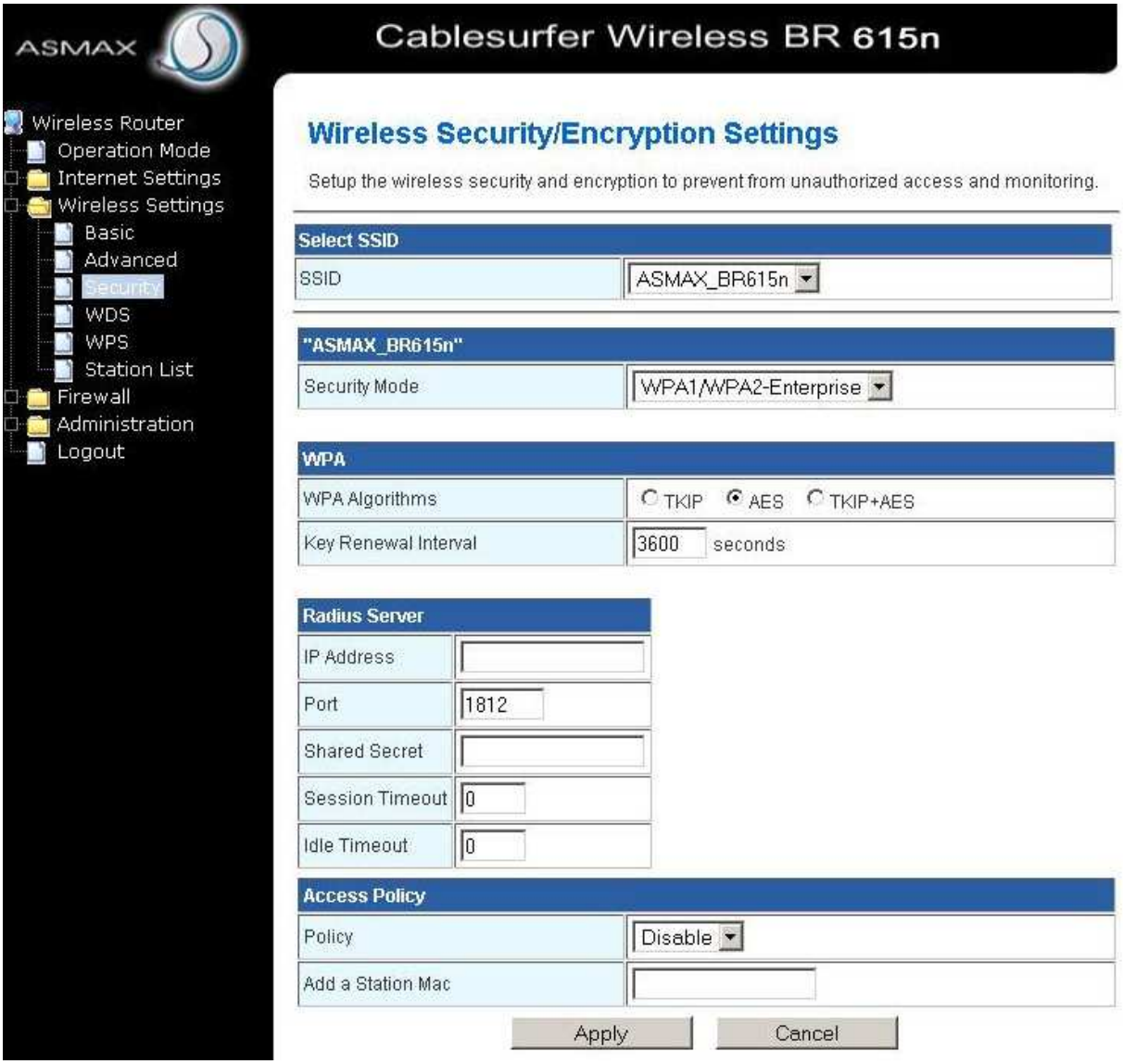
Pass Phrase - W tym miejscu należy wpisać klucz szyfrowania złożony z 8–63 znaków ASCII.

Key Renewal Interwal - W tym miejscu należy wskazać, jak często ma być odnawiany klucz.

Access Policy – Dodatkowa kontrola poza szyfrowaniem, po włączeniu „Enable" tylko zdefiniowane adresy MAC będą mogły uzyskać połączenie z naszą siecią bezprzewodową.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

WPA1/WPA2-Enterprise



802.1X jest metodą autoryzacji użytkownika z wykorzystaniem serwera RADIUS.

RADIUS (Remote Access Dial-In User Service) jest protokołem klient - serwer typu AAA (Authorization, Authentication, Accounting), używanym do logowania klientów dial-up (autoryzacja, autentykacja, rozliczanie) do serwera dostępu do sieci (Network Access Server). Połączenie składa się z trzech faz:

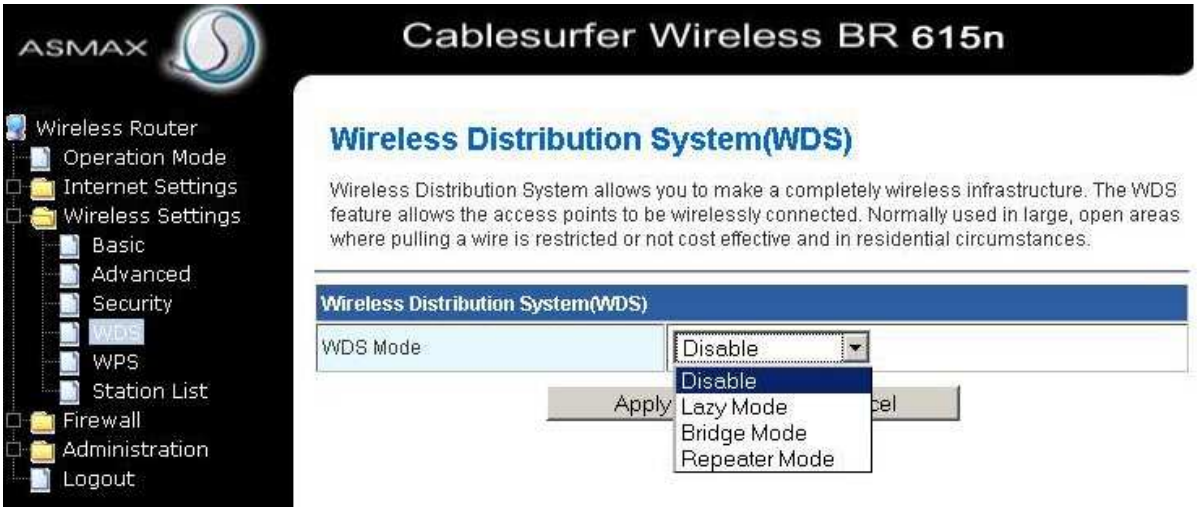
Authentication - weryfikacja nazwy użytkownika i hasła w lokalnej bazie danych. Po pomyślnej weryfikacji następuje proces autoryzacji.

Authorization - określa czy żądanie dostępu do zasobów może zostać zrealizowane. Klient Dial-up otrzymuje adres IP.

Accounting - gromadzenie informacji o połączeniu (billing, statystyki).

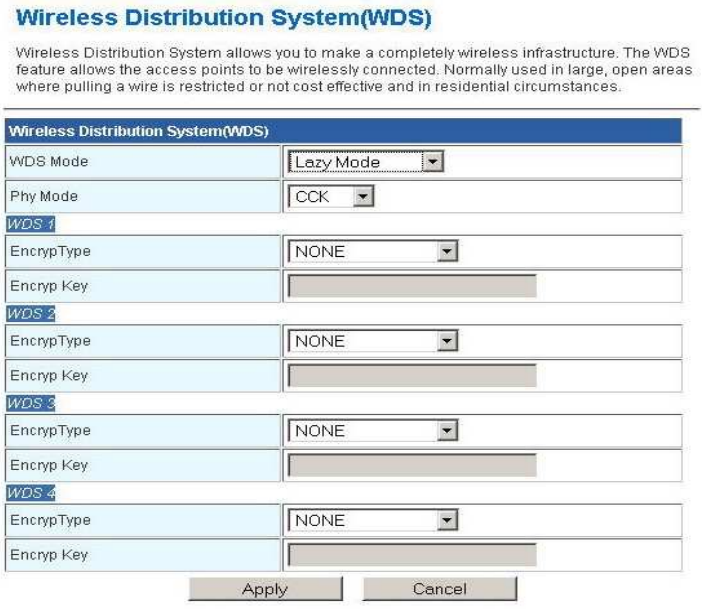
Wireless Distribution System (WDS)

Funkcja „Wireless Distributed System” umożliwia ustawienie parametrów wbudowanego w router modułu bezprzewodowego w trybie WDS. Dla urządzeń pracujących w trybie bridge, WDS umożliwia komunikację pomiędzy wszystkimi urządzeniami bezprzewodowymi (klienci) poprzez interfejsy bezprzewodowe tych dwóch urządzeń. W tym celu należy ustawić ten sam kanał transmisji i zarejestrować adresy MAC przeciwnych stron. Jeśli są używane zabezpieczenia transmisji bezprzewodowej to ustawienia muszą być takie same na obu urządzeniach. bezprzewodowej. Asmax BR615N oferuje trzy tryby pracy: bierny „Lazy Mode”, most „Bridże Mode”, wzmacniacz „Repeater Mode”.

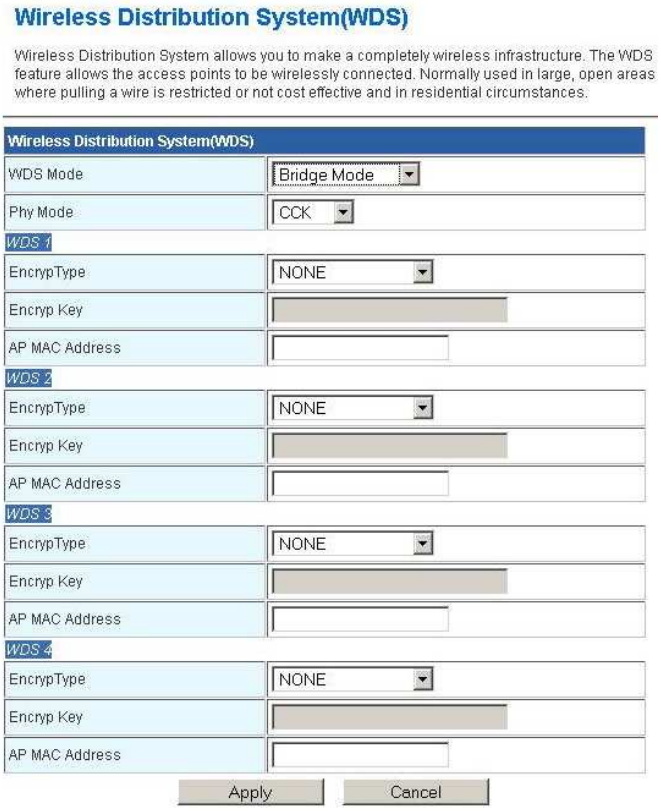


Parametry:

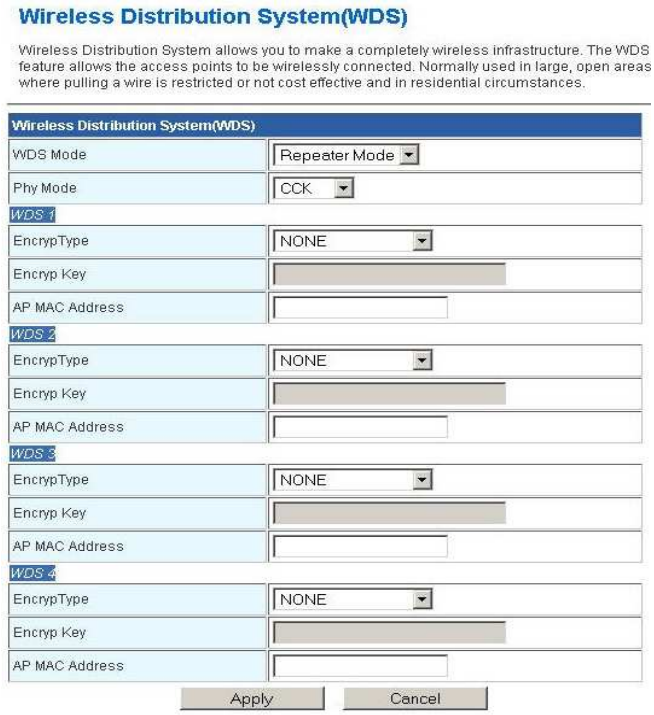
Lazy Mode - W przypadku trybu „Lazy Mode” ustawienia podłączone urządzenie może działać w trybie mostu (Bridge Mode) lub wzmacniacza (Repeter Mode), a nawiązanie połączenia wymaga podania identyfikatora BSSID routera.



Bridge Mode - W trybie mostu urządzenie może się komunikować tylko z innymi punktami dostępowymi WDS. W tym trybie konieczne jest dodanie adresu MAC podłączanego urządzenia do tabeli adresów MAC punktu dostępowego routera lub wybranie go z tabeli skanowania.



Repeater Mode – Tryb wzmacniacza umożliwia zwiększenie zasięgu transmisji radiowej w sieci bezprzewodowej. Wymaga to wzajemnego dodania adresów MAC punktów dostępowych do ich tabel adresów MAC, ręcznie lub przy użyciu funkcji skanowania.



Encrypt Type - W tym miejscu wybieramy szyfrowanie WEP, TKIP lub AES.

Encryp Key - W tym miejscu należy wpisać klucz szyfrowania na potrzeby urządzeń bezprzewodowych.

AP MAC Address - W tym miejscu należy wpisać adres MAC drugiego (współpracującego) routera bezprzewodowego, z którym ma zostać nawiązane połączenie.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień. Należy pamiętać, aby konfiguracja w obu routerach bezprzewodowych przepustowości, numeru kanału i ustawień zabezpieczeń była taka sama.

Wi-Fi Protected Setup

Funkcja „Wi-Fi Protected Setting (WPS)" zdecydowanie przyspiesza tworzenie szyfrowanych połączeń między naszym urządzeniem a klientami sieci bezprzewodowej, który posiada sprzęt posiadający funkcje WPS. Aby skonfigurować funkcję „Wi-Fi Protected Setting" użytkownik podaje tylko kod PIN lub naciska przycisk WPS na tylnim panelu urządzenia bez konieczności ręcznego wybierania metod szyfrowania i tajnych kluczy. Aby wyświetlić poniższy rysunek, należy zaznaczyć „Enable" w polu WPS.

Parametry:

WPS - Opcja służąca do włączania „Enable” i wyłączania „Disable” funkcji WPS w routerze. Domyślnie opcja jest wyłączona.

WPS Summary - W tabelce widoczne są informacje o działaniu funkcji WPS, w tym o trybie autoryzacji, typie szyfrowania i kluczu domyślnym.

WPS Current Statu - Wartość „Idle” oznacza, że funkcja WPS znajduje się w stanie bezczynności. Wartość „Start MSC process” oznacza, że proces został rozpoczęty i trwa oczekiwanie na połączenie. Wartość „Configured” oznacza, że negocjowanie między serwerem a klientami zakończyły się pomyślnie.

WPS Configured - Wartość „Yes” oznacza, że funkcja WPS jest włączona i aktywna. Wartość „No” oznacza, że funkcja nie jest używana. Zwykle w przypadku włączenia zabezpieczeń punktu dostępowego wyświetlana jest wartość „No”.

WPS SSID - W tym miejscu widoczny jest główny identyfikator SSID ustawiony w ramach funkcji WPS.

WPS Auth. Mode - W tym miejscu znajduje się informacja o trybie autoryzacji stosowanym w ramach funkcji WPS. Zazwyczaj jest to tryb osobisty WPA/WPA2.

WPS Encrypt Type - W tym miejscu znajdują się informacja o typie szyfrowania stosowanym w ramach funkcji WPS. Zazwyczaj jest to AES/TKIP.

WPS Key - W tym miejscu wyświetlany jest obowiązujący klucz generowany automatycznie przez punkt dostępowy.

AP PIN - W tym miejscu znajduje się stosowany domyślnie kod PIN. Przyciskiem „Generate” możemy wygenerować nowy kod PIN.

Reset OOB - Kliknięcie tego przycisku powoduje przejście klienta funkcji WPS w stan bezczynności i wyłączenie kontrolki WPS. Punkt dostępowy nie będzie reagować na żądania klientów funkcji WPS, a ponadto zostanie przywrócony tryb zabezpieczeń WPA.

WPS Progress/WPS mode – Posiadamy do wyboru dwie opcje, konfiguracja za pomocą przycisku - PBC i za pomocą kodu PIN.

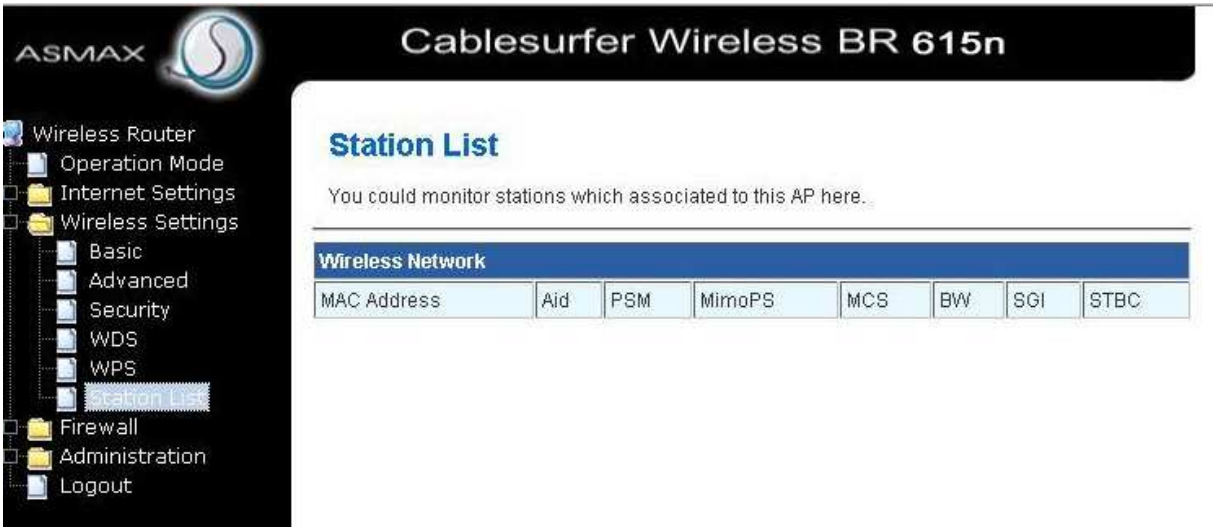
PBC - Aby skorzystać z tej opcji, należy wybrać ustawienie PBC lub nacisnąć i przytrzymać przez sekundę przycisk WPS na tylnim panelu urządzenia. Po włączeniu funkcji WPS kontrolka WPS miga przez około 2 minuty. W tym czasie należy włączyć drugie urządzenie, aby rozpocząć negocjowanie połączenia WPS w trybie PBC. Po dwóch minutach kontrolka WPS gaśnie, co oznacza zakończenie nawiązywania połączenia WPS. Aby dodać kolejne urządzenia klienckie, należy powtórzyć powyższe czynności.

PIN - W przypadku wybrania tej opcji należy wpisać w pustym polu kod PIN dla klienta bezprzewodowego, a następnie skorzystać z tego samego kodu w urządzeniu klienckim zgodnym z funkcją WPS.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

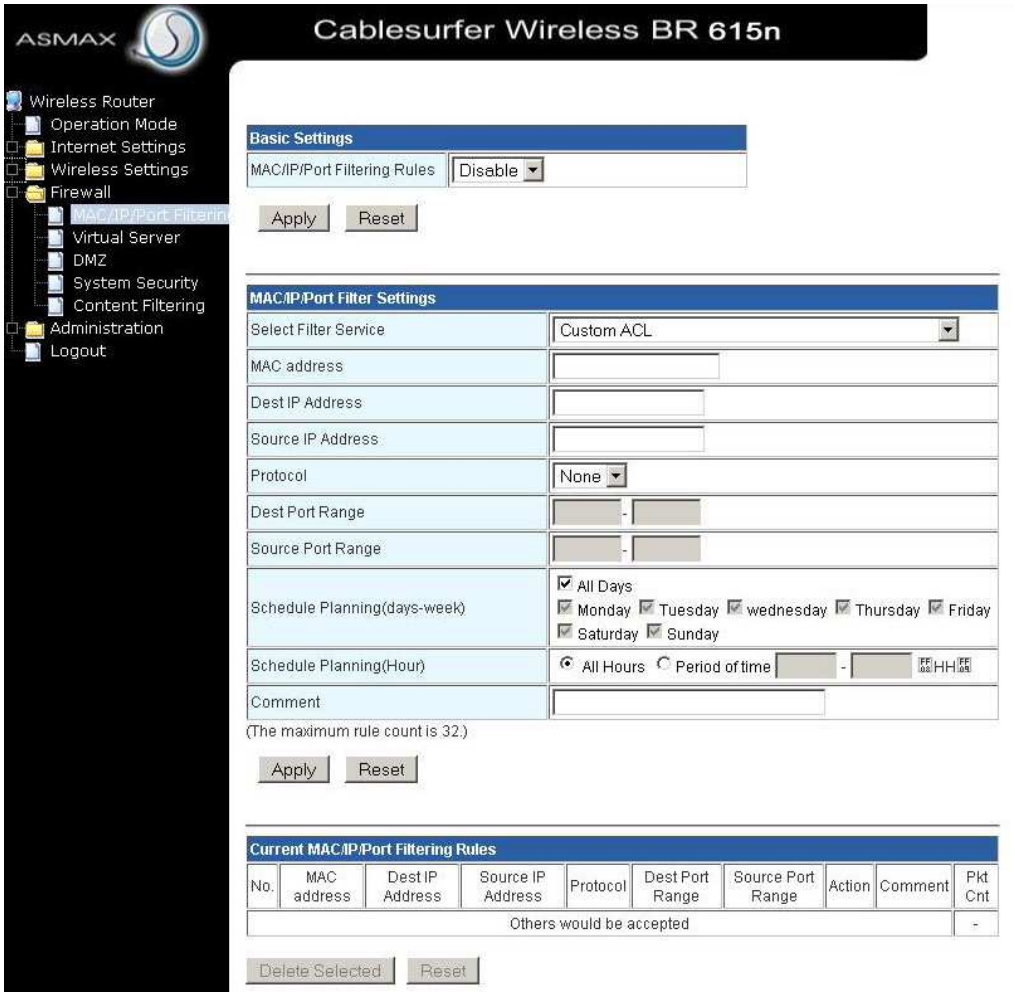
Station List

W poniższej tabeli widzimy podłączone bezprzewodowo stacje klienckie w tym informacje. takie jak adres MAC klienta, prędkość połączenia.

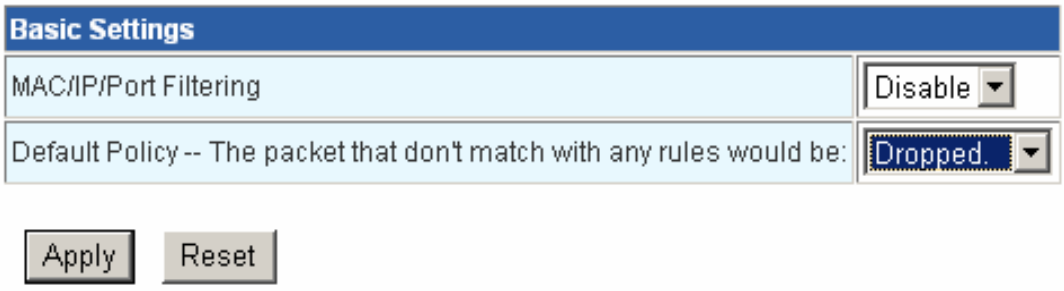


Firewall/ MAC/IP/Port Filtering Settings

Router Asmax BR615N posiada rozbudowaną zaporę sieciową, która polega na kontroli parametrów połączeń, skutecznie blokując wszelkie ataki z Internetu oraz od strony sieci lokalnej. Dodatkowo router umożliwia swobodną konfigurację klientów w celu umieszczenia na nich różnego rodzaju serwerów lub wystawnie jednego z komputerów do specjalnej strefy DMZ, gdzie będzie on całkowicie widoczny od strony Internetu. Możemy ograniczyć dostęp użytkownikom sieci LAN na podstawie ich adresów IP, numerów portów, adresów MAC lub nazw URL.



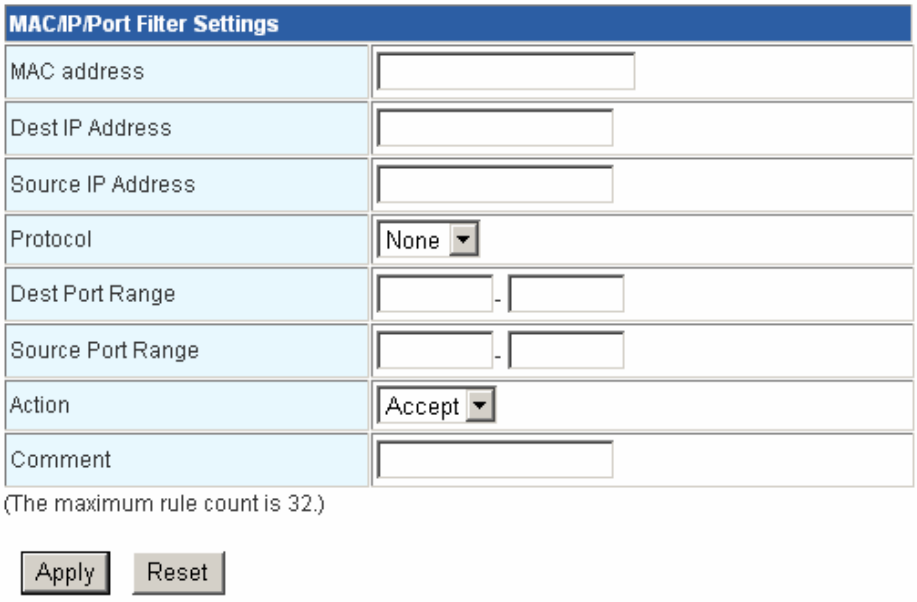
Basic Settings



MAC/IP/Port Filtering – Włączenie „Enable" lub wyłączenie „Disable" funkcji filtracji. Domyślnie filtracja jest wyłączona.

Default Policy – Domyślnie urządzenie będzie akceptować wszystkie pakiety, które nie pasują do żadnej reguły.

MAC/IP/Port Filter Settings



Parametry:

MAC Filter – Funkcja „MAC Filter" może zablokować komputerom w sieci lokalnej dostęp do Internetu.

IP Filter – Funkcja **„**Filtr IP" można zablokować użytkownikowi sieci dostęp do Internetu.

Port Filter – Funkcja „Filtr Port" może blokować niektóre porty wybranych adresów IP lub ruchu na wszystkich portach.

Gdy pakiety danych są zgodne z opisanymi parametrami, pakiety danych będą odrzucane.

MAC Address – Adresy MAC zawarte w pakietach danych. Można podać docelowy adres MAC lub źródłowy.

Dest IP Address – Docelowy adres IP.

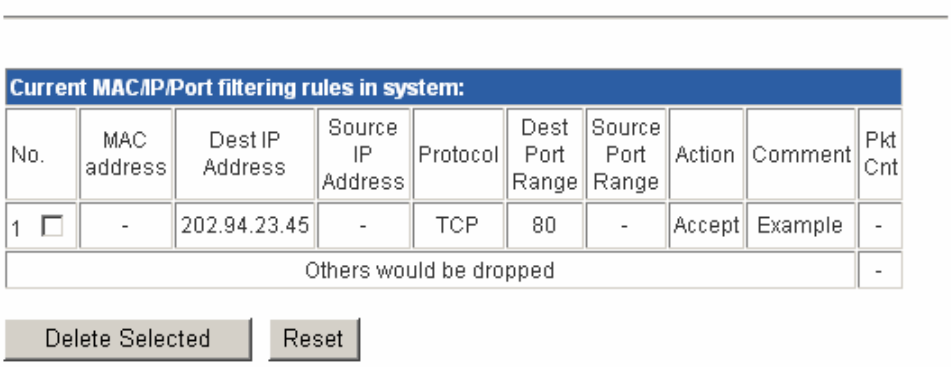
Source IP Address – Źródłowy adres IP.

Protocol - Typów pakietów protokołu danych, TCP, UDP i ICMP.

Dest Port Range – Docelowy zakres portów z zakresu od 1 do 65535.

Source Port Range – Źródłowy zakres portów z zakresu od 1 do 65535.

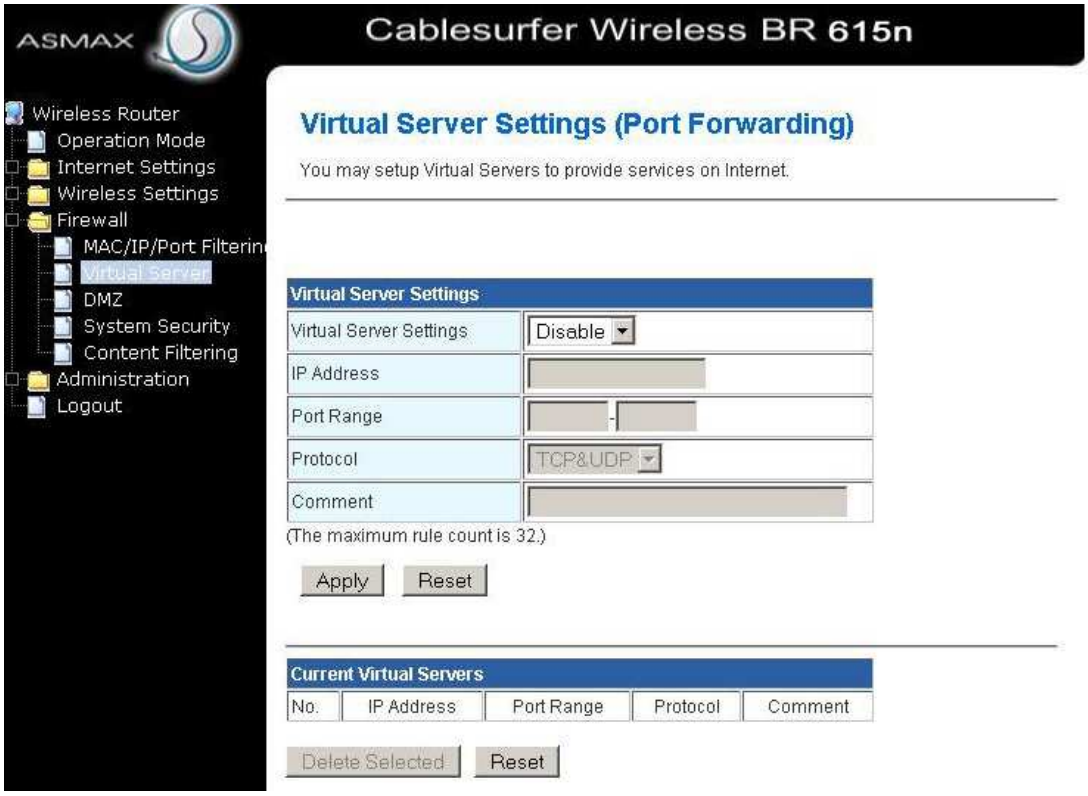
Comment – Komentarz do reguły.



Powyższy rysunek pokazuje obecne reguły filtrów w urządzeniu.

Virtual Server Settings (Port Forwarding)

Funkcja „Port Forwarding” umożliwia mapowanie zewnętrznych portów routera na określony host w sieci LAN. Domyślnie na routerze działa translacja adresów sieciowych NAT (wszystkie porty TCP i UDP od strony WAN urządzenia są zamknięte), przez co komputery podpięte do routera w Internecie będą widziane jako jedna maszyna. Normanie użytkownicy z Internetu nie mogą dostać się do Twojej sieci będącej za routerem. Ale możemy ustawić, aby taki dostęp był możliwy, np. w przypadku, gdy na jakimś komputerze w sieci mamy uruchomiony serwer WWW, FTP lub jakiejś gry i chcemy, aby ktoś z poza naszej sieci lokalnej miał do nich dostęp. Aby taki dostęp był możliwy musimy przekierować odpowiednie porty w routerze. Po jego skonfigurowaniu, jeśli router otrzyma prośbę od użytkownika z Internetu i zidentyfikuje daną usługę, po czym połączy ją z numerem portu, na którym ona działa, wtedy uzyska do niej dostęp.



Parametry:

Virtual Server Settings – Wybieramy, czy funkcja ma być włączona „Enable”, czy wyłączona „Disable”.

IP Address – Adres IP komputera/urządzenia w sieci lokalnej, który będzie miał przekierowany port lub zakres portów.

Protocol – Wybieramy protokół, jaki będziemy przekierowywać (TCP, UDP albo oba TCP&UDP).

Port Range – Wpisz zakres portów do przekierowania. Aby podać jeden numer portu wpisz ten sam numer w obu polach.

Comment – Komentarz do reguły przekierowania.

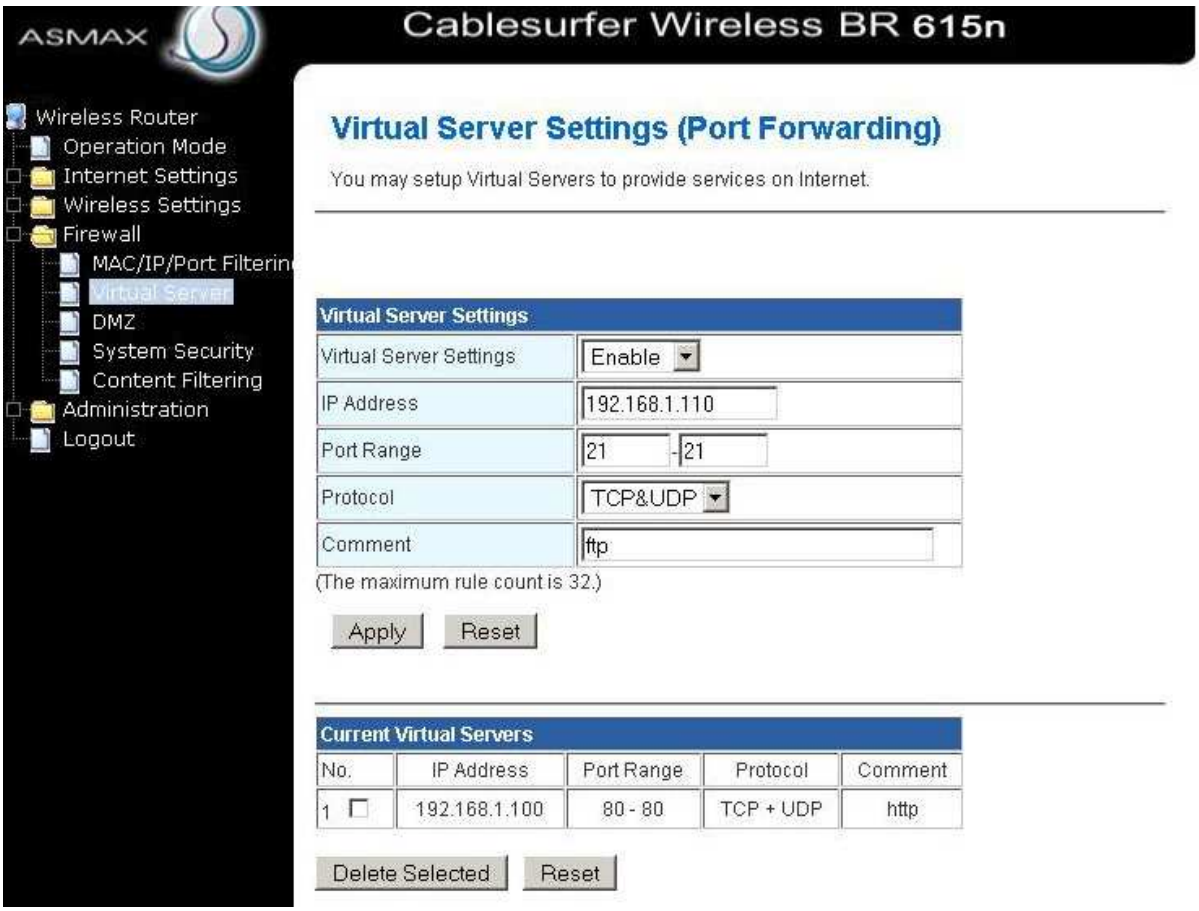
Najczęściej funkcję „Port Forwarding" wykorzystuje się celem udostępnienia lokalnego serwera WWW, FTP, gry użytkownikom Internetu. Również, aby móc korzystać z programów p2p (peer-to-peer) z pełną przepustowością (High ID) lub aplikacji multimedialnych należy przekierować określony port lub porty.

UWAGA! Dany port można przekierować tylko dla jednego adresu IP. Jeżeli zostanie przekierowany port TCP 80 dla adresu 192.168.1.200 to nie można przekierować portu 80 dla żadnego innego adresu IP w sieci LAN.

Aby udostępnić port 88 użytkownikowi 192.168.1.200, zaznacz opcję „Enable" w polu „Virtual Server Settings", wpisz w polu „IP Address" adres 192.168.1.200, pole „Protocol", pozostaw na „TCP&UDP" w polu „Port Range" wpisz wartość 88 lub zakres 88 – 88 i kliknij „Apply". Teraz wszystkie zapytania przychodzące z Internetu do routera na port 88 będą kierowane na port 88 do użytkownika 192.168.1.200.

Przykład: Udostępnienie serwera WWW oraz ftp znajdującego się w sieci LAN. Na komputerze o adresie 192.168.1.100 jest zainstalowany serwer WWW. Na komputerze o adresie 192.168.1.110 jest zainstalowany serwer FTP. Router otrzymał od ISP od strony WAN adres IP: 88.80.100.254

Należy za pomocą funkcji „*Virtual Server Settings*" dodać następujące dwa wpisy:



Po zastosowaniu zmian i ponownym uruchomieniu urządzenia serwery są widoczne pod następującymi adresami:

Dla użytkowników sieci LAN:

ftp – 192.168.1.110, np. ftp://192.168.1.110

www – 192.168.1.100, np. http://192.168.1.100

Dla użytkowników z Internetu:

ftp - 88.80.100.254, np. ftp:// 88.80.100.254

www - 88.80.100.254, np. http:// 88.80.100.254

* przy wykorzystaniu funkcji DDNS:

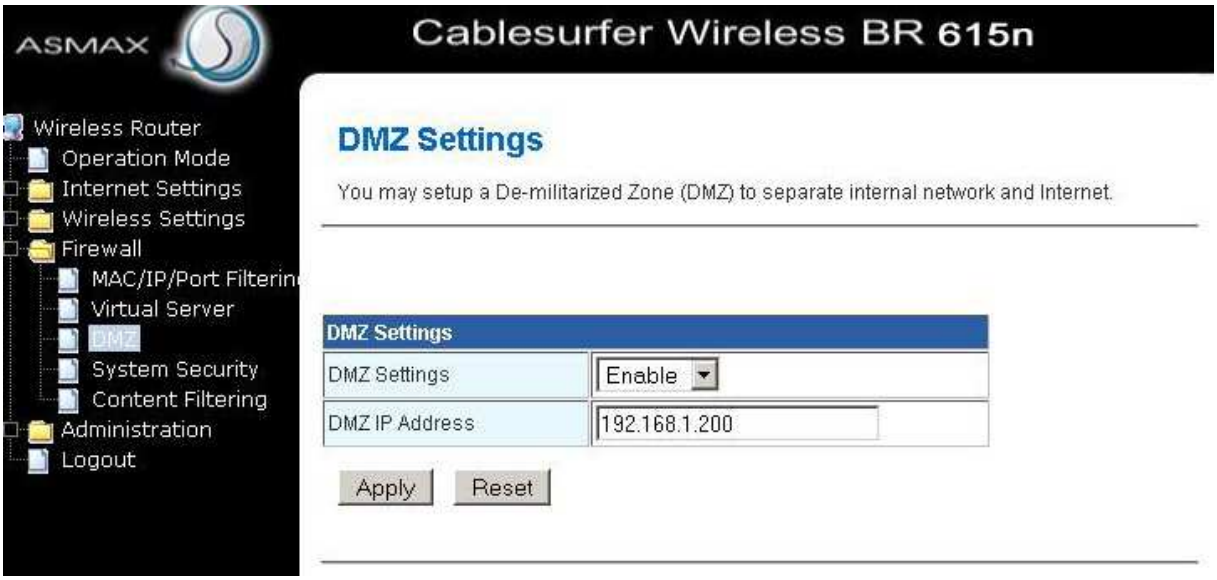
ftp://uzytkownik.dyndns.org i http://uzytkownik.dyndns.org

Sugestia: Użyj mechanizmu DDNS, aby w przypadku dynamicznie przyznawanego adresu publicznego mieć zawsze dostęp do uruchomionych serwerów i usług (opis funkcji w rozdziale: DDNS).

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

DMZ Settings

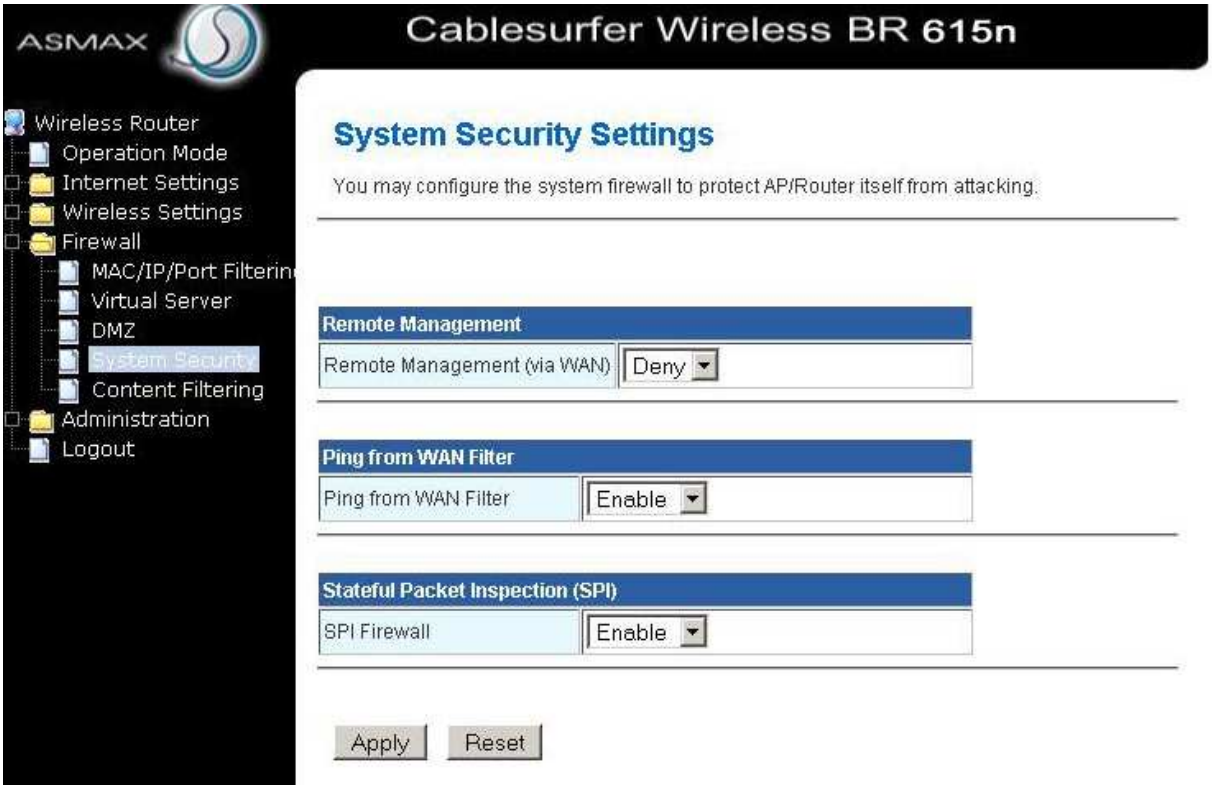
Funkcja DMZ umożliwia zarządzanie strefą zdemilitaryzowaną. DMZ (Demilitarized Zone) jest obszarem pomiędzy chronioną za pomocą NAT siecią LAN a siecią WAN. Umożliwia ona wystawienie hosta z sieci LAN do sieci WAN pod adresem interfejsu WAN routera. Host będzie widoczny w sieci LAN pod jego adresem IP w sieci LAN, natomiast w sieci WAN pod adresem WAN routera. W praktyce oznacza to przekierowanie całego zakresu portów (1 - 65535). Aby uaktywnić funkcję w polu „DMZ IP Address" proszę podać adres IP komputera w sieci, który ma być widoczny od strony Internetu. Wcześniej uaktywnij funkcję klikając w polu „DMZ Settings" → „Enable".



Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

System Security Settings

Zakładka ta pozwala skonfigurować poziom bezpieczeństwa i możliwość zdalnego dostępu do urządzenia.



Parametry:

Remote management(Via WAN) – Włącz „Allow" lub wyłącz „Deny" zdalne zarządzanie. W przypadku wyboru opcji „Allow" użytkownicy w innych regionach świata, mający dostęp do Internetu mogą konfigurować urządzenie (Bardzo istotne jest, aby zmienić domyślne hasło i nazwę użytkownika na trudne do odgadnięcia).

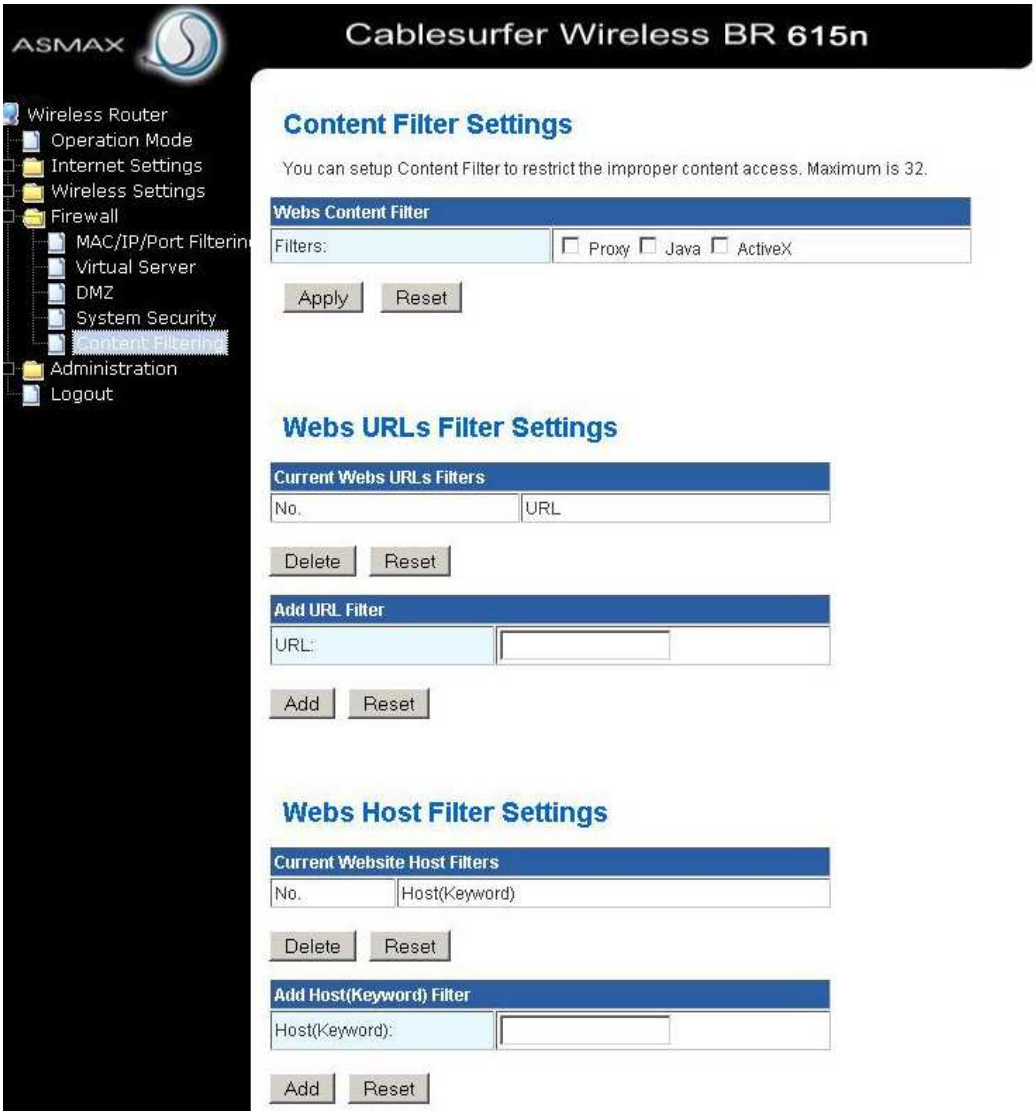
WAN Ping Filter – Włącz „Enable" lub wyłącz „Disable" możliwość „pingowania" naszego urządzenia od strony interfejsu WAN.

SPI Firewall - Włącza „Enable" lub wyłącza „Disable" funkcję zapory/firewalla SPI (Stateful Packet Inspection). Kontroli są poddawane wszystkie połączenia przechodzące przez interfejs zapory. Kiedy pakiet IP dotrze do zapory z Internetu, firewall sprawdza pakiet, aby zobaczyć, jakie połączenia zostały otwarte od wewnątrz sieci do Internetu. Jeśli jest otwarte połączenie dotyczące danego pakietu, który został przysłany z Internetu to taki pakiet jest przepuszczany, inaczej przychodzący pakiet zostaje odrzucony. W porównaniu z NAT poziom bezpieczeństwa firewall SPI jest wyższy.

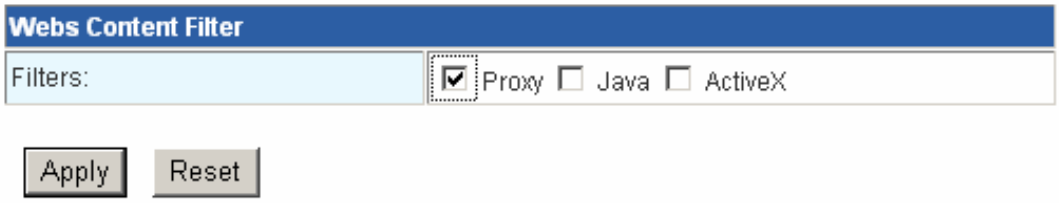
Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

Content Filter Settings

Filtr treści może blokować dostęp użytkownikowi sieci do pewnych witryn sieci Web w Internecie.



Webs Content Filter



Parametry:

Proxy - Do filtrowania stron proxy.

Java - Do filtrowania stron, które używają skryptu Java.

ActiveX – Do filtrowania stron zawierających ActiveX.

Current Webs URL Filters

Powyższy rysunek pokazuje, filtry URL już dodane.

Add a URL filter

URL: Wpisz adres URL, który musi być filtrowany.

Current Website Host Filters

Powyższy rysunek pokazuje już dodane strony do filtrowania.

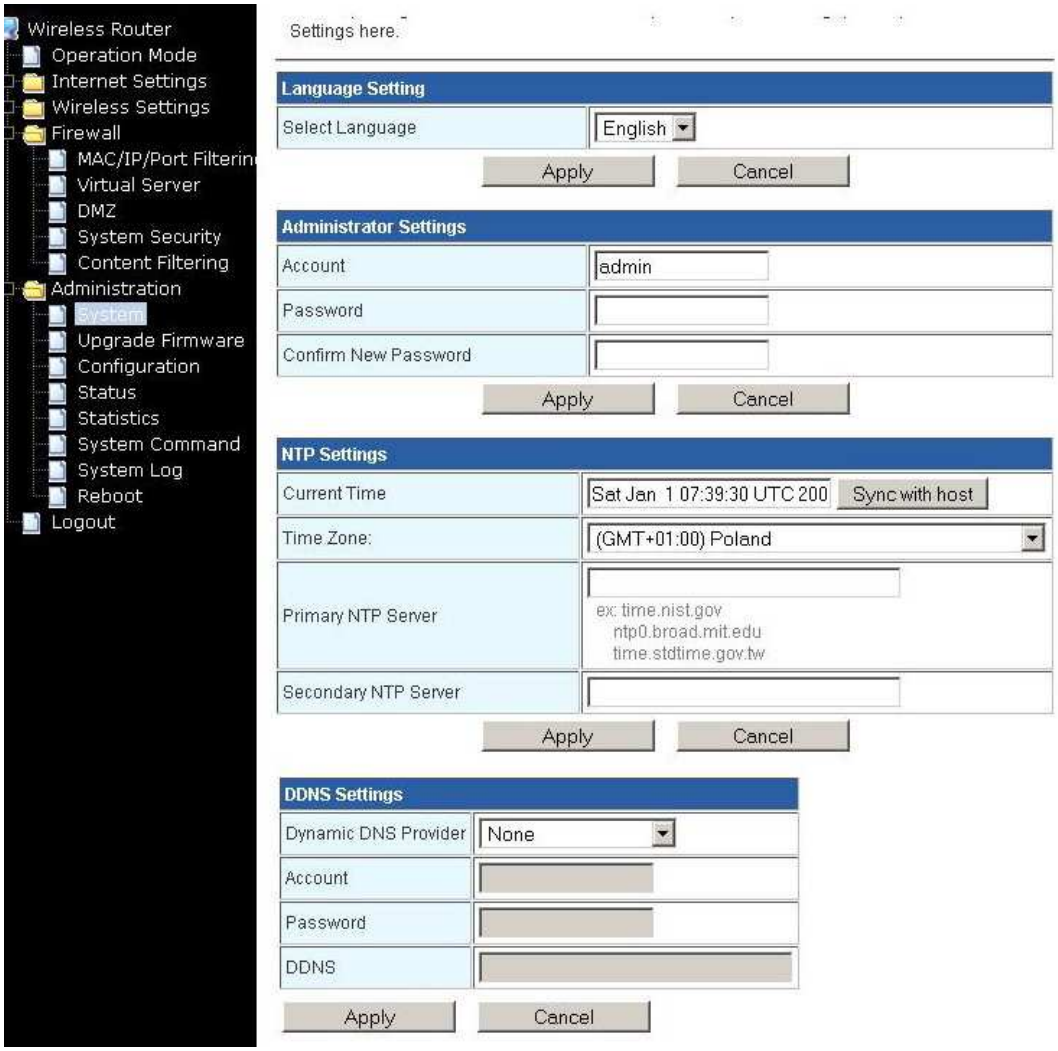
Add Host (słowo kluczowe)

Słowo kluczowe: Wpisz słowa kluczowe w pustym polu, podane słowa kluczowe będą filtrowane. Po zakończeniu wprowadzania ustawień, kliknij przycisk Dodaj, aby dodać nowy filtr przyjmującego.

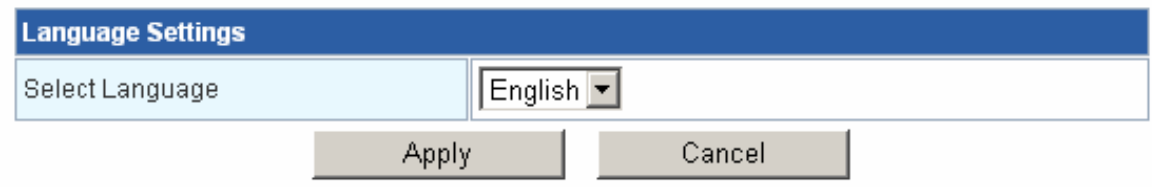
Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply”, aby zapisać wprowadzone ustawienia lub „Cancel”, aby zakończyć bez zapisywania ustawień.

System Management

Zakładka „System Management” odpowiedzialna jest za zarządzanie urządzeniem. Umożliwia prezentację jego statusu, konfigurację strefy czasowej, dynamicznego DNS, zmianę parametrów dostępu do strony konfiguracyjnej, aktualizację oprogramowania oraz zapisywanie konfiguracji urządzenia do pliku.



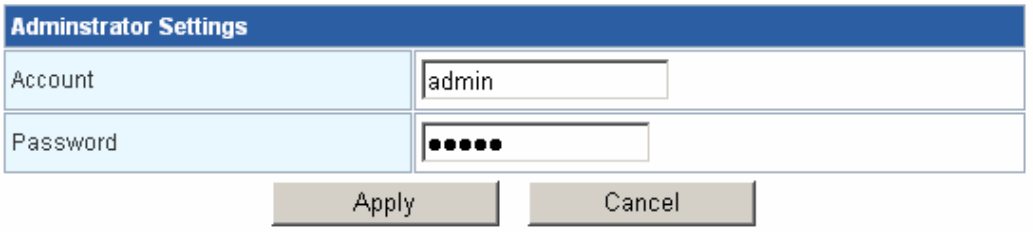
Language Settings



Wybór języka (Select Language) – aktualnie tylko język angielski.

Administrator Settings – zmiana loginu i hasła dostępowego

W tej części zakładki możemy zmienić domyślną nazwę użytkownika i domyślne hasło (admin/admin) na inne, jest zdecydowanie zalecane. Pozostawiając domyślne hasło narażamy się na niebezpieczeństwo uszkodzenia urządzenia lub inną szkodę.



Parametry:

Account – Nazwa użytkownika urządzenia, domyślnie: admin.

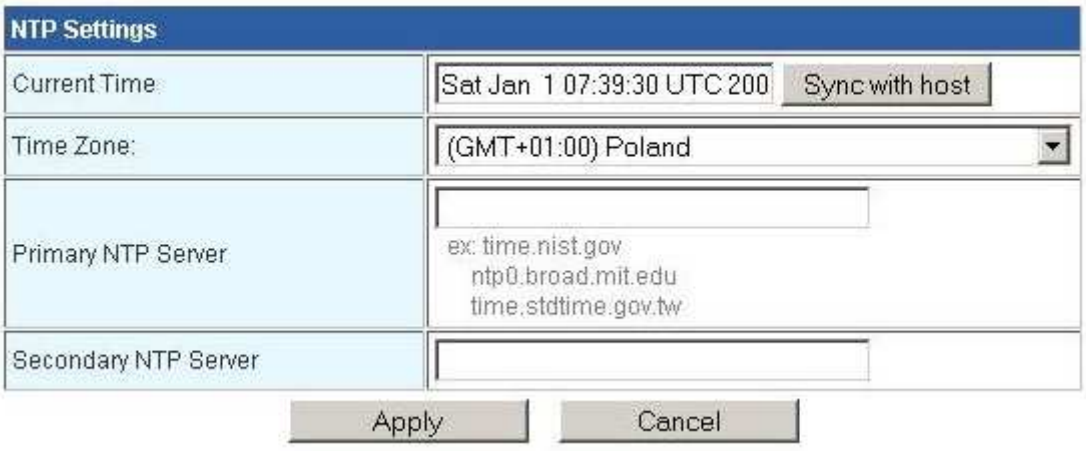
Password – Hasło użytkownika urządzenia, domyślnie: admin.

UWAGA: W nazwie użytkownika podobnie jak w haśle rozróżniane są wielkie i małe litery. W przypadku zgubienia hasła lub nazwy użytkownika należy urządzenie przywrócić do ustawień domyślnych. Należy przy włączonym urządzeniu wcisnąć i trzymać wciśnięty przycisk „Reset" przez około 10 sekund. Po tym czasie urządzenie uruchomi się ponownie z domyślnymi ustawieniami.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

NTP Settings

Ta strona umożliwia ręczne ustawienie daty i czasu routera lub pobranie danych z Internetu.



Parametry:

Current Time - Wyświetlanie bieżącego czasu systemowego. Kliknij przycisk „Sync with host", aby pobrać aktualny czas z Twojego komputera.

Time Zone – Wybierz swoją strefę czasową.

NTP Server – Wprowadź adres IP swojego serwera czasu.
NTP synchronization (hours) – Określ czas, w którym urządzenie ma łączyć się z serwerem czasu.

Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

DDNS Settings

W tej zakładce możesz modyfikować ustawienia dynamicznego serwera DNS. Zakładka DDNS umożliwia konfigurację parametrów klienta DDNS. DDNS (Dynamic Domain Name System) umożliwia tłumaczenie nazwy domenowej routera na jego aktualny publiczny adres IP. Istotne zwłaszcza przy dynamicznym publicznym adresie IP. Umożliwia to łatwy dostęp do usług udostępnionych na serwerach wirtualnych, czy DMZ urządzenia pracującego z dynamicznym adresem IP. Router umożliwia przypisanie domenowej nazwy hosta za pomocą serwera DDNS, np. www.dyndns.org. Aby możliwe było korzystanie z usługi serwera DDNS użytkownik musi wcześniej posiadać na nim swoje indywidualne konto oraz zarejestrować swoją nazwę hosta. Proces rejestracji dokonuje się poprzez stronę www jednego z powyższych serwerów.

Parametry:
Dynamic DNS Provider – Wybierz jednego z dostawców usługi z listy (Dyndns.org, freedns.afraid.org, www.zoneedit.com, and www.no-ip.com).
Account – Zarejestrowana nazwa konta w wybranym serwisie DDNS.
Password – Hasło do zarejestrowanego konta w wybranym serwisie DDNS.
DDNS - Nazwa domeny, wpisz nazwę domeny lub adres URL przyznany przez operatora usługi DDNS w postaci, np. asmax.dyndns.org.

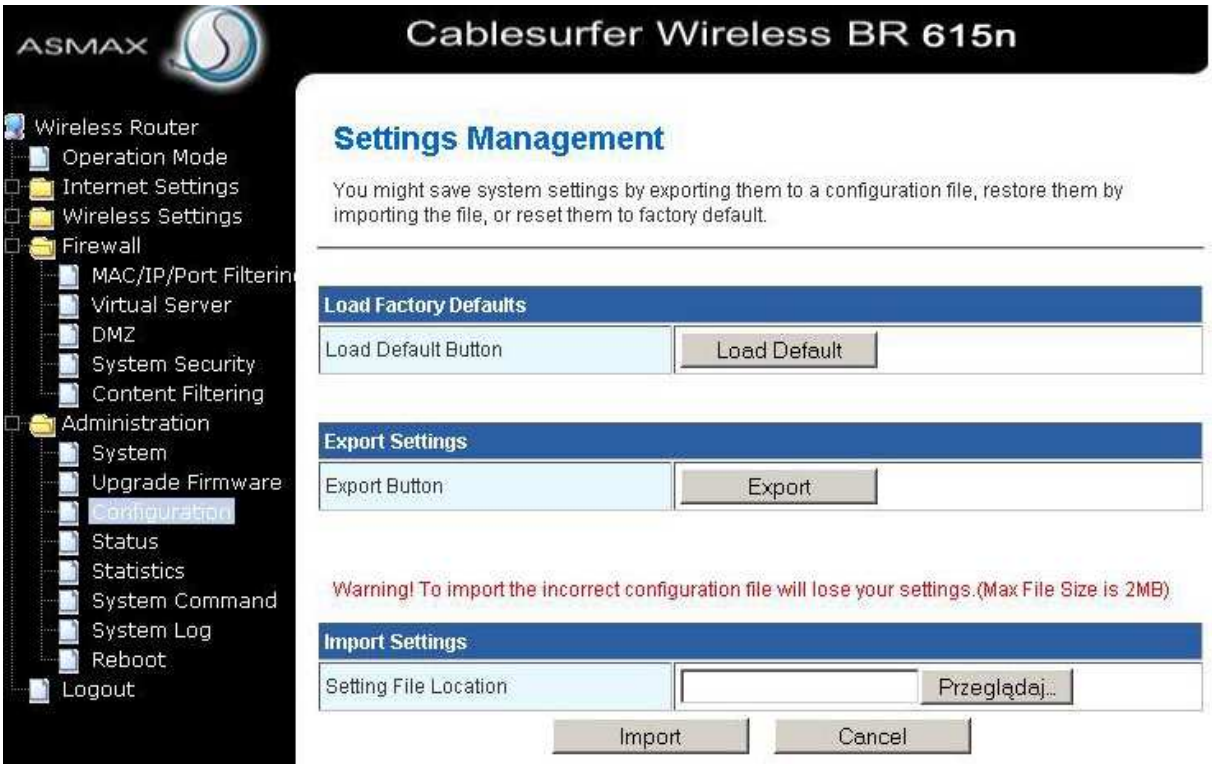
Po zakończeniu wprowadzania odpowiednich parametrów dla konfiguracji naszego połączenia kliknij przycisk „Apply", aby zapisać wprowadzone ustawienia lub „Cancel", aby zakończyć bez zapisywania ustawień.

Upgrade Firmware – aktualizacja oprogramowania

Funkcja „Upgrade Firmware” umożliwia aktualizację oprogramowania urządzenia (firmware). Aby zaktualizować oprogramowanie należy pobrać z Internetu plik z firmware i zapisać go na dysku twardym komputera w sieci LAN. Wskazać jego lokalizację klikając przycisk „Przeglądaj”. Po zaakceptowaniu nazwa pliku zostanie wyświetlona w polu „Location”. Następnie kliknij przycisk „Apply”. Proces aktualizacji może potrwać kilka minut. W tym czasie nie wolno wyłączać, ani restartować routera. Po udanej aktualizacji oprogramowania sprzętowego wyświetlony zostanie komunikat o sukcesie operacji, a urządzenie automatycznie uruchomi się ponownie. Aktualizacja oprogramowania może odbywać się wyłącznie za pomocą kabla sieciowego.

WAŻNE: Proces aktualizacji oprogramowania trwa około dwie minuty, po upływie tego czasu router automatycznie uruchomi się ponownie. Nie wyłączaj urządzenia podczas uaktualniania oprogramowania. Po aktualizacji oprogramowania zalecane jest przywrócenie urządzenia do jego ustawień domyślnych i ponowne skonfigurowanie ustawień routera.

Configuration – przywracanie ustawień domyślnych, kopia konfiguracji urządzenia



Parametry:

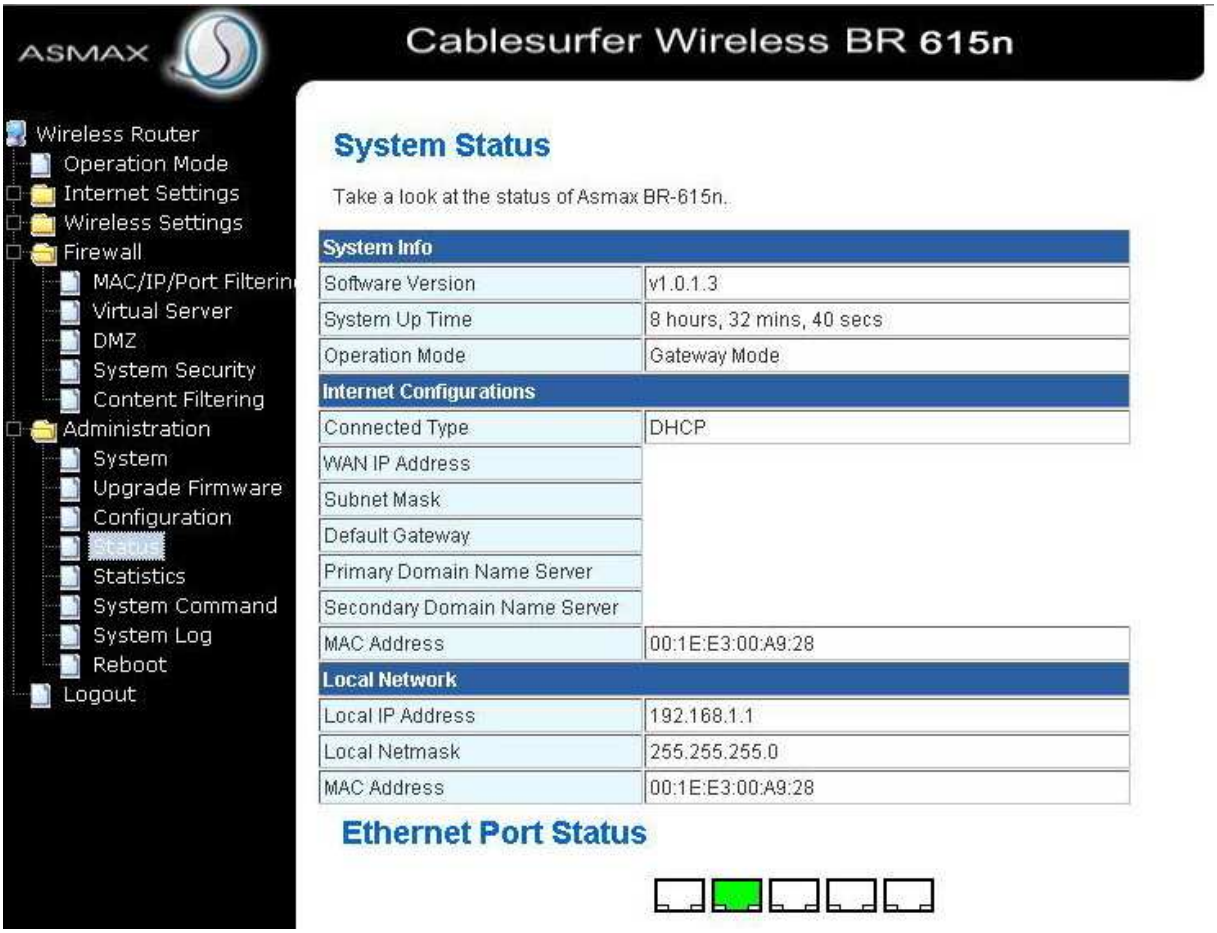
Export Settings - Kliknij przycisk „Export”, aby zapisać ustawienia na Twoim komputerze.

Import Settings - Kliknij przycisk „Przeglądaj ...”, aby wybrać ustawienia na komputerze, a następnie kliknij przycisk „Import”, aby zaimportować ustawienia urządzenia do pamięci.

Load Factory Defaults - Kliknij przycisk „Load Default”, aby system przywrócił ustawienia domyślne. Cała konfiguracja urządzenia zostanie usunięta.

System Status

Zakładka „System Status” odpowiedzialna jest za wyświetlanie aktualnych informacji o naszym urządzeniu. Umożliwia prezentację jego statusu, konfigurację serwera DHCP, strefy czasowej itd.



Parametry:

System Up Time - Czas działania urządzenia od jego uruchomienia.

Operation Mode – Tryb pracy urządzenia.

Connection Type – Typ połączenia wykorzystywany na porcie WAN.

IP Address - Adres IP sieci lokalnej.

Subnet Mask - Maska podsieci.

Default Gateway - Adres IP domyślnej bramy urządzenia.

DHCP Server - Serwer DHCP.

MAC Address - Adres MAC interfejsu sieci lokalnej.

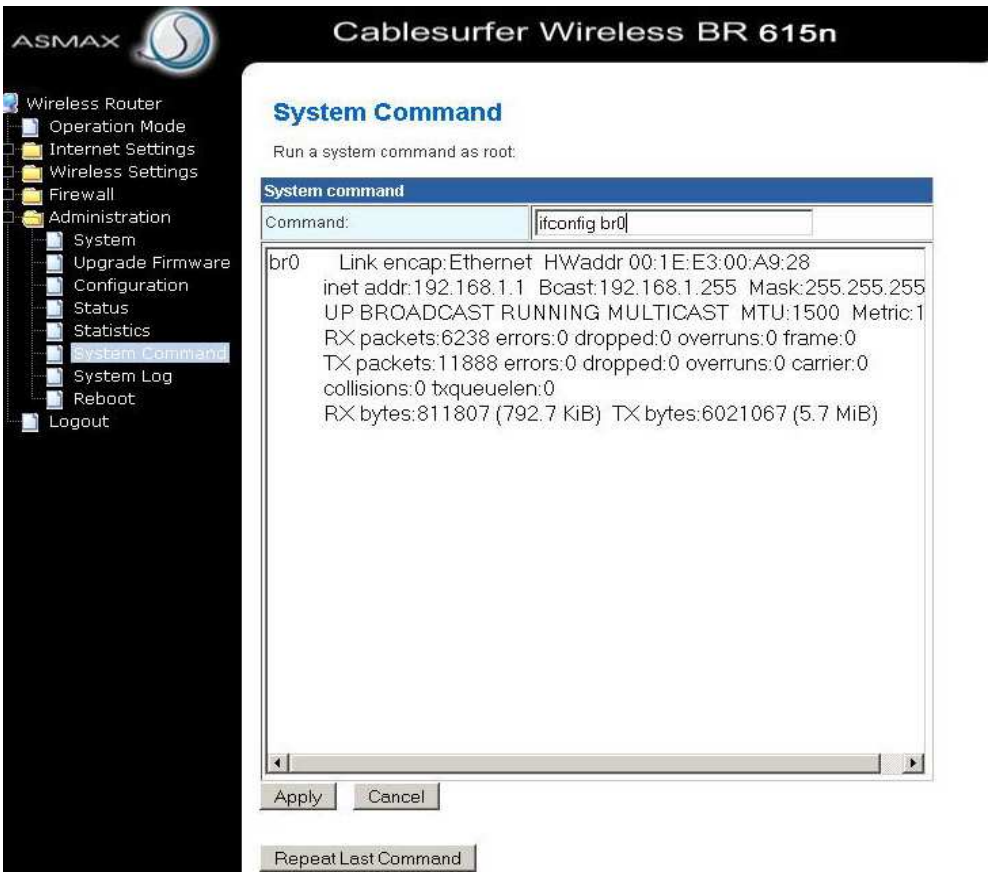
Ethernet Port Status – Wyświetla aktywne porty RJ-45

Statystyki

Zakładka wyświetlająca informacje o stanie interfejsów routera: Wireless LAN, Ethernet LAN, Ethernet WAN. Wyświetla, ile pakietów dany interfejs otrzymał i ile wysłał.

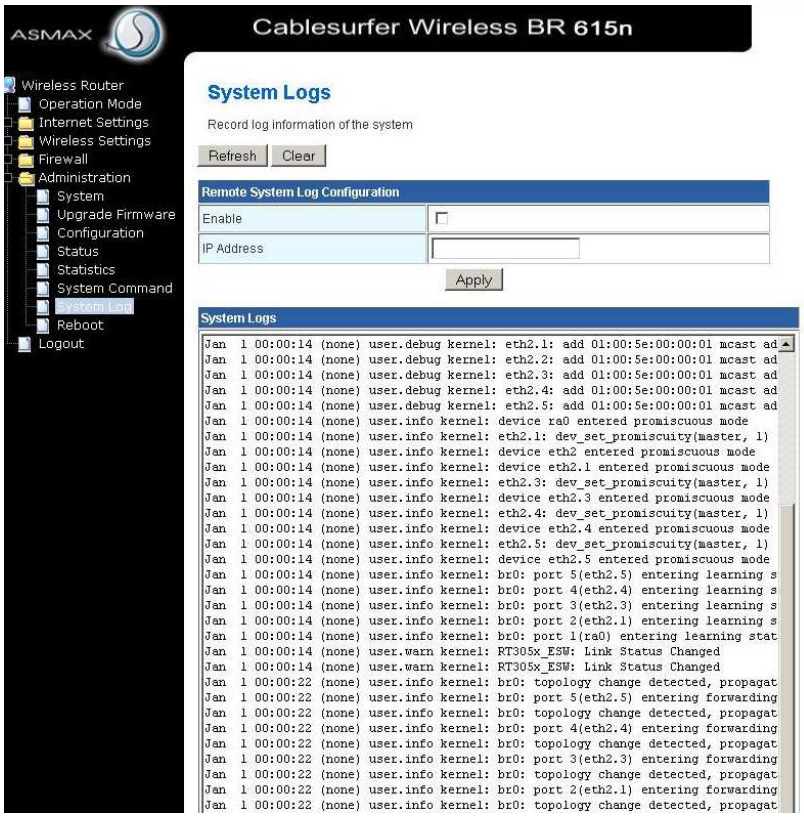
System Command

Zakładka pozwalająca użytkownikowi z poziomu interfejsu graficznego przeglądarki wprowadzać komendy z uprawnieniami użytkownika root.



System Logs

Zakładka prezentująca dokładne informacje o stanie urządzenia.

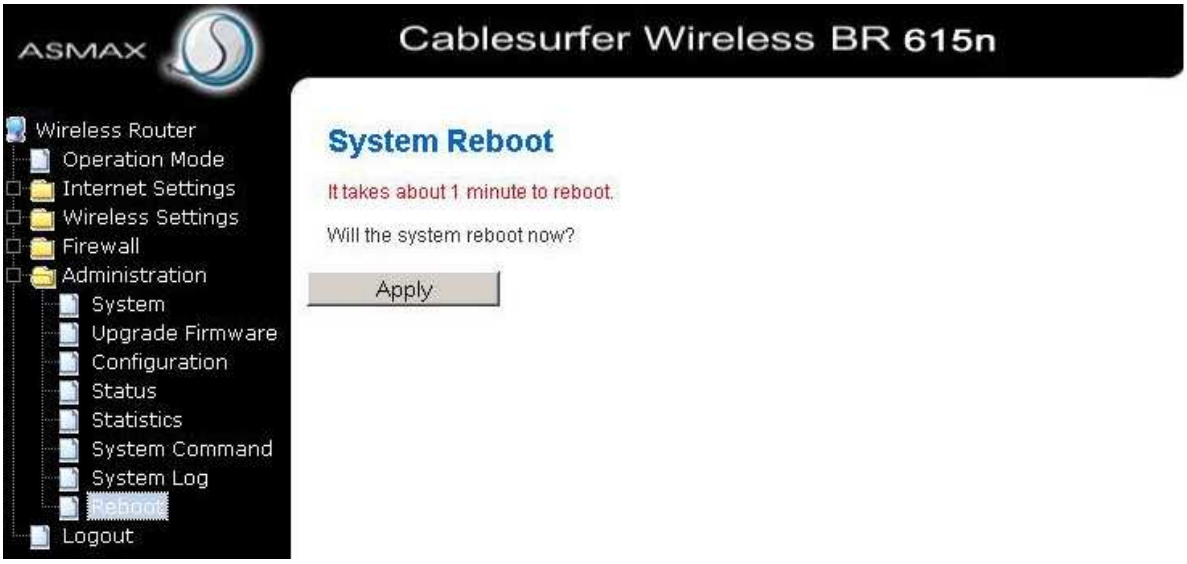


Parametry:

Remote System Log Configuration – Włączenie zdalnego logowania zdarzeń.

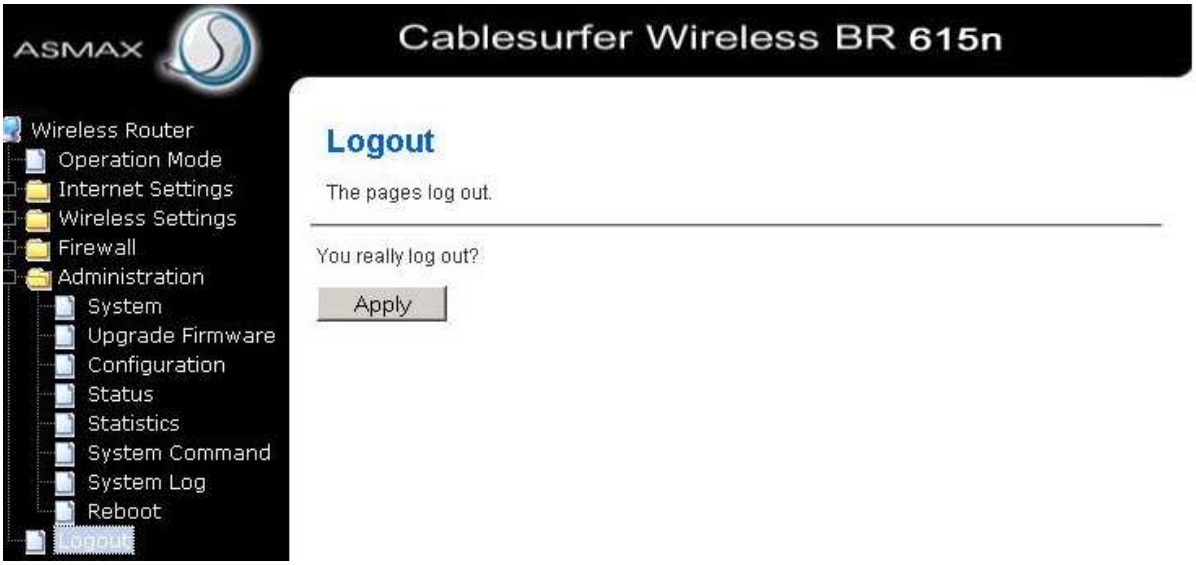
System Reboot

W zakładce „System Reboot” możemy zapisać wszystkie wprowadzone ustawienia i uruchomić ponownie urządzenie. Kliknij przycisk „Apply”.



Logout

Po zakończeniu konfiguracji urządzenia przejdź do zakładki „Logout” i kliknij „Apply” , aby się wylogować z urządzenia. Tylko jeden użytkownik może być zalogowany jednocześnie.



Rozwiązywanie podstawowych problemów

Brak połączenia z urządzeniem

- Sprawdź, czy poprawnie świecą diody urządzenia
- sprawdź fizyczne połączenie komputera z urządzeniem
- sprawdź za pomocą polecenia ***ipconfig*** swój adres IP, odśwież adres za pomocą polecenia ***ipconfig /release*** oraz ***ipconfig /renew*** w systemach Windows 2000/XP, a poleceniem ***winipcfg*** w systemie Windows 98SE
- jeżeli posiadasz prawidłowy adres IP sprawdź, czy router odpowiada na polecenie ping (np. *ping 192.168.1.1).*
- sprawdź ustawienia zapory sieciowej systemu Windows lub programowego firewall'a (jeżeli jest zainstalowany), czy nie jest zablokowane połączenie
- sprawdź ustawienia przeglądarki internetowej

Dioda LAN 1 - 4 nie świeci

- sprawdź, czy podłączony jest komputer za pomocą kabla sieciowego RJ-45 do urządzenia
- sprawdź, czy posiadasz sprawną, poprawnie zainstalowaną kartę sieciową
- sprawdź, czy świeci się dioda LINK w karcie sieciowej komputera
- jeżeli dioda LINK na karcie sieciowej ani w urządzeniu nie świecą się może być uszkodzony kabel sieciowy

Dioda WAN nie świeci

- sprawdź, czy podłączony jest główny kabel sieciowy z sieci WAN, modemu kablowego lub modemu ADSL
- spróbuj wymienić kabel sieciowy RJ-45 na inny

Dioda WLAN nie świeci

- sprawdź, czy włączony jest wbudowany moduł bezprzewodowy w urządzeniu zakładka *Wireless Settings → Basic* - parametr „Radio On/Off" powinien włączony.
- sprawdź, czy podłączona jest prawidłowo antena
- przywróć ustawienia fabryczne urządzenia

Nie pamiętam nazwy użytkownika i hasła

- Domyślna nazwa użytkownika to „admin". Domyślne hasło to „admin". W polach nazwy użytkownika i hasła wielkie i małe litery są istotne. Upewnij się, że wpisujesz właściwą nazwę użytkownika i hasło, używając odpowiednich wielkich i małych liter.
- Jeśli zapomnisz hasła dostępowego do routera, należy przywrócić ustawienia fabryczne routera. Użyj przycisku RESET: Naciśnij przycisk RESET i trzymaj wciśnięty przez około 6 sekund, a następnie zwolnij przycisk i poczekaj aż router zostanie uruchomiony ponownie.

Gry i aplikacje sieciowe nie działają

- musisz przekierować port/porty aplikacji za pomocą funkcji „Firewall/Virtual Server"
- sprawdź, czy aplikacja działa w przypadku uaktywnienia opcji ***DMZ***

Skąd mogę dowiedzieć się o nowszych wersjach oprogramowania wewnętrznego (firmware)?

- Informacje o nowych wersjach oprogramowania są umieszczane na stronie http://www.asmax.pl. Natomiast z serwera ftp://ftp.asmax.pl/pub/sterowniki można je bezpłatnie pobrać.

Czy jest istotna różnica w pracy urządzenia przy stosowaniu statycznej adresacji IP w porównaniu z adresacją dynamiczną?

- Nie, nie ma żadnej różnicy w pracy urządzenia. Stosowanie serwera DHCP ułatwia jedynie konfigurację komputerów pracujących w naszej sieci lokalnej. Przy wyłączonym serwerze DHCP wszystkie parametry protokołu IP musimy wprowadzać ręcznie:

- adres IP komputera
- maska podsieci
- adres IP bramki
- adresy serwerów DNS

Parameter	Specyfikacja
Specyfikacja systemu	
Chipset	RT 3050
SDRAM	16 MB
Flash	4 MB
Właściwości	
Protokoły	● IEEE 802.11b ● IEEE 802.11g ● IEEE 802.11n ● RFC768 User Datagram Protocol (UDP) ● RFC791 Internet Protocol (IP) ● RFC792 Internet Control Message Protocol (ICMP) ● RFC793 Transmission Control Protocol (TCP) ● RFC826 Address Resolution Protocol (ARP) ● RFC2516 PPP over Ethernet (PPPoE) ● RFC2131 Dynamic Host Configuration Protocol (DHCP) ● ALG
Wspierane systemy	Windows 98SE, Windows 2000, Windows ME, Windows XP, Windows Vista, Windows 7, Linux
Modulacja	Wspracie dla 256/64/16/8-QAM, QPSK, BPSK, MCS0 ~ MCS15
Szyforwanie	4/128 bit, WEP, 802.1x, WPA, i WPA2
QoS	Wsparcie grup i usług
Moc nadawania	15±1.5dBm@11g,18±1.5dbm@11b, 15±1.5dBm@11n
SNMPv2 lub v3	Wspiera
Interfejs LAN	4 porty x RJ45 dla 10/100 LAN Ethernet 1 port x RJ45 dla 10/100 WAN Ethernet
Diody	● Power ● WLAN ● WPS ● WAN ● LAN 1~4
Pobór mocy	4W(max)
Wymagania środowiskowe	
Temperatura pracy	0ºC~45ºC
Temperatura przechowywania	-20ºC~70ºC
Wilgotność pracy	10%~90%, bez kondensacji
Wilgotność przechowywania	5%~90%, bez kondensacji
Zasilacz	● Wejście: 100-240VAC, 50/60Hz ● Wyjście:12VDC/500mA
Certyfikaty	
Zgodność z przepisami	● FCC Part 15 Class B ● CE
Przepisy bezpieczeństwa	UL
Ochrona środowsika	RoHS
Wymiary/waga	
Wymiary	PCB Długość x Szerokość x Wysokość: 98 mm x 103.5 mm x 1.6 mm
Waga	200g

Słowniczek podstawowych pojęć

802.11b

Standard 802.11b cechuje połączenie bezprzewodowe o prędkości 11Mbps, wykorzystujące technologię bezpośredniego modulowania nośnej sekwencją kodową (DSSS) w nielicencjonowanym paśmie radiowym o częstotliwości 2.4GHz, z zabezpieczeniem w postaci szyfrowania WEP. Sieci 802.11b bywają nazywane sieciami Wi-Fi.

802.11g

Standard 802.11g cechuje połączenie bezprzewodowe o prędkości 54 Mbps, wykorzystujące technologię bezpośredniego modulowania nośnej sekwencją kodową (DSSS) oraz modulację OFDM w nielicencjonowanym paśmie radiowym o częstotliwości 2.4GHz, kompatybilne wstecznie z urządzeniami IEEE 802.11b oraz z zabezpieczeniem w postaci szyfrowania WEP.

Ad-hoc Network

Sieć Ad-hoc jest grupą komputerów wyposażonych w adaptery bezprzewodowe, połączonych w niezależną, bezprzewodową sieć LAN 802.11. Komputery bezprzewodowe w sieci Ad-hoc działają w oparciu o połączenia peer-to-peer, komunikując się bezpośrednio ze sobą, z pominięciem punktu dostępowego. Tryb Ad-hoc jest również nazywany Independent Basic Service Set (IBSS), lub trybem peer-to-peer i jest przydatny w skali poszczególnych działów w segmencie SOHO.

DHCP

DHCP (ang. Dynamic Host Configuration Protocol - protokół dynamicznego konfigurowania węzłów) to protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski sieci. W sieci opartej na protokole TCP/IP każdy komputer ma co najmniej jeden adres IP i jedną maskę podsieci; dzięki temu może się komunikować z innymi urządzeniami w sieci.

DSSS

(Direct-Sequence Spread Spectrum) - Bezpośrednie modulowanie nośnej sekwencją kodową. DSSS generuje niepotrzebne, niewielkie ilości bitów, dla wszystkich przesyłanych danych. Nazywane są one „chip" (lub „chipping code"). Nawet w przypadku uszkodzenia jednego lub większej ilości bitów w chipie podczas transmisji, wbudowana w odbiornik technologia Statistics, może odtworzyć oryginalną postać danych, bez konieczności ponownej transmisji. Dla „niewtajemniczonego" odbiornika, DSSS jest niskiej mocy szerokopasmowym szumem i jako taki jest odrzucany (ignorowany) przez większość odbiorników pracujących w wąskich pasmach. Jednak przez odbiornik „wtajemniczony" (np. inną końcówkę bezprzewodowej sieci LAN), sygnał DSSS jest rozpoznawany jako jedyny prawidłowy sygnał, a wszelkie zakłócenia są w odpowiedni sposób odrzucane (ignorowane).

Ethernet

Ethernet to technologia, w której zawarte są standardy wykorzystywane w budowie głównie lokalnych sieci komputerowych. Obejmuje ona specyfikację kabli oraz przesyłanych nimi sygnałów. Ethernet opisuje również format ramek i protokoły z dwóch najniższych warstw Modelu OSI. Jego specyfikacja została podana w standardzie 802.3 IEEE. Ethernet jest najpopularniejszym standardem w sieciach lokalnych.

Firewall

Firewall jest aplikacją lub urządzeniem chroniącym lokalną sieć przed zagrożeniami pochodzącymi zarówno z Internetu, jak i samej sieci lokalnej. Tylko połączenia, które będą posiadały dostęp do sieci będą mogły zostać zrealizowane poprzez Firewall. Zazwyczaj połączenie jest inicjowane z sieci LAN, np. poprzez przeglądarkę internetową, klienta poczty elektronicznej czy grę sieciową. Firewall umożliwia ograniczenie użytkownikom dostępu do pewnych zasobów sieci.

Gateway

Brama sieciowa (ang. gateway) – maszyna podłączona do sieci komputerowej za pośrednictwem której komputery z sieci lokalnej komunikują się z komputerami w innych sieciach. Brama sieciowa może trasować pakiety między sieciami TCP/IP lub innych protokołów trasowanych – jest wtedy routerem. W sieci TCP/IP domyślna brama (sieciowa) (ang. default gateway) oznacza router, do którego komputery sieci lokalnej mają wysyłać pakiety o ile nie powinny być one kierowane w sieć lokalną lub do innych, znanych im routerów. W typowej konfiguracji sieci lokalnej TCP/IP wszystkie komputery korzystają z jednej domyślnej bramy, która zapewnia im łączność z innymi podsieciami lub z Internetem.

Idle Timeout

Funkcja automatycznego przerwania połączenia z Internetem, jeśli przez określony czas nie występuje żaden ruch w obrębie połączenia Internetowego.

IEEE 802.11 Standard

802.11 to grupa standardów IEEE dotyczących sieci bezprzewodowych sporządzonych przez grupę 11 z IEEE 802. Czasami określenia 802.11 używa się też w stosunku do pierwszego standardu z tej rodziny. Standardy 802.11 stanowią podstawę certyfikatów Wi-Fi.

Infrastructure

Sieć LAN, w której każda stacja bezprzewodowa komunikuje się z siecią poprzez punkt dostępowy (AP). Transmisja i odbiór danych przez każdą stację bezprzewodową jest realizowana poprzez punkt dostępowy (AP).

IP Adres

Adres IP – liczba nadawana interfejsowi sieciowemu, grupie interfejsów (broadcast, multicast), bądź całej sieci komputerowej opartej na protokole IP, służąca identyfikacji elementów warstwy trzeciej modelu OSI – w obrębie sieci oraz poza nią (tzw. adres publiczny). Adres IP nie identyfikuje jednoznacznie fizycznego urządzenia.

ISP

Internet Service Provider - Dostawca Usług Internetowych. Rodzaj działalności handlowej polegający na dostarczaniu połączeń z Internetem dla odbiorców indywidualnych lub innego rodzaju odbiorców.

Local Area Network (LAN)

Sieć lokalna (ang. Local Area Network stąd używany także w języku polskim skrót LAN) (wewnętrzna sieć) – najmniej rozległa postać sieci komputerowej, zazwyczaj ogranicza się do jednego budynku lub kilku pobliskich budynków (np. bloków na osiedlu).Technologie stosowane w sieciach lokalnych można podzielić na rozwiązanie oparte na przewodach (kable miedziane, światłowody) lub komunikacji radiowej (bezprzewodowe). W sieciach lokalnych przewodowych najczęściej używaną

technologią jest Ethernet (za pośrednictwem kart sieciowych i urządzenia pośredniczącego huba tzw. koncentratora funkcję tę może pełnić również przełącznik). Czasem są to takie urządzenia, jak np. port szeregowy, port równoległy czy port podczerwieni. W sieciach lokalnych bezprzewodowych najczęściej używaną technologią jest WLAN, zwany także Wi-Fi, określony standardami IEEE 802.11.

MAC Address

MAC (Media Access Control) – Kontrola Dostępu do Medium Transmisyjnego. Adres urządzenia podłączonego do sieci. Jest to unikalny identyfikator urządzeń z interfejsem Ethernet. Składa się z dwóch części: 3 bajtów danych związanych z ID Producenta (odrębny identyfikator każdego producenta), oraz kolejnych 3 bajtów, często używanych jako numer seryjny producenta.

NAT

Network Address Translator – Translator Adresów Sieciowych. Umożliwia wszystkim komputerom w sieci lokalnej posługiwanie się jednym publicznym adresem IP. Korzystając z tej właściwości NAT, możesz uzyskać dostęp do Internetu z jakiegokolwiek komputera sieci loklanej, bez potrzeby wykupienia dodatkowych adresów IP u dostawcy usług internetowych.

Port

Z portów korzystamy w celu odróżniania jednych protokołów aplikacji sieciowych od innych. Numery portów reprezentowane są przez liczby naturalne z zakresu od 0 do 65535. Niektóre numery portów (od 0 do 1023) są znane i zarezerwowane na standardowo przypisane do nich usługi takie, jak np. WWW czy poczta elektroniczna. Dzięki temu możemy identyfikować nie tylko procesy, ale ogólnie znane usługi działające na odległych systemach. Różne usługi mogą używać tych samych numerów portów pod warunkiem, że korzystają z innego protokołu TCP albo UDP, niektóre usługi korzystają jednocześnie z danego numeru portu i obydwu protokołów (DNS korzysta z portu 53 za pomocą TCP i UDP jednocześnie). Zdarza się także, że jedna usługa może korzystać z dwóch różnych portów używanych do innych zadań np. FTP czy SNMP.

DNS – 53
Finger – 79
FTP – 20, przesyłanie danych
FTP – 21, przesyłanie poleceń
Gopher – 70
HTTP – 80
Proxy - 3128, 8080
HTTPS – 443
IMAP – 143
IMAP3 – 220
IRC – 6667
XMPP – 5222
XMPP – 5223
LDAP – 389
LDAPS – 636
MySQL – 3306
NNTP - 119
POP3 – 110
SPOP3 – 995
PostgreSQL – 5432
Rsync – 873
SMTP – 25
SSH – 22
Syslog – 514
Telnet – 23
TFTP – 69
X11 – od 6000 do 6007

PPPoE

Point-to-Point Protocol over Ethernet. Protokół Point-to-Point, to metoda bezpiecznej transmisji danych, początkowo stworzona dla połączeń typu dial-up; PPPoE przeznaczony jest do połączeń Ethernet. PPPoE opiera się na dwóch szeroko akceptowanych standardach, Ethernet i Point-to-Point Protocol. Jest to protokół komunikacyjny do transmitowania informacji przez Ethernet pomiędzy różnymi wytwórcami.

Radius

(Remote Access Dial-In User Service) jest protokołem klient - serwer typu AAA (Authorization, Authentication, Accounting) używanym do logowania klientów dial-up (autoryzacja, autentykacja, rozliczanie) do serwera dostępu do sieci (Network Access Server). Połączenie składa się z trzech faz: Authentication - weryfikacja nazwy użytkownika i hasła w lokalnej bazie danych. Po pomyślnej weryfikacji następuje proces autoryzacji. Authorization - określa czy żądanie dostępu do zasobów może zostać zrealizowane. Klient Dial-up otrzymuje adres IP. Accounting - gromadzenie informacji o połączeniu (billing, statystyki).

Router

Router jest to sieciowe urządzenie trasujące (przekaźnik), odpowiedzialne za przesyłanie pakietów między dwoma odległymi od siebie komputerami. Router (lub routery - gdyż im większe odległości między komunikującymi się komputerami tym więcej tego typu urządzeń pośredniczy w przekazywaniu informacji) łączy daną sieć komputerową WAN z inną, tworząc pomost dla przesyłanych informacji. Z uwagi na to, że w dużych sieciach droga z jednego komputera do drugiego (i z powrotem) może przebiegać przez wiele różnych alternatywnych ścieżek, router ma za zadanie skierować nadchodzący pakiet zawsze tą ścieżką, która w danej chwili rokuje najszybszy i/lub najlepszy transfer do miejsca docelowego lub następnego węzła komunikacyjnego -routera. Tablice routingu monitorujące na bieżąco wszystkie połączenia zawierają nieustannie aktualizowane dane o stanie połączonych sieci na podstawie, których router dokonuje wyboru dalszej drogi dla nadchodzącego pakietu.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (ang. Prosty Protokół Zarządzania Siecią) — standard protokołu używanego do nadzoru i zarządzania różnymi elementami sieci telekomunikacyjnych, takimi jak routery, przełączniki, komputery czy centrale telefoniczne.

Spread Spectrum

Technologia rozproszonego widma. Spread Spectrum jest szerokopasmową techniką wykorzystującą częstotliwości radiowe, stworzoną przez wojsko do użytku w zaufanych, bezpiecznych i o decydującym znaczeniu systemach komunikacyjnych. Została ona stworzona w celu wykorzystania możliwości całego pasma z zachowaniem pewności, bezpieczeństwa i integralności. Innymi słowy, wykorzystywana jest większa część pasma, niż w przypadku transmisji wąskopasmowej, ale w zamian otrzymuje się sygnał mocniejszy, będący w efekcie łatwiejszy do wykrycia, pod warunkiem, że odbiornik zna parametry danego sygnału częstotliwości, sygnał szerokopasmowy jest przez niego postrzegany jako niewielki szum w tle. Direct Sequence Spread Spectrum (DSSS) oraz Frequency Hopping Spread Spectrum (FHSS) to dwie podstawowe alternatywy.

SSID

Service Set Identification. Jest to maksymalnie 32-znakowy klucz alfanumeryczny, identyfikujący bezprzewodową sieć LAN. By móc się ze sobą komunikować w jednej sieci bezprzewodowej, wszystkie urządzenia muszą być skonfigurowane z użyciem tego samego SSID. Jest to typowy parametr konfiguracyjny dla bezprzewodowej karty PC. Ma on związek z ESSID w bezprzewodowym punkcie dostępu i z nazwą sieci bezprzewodowej. Zobacz również Nazwa Sieci Bezprzewodowej oraz ESSID.

Subnet Mask

Maska Podsieci, która może być częścią informacji TCP/IP, dostarczonej przez dostawce usług internetowych, to zbiór czterech liczb (np. 255.255.255.0) skonfigurowanych jak adres IP. Używana jest do utworzenia liczb adresu IP tylko w obrębie konkretnej sieci (w przeciwieństwie do ważnych liczb adresów IP rozpoznawanych przez Internet, które muszą być przypisane przez InterNIC).

Transmission Control Protocol / Internet Protocol (TCP/IP)

TCP/IP (ang. Transmission Control Protocol / Internet Protocol) jest pakietem najbardziej rozpowszechnionych protokołów komunikacyjnych współczesnych sieci komputerowych. Następca protokołu NCP. Najczęściej obecnie wykorzystywany standard sieciowy, stanowiący podstawę współczesnego Internetu. Nazwa pochodzi od dwóch najważniejszych jego protokołów: TCP oraz IP. TCP/IP jest standardem komunikacji otwartej. Otwartość oznacza tu możliwości komunikacji między dowolnymi typami urządzeń, bez względu na ich fizyczną różnorodność. TCP/IP zwany jest także stosem protokołów ze względu na strukturę warstwową, w której ramka protokołu wyższej warstwy jest zawarta jako dane w protokole warstwy niższej.

TTL

TTL (Time To Live) jest parametrem określającym czas życia pakietu IP. Każdy pakiet IP wysyłany jest od nadawcy do odbiorcy z określoną wartością TTL (np. 64). Pakiet przechodząc przez dowolny router po drodze (w procesie routingu) ma zmniejszany za każdym razem parametr TTL o 1. Pakiet z TTL równym 0 jest usuwany i nie przesyłany dalej. W ten sposób zapobiega to tworzeniu się pętli w sieci Internet. Aby ograniczyć możliwość rozdzielania łącza we własnym zakresie przez abonentów, dostawca usług Internetowych może ustawiać wartość parametru TTL pakietów IP na 1. W ten sposób po dotarciu do routera jest on usuwany. Funkcja TTL umożliwia zwiększenie wartości TTL o 1 przed jej odjęciem przez router. W konsekwencji powoduje to, że pakiety przechodzące przez router nie mają zmienianych wartości TTL.

Web-based management Graphical User Interface (GUI)

Wiele urządzeń obsługuje interfejs użytkownika graficznego, który oparty jest na wyszukiwarce sieciowej. Oznacza to, że użytkownik może posługiwać się rodziną Netscape lub Microsoft Internet Explorer w celu kontrolowania, konfigurowania lub monitorowania obsługiwanego urządzenia.

WEP (Wired Equivalent Privacy)

Mechanizm ochrony danych, oparty na 64-bitowym, 128-bitowym lub 152-bitowym algorytmie współdzielonego klucza, opisany w punkcie Standard IEEE 802.11.

Wi-Fi

Nazwa handlowa standardu bezprzewodowego 802.11b, nadana przez Wireless Ethernet Compatibility Alliance (WECA, zobacz http://www.wi-fi.net), organizację zajmującą się standardami przemysłowymi, promującą kompatybilność wszystkich urządzeń 802.11b. WLAN (Wireless Local Area Network) – Grupa komputerów i skojarzonych urządzeń, komunikujących się ze sobą bezprzewodowo, z ograniczoną lokalnie grupą
użytkowników.

Wide Area Network (WAN)

Sieć WAN (z ang. Wide Area Network, rozległa sieć komputerowa) – sieć komputerowa znajdująca się na obszarze wykraczającym poza jedno miasto (bądź kompleks miejski).

WPA/WPA2 – WPA

(ang. WiFi Protected Access) to standard szyfrowania stosowany w sieciach bezprzewodowych standardu IEEE 802.11. WPA jest następcą mniej bezpiecznego standardu WEP. Standard WPA został wprowadzony przez organizację WiFi. WPA został wprowadzony jako standard przejściowy pomiędzy WEP a zabezpieczeniem 802.11i czyli WPA2 w celu zwiększenia bezpieczeństwa użytkowników sprzętu mającego na stałe zaimplementowany WEP bez konieczności ich wymiany. Osiągnięto to przez cykliczną zmianę klucza szyfrującego WEP, co przy odpowiedniej częstotliwości zmian uniemożliwia jego złamanie pomimo istniejących podatności. Także dzięki temu zabiegowi wyposażenie systemu lub urządzenia w WPA jest możliwe bez zmiany sprzętu - wystarczy zmienić oprogramowanie (sterownik w przypadku kart sieciowych, a w przypadku punktów dostępowych firmware). WPA dzieli się na: Enterprise – korzysta z serwera RADIUS, który przydziela różne klucze do każdego użytkownika i Personal - nie dzieli kluczy na poszczególnych użytkowników, wszystkie podłączone stacje wykorzystują jeden klucz dzielony (PSK - Pre-Shared Key).Najważniejszą różnicą pomiędzy WPA a WPA2 jest używana metoda szyfrowania. Podczas, gdy WPA wersji pierwszej korzysta z TKIP/RC4 oraz Michael (MIC), WPA2 wykorzystuje CCMP/AES. Uwierzytelnienie w protokole WPA-PSK jest podatne na ataki słownikowe. Szyfrowanie TKIP w WPA jest także podatne na atak kryptoanalityczny o ograniczonym zasięgu.

Informacje kontaktowe

Aby uzyskać pomoc dotyczącą instalacji lub obsługi urządzenia Asmax BR615N, prosimy o kontakt z infolinią Asmax pod numerem **0801-324-084**. Sterowniki i instrukcje do pobrania z ftp://ftp.asmax.pl
Storna internetowa: http://www.asmax.pl

Informacja dla użytkowników o pozbywaniu się urządzeń elektrycznych i elektronicznych (dotyczy gospodarstw domowych)

Przedstawiony symbol umieszczony na produktach lub dołączonej do nich dokumentacji informuje, że niesprawnych urządzeń elektrycznych lub elektronicznych nie można wyrzucać razem z odpadami gospodarczymi. Prawidłowe postępowanie w razie konieczności utylizacji, powtórnego użycia lub odzysku podzespołów polega na przekazaniu urządzenia do wyspecjalizowanego punktu zbiórki, gdzie będzie przyjęte bezpłatnie. W niektórych krajach produkt można oddać lokalnemu dystrybutorowi podczas zakupu innego urządzenia. Prawidłowa utylizacja urządzenia umożliwia zachowanie cennych zasobów i uniknięcie negatywnego wpływu na zdrowie i środowisko, które może być zagrożone przez nieodpowiednie postępowanie z odpadami. Szczegółowe informacje o najbliższym punkcie zbiórki można uzyskać u władz lokalnych. Nieprawidłowa utylizacja odpadów zagrożona jest karami przewidzianymi w odpowiednich przepisach lokalnych. W razie konieczności pozbycia się urządzeń elektrycznych lub elektronicznych, prosimy skontaktować się z najbliższym punktem sprzedaży lub dostawcą, którzy udzielą dodatkowych informacji.