Instrukcja instalacji i obsługi

PENTAGRAM Cerberus
ADSL2 Wi-Fi Plus
(P 6331-6)

PENTAGRAM
THE PERFECT SIMPLICITY

Najnowsze wersje instrukcji, sterowników oraz aplikacji są dostępne na stronie www.pentagram.pl

2008-10-08

UWAGA! Wszystkie informacje i dane techniczne mogą ulec zmianie bez wcześniejszego powiadomienia i/lub wskazania w niniejszej instrukcji.

© 2007 PENTAGRAM
Wszelkie prawa zastrzeżone, powielanie i kopiowanie zabronione.

SPIS TREŚCI

WPROWADZENIE 5
FUNKCJE 5
ZAWARTOŚĆ PUDEŁKA 7
OMÓWIENIE PRODUKTU 8
UWAGI 8
PANEL PRZEDNI 8
PANEL TYLNY 9
USTAWIENIA DOMYŚLNE 9
RESETOWANIE ROUTERA 10
PODŁĄCZANIE URZĄDZENIA CERBERUS DO KOMPUTERA 10
KONFIGURACJA PROTOKOŁU TCP/IP 10
KONFIGURACJA ROUTERA POPRZEZ PRZEGLĄDARKĘ WWW 14
LOGOWANIE 14
NAWIGACJA 15
ZAKŁADKA STATUS 16
ZAKŁADKA QUICK START 20
ZAKŁADKA CONFIGURATON 22
ZAKŁADKA SAVE CONFIGURATION TO FLASH 62
ZAKŁADKA RESTART 62
ROZWIĄZYWANIE PROBLEMÓW 63
ZASTOSOWANIE DIOD LED W CELU DIAGNOZOWANIA PROBLEMÓW 63
PROBLEMY Z INTERFEJSEM WWW 63
PROBLEMY Z NAZWĄ UŻYTKOWNIKA I HASŁEM 64
PROBLEMY Z INTERFEJSEM LAN 64
PROBLEMY Z INTERFEJSEM WAN 64
PROBLEMY Z DOSTĘPEM DO INTERNETU 66

PENTAGRAM
THE PERFECT SIMPLICITY

Wprowadzenie

Dziękujemy za zakup modemu/routera ADSL2+ Cerberus ADSL2 Wi-Fi Plus (P6331-6) firmy PENTAGRAM. Twój nowy router jest urządzeniem wielofunkcyjnym łączącym w sobie modem ADSL, router ADSL, przełącznik sieciowy Ethernet oraz punkt dostępu bezprzewodowego, tak aby zapewnić wszelkie możliwości podłączenia komputerów do Internetu za pomocą szerokopasmowego łącza ADSL.

Router Cerberus ADSL2 Wi-Fi Plus (P 6331-6) odpowiada międzynarodowym standardom wdrożeniowym ADSL2+ i obsługuje transmisje o szybkości do 24 Mb/s w kierunku do komputera oraz do 1 Mb/s w kierunku do Internetu. Router ten, zaprojektowany z myślą o małych biurach, domowych zastosowaniach biurowych oraz użytkownikach prywatnych pozwoli uzyskać szybsze połączenia internetowe. Można dzięki niemu cieszyć się całą gamą usług ADSL i szerokopasmowych zastosowań multimedialnych, takich jak gry interaktywne czy strumieniowe transmisje wideo oraz dźwięku w czasie rzeczywistym realizowane w sposób łatwiejszy i szybszy niż kiedykolwiek wcześniej.

Funkcje

- Wbudowany 4-portowy przełącznik Ethernet 10/100 Mb/s ma funkcję automatycznego wykrywania przeplotu dla portów 10Base-T oraz 100Base-TX, co umożliwia zastosowanie krosowanych lub bezpośrednich kabli Ethernet.

- Wbudowany punkt dostępowy 802.11g umożliwia poszerzenie wachlarza środków łączności o sieci WLAN, zabezpieczając jednocześnie sieci bezprzewodowe za pomocą technologii WEP, WPA/WPA2 i WDS.

- Funkcja translacji adresów sieciowych (Network Address Translation – NAT) umożliwia wielu użytkownikom jednoczesny dostęp do zasobów zewnętrznych, np. Internetu, z jednego adresu IP lub konta dostępowego. Obsługa wielu bram warstwy aplikacji (ALG) np. dla przeglądarek internetowych, ICQ, FTP, Telnetu, poczty elektronicznej, grup dyskusyjnych, Net2phone, Ping, NetMeeting, telefonów IP itp.

- UPnP – protokół używany w celu zapewnienia prostej i wydajnej łączności pomiędzy wieloma odrębnymi urządzeniami i komputerami pochodzącymi od różnych producentów. Dzięki niej zestawienie sieci staje się proste i niedrogie. Architektura UPnP wykorzystuje protokół TCP/IP oraz dostęp WWW w celu umożliwienia pracy sieciowej na małej przestrzeni oraz w celu kontroli i przesyłu danych pomiędzy urządzeniami sieciowymi. Jeżeli ta funkcja jest włączona, użytkownik może płynnie łączyć się z aplikacjami Net Meeting albo MSN Messenger.

- Usługa Dynamicznego DNS umożliwia skojarzenie dynamicznego adresu IP ze stałą nazwą hosta. Dynamiczny adres IP to adres IP z sieci WAN. W celu zastosowania tej usługi należy najpierw założyć konto u usługodawcy DDNS, np. na stronie http://www.dyndns.org/.

- Urządzenie Cerberus ADSL2 Wi-Fi Plus (P6311-6) oferuje wbudowaną funkcję klienta PPPoE używaną do ustanawiania połączeń. Dzięki niej uzyskuje się większą szybkość dostępu bez zmiany samej zasady działania oraz przy użyciu tego samego konta dostawcy usług internetowych (przez co nie trzeba płacić za dodatkowe konto dostępowe). Komputer lokalny nie musi być wyposażony w oprogramowanie klienckie

PPPoE. Zapewnione są również funkcje automatycznego odnawiania połączenia oraz rozłączania połączenia nieaktywnego.

- Virtual Server (serwera wirtualnego): Użytkownik może określić, które usługi będą widoczne dla użytkowników zewnętrznych. Router wykrywa odbierane żądania usług i przesyła je do konkretnego komputera lokalnego w celu obsługi. Przykładowo, można przypisać komputer z sieci lokalnej do funkcji serwera WWW i ujawnić go w sieci zewnętrznej. Użytkownicy zewnętrzni mogą bezpośrednio przeglądać ten serwer WWW, chroniony za pomocą mechanizmu NAT. Komputery lokalne udostępnione w zewnętrznej sieci internetowej mogą być również zdefiniowane jako hosty „strefy zdemilitaryzowanej" DMZ.

- Klient oraz serwer protokołu dynamicznej konfiguracji hosta (Dynamic Host Configuration Protocol – DHCP): po stronie sieci rozległej, klient sieci DHCP może automatycznie uzyskać adres IP od dostawcy usług internetowych (ISP). Po stronie sieci lokalnej, serwer DHCP przydziela dostępny zakres adresów IP klientów, włącznie z maskami podsieci i adresami IP serwerów DNS, oraz dystrybuuje je pomiędzy komputerami lokalnymi. Jest to prosty sposób na zarządzanie lokalną siecią IP.

- Routing statyczny oraz RIP1/2: Funkcja routingu jest realizowana za pomocą prostej tablicy routingu statycznego lub protokołu RIP1/2.

- SNMP (Simple Network Management Protocol): SNMP umożliwia wygodne zdalne zarządzanie routerem.

- Interfejs użytkownika działający poprzez WWW: Graficzny interfejs WWW umożliwia prostą konfigurację i zarządzanie urządzeniem. Jest to rozwiązanie przyjazne dla użytkownika, zawiera pomoc online oraz jest wyposażone w funkcje zarządzania dla użytkowników zdalnych, którzy również mają możliwość konfigurowania produktu i zarządzania nim.

- Możliwość aktualizacji oprogramowania sprzętowego: interfejs WWW umożliwia również aktualizację oprogramowania sprzętowego routera do najnowszej wersji.

- Funkcja Quality of Service (QoS) daje użytkownikowi pełną kontrolę nad tym, jaki rodzaj ruchu wychodzącego powinien otrzymać priorytet na routerze, dzięki czemu ważne transmisje, np. pakiety danych pochodzące z gier, informacje o klientach lub dane z zakresu zarządzania zostaną przetworzone przez router z błyskawiczną szybkością – nawet jeżeli jest on pod dużym obciążeniem. Funkcje QoS można konfigurować pod kątem źródłowego adresu IP, docelowego adresu IP, protokołu oraz portu. Można też wyregulować szybkość, z jaką poszczególne rodzaje danych mają przepływać przez router, tak aby np. użytkownicy sieci P2P nie zapełnili całej dostępnej przepustowości w kierunku wysyłania albo aby działania biurowe nie spowodowały zatrzymania pracy klienta WWW. Dodatkowo – albo alternatywnie – można po prostu zmienić priorytety poszczególnych typów wysyłanych danych i zezwolić routerowi na regulowanie poszczególnych szybkości transmisji.

- Szybki dostęp do Internetu: pobieranie danych z prędkością do 24 Mb/s oraz wysyłanie z prędkością do 1 Mb/s. Urządzenie Cerberus ADSL2 Wi-Fi Plus (P6311-6) jest zgodne z następującymi standardami:
  ANSI T1.413 edycja 2,
  ITU-T G.992.1 (G.dmt),
  ITU-T G.992.2 (G.lite),
  ITU-T G.992.3 (ADSL2 G.dmt.bis),

ITU-T G.992.5 (ADSL2+),
ITU-T G.994.1 (G.hs),
Reach Extended ADSL (RE ADSL).

- Obsługa wielu protokołów w zakresie zestawiania połączenia: router obsługuje następujące protokoły w celu nawiązania połączenia z dostawcą usług internetowych (ISP):
  PPPoA (PPP over ATM Adaptation Layer 5 – RFC 2364),
  PPPoE (PPP over Ethernet – RFC 2516)
  RFC 1483/2684 Enkapsulacja poprzez ATM (mostkowana lub routowana),
  Router obsługuje również multipleksowanie typu VC i LLC.

Zawartość pudełka

1. Urządzenie PENTAGRAM Cerberus ADSL2 Wi-Fi Plus (P6331-6)
2. Zasilacz 12 V, 1 A
3. Kabel Ethernet (RJ-45)
4. Kabel telefoniczny (RJ-11)
5. Płyta CD
6. Podręcznik szybkiej instalacji

PENTAGRAM THE PERFECT SIMPLICITY

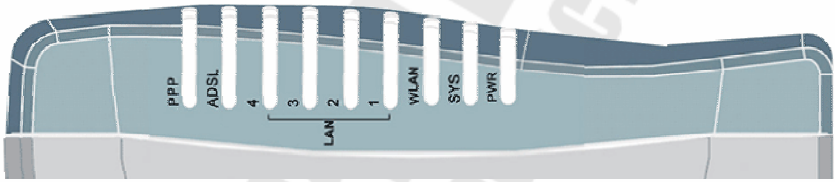
Omówienie produktu

Uwagi

- Nie użytkuj routera w miejscach o podwyższonej temperaturze i wilgotności.
- Nie używaj tego samego źródła do zasilania routera i innych urządzeń.
- Nie otwieraj obudowy ani nie naprawiaj urządzenia samodzielnie. Jeśli router stanie się bardzo gorący, natychmiast wyłącz go z gniazdka zasilającego, a następnie dostarcz do autoryzowanego serwisu w celu naprawy.
- Unikaj użytkowania tego produktu i jego osprzętu na wolnym powietrzu.
- Ustaw router na stabilnej powierzchni.

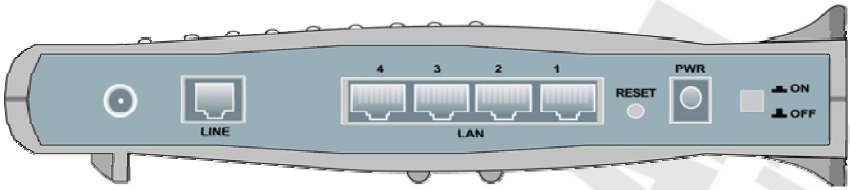
- Używaj tylko zasilacza dołączonego do zestawu. Zastosowanie zasilacza o innym napięciu znamionowym może doprowadzić do uszkodzenia routera.

Panel przedni



Dioda LED	Stan	Opis
PWR	Wyłączona	Brak źródła zasilania urządzenia
	Stałe światło	Urządzenie podłączone do źródła prądu zmiennego
SYS	Stałe światło	System w gotowości
WLAN	Wyłączona	Punkt dostępowy jest wyłączony
	Stałe światło	Punkt dostępowy jest włączony
	Migotanie	Wysyłanie lub odbiór danych
LAN (1-4)	Wyłączona	Brak połączenia Ethernet
	Stałe światło	Urządzenie podłączone do portu Ethernet
	Migotanie	Wysyłanie lub odbiór danych
ADSL	Wyłączona	Brak sygnału ADSL
	Stałe światło	Uzyskano sygnał ADSL
	Migotanie	Uzyskiwanie sygnału ADSL
PPP	Stałe światło	Nawiązano połączenie PPPoA / PPPoE

Panel tylny



Oznaczenie	Zastosowanie...
Złącze RP-SMA	Podłączenie zewnętrznej anteny
LINE (RJ-11)	Podłączanie kabla telefonicznego
LAN 1-4 (RJ-45)	Łączenie z komputerami (lub innymi urządzeniami) za pomocą kabla Ethernet
RESET	Resetowanie urządzenia
PWR	Gniazdo zasilacza dołączonego do zestawu
ON/OFF	Przełącznik do włączania i wyłączania urządzenia

Ustawienia domyślne

Przed zmianą konfiguracji należy zaznajomić się z następującymi ustawieniami domyślnymi.

Adres IP	192.168.1.100
Maska podsieci	255. 255. 255.0
SSID	Pentagram P 6331-6
Serwer DHCP	Włączony
Pula adresów IP serwera DHCP	100 adresów IP, począwszy od 192.168.1.101
Czas dzierżawy adresu IP	43200 sekund (12 godzin)
Nazwa użytkownika	**admin**
Hasło	**pentagram**

Zalecamy jak najszybszą zmianę nazwy użytkownika i hasła.
W przypadku utraty hasła logowania, istnieje możliwość przywrócenia domyślnych fabrycznych ustawień urządzenia. Procedura ta jest opisana na następnej stronie.

Resetowanie routera

- Włącz router i odczekaj ok. 2 minuty, aby inicjalizacja urządzenia dobiegła końca
- Przytrzymaj wciśnięty przycisk **RESET**, tak aby wszystkie diody LED wyłączyły się, włączyły i na powrót wyłączyły. Router dokona przywrócenia ustawień fabrycznych i uruchomi się ponownie. Następnie możesz uzyskać do niego dostęp za pomocą interfejsu WWW.

Podłączanie urządzenia Cerberus do komputera

Cerberus może być podłączony do komputera na dwa różne sposoby:

Podłączanie przez port Ethernet (karta sieciowa)

Wszystkie porty Ethernetowe routera wykonane są w technologii umożliwiającej automatyczne włączenie autoprzeplotu, jeśli jest wymagany. Router automatycznie dobierze maksymalną dostępną prędkość połączenia dzięki funkcji autonegocjacji prędkości. Transmisja z prędkością 10/100 Mb/s wymaga kabla kategorii 5 z zaciśniętymi przewodami we wtyczce 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 auto-diagnostyki portu oraz negocjację prędkości połączenia.

Podłączenie przez interfejs WLAN (karta bezprzewodowa)

Aby możliwe było połączenie Cerberusa za pomocą sieci bezprzewodowej, karta WLAN musi być poprawnie zainstalowana w systemie, Cerberus musi znajdować się w zasięgu pracy karty bezprzewodowej komputera oraz należeć do tej samej podsieci.

Konfiguracja protokołu TCP/IP

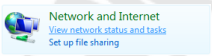
Po podłączeniu komputera do routera (LAN lub WLAN), należy skonfigurować w systemie protokół TCP/IP. Protokół ten powinien być automatycznie instalowany przez system podczas instalacji sterowników karty sieciowej. Zaleca się skonfigurowanie protokołu TCP/IP tak, aby adres IP i inne parametry połączenia były pobierane z serwera DHCP routera. Poniżej opisana jest taka konfiguracja dla różnych systemów Windows.

Uwaga: W niektórych przypadkach system komputer z zainstalowanym systemem Windows Vista lub Windows XP z Service Pack 3 nie może uzyskać adresu IP z serwera DHCP routera. Aby rozwiązać ten problem, 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).

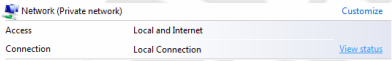
Windows Vista

Uwaga: Konfiguracja sieci wymaga uprawnień administracyjnych. Jeśli pojawi się okno *Kontrola konta użytkownika*, kliknij Kontynuuj (konto typu Administrator) lub wybierz konto typu Administrator i wpisz poprawne hasło (konto typu Użytkownik standardowy).

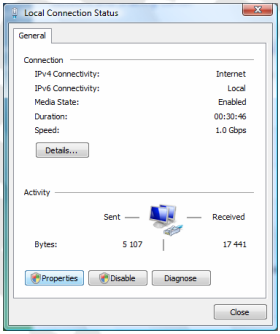
1. Kliknij **Start** → **Panel sterowania**.



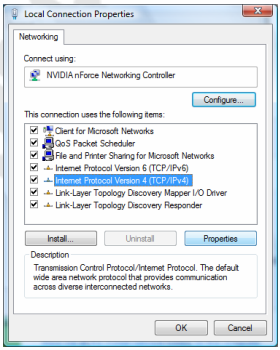
2. Kliknij **Wyświetl stan sieci i zadania**.
3. Kliknij **Wyświetl stan** dla właściwego połączenia.



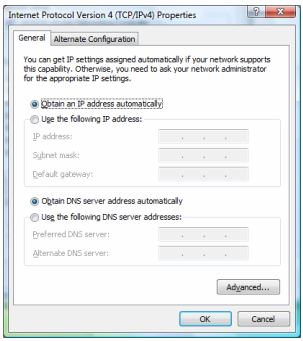
4. Na zakładce **Ogólne** kliknij **Właściwości**.



5. Na zakładce **Ogólne** zaznacz **Protokół internetowy w wersji 4 (TCP/IPv4)** i kliknij **Właściwości**.



6. Na zakładce **Ogólne** zaznacz **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**.
7. Kliknij **OK**, aby zapisać ustawienia i zamknąć okno **Właściwości: Protokół internetowy w wersji 4 (TCP/IPv4)**.



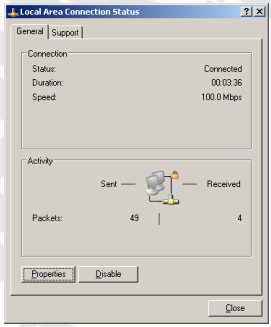
Windows 2000/XP

1. Kliknij **Start** → **Ustawienia** → **Panel sterowania**.

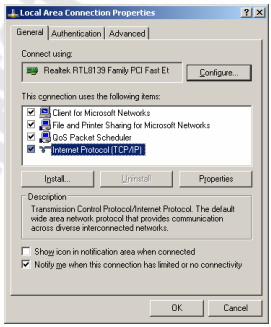
2. Dwukrotnie kliknij na ikonie **Połączenia sieciowe** (2000/XP widoku klasycznym) lub **Połączenia sieciowe i internetowe** a następnie **Połączenia sieciowe** (XP w widoku domyślnym).

3. Dwukrotnie kliknij na **Połączenie lokalne**.

4. Na zakładce **Ogólne** kliknij **Właściwości**.

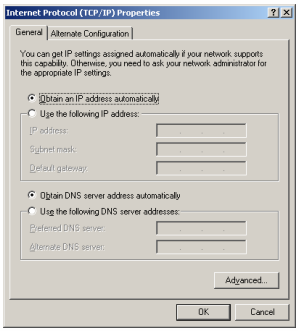


5. Na zakładce **Ogólne** zaznacz **Protokół internetowy (TCP/IP)** i kliknij **Właściwości**.



6. Na zakładce **Ogólne** zaznacz **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**.

7. Kliknij **OK**, aby zapisać ustawienia i zamknąć okno **Właściwości: Protokół internetowy (TCP/IP)**.

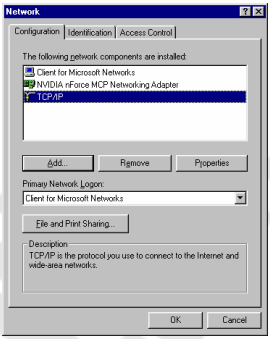


Windows 95/98/Me

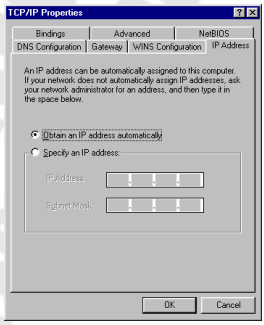
1. Kliknij **Start** → **Ustawienia** → **Panel sterowania**.

2. Dwukrotnie kliknij na ikonie **Sieć**.

3. Na zakładce **Konfiguracja** zaznacz **TCP/IP** dla właściwej karty sieciowej i kliknij **Właściwości**.

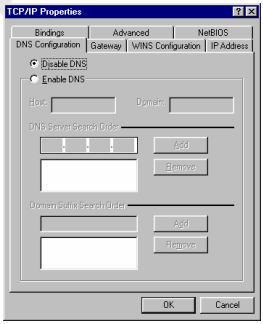


4. Na zakładce **Adres IP** zaznacz opcję **Automatycznie uzyskaj adres IP**.



5. Na zakładce **Konfiguracja DNS** zaznacz **Wyłącz DNS**

6. Kliknij **OK**, aby zapisać ustawienia i zamknąć okno **Właściwości Protokół TCP/IP**.



Aby sprawdzić czy karta posiada właściwy adres IP:

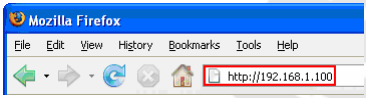
1. kliknij **Start** > **Uruchom**
2. wpisz **cmd** (Win 2000/XP) lub **command** (Win 98/ME) i naciśnij Enter
3. wpisz w linię poleceń **ipconfig /all** i naciśnij Enter
4. sprawdź czy wpis **IP Address** dla odpowiedniej karty sieciowej ma wartość **192.168.1.x**

Konfiguracja routera poprzez przeglądarkę WWW

Router Cerberus ADSL2 Wi-Fi Plus (P6331-6) może zostać skonfigurowany za pomocą przeglądarki internetowej, która zazwyczaj jest zintegrowana z systemem operacyjnym. Router jest obsługiwany za pomocą przejrzystego, prostego interfejsu.

Logowanie

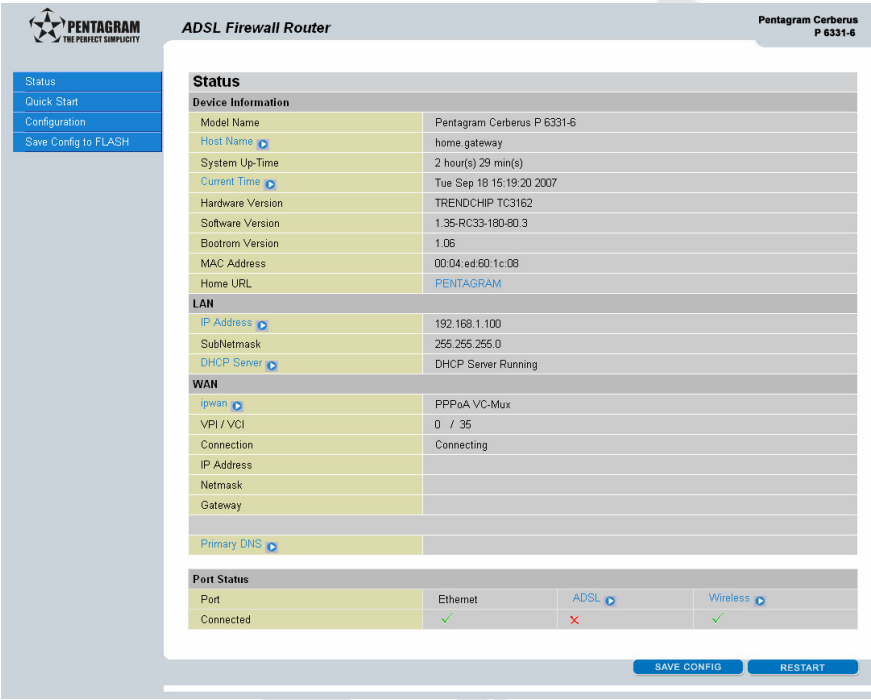
1. Uruchom przeglądarkę WWW
2. W pasku adresu wpisz domyślny adres IP: **http://192.168.1.100**



3. Wpisz nazwę użytkownika i hasło – domyślnie: **admin** / **pentagram**

PENTAGRAM THE PERFECT SIMPLICITY

Nawigacja



Przyciski

- **Save Settings (Zapisz ustawienia)** – Przycisk otwiera stronę zapisu konfiguracji do pamięci flash.
- **Restart Router (Ponownie uruchom router)** – Przycisk otwiera stronę ponownego uruchomienia.

Zakładki

Interfejs WWW zawiera następujące zakładki:

- **Status (Stan) - ARP Table (Tablica ARP), Wireless Association (Skojarzenia sieci bezprzewodowej), Routing Table (Tablica routingu), DHCP Table (Tablica DHCP), System Log (Dziennik systemowy), Security Log (Dziennik bezpieczeństwa)**
- **Quick Start (Szybkie uruchomienie)**
- **Configuration (Konfiguracja) – LAN (Sieć lokalna), WAN (Sieć rozległa), System, Firewall (Zapora sieciowa), QoS, Virtual Server (Serwer wirtualny), Advanced (Zaawansowane)**
- **Save Config to FLASH (Zapis konfiguracji do pamięci flash)**

Zakładka Status

Status	
Device Information	
Model Name	Pentagram Cerberus P 6331-6
Host Name	home.gateway
System Up-Time	2 hour(s) 29 min(s)
Current Time	Tue Sep 18 15:19:20 2007
Hardware Version	TRENDCHIP TC3162
Software Version	1.35-RC33-180-80.3
Bootrom Version	1.06
MAC Address	00:04:ed:60:1c:08
Home URL	PENTAGRAM
LAN	
IP Address	192.168.1.100
SubNetmask	255.255.255.0
DHCP Server	DHCP Server Running
WAN	
ipwan	PPPoA VC-Mux
VPI / VCI	0 / 35
Connection	Connecting
IP Address	
Netmask	
Gateway	
Primary DNS	

Port Status			
Port	Ethernet	ADSL	Wireless
Connected	✓	✗	✓

Device Information

- **Host Name (Nazwa hosta)** – Pole zawiera nazwę routera nadawaną do potrzeb identyfikacji. Pole to umożliwia zmianę nazwy routera.

Host Name	
Device Host Name	
Host Name	home.gateway
Apply	

- **System Up-Time (Czas pracy systemu)** – Pole rejestruje czas niezakłóconej pracy systemu.
- **Current Time (Aktualny czas)** – Opcja służąca do ustawienia aktualnej godziny. Bliższe informacje – zob. ustęp poświęcony strefom czasowym.
- **Hardware Version (Wersja sprzętu)** – Wersja układu sprzętowego
- **Software Version (Wersja oprogramowania)** – Wersja oprogramowania sprzętowego
- **LAN MAC Address (Adres MAC sieci LAN)** – Adres MAC sieci lokalnej
- **WAN MAC Address (Adres MAC sieci WAN)** – Adres MAC sieci rozległej
- **Home URL (Adres strony domowej)** – Opcja nawiązuje połączenie ze stroną domową.

LAN

- **IP Address (Adres IP)** – Adres IP portu sieci lokalnej.
- **Sub Net Mask (Maska podsieci)** – Maska podsieci IP portu sieci lokalnej.
- **DHCP Server (Serwer DHCP)** – Rola DHCP portu sieci lokalnej – Server (serwer), Relay (przekaźnik) lub None (brak).

WAN

- **IP WAN** – Nazwa połączenia WAN.
- **VPI/VCI** – Identyfikatory Virtual Path Identifier oraz Virtual Channel Identifier
- **Connection (Połączenie)** – Wybór opcji „Disconnected" (brak połączenia) lub „Connected" (połączenie).
- **IP Address (Adres IP)** – Adres IP portu sieci rozległej.
- **Net mask (Maska sieci)** – Maska podsieci IP portu sieci rozległej.
- **Gateway (Brama)** – Adres IP bramy domyślnej.

Port status

Użytkownik może tu sprawdzić stan swoich połączeń.

Status / ARP Table

Tablica ARP (Address Resolution Protocol) routera przedstawia przypisanie adresów internetowych (IP) do adresów Ethernet (MAC). Jest to dobry sposób na szybkie ustalenie adresów MAC interfejsu sieciowego swoich komputerów w celu wykorzystania ich do potrzeb funkcji **Firewall – MAC Address Filter (Zapora sieciowa – filtr adresów MAC)** routera. Bliższe informacje można znaleźć w rozdziale niniejszej instrukcji poświęconym zaporze sieciowej.

ARP Table			
IP <> MAC List			
IP Address	MAC Address	Interface	Static
192.168.1.101	00:0E:2E:00:11:5F	iplan	No
192.168.1.102	00:0C:76:73:00:51	iplan	No

- **IP Address (Adres IP)** – Lista adresów IP urządzeń w sieci lokalnej.
- **MAC Address (Adres MAC)** – Adres MAC (Media Access Control) każdego urządzenia w sieci lokalnej.
- **Interface (Interfejs)** – Nazwa interfejsu (w routerze), z którym łączy się dany adres IP.
- **Static (Stan statyczny)** – Stan statyczny pozycji tablicy ARP:
  no (nie) dla dynamicznie generowanych pozycji tablicy ARP
  yes (tak) dla statycznych pozycji tablicy ARP dodanych przez użytkownika

Status / Wireless Association

Wireless Association Table	
Wireless client's MAC address and the corresponding IP address	
IP Address	MAC
192.168.1.101	00:0E:2E:00:11:5F

IP Address (Adres IP) – Adres IP klienta bezprzewodowego, który dołącza do sieci.
MAC – Adres MAC klienta bezprzewodowego.

Status / Routing Table

Routing Table

Routing Table

#	Destination	Netmask	Gateway/Interface	Cost		
1	239.255.255.250	255.255.255.255	0.0.0.0/iplan	0	Edit	Delete
2	192.168.1.0	255.255.255.0	0.0.0.0/iplan	0	Edit	Delete

Create

Static Route

Add Rule3

Destination			
Netmask			
Gateway		Interface	Please Select
Cost	0		

Apply Cancel

 # (Nr) – Numer pozycji
Destination (Punkt docelowy) – Adres IP sieci docelowej.
Netmask (Maska sieci) – Adres maski sieci docelowej.
Gateway/Interface (Brama/intefejs) – Adres IP bramy lub istniejącego interfejsu, jakiego używa dana trasa.
Cost (Koszt) – Koszt transmisji dla potrzeb routingu. Podana wielkość nie musi być precyzyjna, ale powinna się mieścić w przedziale od 0 do 65535.
Interface (Interfejs) – Wybór interfejsu, za pomocą którego przesyłane są pakiety.

Status / DHCP Table

DHCP Table

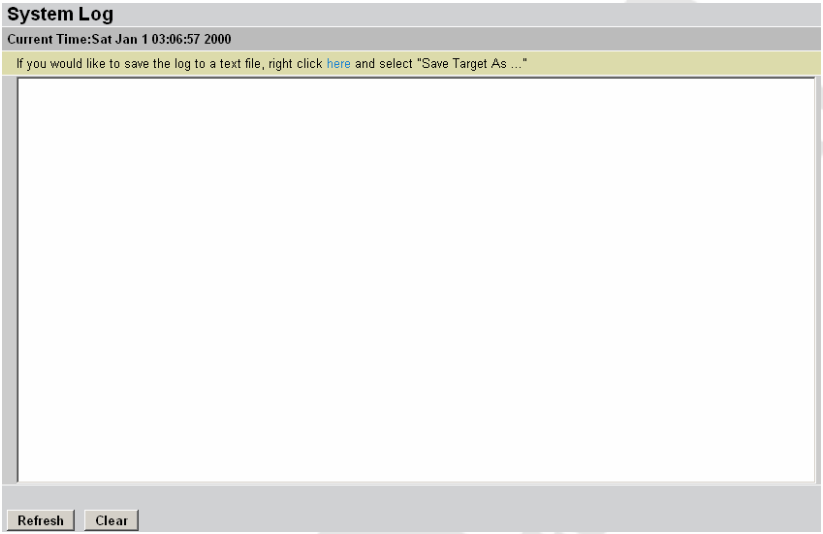
Leased Table

IP Address	MAC Address	Client Host Name	Register Time
192.168.1.101	00:0e:2e:00:11:5f	PENTLAB_05	2000/01/01 02:29:32 - 2000/01/01 14:29:32
192.168.1.102	00:0c:76:73:00:51	PENTLAB_02	2000/01/01 00:49:25 - 2000/01/01 12:49:25

Leased (Dzierżawa) – Informacje o adresach IP przydzielonych przez DHCP.
IP Address (Adres IP) – Adresy IP urządzeń w sieci lokalnej.
MAC Address (Adres MAC) – Adres MAC, do którego przydzielany jest stały adres IP
Client Host Name (Nazwa hosta klienta) – Informacje o przedawnionych adresach IP
Register Time (Czas rejestracji) – Dane o czasie rejestracji

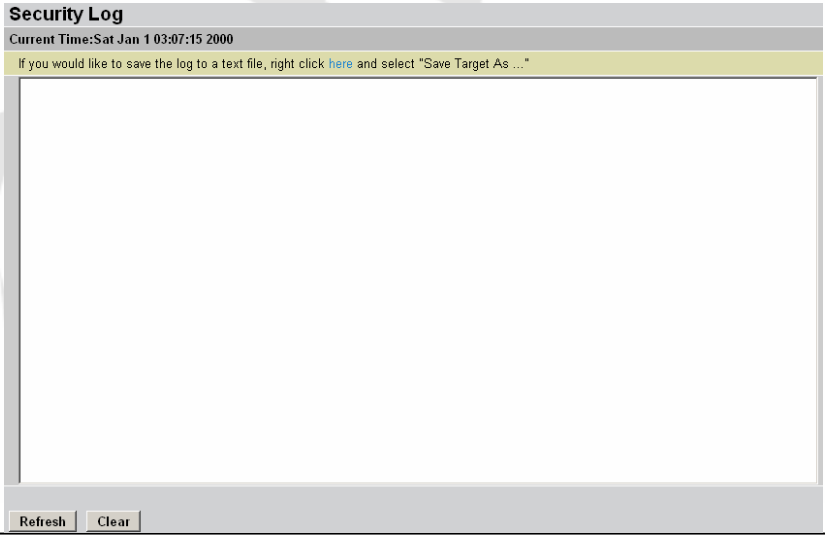
Status / System Log

Zakładka wyświetla dzienniki systemowe nagromadzone aż do chwili bieżącej. Dzięki tej funkcji można prześledzić informacje historyczne.



Status / Security Log

Ten ekran przedstawia dane z dziennika bezpieczeństwa. Jeżeli serwer zostanie zaatakowany przez hackera, funkcja zapory wyodrębnia odpowiednie dane, które zostają zapisane przez router. Dzięki nim można ustalić, skąd atakował hacker.

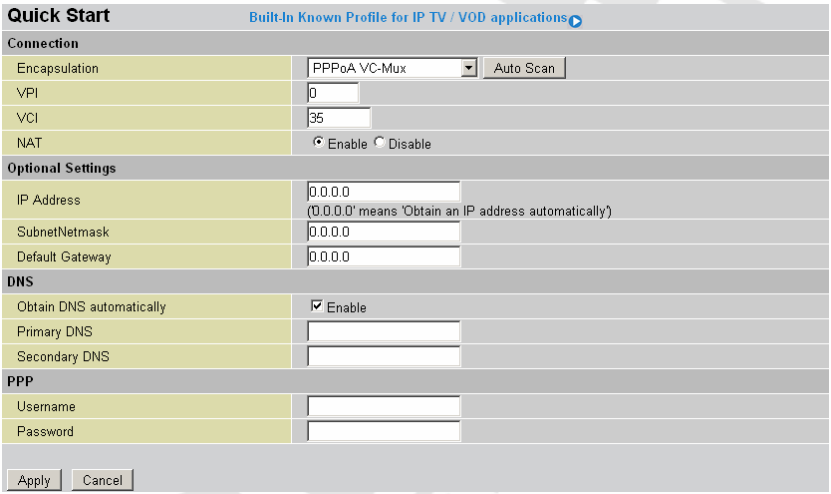


Zakładka Quick Start

Szczegółowe informacje na temat konfiguracji ustawień WAN można znaleźć w rozdziale **WAN** w niniejszej instrukcji.

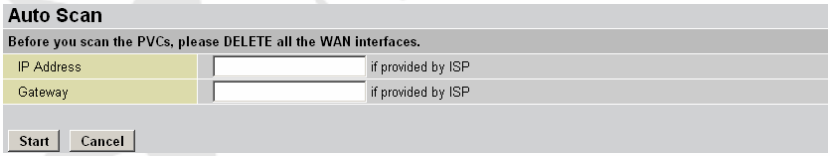
Informacje, które będą potrzebne kreatorowi Szybkiego Uruchomienia w celu ustanowienia łączności, to: nazwa użytkownika (zazwyczaj w postaci nazwaużytkownika@nazwadostawcyusługinternetowych), hasło oraz typ enkapsulacji.

Dostawca usług internetowych powinien dostarczyć wszystkie niezbędne informacje. Alternatywnie, jeżeli usunięto bieżące Połączenie WAN w sekcji **WAN – ISP (WAN – Dostawca usług internetowych)** interfejsu, można użyć funkcji PVC Scan routera w celu wykrycia typu enkapsulacji używanego przez dostawcę usług.



Connection (Połączenie)

Encapsulation (Enkapsulacja) – Wybierz rodzaj enkapsulacji stosowanej przez dostawcę usług internetowych lub opcję **Auto Scan (Sprawdzenie automatyczne)**.



Kliknij przycisk **Start**, aby rozpocząć sprawdzenie typów enkapsulacji oferowanej przez dostawcę usług internetowych. Jeżeli sprawdzenie przebiegnie pomyślnie, na ekranie pojawi się lista obsługiwanych opcji.

VCI – Wpisz przydzielony identyfikator VCI. Pole to może już być skonfigurowane.
VPI – Wpisz przydzielony identyfikator VPI. Pole to może już być skonfigurowane.
NAT – Wybierz wartość „Enabled” (włączone) lub „Disabled” (wyłączone).

Optional Setting (Ustawienia opcjonalne)

IP Address (Adres IP) – W polu tekstowym Adres IP wpisz adres IP przydzielony przez dostawcę usług internetowych.

Subnet Mask (Maska podsieci) – Wpisz maskę podsieci w notacji dziesiętnej rozdzielonej kropkami.

Default Gateway (Brama domyślna) – W tym miejscu należy określić adres IP bramy (podany przez dostawcę usług internetowych).

DNS

Obtain DNS automatically (Uzyskaj DNS automatycznie) – Zaznacz to pole, aby korzystać z DNS.

Primary DNS (DNS podstawowy) – Wpisz adresy IP serwerów DNS. Serwery DNS są przekazywane do klientów DHCP wraz z adresami IP oraz maską podsieci.

Secondary DNS (DNS drugorzędny) – Wpisz adresy IP serwerów DNS. Serwery DNS są przekazywane do klientów DHCP wraz z adresami IP oraz maską podsieci.

PPP

Username (Nazwa użytkownika) – Wpisz nazwę użytkownika podaną przez dostawcę usług internetowych. Można tu wpisać do 128 znaków alfanumerycznych (wielkość liter ma znaczenie). Nazwa ma zazwyczaj format „nazwaużytkownika@nazwadostawcyusługinternetowych” zamiast po prostu „nazwa użytkownika”.

Password (Hasło) – Wpisz hasło podane przez dostawcę usług internetowych. Można tu wpisać do 128 znaków alfanumerycznych (wielkość liter ma znaczenie).

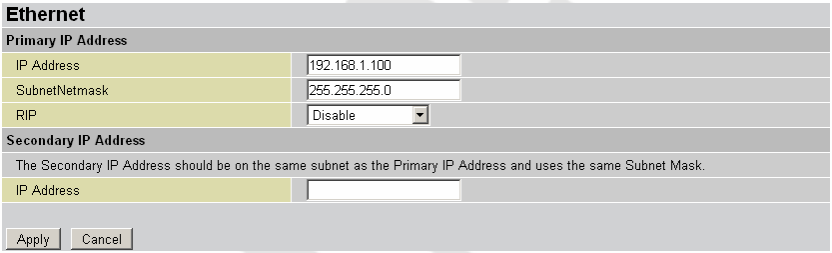
Zakładka Configuraton

Kliknij tę pozycję, aby uzyskać dostęp do następujących obszarów konfiguracji routera ADSL: **LAN (Sieć lokalna)**, **WAN (Sieć rozległa)**, **System**, **Firewall (Zapora sieciowa)**, **QoS**, **Virtual Server (Serwer wirtualny)** oraz **Advanced (Zaawansowane)**. Funkcje te są szczegółowo opisane w kolejnych podrozdziałach.

Configuration / LAN

Sieć lokalna (LAN) to współużytkowany system łączności, do którego jest podłączonych wiele komputerów i który jest ograniczony po względem przestrzennym, zazwyczaj do obrębu jednego budynku lub piętra.
W sekcji poświęconej sieci lokalnej znajdują się cztery obszary: **Ethernet**, **Wireless (Sieci bezprzewodowe)**, **Wireless Security (Bezpieczeństwo sieci bezprzewodowych)** oraz **DHCP Server (Serwer DHCP)**.

- **Ethernet**
  Router obsługuje dwa adresy IP Ethernetu w sieci lokalnej oraz dwie różne podsieci LAN, poprzez które można równocześnie uzyskiwać dostęp do Internetu. Użytkownicy mają zazwyczaj w swojej sieci lokalnej tylko jedną podsieć, toteż nie ma potrzeby definiowania drugorzędnego adresu IP. Domyślny adres IP routera to 192.168.1.254.



RIP – RIP v1, RIP v2, RIP v1+v2 oraz RIP v2 Multicast.

Uwaga: Maska podsieci drugorzędnego adresu IP jest uzależniona od ustawienia podstawowego adresu IP.

- ## Wireless

Wireless	
Parameters	
WLAN service	◉ Enable ○ Disable
Mode	802.11b+g
ESSID	Pentagram P 6331-6
Hide ESSID	○ Enable ◉ Disable
Regulation Domain	Europe
Channel ID	Channel 1 (2.412 GHz)
WMM (QOS)	◉ Enable ○ Disable
WMM-APSD	○ Enable ◉ Disable
MAC Address	00:13:D3:71:CD:86
AP Version	RT2561T 1.0.8.0-3
Wireless Distribution System (WDS)	
WDS Service	○ Enable ◉ Disable
1.Peer WDS MAC Address	
2.Peer WDS MAC Address	
3.Peer WDS MAC Address	
4.Peer WDS MAC Address	
** WDS depends on the settings of main security encrption type. **	
Apply	Cancel

Mode (Tryb) – 802.11b+g (Tryb mieszany), 802.11b i 802.11g. Domyślne ustawienie fabryczne to 802.11b+g.
ESSID – W tym miejscu wpisz niepowtarzalny identyfikator przydzielony punktowi dostępowemu, wbudowanemu w interfejs sieci bezprzewodowych routera. W celu połączenia z tym urządzeniem klienty powinny mieć taki sam numer ESSID jak urządzenie.
Regulation Domain (Domena regulacyjna) – Można tu wybrać jedną z pięciu domen regulacyjnych: Ameryka Północna, Europa, Francja itd. Ustawienie to wpływa na kształt identyfikatora kanału.
Channel ID (Identyfikator kanału) – Wybierz identyfikator kanału, którego chcesz używać.
MAC Address (Adres MAC) – Adres MAC punktu dostępowego
AP Version (Wersja AP) – Wersja oprogramowania sprzętowego punktu dostępowego.

Wireless Distribution System (WDS)

Jest to tryb pracy bezprzewodowego punktu dostępowego, umożliwiający bezprzewodową łączność z innymi punktami dostępowymi. Jego instalacja jest bardzo prosta: wystarczy zdefiniować adres MAC dołączanego punktu dostępowego. Mechanizm WDS gwarantuje oszczędność i elastyczność, gdyż daje możliwość połączenia dwóch punktów dostępowych bez żadnego dodatkowego bezprzewodowego urządzenia klienckiego, co z kolei pozwala łatwo rozbudowywać posiadaną infrastrukturę przewodową lub bezprzewodową, tak aby powiększyć swoją sieć.
Dodatkowo, mechanizm WDS gwarantuje bezpieczeństwo łączy za pomocą technologii WEP. W takim wypadku szyfrowanie klucza WEP dla obydwóch punktów dostępowych musi być jednakowe.

WDS Service (Usługa WDS) – Ustawienie domyślne to Disable (wyłączona). Zaznacz pole Enable (włączona), aby uaktywnić tę funkcję.
Peer WDS MAC Address (Adres MAC WDS urządzenia równorzędnego) – Adres MAC dołączanego punktu dostępowego. Istotne jest również, aby w konfiguracji

docelowego punktu dostępowego również zawrzeć adres MAC tego urządzenia, tak aby mogły one się rozpoznać i nawiązać łączność.

Uwaga: W adresach MAC należy pamiętać o użyciu dwukropka (:).

- **Wireless Security**

Istnieje możliwość włączenia lub wyłączenia mechanizmów WPA lub WEP zabezpieczających sieć bezprzewodową. Domyślnie zabezpieczenia łączności bezprzewodowej są: **wyłączone**.

Wireless Security	
Parameters	
Security Mode	Disable
Apply	Cancel

WPA Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA Pre-Shared Key
WPA Algorithm	TKIP
WPA Shared Key	0000000000
Group Key Renewal	3600 Seconds
Apply	Cancel

WPA Algorithm (Algorytm WPA) – Protokół TKIP (Temporal Key Integrity Protocol) wykorzystuje efektywne metody szyfrowania oraz zawiera kod Message Integrity Code (MIC) w celu zapewnienia ochrony przed hackerami.
WPA Shared Key (Klucz udostępniany WPA) – Klucz uwierzytelnienia sieciowego. Wpisane hasło powinno liczyć od 8 do 63 znaków (wielkość liter ma znaczenie).
Group Key Renewal (Odnowienie klucza grupowego) – Okres odnowienia określający termin zmiany klucza zabezpieczającego pomiędzy klientem bezprzewodowym a punktem dostępowym.

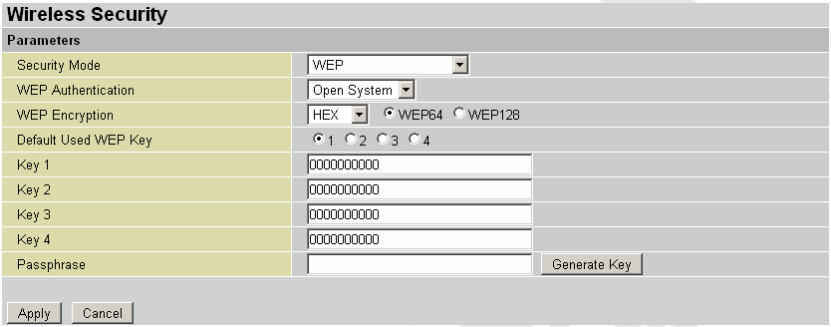
WPA2 Pre-Shared Key

Wireless Security	
Parameters	
Security Mode	WPA2 Pre-Shared Key
WPA2 Algorithm	TKIP
WPA2 Shared Key	0000000000
Group Key Renewal	3600 Seconds
Apply	Cancel

WPA2 Algorithm (Algorytm WPA2) – Protokół TKIP (Temporal Key Integrity Protocol) wykorzystuje efektywne metody szyfrowania oraz zawiera kod Message Integrity Code (MIC) w celu zapewnienia ochrony przed hackerami.
WPA2 Shared Key (Klucz udostępniany WPA2) – Klucz uwierzytelnienia sieciowego. Wpisane hasło powinno liczyć od 8 do 63 znaków (wielkość liter ma znaczenie).

Group Group Key Renewal (Odnowienie klucza grupowego) – Okres odnowienia określający termin zmiany klucza zabezpieczającego pomiędzy klientem bezprzewodowym a punktem dostępowym.

WEP



WEP Encryption (Szyfrowanie WEP) – W celu uniemożliwienia nieuprawnionym odbiorcom bezprzewodowym dostępu do danych przesyłanych w sieci, router oferuje bezpieczne szyfrowanie danych WEP. Jeżeli użytkownik oczekuje wysokiego stopnia bezpieczeństwa, może wybrać jedną z dwóch alternatyw: **WEP 64** lub **WEP 128**. WEP 128 jest mechanizmem o silniejszych zabezpieczeniach niż WEP 64.
Passphrase (Wyrażenie-hasło) – Opcja ta służy do automatycznego generowania klucza WEP na podstawie wpisanego ciągu oraz zdefiniowanego algorytmu mechanizmów WEP64 lub WEP128. Ten sam ciąg można wpisać w punkcie dostępowym oraz na kliencie i doprowadzi to do wygenerowania takich samych kluczy WEP. Należy pamiętać, że przy włączeniu opcji **Passphrase** nie ma potrzeby wypełniania pól **Key (1-4)**.
Key (1-4) (Klucz 1-4) – Wpisz klucz szyfrujący dane bezprzewodowe. W celu umożliwienia transmisji zaszyfrowanych danych, wartości klucza szyfrowania WEP na wszystkich stanowiskach bezprzewodowych muszą być identyczne jak na routerze. Istnieje możliwość wyboru czterech kluczy. Klucze są wpisywane w formacie szesnastkowym liczącym 5 albo 13 liczb w trybach, odpowiednio, WEP64 albo WEP128. Separatorem liczb jest znak „-”. Przykładowo, przy zastosowaniu WEP64, klucz 11-22-33-44-55 jest prawidłowy, natomiast 1122334455 będzie nieprawidłowy.
Hide ESSID (Ukryj ESSID) – Użytkownik może ukryć lub ujawnić identyfikator ESSID.

- ## DHCP Server

Istnieje możliwość włączenia lub wyłączenia serwera DHCP (Dynamic Host Configuration Protocol) albo włączenia funkcji przekaźnika DHCP routera. Protokół DHCP pozwala routerowi na dynamiczne przydzielanie adresów komputerom w sieci, o ile są one skonfigurowane do automatycznego uzyskiwania adresów IP.

DHCP Server	
Configuration	
DHCP Server Mode	○ Disable ◉ DHCP Server ○ DHCP Relay Agent
Next	

DHCP Server Status	
Status	DHCP Server Running
Subnet Definitions	
Subnet Value	192.168.1.0
SubnetNetmask	255.255.255.0
Domain Name	home.gateway
DNS Server	192.168.1.100
Maximum/Default Lease Time	86400 / 43200 seconds
IP Range	192.168.1.100 - 192.168.1.199

W celu wyłączenia Serwera DHCP routera zaznacz pole **Disabled (Wyłączony)**, kliknij przycisk **Next (Dalej)**, a potem **Apply (Zastosuj)**. Kiedy Serwer DHCP jest wyłączony, należy ręcznie przydzielić stały adres IP każdemu komputerowi w sieci i wskazać adres IP routera jako domyślną bramę dla każdego komputera (domyślnie jest to adres 192.168.1.254).

DHCP
Disable server and relay agent
The DHCP server and relay agent will be disabled.
Apply Cancel

W celu konfiguracji Serwera DHCP routera zaznacz pole **DHCP Server (Serwer DHCP)** i przycisk **Next (Dalej)**. Możesz następnie skonfigurować parametry Serwera DHCP, w tym pulę adresów IP (początkowy i końcowy adres IP puli, jaka ma być przydzielana komputerom w sieci), czas dzierżawy dla każdego przydzielonego adresu IP (okres, przez jaki przydział adresu IP będzie obowiązywał), adres IP DNS oraz adres IP bramy. Dane takie są przesyłane do klienta DHCP (tzn. komputera), kiedy zgłosi on do serwera DHCP żądanie przydziału adresu IP. Kliknij przycisk **Apply (Zastosuj)**, aby włączyć tę funkcję. Jeżeli zaznaczysz pole **Use Router as a DNS Server (Używaj routera jako serwera DNS)**, router ADSL sprawdzi nazwę domeny, automatycznie wyszuka adres IP w sieci zewnętrznej i przekaże go do komputera w sieci lokalnej, który zgłosił takie żądanie.

DHCP SERVER

Parameters

Domain Name	home.gateway	
Use Router as DNS Server	☑	
Primary DNS Server Address	192.168.1.100	
Secondary DNS Server Address		
Default Lease Time	43200	seconds
Maximum Lease Time	86400	seconds
Range Start	192.168.1.101	
Range End	192.168.1.200	
TFTP Server Name(Option 66)		

Specify fixed Mac Address Mapping to fixed IP Address (optional)

****Please note that the IP Address can only be set within the IP *Range Start* and IP *Range End* specified above in the DHCP SERVER Paremeters**

	Host Name	MAC Address	IP Address
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

The MAC address is represented as a string of 2 digit hexadecimal numbers seperated by colons (:) - (eg. 00:11:22:33:44:55)

Apply Cancel

Jeżeli zaznaczysz pole **DHCP Relay Agent (Przekaźnik DHCP)** i klikniesz **Next (Dalej)**, w następnej kolejności musisz wpisać adres IP serwera DHCP, który będzie przydzielał adresy IP klientowi DHCP w sieci lokalnej. Funkcję tę należy stosować wyłącznie, jeżeli tak zaleca administrator sieci lub dostawca usług internetowych. Kliknij przycisk **Apply (Zastosuj)**, aby włączyć tę funkcję.

DHCP Relay

Parameters

DHCP Relay Server	

Apply Cancel

Configuration / WAN

WAN (Wide Area Network, sieć rozległa) to zewnętrzne połączenie z inną siecią lub Internetem. Sekcja WAN mieści trzy obszary: **ISP**, **DNS** oraz **ADSL**.

- **ISP**
  Wartość domyślna to PPPoA. Jeżeli dostawca usług internetowych wykorzystuje ten protokół dostępowy, kliknij przycisk **Edit (Edycja)** i wpisz pozostałe parametry określone poniżej. Jeżeli dostawca usług internetowych nie używa protokołu PPPoA, można zmienić domyślną wartość pola WAN za pomocą przycisku **Change (Zmień)**.
  Prostszą alternatywą jest wybór opcji **Quick Start (Szybkie uruchomienie)** z menu głównego po lewej stronie. Bliższe informacje na ten temat można znaleźć w rozdziale **Quick Start (Szybkie uruchomienie) w** niniejszej instrukcji.

Main WAN Connection

Main WAN Connection Configuration

Name	Description	Creator	VPI	VCI		
PPPoA Routed	PPPoA	admin	0	35	Edit	Change

Changing wan service will save your configuration to flash and immediately restart the router.

Other WAN Bridge Connection

Bridged WAN connection List

Name	Description	Creator	VPI	VCI		

Create

Built-In Known Profile for IP TV / VOD applications

0: Standard Default;Auto PVC, WAN-DHCP, LAN NAT -DHCP

Apply Cancel

Changing IP TV / VOD type will save your configuration to flash and immediately restart the router.

RFC 1483 Routed Connections

WAN Connection

RFC 1483 Routed

Description	1483_Routed_mode	
VPI	0	
VCI	35	
NAT	Enable Disable	
Encapsulation Method	LLC Bridged	
IP Assignment	Obtain an IP address automatically via DHCP client	
	Use the following IP address	
	IP Address	
	Netmask	
	Gateway	
RIP	Disable	

Apply Cancel

Description (Opis) – Dowolny opis połączenia, wpisywany przez użytkownika.
VPI / VCI – W tym polu wpisz odpowiednie dane dostarczone przez dostawcę usług internetowych.
NAT – Funkcja NAT (Network Address Translation, translacja adresów sieciowych) umożliwia podłączenie do Internetu wielu użytkowników za pomocą jednego konta IP

współdzielącego ten sam adres IP. Jeżeli użytkownicy w sieci lokalnej mają publiczne adresy IP i mogą bezpośrednio uzyskiwać dostęp do Internetu, funkcję NAT można wyłączyć.

Encapsulation method (Metoda enkapsulacji) – Wybierz format enkapsulacji; ustawienie domyślne to typ LLC Bridged (LLC mostkowany). Wprowadź tu ustawienie podane przez dostawcę usług internetowych.

DHCP client (Klient DHCP) – Włączenie lub wyłączenie klienta DHCP. W ten sposób można określić, czy router powinien automatycznie uzyskiwać adres IP od dostawcy usług internetowych, czy też nie.

Zaznacz pole **Obtain an IP address automatically via DHCP client (Uzyskuj adres IP automatycznie poprzez klienta DHCP)**, aby włączyć funkcję klienta DHCP, albo też wybierz opcję **Specify an IP address (Określ adres IP)**, aby wyłączyć klienta DHCP i ręcznie określać adres IP. Ustawienie tego parametru powinno zostać określone przez dostawcę usług internetowych.

RIP – RIP v1, RIP v2, RIP v1+v2 oraz RIP v2 Multicast.

PPPoA Routed Connections

PPPoA oznacza to skrót określający protokół Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). Udostępnia on możliwości kontroli dostępu i funkcje bilingowe w sposób zbliżony do usług dostępu wdzwanianego (dial-up) opartego na protokole PPP.

WAN Connection	
PPPoA Routed	
Description	PPPoA
VPI	0
VCI	35
Encapsulation Method	VcMux
NAT	Enable Disable
Username	
Password	
IP Address	0.0.0.0 (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
RIP	Disable
MTU	1472
Apply Cancel	

Description (Opis) – Nazwa połączenia definiowana przez użytkownika.

VPI / VCI – W tym polu wpisz odpowiednie dane dostarczone przez twojego dostawcę usług internetowych.

NAT – Funkcja NAT (Network Address Translation, translacja adresów sieciowych) umożliwia podłączenie do Internetu wielu użytkowników za pomocą jednego konta IP współdzielącego ten sam adres IP. Jeżeli użytkownicy w sieci lokalnej mają publiczne adresy IP i mogą bezpośrednio uzyskiwać dostęp do Internetu, funkcję NAT można wyłączyć.

Username (Nazwa użytkownika) – Wpisz nazwę użytkownika określoną przez dostawcę usług internetowych. Można tu wpisać do **128** znaków alfanumerycznych (wielkość liter ma znaczenie). Nazwa użytkownika ma postać „nazwaużytkownika@nazwadostawcyusługinternetowych” zamiast po prostu „nazwaużytkownika”.

Password (Hasło) – Wpisz hasło określone przez dostawcę usług internetowych. Można tu wpisać do **128** znaków alfanumerycznych (wielkość liter ma znaczenie).

IP Address (Adres IP) – Adres IP sieci WAN. Jeżeli użytkownik pozostawi tu wartość 0.0.0.0, adres IP zostanie automatycznie pobrany od dostawcy usług internetowych.
Authentication Protocol Type (Typ protokołu uwierzytelnienia) – Wartość domyślna to: **Chap (Auto)**. Dostawca usług internetowych powinien wskazać, czy należy stosować ustawienie **Chap**, czy **Pap**.
Connection (Połączenie) – Zaznacz to pole, jeżeli router ma zestawiać sesję PPPoA po włączeniu oraz automatycznie odnawiać ją w przypadku rozłączenia przez dostawcę usług internetowych.
RIP – RIP v1, RIP v2, RIP v1+v2 oraz RIP v2 Multicast.
MTU – Parametr Maximum Transmission Unit. Rozmiar największego datagramu (bez nagłówków typowych dla konkretnego medium), jaki protokół IP będzie próbował przesłać przez interfejs.

PPPoE Routed Connections

Protokół PPPoE (PPP over Ethernet) oferuje możliwość kontroli dostępu w sposób zbliżony do usług dostępu wdzwanianego (dial-up) opartego na protokole PPP.

WAN Connection	
PPPoE Routed	
Description	PPPoE
VPI	0
VCI	35
Encapsulation Method	LLC
NAT	Enable Disable
Username	
Password	
Service Name	
IP Address	0.0.0.0 (0.0.0.0' means 'Obtain an IP address automatically')
Authentication Protocol	Auto
Connection	Always On
Idle Timeout	10 minutes
RIP	Disable
MTU	1472
PPPoE Relay	Enable
Apply Cancel	

Description (Opis) – Nazwa połączenia definiowana przez użytkownika.
VPI / VCI – W tym polu wpisz odpowiednie dane dostarczone przez dostawcę usług internetowych.
NAT – Funkcja NAT (Network Address Translation, translacja adresów sieciowych) umożliwia podłączenie do Internetu wielu użytkowników za pomocą jednego konta IP, współdzielącego ten sam adres IP. Jeżeli użytkownicy w sieci lokalnej mają publiczne adresy IP i mogą bezpośrednio uzyskiwać dostęp do Internetu, funkcję NAT można wyłączyć.
Username (Nazwa użytkownika) – Wpisz nazwę użytkownika określoną przez dostawcę usług internetowych. Można tu wpisać do **128** znaków alfanumerycznych (wielkość liter ma znaczenie). Nazwa użytkownika ma postać „nazwaużytkownika@nazwadostawcyusługinternetowych” zamiast po prostu „nazwaużytkownika”.
Password (Hasło) – Wpisz hasło określone przez dostawcę usług internetowych. Można tu wpisać do **128** znaków alfanumerycznych (wielkość liter ma znaczenie).

Service Name (Nazwa usługi) – To pole ma znaczenie identyfikacyjne. Jeżeli jest ono wymagane, dostawca usług internetowych winien o tym poinformować. Może ono zawierać do 20 znaków alfanumerycznych.

IP Address (Adres IP) – Adres IP sieci WAN. Jeżeli użytkownik pozostawi tu wartość 0.0.0.0, adres IP zostanie automatycznie pobrany od dostawcy usług internetowych.

Authentication Protocol (Protokół uwierzytelnienia) – Wartość domyślna to Chap. Dostawca usług internetowych powinien wskazać, czy należy stosować ustawienie Chap, czy Pap.

Connection (Połączenie):

- **Always on (Zawsze włączone)** – Zaznacz to pole, jeżeli router ma zestawiać sesję PPPoE po włączeniu oraz automatycznie odnawiać ją w przypadku rozłączenia przez dostawcę usług internetowych.
- **Connect on Demand (Łącz na żądanie)** – Zaznacz to pole, jeżeli router ma zestawiać sesję PPPoE tylko, kiedy w systemie pojawi się pakiet żądający dostępu do Internetu (tzn. kiedy program na komputerze podejmie próbę dostępu do Internetu).

Idle Timeout (Rozłączenie przy braku aktywności) – Automatyczne rozłączenie bramy zapory szerokopasmowej, jeżeli na linii przez określony czas nie odnotowuje się żadnej aktywności.

RIP – RIP v1, RIP v2, RIP v1+v2 oraz RIP v2 Multicast.

MTU – Parametr Maximum Transmission Unit. Rozmiar największego datagramu (bez nagłówków typowych dla konkretnego medium), jaki protokół IP będzie próbował przesłać przez interfejs.

RFC 1483 Bridged Connections

WAN Connection	
RFC 1483 Bridged	
Description	1483_Bridged_mode
VPI	0
VCI	35
ATM Class	UBR
PCR	0
SCR	0
MBS	0
Encapsulation Method	LLC Bridged

Apply Cancel

Description (Opis) – Nazwa połączenia definiowana przez użytkownika.

VPI / VCI – W tym polu wpisz odpowiednie dane dostarczone przez dostawcę usług internetowych.

Encapsulation method (Metoda enkapsulacji) – Wybierz format enkapsulacji. Informacja ta winna być dostarczona przez dostawcę usług internetowych.

- **DNS**

DNS	
Parameters	
Obtain DNS Automatically	☑ Enable
Primary DNS	
Secondary DNS	
Apply Cancel	

Mechanizm Domain Name System (DNS) zawiera tablicę skojarzeń nazw domen z adresami IP. Każdy host działający w Internecie ma niepowtarzalną nazwę, łatwo zapamiętywalną dla użytkownika (tzw. nazwę domeny), np. *www.pentagram.eu*, oraz adres IP. Adres IP to numer 32-bitowy zapisany w formacie xxx.xxx.xxx.xxx, np. 192.168.1.254. Adres IP można traktować jako swego rodzaju numer telefonu poszczególnych urządzeń w Internecie. System DNS umożliwia znalezienie takiego numeru telefonu dla dowolnej nazwy domeny. Zważywszy, iż adres IP jest trudny do zapamiętania, system DNS zamienia wygodną dla użytkownika nazwę na odpowiadający jej adres IP.
Adres IP w systemie Domain Name System (DNS) można uzyskać automatycznie, o ile dostawca usług internetowych udostępnił go przy logowaniu. Zazwyczaj przy zastosowaniu protokołów PPPoE lub PPPoA do obsługi sieci rozległej dostawcy usług internetowych, taki dostawca automatycznie udostępnia adres IP DNS. Pole konfiguracyjne może pozostać niewypełnione. Alternatywnie, dostawca może udostępnić własny adres IP DNS. Adres taki należy wówczas wpisać w systemie.
W przypadku wyboru jednego z pozostałych protokołów, RFC1483 w wersji trasowanej lub mostkowanej, należy skonsultować się z dostawcą usług internetowych, gdyż może on udostępnić własny adres IP DNS. Adres IP DNS należy obowiązkowo wpisać, jeżeli chcesz jako adres Serwera DNS w swoim komputerze ustawić adres IP routera lokalnego.

- **ADSL**

ADSL	
Parameters	
ADSL Mode	Annex A
Modulator	ADSL Multimode
DSP FirmwareVersion	DMT FwVer: 3.5.18.0_A_TC, HwVer:T14F7_1.0
DMT Status	Down
Operational Mode	----------
Upstream	0 kbps
Downstream	0 kbps
Noise Margin (Upstream)	N/A (ADSL is not UP)
Noise Margin (Downstream)	N/A (ADSL is not UP)
Attenuation (Upstream)	N/A (ADSL is not UP)
Attenuation (Downstream)	N/A (ADSL is not UP)
Apply Refresh	

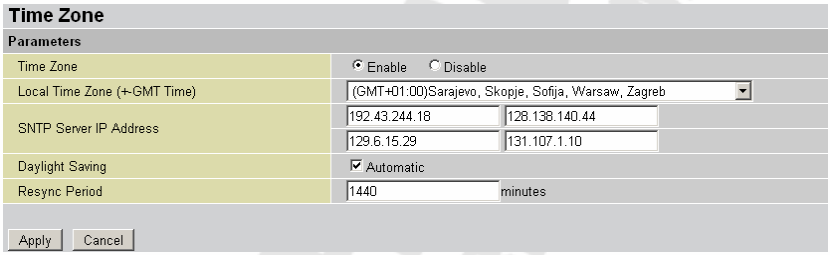
ADSL Mode (Tryb ADSL) – Istnieją cztery możliwe tryby **Open Annex Type and Follow DSLAM's Setting (Otwórz typ aneksu i przyjmij ustawienie DSLAM)**, **Annex A**, **Annex L**, **Annex M** oraz **Annex J**, pomiędzy którymi może wybierać użytkownik.
Modulator – Istnieją cztery możliwe tryby: **AUTO**, **ADSL multimode**, **ADSL2** oraz **ADSL2+** , jakie użytkownik może wybrać dla danego połączenia.

DSP Firmware Version (Wersja oprogramowania sprzętowego DSP) – Wersja kodu DSP
DMT Status (Stan DMT) – Stan DMT
Operational Mode (Tryb operacyjny) – Opcja prezentująca stan pracy, jeżeli użytkownik określił tryb połączenia jako „AUTO".
Annex Type (Typ aneksu) – Opcja prezentująca typ routera, np. Annex A, Annex B
Upstream (Wysyłanie) – Szybkość wysyłania danych.
Downstream (Pobieranie) – Szybkość pobierania danych.
Noise Margin / Attenuation (Zakres zakłóceń / tłumienie) – Charakterystyka linii ADSL.

Configuration / System

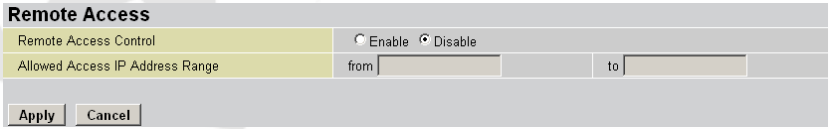
Sekcja System mieści sześć obszarów: **Time Zone (Strefa czasowa)**, **Remote Access (Dostęp zdalny)**, **Firmware Upgrade (Aktualizacja oprogramowania sprzętowego)**, **Backup/Restore (Kopie zapasowe i przywracanie)**, **Restart (Ponowne uruchomienie)** oraz **User Management (Zarządzanie użytkownikami)**.

- ### Time Zone (Strefa czasowa)



Router nie ma własnego zegara czasu rzeczywistego. Posługuje się on protokołem Simple Network Time Protocol (SNTP) w celu pobierania bieżącego odczytu czasu z serwera SNTP spoza sieci. Wybierz lokalną strefę czasową, kliknij przycisk **Enable (Włącz)** i kliknij przycisk **Apply (Zastosuj)**. Po pomyślnym uzyskaniu połączenia z Internetem router pobierze prawidłowy czas lokalny ze wskazanego serwera SNTP. Jeżeli wolisz wskazać inny serwer SNTP niż te obecne na rozwijanej liście, wpisz jego adres IP w przedstawionej powyżej postaci. Dostawca usług internetowych może zaoferować wykorzystanie własnego serwera SNTP.
Resync Period (Okres resynchronizacji) (wyrażony w minutach) to interwał, po jakim router ponownie zsynchronizuje czas routera z czasem wskazanego serwera SNTP. Aby uniknąć zbędnego przeciążania wybranego serwera SNTP, interwał powinien być jak największy – co najmniej kilka godzin lub nawet dni.

- ### Remote Access (Dostęp zdalny)

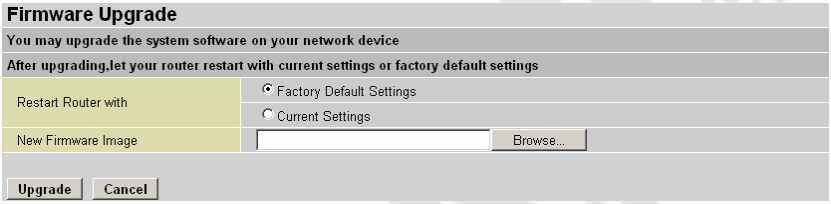


W celu czasowego umożliwienia zdalnej administracji routera (tzn. spoza sieci lokalnej) zdefiniuj czas, przez jaki router ma umożliwiać dostęp zdalny, i kliknij przycisk **Enable (Włącz)**. Pozostałe opcje konfiguracyjne interfejsu zarządzania przez WWW można

zmienić w polu **Device Management (Zarządzanie urządzeniami)** w sekcji **Advanced (Zaawansowane)** interfejsu.

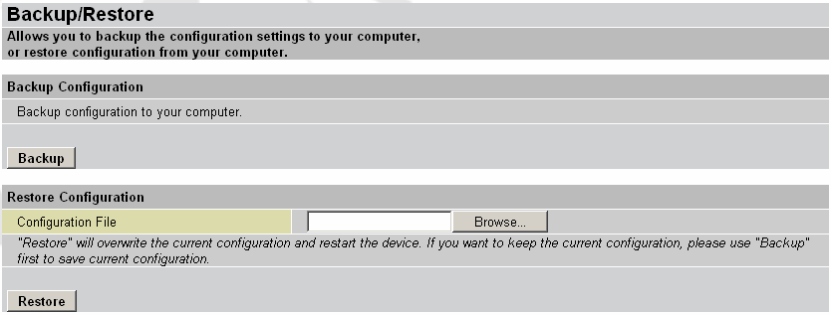
- ## Firmware Upgrade

Oprogramowanie sprzętowe routera to zbiór procedur umożliwiających działanie urządzenia i zapewniających realizację wszystkich jego funkcji. Router należy traktować jako wyspecjalizowany komputer, zaś oprogramowanie sprzętowe to programy, które na nim działają. W miarę upływu czasu, programy te będą poprawiane i zmieniane. Aby móc skorzystać z tych zmian, router umożliwia aktualizację oprogramowania.
Kliknij przycisk **Browse (Przeglądaj)**, aby wskazać nowy plik obrazu oprogramowania, pobrany na komputer. Po wybraniu odpowiedniego pliku wybierz opcję Upgrade (Aktualizuj) w celu zaktualizowania oprogramowania sprzętowego w routerze.



Restart Router with (Ponownie uruchom router z...) – Wybierz opcję **Factory Default Setting (Domyślne ustawienia fabryczne)** lub **Current Settings (Bieżące ustawienia)**, którą preferujesz.
New Firmware Image (Nowy obraz oprogramowania sprzętowego) – W tym polu wpisz lokalizację pliku, który chcesz wczytać, lub kliknij przycisk **Browse (Przeglądaj)** i wskaż go.
Browse... (Przeglądaj) – Kliknij przycisk **Browse...**, aby wskazać plik .afw, który chcesz wczytać. Pamiętaj, że przed wczytaniem plików należy rozpakować skompresowane archiwum plików (.zip).
Upgrade (Aktualizuj) – Kliknij ten przycisk, aby rozpocząć proces wczytywania. Może on zająć do dwóch minut.
Uwaga: NIE wyłączaj routera ani nie przerywaj działania procesu aktualizacji oprogramowania. Nieprawidłowe działania mogą doprowadzić do uszkodzenia routera.

- ## Backup / Restore

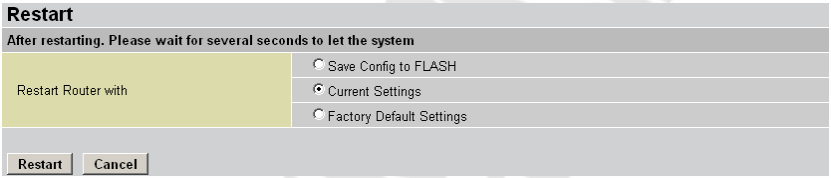


Te funkcje umożliwiają zapisanie i stworzenie kopii zapasowej aktualnych ustawień routera w postaci pliku na komputerze lub przywrócenie ustawień na podstawie takiego

właśnie pliku. Są one przydatne, jeżeli użytkownik chce wypróbować różne ustawienia, wiedząc, że posiada sprawdzoną kopię zapasową, która odtworzy prawidłowy stan urządzenia w przypadku ewentualnych błędów. Zaleca się tworzenie kopii zapasowej routera przed wprowadzeniem jakichkolwiek istotnych zmian w konfiguracji routera.
Wciśnij przycisk **Backup (Kopia zapasowa)** i wskaż, w którym miejscu na komputerze lokalnym ma zostać zapisany plik ustawień. Możesz również zmienić nazwę zapisywanego pliku (jest to przydatne, jeżeli chcesz posiadać kilka zapisanych plików z ustawieniami).
Wciśnij przycisk **Browse (Przeglądaj)**, aby wskazać na komputerze plik, który ma zostać wykorzystany jako podstawa do przywracania ustawień. Ustawienia powinno się przywracać wyłącznie z plików, które zostały wygenerowane za pomocą funkcji Backup i które zostały stworzone przy użyciu **bieżącej wersji** oprogramowania wbudowanego routera. **Pliki ustawień zapisane na komputerze nie powinny być w żadnym wypadku edytowane ręcznie.**
Wybierz plik z ustawieniami, które chcesz odtworzyć, i wciśnij przycisk **Restore (Odtwórz)** w celu wczytania tych ustawień do routera.

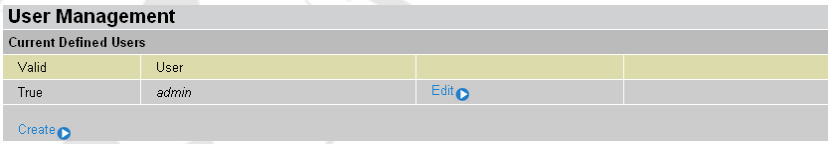
- ## Restart Router

Kliknij przycisk Restart (Uruchom ponownie) z opcją Current Settings (Ustawienia bieżące), aby od nowa uruchomić router i przywrócić ostatnią zapisaną konfigurację.



Jeżeli chcesz ponownie uruchomić router przy użyciu domyślnych ustawień fabrycznych (np. po aktualizacji oprogramowania sprzętowego albo po zapisaniu w pamięci nieprawidłowej konfiguracji), wybierz opcję **Factory Default Settings (Domyślne ustawienia fabryczne)** w celu przywrócenia urządzenia do domyślnych ustawień fabrycznych.
Ten sam efekt można również uzyskać, wciskając igłowy przycisk Reset na tylnym panelu urządzenia przez ok. 10-12 sekund w trakcie pracy routera.

- ## User Management



Aby uniemożliwić osobom nieuprawnionym dostęp do interfejsu konfiguracyjnego routera, wszyscy użytkownicy są zobowiązani logować się za pomocą hasła. Istnieje możliwość stworzenia wielu kont użytkowników, z których każde będzie chronione odrębnym hasłem.
Istnieje również możliwość edytowania **(Edit)** istniejących użytkowników oraz tworzenia **(Create)** nowych użytkowników, którzy będą mogli uzyskać dostęp do interfejsu konfiguracyjnego urządzenia. Jeżeli klikniesz przycisk **Edit**, na ekranie pojawią się następujące opcje:

User Management

Edit

Username	admin
Password	*********
Valid	True

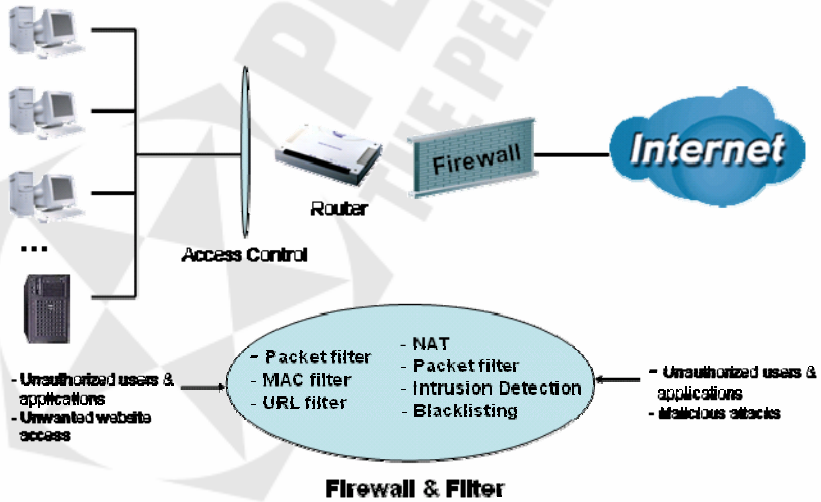
Apply Cancel

Możesz zmienić hasło **(password)** użytkownika, zadecydować, czy jego konto jest aktywne i ważne **(Valid)** oraz opisać każde konto użytkownika swoim komentarzem. Podczas tworzenia konta użytkownika masz do dyspozycji te same opcje z zastrzeżeniem, iż po jego utworzeniu nie można już zmienić nazwy użytkownika. Nie można usunąć domyślnego konta administratora; możesz jednak usunąć dowolne inne stworzone konto, klikając przycisk **Cancel (Anuluj)** podczas edytowania danego użytkownika.
Zalecamy zmianę hasła domyślnego konta „**admin**" natychmiast po otrzymaniu routera oraz po każdym przywróceniu konfiguracji do domyślnych ustawień fabrycznych.

Configuration / Firewall

Firewall and Access Control

Router zawiera pełną zaporę sieciową SPI (Stateful Packet Inspection) służącą do kontroli dostępu do Internetu z sieci lokalnej, jak również zapobiegającą atakom hackerów. Co więcej, jeżeli stosowany jest mechanizm NAT (Network Address Translation), router działa jako „naturalna" zapora sieciowa, ponieważ w sytuacji, gdzie wszystkie komputery z sieci lokalnej używają prywatnych adresów IP, nie można do nich uzyskać bezpośredniego dostępu z Internetu. Bliższe dane na temat NAT można znaleźć w rozdziale poświęconym konfiguracji **WAN**.



Firewall (Zapora sieciowa) – Uniemożliwia dostęp spoza sieci. Router oferuje trzy poziomy zabezpieczeń:

NAT natural firewall (Naturalna zapora sieciowa NAT) – Ta funkcja ukrywa adresy IP użytkowników z sieci lokalnej, którzy są niewidzialni dla użytkowników zewnętrznych z Internetu, co znacznie utrudnia hackerowi atak na konkretny komputer. Taka naturalna zapora jest obecna, jeżeli funkcja NAT jest włączona.

Uwaga: W przypadku stosowania mechanizmu serwerów wirtualnych (przekierowania portów), komputery są narażone na atak w stopniu określonym w ustawieniach funkcji Virtual Server, pod warunkiem iż w ustawieniach zapory dotyczących filtrowania pakietów zostały otwarte odpowiednie porty.

Firewall Security and Policy (General Settings) (Bezpieczeństwo i reguły zapory sieciowej – ustawienia ogólne) – Reguły filtra pakietów przychodzących uniemożliwiają nieuprawnionym komputerom lub aplikacjom dostęp do sieci lokalnej z Internetu.

Intrusion Detection (Wykrywanie ataków) – Włącz funkcję Intrusion Detection, aby wykrywać i rejestrować złośliwe ataki oraz zapobiegać im.

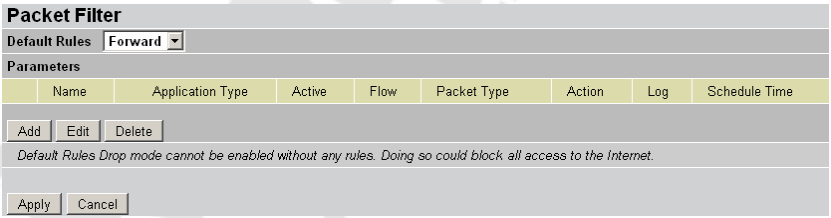
MAC Filter rules (Reguły filtra MAC) – Opcja uniemożliwiająca nieuprawnionym komputerom dostęp do Internetu.

URL Filter (Filtr URL) – Opcja blokująca komputerom z sieci lokalnej dostęp do niepożądanych serwisów WWW.

Sekcja **Firewall** składa się z sześciu obszarów, które są szczegółowo omówione poniżej: **Packet Filter (Filtr pakietowy)**, **Ethernet MAC Filter (Filtr Ethernet MAC)**, **Wireless MAC Filter (Filtr MAC dla sieci bezprzewodowych)**, **Intrusion Detection (Wykrywanie ataków)**, **Block WAN Request (Blokowanie żądań WAN)** oraz **URL Filter (Filtr URL)**.

- ## Packet Filter

  Filtrowanie pakietów pozwala skonfigurować router w taki sposób, aby blokować konkretnym użytkownikom zewnętrznym lub wewnętrznym (wg adresu IP (**IP address**)) dostęp do Internetu, albo też wyłączyć konkretne żądania usług (wg numeru portu (**Port number**)) w kierunku do i z Internetu. Ten program konfiguracyjny umożliwia określenie do 6 różnych reguł filtra dla różnych użytkowników w zależności od ich adresów IP oraz numeru portu sieciowego. Wszystkie operacje są powiązane łącznikiem „**albo**”, co oznacza, że router kolejno sprawdza wszystkie reguły filtra, począwszy od pierwszej. Jeżeli choć jedna z zasad jest spełniona, zaplanowana czynność zostaje podjęta.



Add (Dodaj) – Kliknij ten przycisk, aby dodać nową regułę filtra pakietowego – na ekranie pojawi się kolejna pozycja.

Edit (Edytuj) – Zaznacz regułę, którą chcesz edytować, a następnie kliknij przycisk „Edit”.

Delete (Usuń) – Zaznacz regułę, którą chcesz usunąć, a następnie kliknij przycisk „Usuń”.

Packet Filter (Application Based)

Parameters			
Application Type	User Defined (You may select a predefined packet filtering profile for a well-known application here.)		
Parameters			
Name	APPL1	Packet Flow	Outgoing(Local to Remote) / Incoming(Remote to Local)
Active	Yes	Packet Type	Any
Log	No	Action When Matched	Drop
Local Machine IPs	from	to	
Remote Machine IPs	from	to	
Local Application Ports	from	to	
Remote Application Ports	from	to	
Schedule Time	Always		
	Schedule from	08 : 00 to 18 : 00	
	Sun Mon Tue Wed Thu Fri Sat		

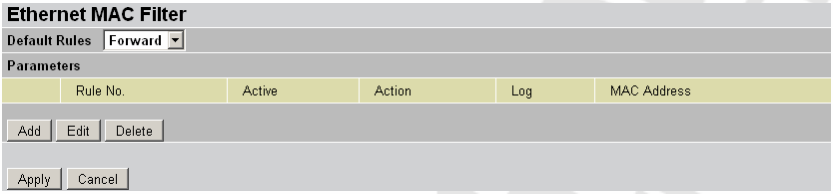
Return Cancel

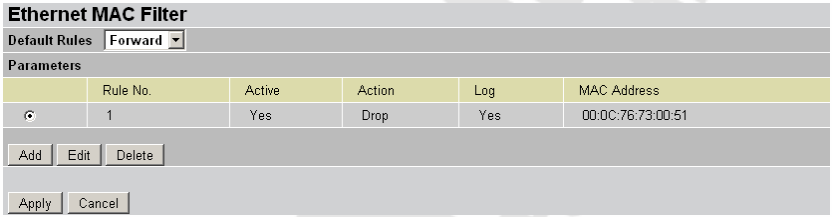
Application (Aplikacja) – Dowolny wybór użytkownika.
Packet Flow (Kierunek pakietów) – Określ, czy reguła ma obowiązywać dla pakietów wychodzących, czy przychodzących.
Active (Aktywna) – Wybierz **Yes (Tak)**, aby włączyć daną regułę, lub **No (Nie)**, aby ją wyłączyć.
Packet Type (Typ pakietów) – Określ rodzaj pakietów (TCP, UDP, ICMP lub „any" (dowolne)), jakich ma dotyczyć reguła.
Wybierz pozycję **TCP**, jeżeli chcesz na serwerze zdalnym wyszukać za pomocą numeru portu usługę aplikacyjną opartą na połączeniu. Wybierz pozycję **UDP**, jeżeli chcesz na serwerze zdalnym wyszukać za pomocą numeru portu usługę aplikacyjną bez połączenia.
Log (Rejestruj) – Wybierz **Yes (Tak)**, jeżeli chcesz generować zapisy w dzienniku za każdym razem, kiedy reguła filtra zostaje zastosowana w odniesieniu do pakietu.
Action When Matched (Działanie, jeżeli reguła spełniona) – Jeżeli pakiet odpowiada danej regule filtra, mechanizm przekaże (**Forward)** lub odrzuci (**Drop)** dany pakiet.
Source IP Address (Źródłowy adres IP) – Wpisz adres (lub adresy) IP źródła pakietów przychodzących lub wychodzących.
Source Port (Port źródłowy) – Zaznacz numer (lub numery) portów źródła pakietów przychodzących lub wychodzących TCP albo UDP.
Destination IP Address (Docelowy adres IP) – Wpisz docelowy adres (lub adresy) IP pakietów przychodzących lub wychodzących.
Destination Port (Port docelowy) – Zaznacz numer (lub numery) docelowych portów pakietów przychodzących lub wychodzących TCP albo UDP
Schedule time (Harmonogram) – Użytkownik może zdefiniować czas stosowania filtra pakietowego.

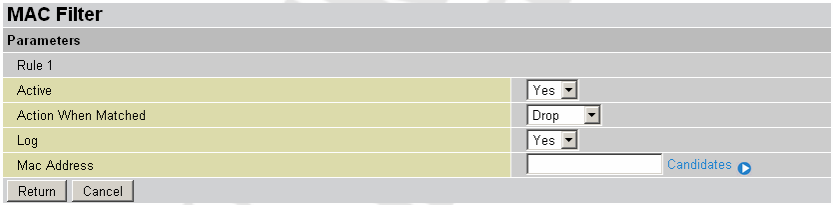
Uwaga: Jeżeli opcja serwera DHCP jest włączona, należy z najwyższą ostrożnością przydzielać adresy IP z filtrowanego zakresu prywatnych adresów IP, tak aby uniknąć potencjalnych konfliktów, gdyż nie wiadomo, który komputer w sieci lokalnej jest przypisany do danego adresu IP. Najprostszą i najbezpieczniejszą metodą jest przydzielanie filtrowanych adresów IP takim komputerom, które nie mają prawa dostępu do zasobów zewnętrznych, np. do Internetu. Należy ręcznie skonfigurować filtrowany adres IP dla takiego komputera, ale nadal pozostaje on w tej samej podsieci, co router.

- ## Ethernet MAC Filter

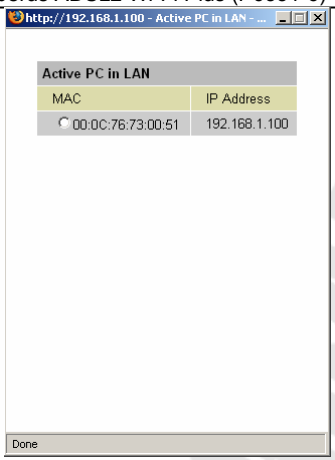
Adres Ethernet MAC (Media Access Control) to niepowtarzalny sprzętowy identyfikator każdego komputera w interfejsie sieciowym (tj. karcie interfejsu sieciowego lub karcie Ethernet). Dzięki funkcji filtra adresów MAC można skonfigurować przełącznik sieciowy w taki sposób, aby przyjmował transmisje wyłącznie od określonych urządzeń, lub przeciwnie – blokował wybranym komputerom dostęp do sieci lokalnej.
Nie ma żadnych wstępnie zdefiniowanych reguł filtra adresów MAC. Użytkownik może swobodnie tworzyć własne reguły, aby zrealizować swoje potrzeby.





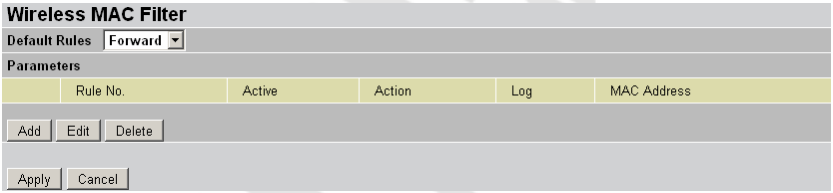


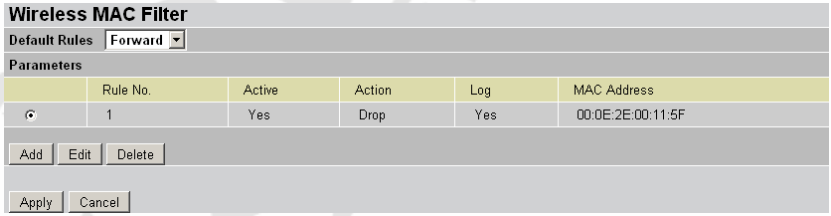
Active (Funkcja aktywna) – Wybierz Yes (Tak) z rozwijanej listy w celu włączenia filtrowania adresów MAC.
Action When Matched (Działanie, jeżeli reguła spełniona) – Wybierz opcję **Drop (Odrzuć)** albo **Forward (Przekaż)**.
Log (Rejestruj) – Wybierz **Yes (Tak)**, jeżeli chcesz generować zapisy w dzienniku za każdym razem, kiedy w odniesieniu do pakietu zastosowana zostaje reguła filtra.
MAC Address (Adres MAC) – Wpisz adres MAC, który chcesz objąć tym mechanizmem.
Candidates (Kandydaci) – Funkcja automatycznie wykrywa urządzenia podłączone do routera za pomocą Ethernetu.

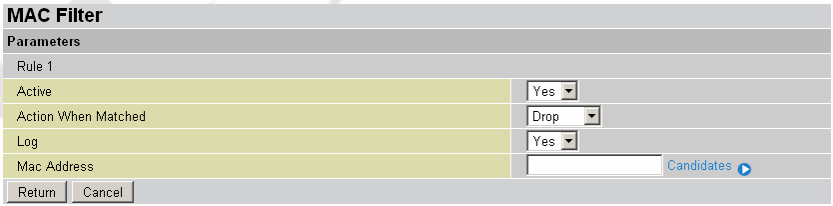


- **Wireless MAC Filter**

  Mechanizm adresów MAC obsługuje do 30 urządzeń w sieci bezprzewodowej i ułatwia kontrolę sieci, tak aby przyjmować transmisje wyłącznie od określonych, uprawnionych komputerów lub uniemożliwić niepożądanym komputerom dostęp do sieci lokalnej.
  Nie ma żadnych wstępnie zdefiniowanych reguł filtra adresów MAC. Użytkownik może swobodnie tworzyć własne reguły, aby zrealizować swoje potrzeby.



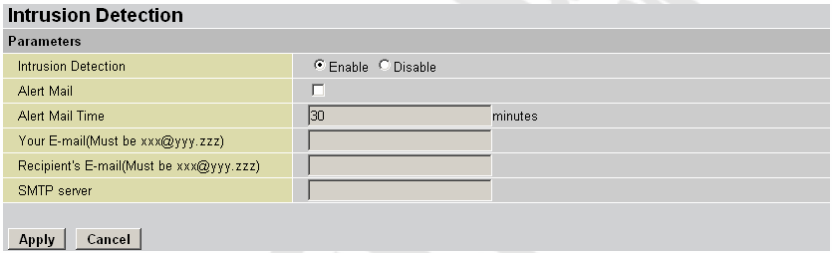




Active (Funkcja aktywna) – Wybierz Yes (Tak) z rozwijanej listy w celu włączenia filtrowania adresów MAC.
Action When Matched (Działanie, jeżeli reguła spełniona) – Wybierz opcję **Drop (Odrzuć)** albo **Forward (Przekaż)**.
Log (Rejestruj) – Wybierz **Yes (Tak)**, jeżeli chcesz generować zapisy w dzienniku za każdym razem, kiedy w odniesieniu do pakietu zastosowana zostaje reguła filtra.
MAC Address (Adres MAC) – Wpisz adres MAC, który chcesz objąć tym mechanizmem.
Candidates (Kandydaci) – Funkcja automatycznie wykrywa urządzenia podłączone do routera za pomocą sieci WLAN.

- ## Intrusion Detection

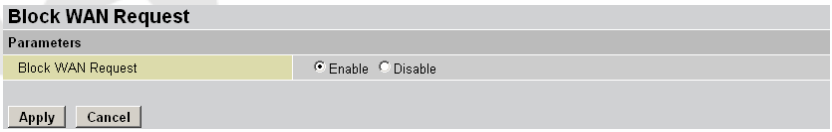
Zaznacz opcję **Enable (Włącz)**, jeżeli chcesz wykrywać intruzów uzyskujących dostęp do twojego komputera w sposób nieuprawniony. Jeżeli użytkownik włączy tę funkcję, router automatycznie wykrywa i blokuje ataki typu DoS (Denial of Service). Ten rodzaj ataku nie ma na celu spenetrowania poufnych danych dostępnych w sieci, a raczej ma zakłócić pracę wybranych elementów sieciowych lub całej sieci. Jeżeli atak powiedzie się, użytkownicy nie będą mogli korzystać z zasobów sieciowych.



Intrusion Detection (Wykrywanie ataków) – Zaznacz opcję **Enable (Włącz)**, jeżeli chcesz wykrywać intruzów uzyskujących dostęp do twojego komputera w sposób nieuprawniony.
Alert Mail (Poczta alarmowa) – Zaznacz to pole, jeżeli chcesz otrzymywać wiadomości pocztowe o alarmach.
Alert Mail Time (Czas poczty alarmowej) – Określ przedział czasu, w jakim będziesz odbierał alarmowe wiadomości pocztowe.
Your E-Mail (Twój adres e-mail) – Określ własny adres e-mail.
Recipient's E-mail (Adres e-mail odbiorcy) – Określ adres e-mail odbiorcy, do którego ma być wysyłane zawiadomienie e-mailowe.
SMTP server (Serwer SMTP) – Określ adres serwera SMTP (pocztowego).

- ## Block WAN Request

Zaznacz pole **Enable (Włącz)**, jeżeli nie chcesz zezwolić, aby do tego routera docierały zewnętrzne żądania PING.



- **URL Filter**

Reguły filtra URL (Uniform Resource Locator – tzn. adres internetowy w postaci http://www.pentagram.eu albo http://www.przyklad.com) pozwalają uniemożliwić użytkownikom z twojej sieci dostęp do konkretnych stron internetowych na podstawie ich adresu URL. Nie ma żadnych wstępnie zdefiniowanych reguł filtra adresów URL. Użytkownik może swobodnie tworzyć własne reguły, aby zrealizować swoje potrzeby.

URL Filter

	Rule No.	Active	PC IPs		Block Mode	Keywords Filtering	Domains Filtering	Restrict URL Features
			from	to				
◉	1	Yes	192.168.1.101	192.168.1.200	Always Block	Disable	Disable	Block Java Applet,Cookies

Add Edit Delete

Apply Cancel

URL Filter

Parameters

Rule 1	Active Yes
PC IP Address Range	
from	to
Block Mode	◉ Always Block ○ Block from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Keywords Filtering	☐ Enable Details
Domains Filtering	☐ Enable Details
Restrict URL Features	☐ Block Java Applet ☐ Block ActiveX ☐ Block Cookies ☐ Block Proxy

Return Cancel

Active (Funkcja aktywna) – Wybierz **Yes (Tak)** z rozwijanej listy, aby włączyć lub wyłączyć funkcję filtra URL.

Always Block (Zawsze blokuj) – Zdecyduj, czy reguły filtra URL muszą być zawsze sprawdzane (tzn. o każdej porze dnia).

Block from (Blokuj od) – Zdefiniuj czas, w jakim należy sprawdzać reguły filtra adresów URL (np. w trakcie godzin roboczych).

Keywords Filtering (Filtrowanie słów kluczowych) – Umożliwia blokowanie witryn wg konkretnych słów kluczowych znajdujących się w adresie URL, zamiast na podstawie całego adresu (np. w celu zablokowania dowolnych obrazów zatytułowanych „reklama.gif"). Jeżeli funkcja ta jest włączona, mechanizm filtra sprawdza listę określonych przez użytkownika słów kluczowych, aby sprawdzić, czy nie występują one w wywołanych adresach URL i w razie potrzeby je zablokować. Należy zauważyć, iż filtr URL blokuje wyłącznie połączenia przeglądarki internetowej (HTTP) wykorzystujące port 80. Przykładowo, adres http://www.abc.com/abcde.html zostałby zablokowany, ponieważ w adresie występuje słowo kluczowe „abcde".

Keywords Filtering

Create

Keyword	

Apply

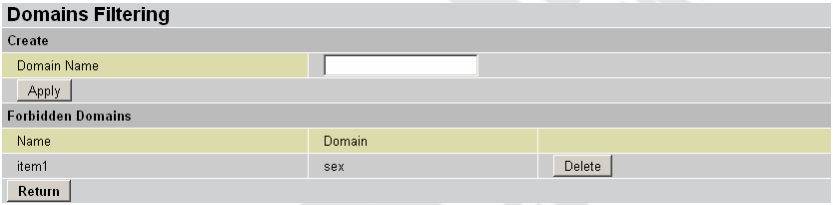
Block WEB URLs which contain these keywords

Name	Keyword	

Return

Domains Filtering (Filtrowanie domen) – Mechanizm sprawdza nazwy domen w wywołanym adresie URL z listą domen dozwolonych lub zakazanych. W zależności od wyniku sprawdzenia, adres URL zostaje przesłany (jako zaufany) lub odrzucony (jako zakazany). Procedura sprawdzenia ma następujący przebieg:

1. Sprawdza się, czy domena z adresu URL znajduje się na liście domen zaufanych. Jeżeli tak, do docelowego serwera WWW wysłane zostaje odpowiednie żądanie połączenia.
2. Jeżeli nie, sprawdza się, czy domena występuje na liście domen zakazanych. Jeżeli tak, żądanie połączenia zostaje anulowane.
3. Jeżeli pakiet nie pasuje do żadnej z list, do docelowego serwera WWW wysłane zostaje odpowiednie żądanie połączenia.
4. Należy zauważyć, że określa się tu wyłącznie domenę, a nie pełny adres URL. Przykładowo, aby blokować transmisje z witryny www.seks.com, należy wpisać „seks” albo „seks.com” zamiast „www.seks.com”. W poniższym przykładzie, żądanie skierowane pod adres URL www.abc.com jest przesyłane do docelowego serwera WWW, ponieważ znajduje się on na liście zaufanej, natomiast żądanie adresu www.seks lub www.seks.com zostanie odrzucone, ponieważ seks.com znajduje się na liście zakazanej.



Restrict URL Features

- **Block Java Applet (Blokuj aplety Java)** – Blokowanie treści WWW zawierających aplety Java, aby zapobiec atakom, które mają na celu uszkodzenie systemu przy wykorzystaniu standardowego protokołu HTTP.
- **Block ActiveX (Blokuj ActiveX)** – Blokowanie elementów ActiveX
- **Block Cookies (Blokuj cookies)** – Blokowanie tzw. cookies
- **Block Proxy (Blokuj serwer proxy)** – Blokowanie serwera proxy

Configuration / QoS

Funkcje Quality of Service – wprowadzenie

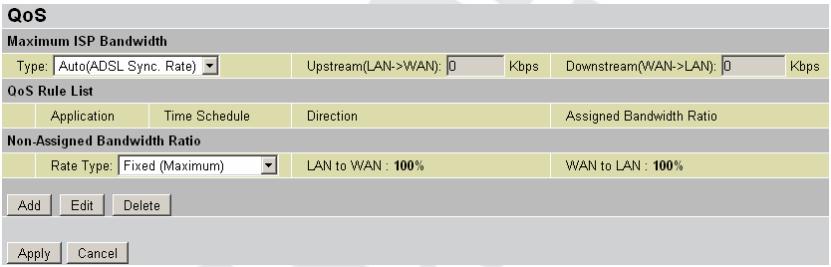
Jeżeli kiedykolwiek dało się odczuć, iż szybkość Internetu spadła do minimalnych wartości, ponieważ inny członek rodziny używał w tym samym czasie programu do obsługi sieci P2P, to warto docenić przełomowe znaczenie funkcji Quality of Service oferowanej przez routery Pentagram w zastosowaniach domowych i biurowych.

QoS: utrzymywanie szybkiej pracy połączenia sieciowego

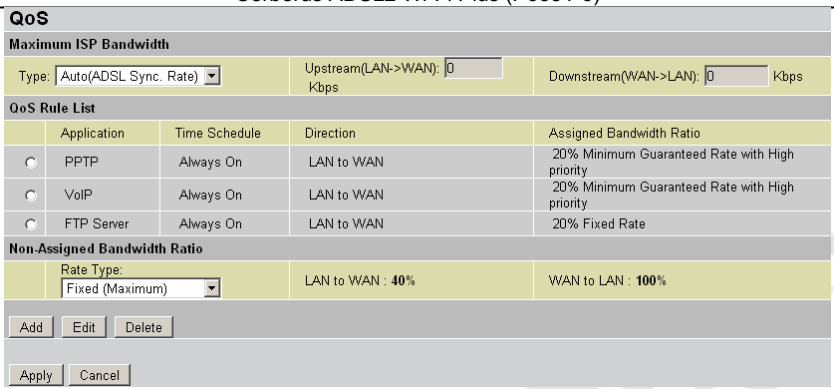
Funkcja Quality of Service (QoS), konfigurowana pod kątem źródłowego adresu IP, docelowego adresu IP, protokołu oraz portu, stwarza możliwości pełnej kontroli nad tym, jakie rodzaje danych wychodzących powinny otrzymywać priorytet na routerze, gwarantując tym samym, iż dane pożerające dużą część przepustowości, np. dane gier interaktywnych, aplikacje wrażliwe na opóźnienia, np. z zakresu przesyłu głosu, lub pliki o kluczowym znaczeniu są przesyłane przez router z błyskawiczną szybkością nawet przy dużym obciążeniu całego urządzenia. Istnieje możliwość regulacji szybkości, z jaką poszczególne typy danych wychodzących są przetwarzane przez router. Co więcej, można również po prostu zmienić priorytet poszczególnych typów wysyłanych danych i pozostawić zadanie przydziału konkretnych szybkości samemu routerowi.

Konfiguracja QoS

Wybierz pozycję **QoS** w opcji **Configuration (Konfiguracja)** w lewym oknie przedstawionym poniżej.



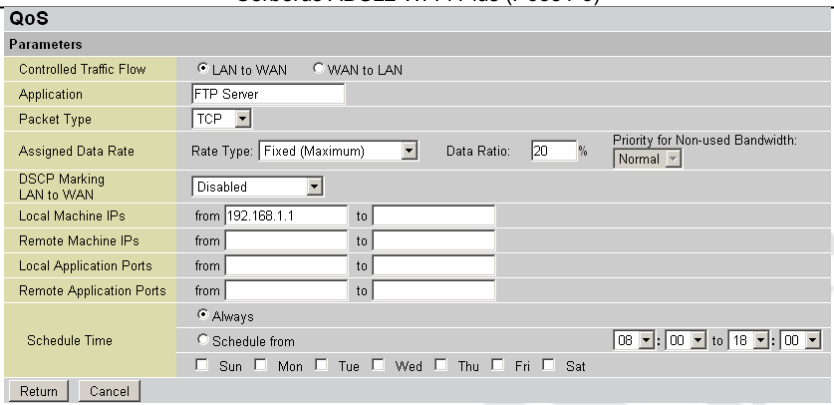
Po kliknięciu pozycji QoS użytkownik może dodawać (Add), edytować (Edit) lub usuwać (Delete) reguły QoS. Ta strona przedstawia skrócone informacje na temat reguł, które zostały dodane lub zmienione. Podaje ona również łączną dostępną przepustowość (nieprzydzieloną), wyrażoną w procentach, którą można przydzielić.



Application (Aplikacja) – Nazwa określająca istniejącą regułę.
Time Schedule (Harmonogram) – Harmonogram zastosowania reguł QoS.
Direction (Kierunek) – Kierunek transmisji, którego ma dotyczyć reguła QoS.
Router oferuje tu dwa możliwe ustawienia:

- **LAN to WAN (z sieci lokalnej do rozległej)** – Kontrola ruchu wychodzącego z sieci lokalnej do świata zewnętrznego, np. jeżeli posiadasz serwer FTP w sieci lokalnej i chcesz, aby reguła QoS kontrolowała szybkość transmisji. W tym celu należy dodać regułę z ustawieniem kierunku „LAN to WAN"
- **WAN to LAN (z sieci rozległej do lokalnej)** – kontrola ruchu przychodzącego z sieci rozległej do sieci lokalnej. Połączenie może być nawiązane zarówno w kierunku od LAN do WAN, jak i odwrotnie.

Assigned Bandwidth Ratio (Przydzielona część pasma) – To pole podaje procent przepustowości przydzielonej przez regułę QoS. Jeżeli istnieje połączenie WAN z Internetem, podana tu będzie szacowana prędkość przesyłu wyrażona w kb/s. Możesz określić stałą prędkość transmisji lub minimalną prędkość gwarantowaną z priorytetem do zajęcia niewykorzystanego pasma.
Non-Assigned Bandwidth Ratio (Nieprzydzielona część pasma) – To pole podaje dostępną przepustowość pasma w kierunku od LAN do WAN oraz odwrotnie, która nie została jeszcze przydzielona.
Add (Dodaj) – Wciśnij ten przycisk, aby dodać nową regułę QoS.
Edit / Delete (Edytuj/Usuń) – Przed użyciem tych przycisków służących do edycji lub usunięcia reguły należy wybrać jedną z reguł, którą chcesz modyfikować.
Apply (Zastosuj) – Po skonfigurowaniu reguł możesz wcisnąć ten przycisk w celu wprowadzenia konfiguracji w życie. Jeżeli zmiana ma zostać trwale zapamiętana w pamięci flash, w lewym oknie wybierz opcję **Save Config to Flash (Zapisz konfigurację w pamięci flash)**.
Po wciśnięciu przycisku **Add** lub **Edit** na ekranie przeglądarki pojawi się następująca strona. Służy ona do definiowania reguł QoS.



Controlled Traffic Flow (Pasmo kontrolowane) – Określ pasmo ruchu, jakie ma być objęte kontrolą. W przypadku protokołu GRE nie ma potrzeby podawania na tej stronie adresów IP ani portów aplikacji. W przypadku innych protokołów należy podać co najmniej jedną wartość.
Packet type (Typ pakietu) – Typ kontrolowanych pakietów. W przypadku protokołu GRE nie ma potrzeba podawania na tej stronie adresów IP ani portów aplikacji. W przypadku innych protokołów należy podać co najmniej jedną wartość.

- **ANY (Dowolnie)** – Brak określonego typu protokołu.
- **TCP**
- **UDP**
- **ICMP**
- **GRE** – Dla połączeń PPTP VPN.

Assigned Data rate (Przydzielona szybkość transmisji) – Określ szybkość transmisji, jaką ma kontrolować niniejsza reguła. Przykładowo, chcemy, aby tylko 20% łącznej przepustowości w kierunku od LAN do WAN było użytkowane na potrzeby serwera FTP. W takim wypadku należy tu określić proporcje przepustowości = 20. Jeżeli dysponujesz linią ADSL o szybkości 256 kb/s, szacunkowa szybkość transmisji dla takiej reguły będzie więc wynosić 20%*256*0,9 = 46 kb/s. (0,9 to szacunkowy współczynnik skutecznej szybkości transmisji dla linii ADSL w kierunku od LAN do WAN. W przypadku kierunku od WAN do LAN, wynosi on pomiędzy 0,85 a 0,8).
Data Ratio (Procent pasma) – Procent pasma przepustowości, jaki ma być kontrolowany przez niniejszą regułę. W powyższym przykładzie z serwerem FTP wynosi on 20.
Rate Type (Typ przepustowości) – Istnieją tu 2 możliwości:

- Fixed (Maximum) – stała szybkość maksymalna: określ stałą szybkość transmisji dla danej reguły. Jest to jednocześnie maksymalna przepustowość dla tej reguły. W powyższym przykładzie z serwerem FTP, jeżeli chcemy „zdławić" szybkość wychodzącej transmisji FTP do 20% z 256 kb/s i ograniczyć się do tej szybkości, można skorzystać z tego ustawienia.
- Guaranteed (Minimum) – gwarantowana szybkość minimalna: określ minimalną szybkość transmisji dla niniejszej reguły. Przykładowo, jeżeli chcemy zapewnić klientom zewnętrznym minimalną przepustowość w celu dostępu do wewnętrznego serwera FTP na poziomie np. 20% całości pasma, można skorzystać z tego ustawienia. Jeżeli następnie jakaś część pasma nie będzie zajęta, zostanie ona przekazana niniejszej regule wg priorytetów określonych w następnym punkcie.

Priority for Non-used Bandwidth (Priorytet użycia niewykorzystanego pasma) – Określ priorytet zastosowania wolnej części pasma. Przykładowo, możesz określić dwie różne reguły QoS dla różnych aplikacji. Obydwie aplikacje wymagają pewnej minimalnej szerokości pasma, ale mogą użytkować również większą jego część, ponad przydzielone minimum, jeżeli jakiś

zakres pasma jest wolny. Dzięki tej funkcji można określić, która aplikacja będzie miała wyższy priorytet w kolejce do wolnej przepustowości.

- **High (Wysoki)**
- **Normal** (Zwykły) – Ustawienie domyślne – zwykły priorytet.
- **Low (Niski)**

Przydział przepustowości regułom o równych priorytetach odbywa się na zasadach pierwszeństwa zgłoszenia.

DSCP Marking (Oznaczenia DSCP) – Oznaczenie Differentiated Services Code Point (DSCP) – pierwsze 6 bitów w bajcie ToS. Oznaczenie DSCP umożliwia użytkownikom klasyfikację ruchu w oparciu o wartość DSCP i skierowanie pakietów do kolejnego routera.

Tablica przypisania DSCP	
Wyłączone	Brak
Maksymalne	Maksymalnie (000000)
Specjalne	Przesyłanie ekspresowe (101110)
Usługa Złota (niska)	Klasa 1, Złoto (001010)
Usługa Złota (średnia)	Klasa 1, Srebro (001100)
Usługa Złota (wysoka)	Klasa 1, Brąz (001110)
Usługa Srebrna (niska)	Klasa 2, Złoto (010010)
Usługa Srebrna (średnia)	Klasa 2, Srebro (010100)
Usługa Srebrna (wysoka)	Klasa 2, Brąz (010110)
Usługa Brązowa (niska)	Klasa 3, Złoto (011010)
Usługa Brązowa (średnia)	Klasa 3, Srebro (011100)
Usługa Brązowa (wysoka)	Klasa 3, Brąz (011110)

Local Machine IPs (Adresy IP komputerów lokalnych) – Adresy IP komputerów lokalnych, które mają być objęte kontrolą. (W przypadku pakietów IP przesyłanych w kierunku od LAN do WAN, jest to źródłowy adres IP. W przypadku pakietów IP przesyłanych od WAN do LAN, jest to docelowy adres IP.)

Remote Machine IPs (Adresy IP komputerów zdalnych) – Adresy IP komputerów zdalnych, które mają być objęte kontrolą. (W przypadku pakietów IP przesyłanych w kierunku od LAN do WAN, jest to docelowy adres IP. W przypadku pakietów IP przesyłanych od WAN do LAN, jest to źródłowy adres IP.)

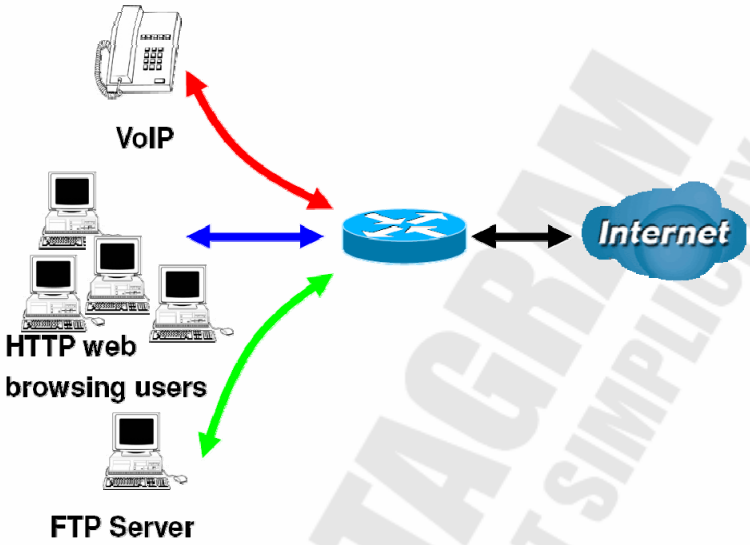
Local Application Ports (Porty aplikacji lokalnych) – Porty aplikacji na komputerach lokalnych, które mają być kontrolowane. (W przypadku pakietów TCP/UDP przesyłanych w kierunku od LAN do WAN, jest to wartość portu źródłowego. W przypadku pakietów TCP/UDP przesyłanych od WAN do LAN, jest to wartość portu docelowego.)

Remote Application Ports (Porty aplikacji zdalnych) – Porty aplikacji na komputerach zdalnych, która mają być kontrolowane. (W przypadku pakietów TCP/UDP przesyłanych w kierunku od LAN do WAN, jest to wartość portu docelowego. W przypadku pakietów TCP/UDP przesyłanych od WAN do LAN, jest to wartość portu źródłowego.)

Schedule Time (Harmonogram) – Harmonogram stosowania reguł QoS.

Przykład zastosowania funkcji QoS w sieci

Schemat połączeń



Szybkość łącza abonenckiego ADSL
Wysyłanie: 256 kb/s
Pobieranie: 2048 Mb/s

Przykładowy plan reguł QoS

Aplikacja	IP lub porty	Kontrola kierunku	Procent pasma	Harmonogram
Użytkownik VoIP	192.168.1.1	Ruch wychodzący	Min. 20% z wysokim priorytetem użycia niezajętego pasma z oznaczeniem DSCP Klasa 1, usługa Złota	Zawsze
Serwer FTP	192.168.1.100	Ruch przychodzący i wychodzący	Ruch wychodzący: min. 30% pasma. Ruch przychodzący: Min. 30% pasma. Oba kierunki z niskim priorytetem użycia niezajętego pasma.	Tylko w godzinach roboczych: między 9:00 a 17:00, od poniedziałku do piątku.
Użytkownicy przeglądając y sieć HTTP	80	Ruch przychodzący i wychodzący	Ruch wychodzący: Ograniczenie do 20% pasma. Ruch przychodzący: Ograniczenie do 30% pasma.	Zawsze

Przykładowa konfiguracja QOS

QoS

Maximum ISP Bandwidth

Type: Auto(ADSL Sync. Rate) | Upstream(LAN->WAN): 0 Kbps | Downstream(WAN->LAN): 0 Kbps

QoS Rule List

	Application	Time Schedule	Direction	Assigned Bandwidth Ratio
○	VoIP	Always On	LAN to WAN	20% Minimum Guaranteed Rate with High priority
○	FTP_Server_Out	Day Time	LAN to WAN	30% Minimum Guaranteed Rate with Low priority
○	FTP_Server_In	Day Time	WAN to LAN	30% Minimum Guaranteed Rate with Low priority
○	HTTP_Browsing_Out	Always On	LAN to WAN	20% Fixed Rate
○	HTTP_Browsing_In	Always On	WAN to LAN	30% Fixed Rate

Non-Assigned Bandwidth Ratio

	Rate Type: Fixed (Maximum)	LAN to WAN : **30%**	WAN to LAN : **40%**

Add | Edit | Delete

Apply | Cancel

- **Aplikacja VoIP**

  Przesył głosu to zastosowanie szczególnie wrażliwe na wszelkie opóźnienia transmisji. Większość urządzeń VoIP stosuje protokół SIP. Moduł SIP automatycznie dokona przydziału numeru portu. Lepiej jest użyć stałego numeru IP do odbioru pakietów VoIP jako danych o wysokim priorytecie.

QoS

Parameters

Controlled Traffic Flow	◉ LAN to WAN ○ WAN to LAN
Application	VoIP
Packet Type	Any
Assigned Data Rate	Rate Type: Guaranteed (Minimum) Data Ratio: 20 % Priority for Non-used Bandwidth: High
DSCP Marking LAN to WAN	Gold service(L)
Local Machine IPs	from 192.168.1.1 to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from to
Schedule Time	◉ Always ○ Schedule from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Return | Cancel

Powyższe ustawienia ułatwią poprawę jakości usługi VoIP nawet przy pełnym obciążeniu łącza.

- **Serwer FTP**

  Część firm tworzy serwery FTP, aby umożliwić klientom pobieranie lub udostępnianie plików za pośrednictwem protokołu FTP.

  Kierunek od LAN do WAN:

QoS	
Parameters	
Controlled Traffic Flow	◉ LAN to WAN ○ WAN to LAN
Application	FTP_Server_Out
Packet Type	Any
Assigned Data Rate	Rate Type: Guaranteed (Minimum) Data Ratio: 30 % Priority for Non-used Bandwidth: Low
DSCP Marking LAN to WAN	Disabled
Local Machine IPs	from 192.168.1.100 to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from to
Schedule Time	○ Always ◉ Schedule from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Return Cancel	

  Kierunek od WAN do LAN:

QoS	
Parameters	
Controlled Traffic Flow	○ LAN to WAN ◉ WAN to LAN
Application	FTP_Server_In
Packet Type	Any
Assigned Data Rate	Rate Type: Guaranteed (Minimum) Data Ratio: 30 % Priority for Non-used Bandwidth: Low
DSCP Marking LAN to WAN	Disabled
Local Machine IPs	from 192.168.1.100 to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from to
Schedule Time	○ Always ◉ Schedule from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Return Cancel	

  Powyższe ustawienia pozwalają ograniczyć wykorzystanie wysyłki danych FTP. Harmonogram pozwala też wprowadzić ograniczenia wyłącznie na czas pracy instytucji.

- **Przeglądanie sieci HTTP**

  W celu kontroli przeglądania stron WWW należy określić regułę dla portu HTTP 80 (lub 8080 dla niektórych serwerów proxy).

  Kierunek od LAN do WAN:

QoS	
Parameters	
Controlled Traffic Flow	(•) LAN to WAN ( ) WAN to LAN
Application	HTTP_Browsing_Out
Packet Type	Any
Assigned Data Rate	Rate Type: Fixed (Maximum) Data Ratio: 20 % Priority for Non-used Bandwidth: Normal
DSCP Marking LAN to WAN	Disabled
Local Machine IPs	from to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from 80 to
Schedule Time	(•) Always ( ) Schedule from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Return Cancel	

  Kierunek od WAN do LAN:

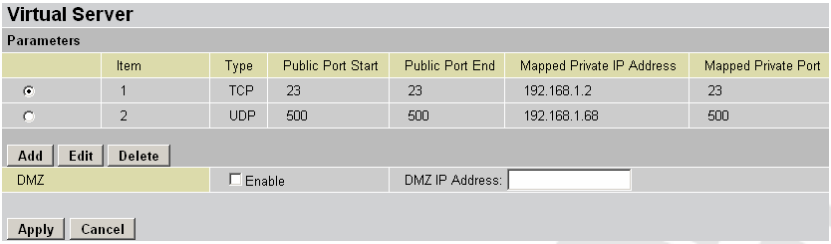
QoS	
Parameters	
Controlled Traffic Flow	( ) LAN to WAN (•) WAN to LAN
Application	HTTP_Browsing_In
Packet Type	Any
Assigned Data Rate	Rate Type: Fixed (Maximum) Data Ratio: 30 % Priority for Non-used Bandwidth: Normal
DSCP Marking LAN to WAN	Disabled
Local Machine IPs	from to
Remote Machine IPs	from to
Local Application Ports	from to
Remote Application Ports	from 80 to
Schedule Time	(•) Always ( ) Schedule from 08 : 00 to 18 : 00 ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat
Return Cancel	

Configuration / Virtual Server

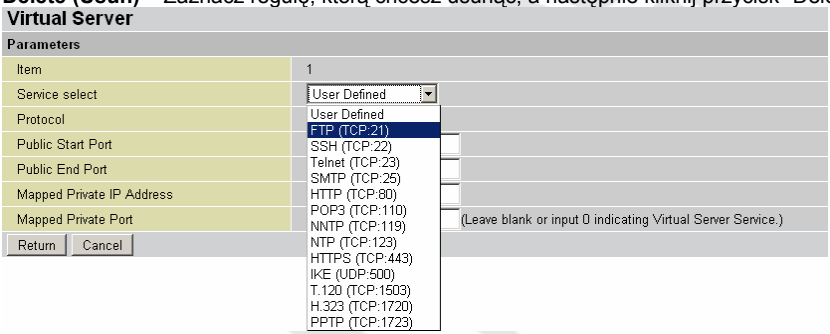
W sieciach TCP/IP oraz UDP, port to numer 16-bitowy stosowany do określenia, do której aplikacji (zazwyczaj działającej jako serwer) należy skierować nadchodzące połączenia. Niektóre porty mają numery formalnie przydzielone przez organizację IANA (Internet Assigned Numbers Authority). Są one określane jako „powszechnie znane porty". Serwery przestrzegają przydziału powszechnie znanych portów, tak aby klienty nie miały kłopotów z ich lokalizacją.
Jeżeli użytkownik chce uruchomić serwer w sieci, do której będzie istniał dostęp z sieci rozległych (tzn. z innych komputerów w Internecie, które funkcjonują poza siecią lokalną) bądź będzie wykorzystywał dowolną aplikację przyjmującą połączenia przychodzące (np. oprogramowanie P2P, takie jak komunikatory internetowe lub klienty sieci wymiany plików P2P) i stosuje mechanizm NAT (Network Address Translation), wówczas należy skonfigurować router w taki sposób, aby przekierowywał połączenia przychodzące do konkretnego komputera w sieci, na którym działa dana aplikacja. Przekierowanie portów jest również niezbędne, jeżeli użytkownik chce pełnić rolę serwera-hosta gry sieciowej.
Jest to wynikiem zastosowania funkcji NAT, na skutek której cała sieć lokalna figuruje pod pojedynczym publicznie dostępnym adresem IP, wskazującym na router, który dopiero musi skierować cały ruch pod odpowiednie prywatne adresy IP używane przez poszczególne komputery. Bliższe informacje na temat mechanizmu NAT można znaleźć w sekcji niniejszej instrukcji poświęconej konfiguracji **WAN**.
Instytucja Internet Assigned Numbers Authority (IANA) jest centralną organizacją koordynującą przydział niepowtarzalnych wartości parametrów dla protokołów internetowych. Zakres numerów portów obejmuje liczby od 0 do 65535, ale tylko porty o numerach od 0 do 1023 są zarezerwowane na usługi uprzywilejowane i określone jako „powszechnie znane porty" Porty zastrzeżone noszą numery od 1024 do 49151. Pozostałe porty, określane jako porty dynamiczne lub prywatne, noszą numery od 49152 do 65535.
Przykłady portów powszechnie znanych oraz zastrzeżonych są przedstawione poniżej. Dalsze informacje są dostępne na witrynie IANA pod adresem: *http://www.iana.org/assignments/port-numbers*

Porty powszechnie znane i zastrzeżone

Numer portu	Protokół	Opis
20	TCP	Dane FTP
21	TCP	Sterowanie FTP
22	TCP i UDP	Protokół logowania zdalnego SSH
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP i UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	WWW HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
119	TCP	NEWS (Network News Transfer Protocol)
123	UDP	NTP (Network Time Protocol)
161	TCP	SNMP
443	TCP i UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
4000	TCP	ICQ
7070	UDP	RealAudio



Item (Nr) – Numer porządkowy
Type (Typ) – Wybierz TCP, jeżeli chcesz z wykorzystaniem numeru portu wyszukiwać na serwerze zdalnym usługi aplikacyjne oparte na połączeniu.
Port Start & Port End (Port początkowy i końcowy) – Wpisz publiczny numer portu i zakres, jaki chcesz skonfigurować.
Add (Dodaj) – Kliknij, aby dodać nową regułę serwera wirtualnego. Kliknij ponownie, aby wyświetlić kolejną pozycję.
Edit (Edytuj) – Zaznacz regułę, którą chcesz modyfikować, a następnie kliknij przycisk „Edit".
Delete (Usuń) – Zaznacz regułę, którą chcesz usunąć, a następnie kliknij przycisk "Delete".



Item (Nr) – Numer porządkowy
Service select (Wybór usługi) – Wybierz usługę, która ma być konfigurowana
Protocol (Protokół) – Opcja ustawiana automatycznie po wybraniu wartości „ Service select"
Start Port & End Port (Port początkowy i końcowy) – Wpisz publiczny numer portu i zakres, jaki chcesz skonfigurować.
IP Address (Adres IP) – Wpisz adres IP konkretnego serwera wewnętrznego, do którego kierowane są żądania z określonego portu.

Z uwagi na to, iż NAT działa jako „naturalna" zapora sieciowa, router chroni sieć przed dostępem użytkowników zewnętrznych, gdyż wszystkie połączenia przychodzące są kierowane do routera. Sytuacja ulega zmianie, jeżeli utworzysz wpisy Serwera wirtualnego, który będzie przekierowywał dane z portów do odpowiednich komputerów w twojej sieci. Jeżeli router ma dopuszczać użytkowników zewnętrznych do serwerów wewnętrznych, np. serwera WWW, serwera FTP, serwera poczty elektronicznej lub serwera gry, wówczas działa on w funkcji „serwera wirtualnego". Możesz skonfigurować serwer lokalny z konkretnymi numerami portów przydzielonymi do wykorzystywanych usług, np. WWW/HTTP (port 80), FTP (port 21), Telnet (port 23), SMTP (port 25) albo POP3 (port 110). Kiedy router odbierze żądanie dostępu skierowane do konkretnego portu, wówczas przekieruje je do odpowiedniego serwera wewnętrznego.

Przykładowo, jeżeli zdefiniujesz, iż port numer 80 (WWW/HTTP) ma być przypisany do adresu IP 192.168.1.2, wówczas wszystkie odbierane żądania HTTP od użytkowników zewnętrznych będą przekierowywane na serwer lokalny (komputer) o adresie IP 192.168.1.2. Jeżeli do danego zastosowania nie jest przydzielony żaden port, można ręcznie dokonać takiego przypisania.

Virtual Server

Parameters

	Item	Type	Public Port Start	Public Port End	Mapped Private IP Address	Mapped Private Port
◉	1	TCP	80	80	192.168.1.2	80

Oprócz określenia użytego numeru portu należy również wskazać używany protokół. Protokół jest zależny od konkretnej aplikacji. Większość programów posługuje się protokołami TCP lub UDP, ale rozwijana lista w menu **Protocol (Protokół)** zawiera również inne możliwości. Ustawienie tego pola na wartość „all" („wszystkie") spowoduje, iż wszystkie przychodzące połączenia wykorzystujące dowolny protokół i skierowane do dowolnego portu będą przekierowywane pod wskazany adres IP.

DMZ – Host strefy zdemilitaryzowanej (Demilitarized Zone – DMZ) to komputer lokalny widoczny w Internecie. Jeżeli użytkownik wskaże konkretny wewnętrzny adres IP jako Hosta DMZ, wówczas wszystkie nadchodzące pakiety zostaną skontrolowane przez algorytmy zapory i NAT, a następnie – jeżeli nie odpowiadają żadnemu z numerów portów określonych we wpisach Serwera wirtualnego – zostaną przesłane do hosta DMZ.

Uwaga: Zastosowanie przekierowania portów ma swoje konsekwencje dla bezpieczeństwa sieci, gdyż dzięki temu mechanizmowi użytkownicy zewnętrzni będą w stanie podłączać się do komputerów w wewnętrznej sieci. Dlatego zaleca się stosowanie konkretnych wpisów Serwera wirtualnego opisujących wyłącznie porty wymagane przez dane aplikacje oraz unikanie tworzenia strefy DMZ albo wpisu dla „wszystkich" protokołów, co w rezultacie spowoduje, że wszystkie żądania połączenia trafiające pod publiczny adres IP trafią do określonego komputera.

Ostrzeżenie: Jeżeli wyłączysz opcję NAT w sekcji WAN-ISP, funkcja Serwera wirtualnego również przestaje działać.

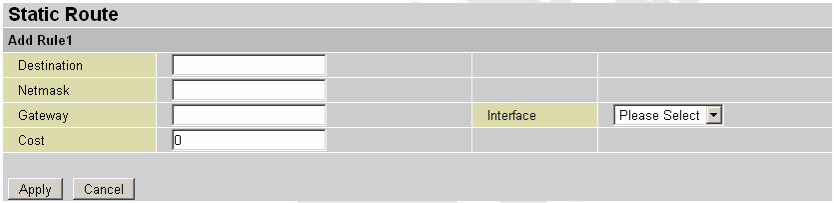
Ostrzeżenie: Jeżeli opcja serwera DHCP jest włączona, należy z najwyższą ostrożnością przydzielać adresy IP Serwerów wirtualnych, tak aby uniknąć potencjalnych konfliktów. Najprostszą metodą konfiguracji Serwerów wirtualnych jest ręczne przydzielanie statycznych adresów IP każdemu komputerowi stanowiącemu serwer wirtualny (z takim adresem, który nie mieści się w zakresie adresów IP rozdzielanych przez serwer DHCP. Istnieje możliwość ręcznego skonfigurowania adresu IP serwera wirtualnego, ale nadal musi on pozostawać w tej samej podsieci, co router.

Configuration / Advanced

Opcje konfiguracyjne ujęte w sekcji Advanced (Zaawansowane) są przeznaczone dla użytkowników pragnących wykorzystać bardziej zaawansowane możliwości routera. Użytkownicy, którzy nie znają dokładnie znaczenia tych funkcji, nie powinni podejmować prób zmian konfiguracji routera, o ile nie zaleci tego wyraźnie personel pomocy technicznej.
Sekcja Zaawansowane mieści sześć pozycji: **Static Route (Routing statyczny)**, **Static ARP (Statyczny ARP)**, **Dynamic DNS (Dynamiczne DNS)**, **VLAN Control (Sterowanie VLAN)**, **Device Management (Zarządzanie urządzeniami)** oraz **IGMP**.

- ### Static Route (Routing statyczny)

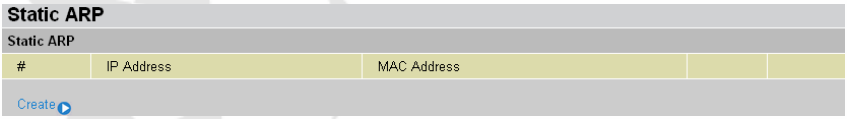
  Kliknij opcję **Static Route** i wciśnij przycisk **Create (Utwórz)**, aby dodać tablicę routingu.

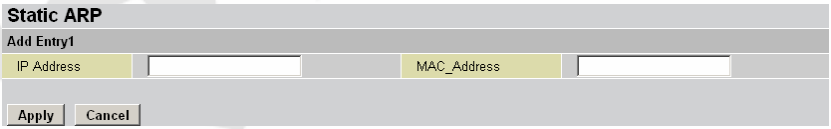


Destination (Punkt docelowy) – Adres IP podsieci docelowej.
Netmask (Maska sieci) – Maska podsieci docelowych adresów IP, na podstawie powyższego adresu docelowego.
Gateway (Brama) – Adres IP bramy, do którego przesyłane są pakiety.
Interface (Interfejs) – Wybór interfejsu, za pomocą którego przesyłane są pakiety.
Cost (Koszt) – Koszt transmisji dla potrzeb routingu. Podana wielkość nie musi być precyzyjna, ale powinna się mieścić w przedziale od 0 do 65535.

- ### Static ARP

  Kliknij opcję **Static ARP** i wciśnij przycisk **Create (Utwórz)**, aby utworzyć statyczną tablicę ARP.



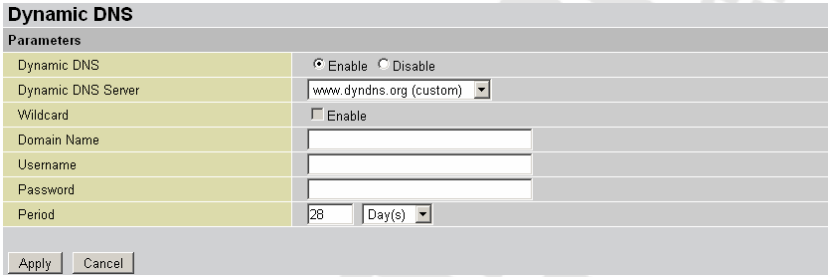


Wpisz **IP Address (Adres IP)** oraz **MAC_Address (Adres MAC)** hosta, który będzie dodany do statycznej tablicy ARP.

- **Dynamic DNS**

Funkcja Dynamic DNS pozwala kojarzyć dynamiczny adres IP ze stałą nazwą hosta. Jeżeli więc dostawca usług internetowych nie przydzieli stałego adresu IP, nadal będziesz mógł używać wybranej nazwy domeny. Funkcja ta jest szczególnie przydatna w przypadku utrzymywania serwerów za pomocą połączenia ADSL, tak iż każdy, kto chce nawiązać połączenie z serwerem, będzie mógł użyć nazwy domeny zamiast dynamicznego adresu IP, który od czasu do czasu ulega zmianom. Ten dynamiczny adres IP to adres IP routera w sieci rozległej, przydzielony przez dostawcę usług internetowych.

Aby móc korzystać z tej usługi, należy w pierwszej kolejności zarejestrować się i założyć konto u dostawcy usług dynamicznego DNS za pomocą odpowiedniej witryny internetowej, np. http://www.dyndns.org/



Urządzenie obsługuje ponad 5 różnych usług DDNS.

Disable (Wyłącz) – Zaznacz to pole, aby wyłączyć funkcję dynamicznego DNS.

Enable (Włącz) – Zaznacz to pole, aby włączyć funkcję dynamicznego DNS. Należy wówczas obowiązkowo wypełnić następujące pola.

Dynamic DNS Server (Serwer dynamicznego DNS) – Wybierz usługę DDNS, w której jest założone konto.

Host – Wpisz nazwę zarejestrowanej przez siebie domeny.

Domain Name, Username and Password (Nazwa domeny, nazwa użytkownika i hasło) – Wpisz swoją zarejestrowaną nazwę domeny, nazwę użytkownika usługi oraz hasło.

Period (Okres) – Zdefiniuj czas pomiędzy aktualizacjami – okres, co jaki router ma wymieniać informacje z serwerem DDNS. Router dokonuje automatycznej aktualizacji zgodnie z tym ustawieniem oraz dodatkowo za każdym razem, kiedy dochodzi do zmiany dynamicznego adresu IP.

Wildcard (Maska) – Zaznacz to pole, aby włączyć funkcję DYNDNS Wildcard.

- **VLAN Control**

VLAN (Virtual Local Area Network, wirtualna sieć lokalna) to grupa urządzeń umieszczonych w różnych segmentach fizycznej sieci lokalnej, które mogą komunikować się ze sobą, tak jakby znajdowały się w tym samym segmencie fizycznej sieci. Klienty i serwery mogą być umiejscowione w dowolnym miejscu w sieci, ale są one grupowane za pomocą technologii VLAN. Wszelkie transmisje są przesyłane do odpowiednich urządzeń w obrębie sieci wirtualnej.

VLAN Group Control

Parameters

	VLAN Group Name	VLAN ID	Ethernet port #1	Ethernet port #2	Ethernet port #3	Ethernet port #4	wireless LAN	Link VLAN Group to WAN Connection interface	WAN Tagging
1	VLAN_GROUP1	2	☐	☐	☐	☐	☐	No	☐
2	VLAN_GROUP2	3	☐	☐	☐	☐	☐	No	☐
3	VLAN_GROUP3	4	☐	☐	☐	☐	☐	No	☐
4	VLAN_GROUP4	5	☐	☐	☐	☐	☐	No	☐
5	VLAN_GROUP5	6	☐	☐	☐	☐	☐	No	☐
6	VLAN_GROUP6	7	☐	☐	☐	☐	☐	No	☐
7	VLAN_GROUP7	8	☐	☐	☐	☐	☐	No	☐
8	VLAN_GROUP8	9	☐	☐	☐	☐	☐	No	☐
LAN Tagging									
			☐	☐	☐	☐	☐		

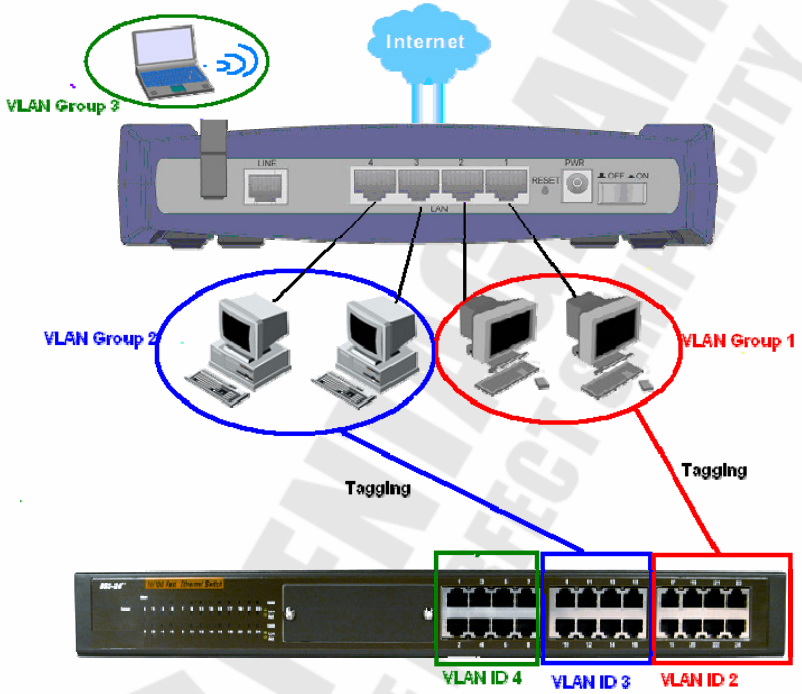
Apply Cancel

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.
WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface.(Only for Bridge)

VLAN Group Name (Nazwa grupy VLAN) – Użytkownik może samodzielnie skonfigurować do ośmiu możliwych grup.
VLAN ID (Identyfikator VLAN) – Identyfikator nazwy grupy.
LAN Tagging (Oznaczenie VLAN) – Powiązanie identyfikatora VLAN z konkretną grupą VLAN dla potrzeb interfejsu Ethernet.
Ethernet port (Port Ethernet) – Nazwa portu routera
Link VLAN Group to WAN connection Interface (Połącz grupę VLAN z interfejsem połączenia WAN) – Wybór interfejsu połączenia WAN łączącego grupę VLAN.

Funkcja sieci wirtualnej stanowi bardzo wygodny sposób zarządzania hostami poprzez grupowanie ich w podziale wg portów fizycznych, tak jak to przedstawiono w poniższym przykładzie.

1. Grupa VLAN 1 składa się z hostów użytkujących port1 i port2, Grupa VLAN 2 składa się z hostów użytkujących port3 i port4, zaś Grupa VLAN 3 składa się z urządzeń lokalnej sieci bezprzewodowej.



2. Po zaznaczeniu pola w celu włączenia funkcji VLAN należy sprawdzić tablicę pod kątem własnych potrzeb.

VLAN Group Control

Parameters

	VLAN Group Name	VLAN ID	Ethernet port #1	Ethernet port #2	Ethernet port #3	Ethernet port #4	wireless LAN	Link VLAN Group to WAN Connection interface	WAN Tagging
1	VLAN_GROUP1	2	☑	☑	☑	☐	☐	Main WAN connection(Management)	☐
2	VLAN_GROUP2	3	☑	☐	☐	☑	☐	WAN Bridge Connection #1 (0/101)	☐
3	VLAN_GROUP3	4	☐	☐	☐	☐	☑	WAN Bridge Connection #1 (0/101)	☐
4	VLAN_GROUP4	5	☐	☐	☐	☐	☐	No	☐
5	VLAN_GROUP5	6	☐	☐	☐	☐	☐	No	☐
6	VLAN_GROUP6	7	☐	☐	☐	☐	☐	No	☐
7	VLAN_GROUP7	8	☐	☐	☐	☐	☐	No	☐
8	VLAN_GROUP8	9	☐	☐	☐	☐	☐	No	☐

LAN Tagging

☐	☐	☐	☐	☐	

Apply Cancel

LAN Tagging: Insert or keep VLAN tag of the packets flow through the specific ethernet port.
WAN Tagging: Insert or keep VLAN tag of the packets flow through the specific Bridged WAN interface.(Only for Bridge)

- **Device Management**

Zaawansowane ustawienia konfiguracyjne z zakresu zarządzania urządzeniami służą do regulacji funkcji bezpieczeństwa routera oraz funkcji monitorowania pracy urządzenia.

Device Management			
Embedded Web Server			
HTTP Port	80	(80 is default HTTP port)	
Universal Plug and Play (UPnP)			
UPnP	◉ Enable ○ Disable		
UPnP Port	2800		
Telnet Configuration			
Telnet	○ Enable ◉ Disable		
SNMP Access Control			
SNMP	○ Enable ◉ Disable		
SNMP V1 and V2			
Read Community	public	IP Address	0.0.0.0
Write Community	password	IP Address	0.0.0.0
Trap Community		IP Address	
SNMP V3			
Username		Password	
Access Right	◉ Read ○ Read/Write		
Apply	Cancel		

Embedded Web Server:

HTTP Port (Port HTTP) – Numer portu wbudowanego serwera WWW routera (do zastosowań konfiguracji poprzez WWW). Wartość domyślna to standardowy port HTTP, czyli port 80. Jeżeli jednak np. w sieci lokalnej działa serwer WWW na jednym z komputerów, można tu wybrać inny numer portu.

Przykład: Użytkownik A zmienia numer portu HTTP na **100**, określa własny adres IP na **192.168.1.55** oraz określa czas wylogowania na **100** sekund. Router umożliwi użytkownikowi A dostęp do interfejsu WWW wyłącznie z adresu IP **192.168.1.55**. W celu zalogowania użytkownik musi wpisać w przeglądarce adres *http://192.168.1.254:100*. Po upływie 100 sekund urządzenie automatycznie wyloguje Użytkownika A.

Universal Plug and Play (UPnP):

Mechanizm UPnP oferuje łączność sieciową komputerów i innych urządzeń sieciowych (na zasadach sieci równorzędnej peer-to-peer) oraz kontrolę i przesył danych pomiędzy urządzeniami. Mechanizm UPnP daje wiele korzyści zwłaszcza użytkownikom wykorzystującym router NAT poprzez funkcję UPnP NAT Traversal. W obsługiwanych systemach mechanizm ten znacznie ułatwia przekierowanie portów dzięki temu, iż zezwala on aplikacji na kontrolę niezbędnych ustawień, przez co użytkownik nie ma potrzeby kontrolowania zaawansowanej konfiguracji swojego urządzenia.

Aby funkcja działała prawidłowo, UPnP musi być obsługiwane nie tylko przez router, ale również przez system operacyjny użytkownika oraz odpowiednie aplikacje. Systemy Windows XP oraz Windows Me fabrycznie obsługują UPnP (jeżeli zainstalowany jest odpowiedni składnik), zaś użytkownicy Windows 98 powinni w tym celu zainstalować klienta Internet Connection Sharing pochodzącego z Windows XP. System Windows 2000 nie obsługuje funkcji UPnP.

Disable (Wyłącz) – Zaznacz to pole, aby wyłączyć funkcję UPnP routera.

Enable (Włącz) – Zaznacz to pole, aby włączyć funkcję UPnP routera.

UPnP Port (Port UPnP) – Ustawienie domyślne to 2800. Zaleca się użytkowanie tego właśnie portu. Wartość tę należy zmienić, jeżeli wywołuje ona konflikt z innymi, już używanymi portami.

SNMP Access Control:

W celu zastosowania tej funkcji niezbędna jest obecność oprogramowania protokołu Simple Network Management Protocol (SNMP) na komputerach znajdujących się w sieci lokalnej.

SNMP V1 i V2:

Read Community (Grupa odczytu) – Określ nazwę, która ma określać tzw. grupę Read Community oraz adres IP. Ciąg ten jest porównywany z ciągiem istniejącym w pliku konfiguracyjnym. Jeżeli ciągi pasują do siebie, dany użytkownik może uzyskać dostęp do adresu IP oraz przeglądać dane.

Write Community (Grupa zapisu) – Określ nazwę, która ma określać tzw. grupę Write Community oraz adres IP. Ciąg ten jest porównywany z ciągiem istniejącym w pliku konfiguracyjnym. Jeżeli ciągi pasują do siebie, dany użytkownik może uzyskać dostęp do adresu IP oraz przeglądać i modyfikować dane.

Trap Community (Grupa komunikatów Trap) – Określ nazwę i adres IP. Ciąg ten jest porównywany z ciągiem istniejącym w pliku konfiguracyjnym. Jeżeli ciągi pasują do siebie, użytkownicy z tego adresu IP otrzymują komunikaty SNMP Trap.

SNMP V3:

Określ nazwę i hasło uwierzytelniające, a następnie określ prawa dostępu przydzielone użytkownikom występującym pod określonymi adresami IP. Po pomyślnym uwierzytelnieniu użytkownicy spod danego adresu IP będą mieli prawo przeglądania i modyfikowania danych.

Wersja SNMP: SNMPv2c i SNMPv3

Wariant SNMPv2c to rozszerzone funkcje protokołu SNMPv2 bez zabezpieczeń SNMPv2. Litera „c" wskazuje, iż protokół SNMPv2c używa paradygmatu ciągu grupy („community”) SNMPv1 w celu „zabezpieczeń", ale jest powszechnie akceptowany jako standard SNMPv2.

SNMPv3 to efektywny mechanizm uwierzytelnienia z możliwościami precyzyjnej regulacji, służący do monitorowania zdalnego.

Obsługiwane komunikaty Trap to: Cold Start, Authentication Failure.

Obsługiwane są następujące bazy MIB:

Z RFC 1213 (MIB-II):
- ✓ Grupa systemowa
- ✓ Grupa interfejsów
- ✓ Grupa translacji adresów
- ✓ Grupa IP
- ✓ Grupa ICMP
- ✓ Grupa TCP
- ✓ Grupa UDP
- ✗ EGP (nie dotyczy)
- ✓ Transmisja
- ✓ Grupa SNMP

Z RFC1650 (EtherLike-MIB):
- ✓ dot3Stats

Z RFC 1493 (Bridge MIB):
- ✓ grupa dot1dBase
- ✓ grupa dot1dTp
- ✓ grupa dot1dStp (w konfiguracji jako Spanning Tree)

Z RFC 1471 (PPP/LCP MIB):
- ✓ grupa pppLink
- ✗ grupa pppLqr

Z RFC 1472 (PPP/Security MIB):
- ✓ Grupa PPP Security Group)

Z RFC 1473 (PPP/IP MIB):
- ✓ Grupa PPP IP

Z RFC 1474 (PPP/Bridge MIB):
- ✓ Grupa PPP Bridge

Z RFC1573 (IfMIB):
- ✓ Grupa ifMIBObjects

Z RFC1695 (atmMIB):
- ✓ atmMIBObjects

Z RFC 1907 (SNMPv2):
- ✓ Tylko snmpSetSerialNo OID

- **IGMP**

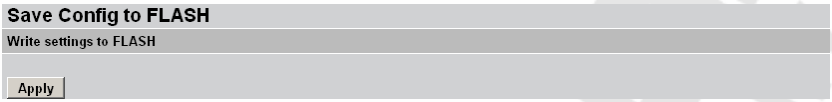
Protokół IGMP czyli Internet Group Management Protocol służy do obsługi hostów zarządzających grupami multikastowymi.

IGMP	
Parameters	
IGMP Proxy	○ Enable ◉ Disable
IGMP Snooping	○ Enable ◉ Disable
Apply Cancel	

IGMP Proxy (Serwer proxy IGMP) – Odbiór pakietu typu multicast. Ustawienie domyślne to **Disable (Wyłączony)**.
IGMP Snooping – Opcja umożliwia przełącznikowi Ethernet sprawdzenie i podjęcie prawidłowych decyzji co do przekierowania danych. Ustawienie domyślne to **Enable (Włączony)**

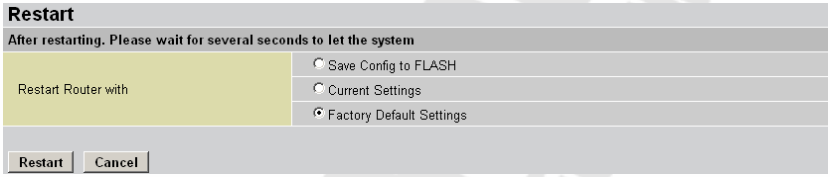
Zakładka Save Configuration to Flash

Po zmianie ustawień konfiguracyjnych routera należy zapisać całość parametrów konfiguracyjnych w pamięci flash, tak aby nie zostały one utracone po wyłączeniu lub zresetowaniu routera. Kliknij przycisk **Save (Zapisz)** w celu zapisania nowej konfiguracji do pamięci flash.



Zakładka Restart

Kliknij przycisk **Restart (Uruchom ponownie)** z opcją **Current Settings (Bieżące ustawienia)**, jeżeli chcesz ponownie uruchomić router i przywrócić ostatnio zapisaną konfigurację).



Jeżeli chcesz ponownie uruchomić router przy użyciu domyślnych ustawień fabrycznych (np. po aktualizacji oprogramowania sprzętowego albo zapisania w pamięci nieprawidłowej konfiguracji), wybierz opcję **Factory Default Settings (Domyślne ustawienia fabryczne)** w celu przywrócenia urządzenia do domyślnych ustawień fabrycznych.

Ten sam efekt można również uzyskać, wciskając igłowy przycisk Reset na tylnym panelu urządzenia przez ok. 10-12 sekund w trakcie pracy routera.

Rozwiązywanie problemów

Jeżeli router nie działa prawidłowo, w pierwszej kolejności należy przeczytać ten rozdział opisujący typowe problemy, a dopiero w następnej kolejności kontaktować się z działem pomocy technicznej dostawcy usług internetowych (ISP).

Zastosowanie diod LED w celu diagnozowania problemów

Diody LED ułatwiają określenie potencjalnych przyczyn problemów.

Dioda LED zasilania

Dioda zasilania **POWER LED** na przednim panelu nie zapala się:

1. Sprawdź, czy do routera jest podłączony zasilacz oraz czy zasilacz jest podłączony do odpowiedniego źródła prądu. Należy stosować wyłącznie zasilacz dołączony do zestawu;
2. Sprawdź, czy router oraz źródło zasilania są włączone oraz czy router otrzymuje odpowiednią moc zasilającą;
3. Wyłącz i włącz router;
4. Jeżeli problem nie ustępuje, istnieje możliwość, że sprzęt jest uszkodzony. W takim wypadku należy skontaktować się z producentem urządzenia.

Dioda LED sieci lokalnej

Dioda sieci lokalnej **LAN LED** na przednim panelu nie zapala się:

1. Sprawdź połączenia kabli Ethernet pomiędzy routerem a komputerem lub koncentratorem;
2. Poszukaj ewentualnych uszkodzeń kabli Ethernet;
3. Sprawdź, czy karta Ethernet w komputerze działa prawidłowo;
4. Jeżeli te kroki nie doprowadzą do rozwiązania problemu, poproś o pomoc lokalnego dystrybutora urządzenia.

Dioda LED połączenia ADSL

Dioda połączenia ADSL LED na przednim panelu nie zapala się:

1. Sprawdź kabel telefoniczny i połączenia pomiędzy portem ADSL routera a gniazdkiem ściennym;
2. Upewnij się, że przedsiębiorstwo telefoniczne sprawdziło linię telefoniczną i przygotowało ją do eksploatacji usługi ADSL;
3. Zresetuj linię ADSL, aby odnowić połączenie z DSLAM;
4. Jeżeli te kroki nie doprowadzą do rozwiązania problemu, poproś o pomoc lokalnego dystrybutora urządzenia.

Problemy z interfejsem WWW

Nie można uzyskać dostępu do interfejsu WWW:

1. Upewnij się, że używasz prawidłowego adresu IP routera. Sprawdź adres IP routera;
2. Aby dostęp z sieci lokalnej był możliwy, adresy IP twojego komputera oraz routera muszą należeć do tej samej podsieci;

3. Jeżeli zmieniałeś adres IP sieci lokalnej routera, wpisz nowy adres w polu adresu przeglądarki;
4. Usuń ewentualne filtry w sieci lokalnej lub rozległej, które mogą blokować usługi WWW.

Problemy z nazwą użytkownika i hasłem

Nie pamiętam swojej nazwy użytkownika oraz/albo hasła:

1. Domyślna nazwa użytkownika to: „**admin**”. Domyślne hasło to: „**pentagram**”. Wielkość liter wpisywanych w polach „Hasło” i „Nazwa użytkownika” ma znaczenie. Upewnij się, że wpisujesz odpowiednie hasło i nazwę użytkownika przy użyciu liter o właściwej wielkości;
2. Wciśnij i przytrzymaj przycisk RESET przez 10-12 sekund, a następnie puść go – przywrócone zostaną ustawienia domyślne, a router uruchomi się ponownie;

Problemy z interfejsem LAN

Nie można uzyskać dostępu do routera z sieci lokalnej, a żaden z komputerów w sieci lokalnej nie odpowiada na polecenie ping:

1. Sprawdź diody LED łącza Ethernet na przednim panelu. Dioda LAN LED odpowiadająca właściwemu numerowi portu, do którego podłączony jest komputer, powinna się świecić. Jeżeli dioda nie świeci się, sprawdź kable łączące router z komputerem. Upewnij się, czy na czas rozwiązywania problemu wyłączyłeś wszelkie programowe zapory internetowe;
2. Sprawdź, czy adres IP oraz maska podsieci są identyczne na routerze oraz na stacji roboczej.
3. W niektórych przypadkach system komputer z zainstalowanym systemem Windows Vista lub Windows XP z Service Pack 3 nie może uzyskać adresu IP z serwera DHCP routera. Aby rozwiązać ten problem, 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).

Problemy z interfejsem WAN

Inicjalizacja połączenia ADSL nie powiodła się:

1. Sprawdź połączenia kablowe pomiędzy portem ADSL a gniazdkiem ściennym. Dioda LED połączenia ADSL na panelu przednim routera powinna być włączona;
2. Sprawdź, czy ustawienia VPI, VCI oraz typ enkapsulacji są identyczne, jak te podane przez przedsiębiorstwo telefoniczne oraz dostawcę usług internetowych;
3. Ponownie uruchom router. Jeżeli problemy nadal będą występować, być może trzeba będzie zweryfikować posiadane ustawienia VPI, VCI oraz typ enkapsulacji w przedsiębiorstwie telefonicznym lub u dostawcy usług internetowych.

Nie można uzyskać adresu IP WAN od dostawcy usług internetowych:

1. Sprawdź, czy wszystkie pozostałe urządzenia podłączone do tej samej linii telefonicznej (np. telefony, faksy, modemy analogowe) mają odpowiedni filtr podłączony na linii pomiędzy urządzeniem a gniazdkiem w ścianie (chyba, że posiadasz urządzenie takie jak np. splitter lub filtr centralny zainstalowane przez wykwalifikowanego, uprawnionego instalatora) oraz sprawdź, czy wszystkie filtry są zainstalowane prawidłowo i w odpowiednim kierunku;
2. Brak filtrów na linii lub nieprawidłowo zainstalowane filtry są przyczyną zakłóceń na linii ADSL i mogą powodować częste zrywanie połączenia.

Częste utraty synchronizacji na linii ADSL (rozłączenia):

1. Dostawca usług internetowych dostarcza adres IP WAN po uwierzytelnieniu. W celu uwierzytelnienia można wykorzystać nazwę użytkownika i hasło, adres MAC albo nazwę hosta;

2. Uwierzytelnienie poprzez nazwę użytkownika i hasło ma zastosowanie wyłącznie w odniesieniu do połączeń PPPoE i PPPoA. Sprawdź, czy zostały wpisane prawidłowe parametry **Service Name (Nazwa usługi)**, **Username (Nazwa użytkownika)** oraz **Password (Hasło)**, przy czym wielkość liter ma znaczenie.

PENTAGRAM THE PERFECT SIMPLICITY

Problemy z dostępem do Internetu

Nie można uzyskać dostępu do Internetu:

1. Sprawdź, czy router jest włączony i podłączony do sieci;
2. Jeśli dioda LED ADSL nie świeci się, patrz punkt **Dioda połączenia ADSL** w niniejszej instrukcji rozwiązywania kłopotów;
3. Sprawdź swoje ustawienia WAN;
4. Upewnij się, że wpisano prawidłową nazwę użytkownika i hasło;
5. W przypadku stanowisk bezprzewodowych, sprawdź, czy zarówno router, jak i stanowiska bezprzewodowe stosują ten sam identyfikator ESSID, kanał oraz klucz szyfrowania (jeżeli szyfrowanie jest włączone).

Połączenie z Internetem rozłącza się:

1. Jeżeli używasz enkapsulacji PPPoA lub PPPoE, sprawdź ustawienie czasu nieaktywności;
2. Skontaktuj się z dostawcą usług internetowych.

Jeżeli napotkasz problemy podczas konfiguracji routera ADSL, prosimy o kontakt.

PENTAGRAM THE PERFECT SIMPLICITY