

Instrukcja instalacji i obsługi

PENTAGRAM Cerberus ADSL2+ Wi-Fi (P 6331-5)



Najnowsze wersje instrukcji, sterowników i oprogramowania dostępne są na stronie www.pentagram.pl

2007-08-29

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

Copyright © 2007 PENTAGRAM

Wszelkie prawa zastrzeżone, powielanie i kopiowanie zabronione.

SPIS TREŚCI

WPROWADZENIE.....	5
FUNKCJE URZĄDZENIA	5
ZAWARTOŚĆ PUDEŁKA	6
OBSŁUGA URZĄDZENIA	7
UŻYTKOWANIE MODEMU/ROUTERA CERBERUS	7
PRZEDNI PANEL	7
TYLNI PANEL	8
USTAWIENIA FABRYCZNE	8
RESETOWANIE URZĄDZENIA	8
PODŁĄCZENIE CERBERUSA DO KOMPUTERA	9
KONFIGURACJA WŁAŚCIWOŚCI SIECI	9
KONFIGURACJA ROUTERA PRZEZ WWW	13
LOGOWANIE	13
NAWIGACJA	14
ZAKŁADKA SETUP	16
ZAKŁADKA BASIC	19
ZAKŁADKA ADVANCED	23
ZAKŁADKA WIRELESS	56
ZAKŁADKA SECURITY	63
ZAKŁADKA STATUS	66
ZAKŁADKA HELP	72
ROZWIĄZYWANIE PROBLEMÓW	73
UŻYCIĘ DIOD LED DO ZDIAGNOZOWANIA PROBLEMU	73
PROBLEM Z KONFIGURACJĄ PRZEZ PRZEGLĄDARKĘ	73
PROBLEMY Z LOGOWANIEM	74
PROBLEMY Z KOMUNIKACJĄ Z SIECIĄ LAN	74
PROBLEMY Z KOMUNIKACJĄ Z SIECIĄ WAN	74
PROBLEMY Z POŁĄCZENIEM DO SIECI INTERNET	75



Wprowadzenie

Dziękujemy za zakup modemu/routera Cerberus ADSL2+ Wi-Fi firmy PENTAGRAM. Twój nowy router łączy sobie modem ADSL, router ADSL, przełącznik sieciowy (Ethernet Switch) oraz punkt dostępowy sieci bezprzewodowej (Access Point), czyli dostarcza Ci wszystko czego potrzebujesz do podłączenia swoich urządzeń sieciowych do sieci Internet za pośrednictwem szerokopasmowego łącza ADSL.

Router Cerberus ADSL2+ Wi-Fi jest zgodny ze standardem ADSL2+, co umożliwia jego wykorzystanie na całym świecie i oferuje prędkości rzędu do 24 Mbps przy pobieraniu oraz do 1 Mbps przy wysyłaniu. Zaprojektowany z myślą o małych biurach, domowych biurach i użytkownikach prywatnych, router umożliwia szybsze połączenie z Internetem. Możesz cieszyć się usługami ADSL czy szerokopasmowymi aplikacjami multimedialnymi takimi jak gry internetowe, strumieniowane video czy audio w czasie rzeczywistym – jest to prostsze i szybsze niż kiedykolwiek dotąd.

Funkcje urządzenia

- Fast Ethernet Switch: 4-portowy koncentrator przełączający służy do podłączania maszyn pracujących po stronie sieci LAN.
- IEEE 802.11g 54Mbps Wireless LAN: interfejs sieci bezprzewodowej; umożliwia dostęp do sieci zewnętrznej (WAN) komputerom połączonym drogą radiową.
- Network Address Translation (NAT): rozbudowane funkcje protokołu NAT pozwalają wielu użytkownikom uzyskiwać dostęp do zasobów sieci zewnętrznej (np. Internet) przy użyciu pojedynczego, publicznego adresu IP.
- Universal Plug and Play (UPnP) oraz UPnP NAT Traversal: protokoły te wykorzystywane są do ustanowienia prostego i szybkiego łącza między urządzeniami i komputerami PC pochodzącymi od wielu różnych producentów. Sprawiają one, że korzystanie z sieci jest łatwiejsze.
- Usługa Dynamiczny DNS umożliwia utrzymywanie stałej domeny użytkownikom korzystającym z dynamicznego adresu IP. Aby korzystać z tej usługi należy zarejestrować się w jednym z serwisów oferujących DDNS, np. <http://www.dyndns.org>.
- Virtual Server: funkcja wirtualnych serwerów pozwala użytkownikowi tak skonfigurować urządzenie, aby móc uzyskiwać dostęp do usług uruchomionych na komputerach w sieci LAN z sieci WAN. Urządzenie potrafi wykryć nadchodzące zapytanie do konkretnej usługi i przekazać je do właściwego komputera, na którym serwer tej usługi jest uruchomiony. Można np. tak skonfigurować Cerberusa, aby użytkownicy z sieci zewnętrznej (WAN) mogli mieć dostęp do serwera WWW pracującego wewnątrz sieci LAN. Istnieje także możliwość skonfigurowania tzw. „strefy zdemilitaryzowanej” (DMZ) dla któregoś z komputerów pracujących w sieci LAN, wówczas komputer taki jest wystawiony na wszelkie zapytania z sieci WAN (np. Internetu).
- Dynamic Host Configuration Protocol (DHCP) Klient oraz Serwer: od strony sieci WAN klient sieci DHCP może automatycznie uzyskać adres IP od dostawcy usług internetowych (ISP). Po stronie sieci lokalnej wbudowany serwer DHCP może automatycznie przydzielić adresy IP, a także ustawienia serwerów DNS nawet 253 komputerom pracującym w sieci, co zdecydowanie ułatwia zarządzanie siecią.

- Routowanie statyczne oraz RIP1/2: wsparcie dla tablicy routowania statycznego oraz obsługa protokołów RIP1/2.
- SNMP (*Simple Network Management Protocol*): protokół pozwalający zbierać informacje o pracy sieci. Cerberus ma wbudowany serwer tego protokołu, dzięki czemu specjalistyczne oprogramowanie może monitorować pracę urządzenia.
- Zdalne zarządzanie przez przeglądarkę WWW: urządzenie zarządzane jest przez graficzny interfejs użytkownika (GUI), do którego uzyskuje się dostęp za pomocą zwykłej przeglądarki WWW. Interfejs jest łatwy w obsłudze. Istnieje także możliwość zarządzania urządzeniem z sieci WAN (np. przez Internet).
- Aktualizacje oprogramowania: oprogramowanie zarządzające urządzeniem może być łatwo zaktualizowane przy użyciu graficznego interfejsu użytkownika.
- Wsparcie dla wielu standardów ADSL: transmisja danych z prędkościami do 24 Mb/s (wysyłanie) oraz do 1 Mb/s (odbieranie). Zgodność ze standardami:
ANSI T1.413 issue 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+),
Reach Extended ADSL (RE ADSL).
- Multi-Protocol do nawiązywania połączeń. Router obsługuje poniższe protokoły do ustanowienia połączenia z usługodawcą internetowym (ISP):
PPPoA (PPP over ATM Adaptation Layer 5 – RFC 2364),
PPPoE (PPP over Ethernet – RFC 2516)
RFC 1483/2684 encapsulation over ATM (mostkowana lub routowana),
CLIP (RFC 2225, poprzednio IPoA – RFC 1577)

Urządzenie obsługuje zarówno enkapsulacje oparte na VC, jak i LCC.

Zawartość pudełka

1. PENTAGRAM Cerberus ADSL2+ Wi-Fi
2. Zasilacz 9 V, 1 A
3. Kabel sieciowy (RJ-45)
4. Kabel telefoniczny (RJ-11)
5. Płyta CD
6. Szybka instrukcja instalacji

Obsługa urządzenia

Użytkowanie Modemu/Routera Cerberus

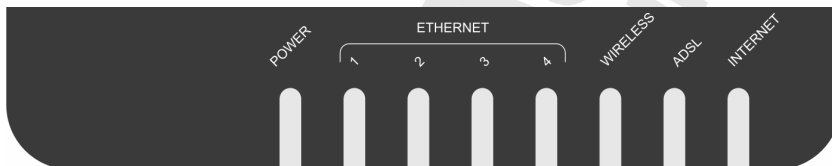


- Nie przechowuj modemu w miejscach o podwyższonej temperaturze i wilgotności.
- Nie używaj tego samego źródła do zasilania modemu i do uruchomienia innego urządzenia.
- Nie otwieraj obudowy modemu, nie naprawiaj urządzenia samodzielnie.
- Jeśli modem stanie się bardzo gorący natychmiast wyłącz go z gniazdka zasilającego, a następnie dostarcz do autoryzowanego serwisu w celu sprawdzenia i/lub naprawy.



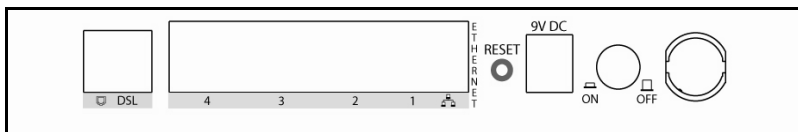
- Ustaw urządzenie na stabilnej powierzchni.
- Używaj tylko zasilacza dołączonego do zestawu.

Przedni panel



Dioda LED	Zachowanie	Opis
POWER	Wyłączona	Urządzenie nie otrzymuje zasilania
	Świeci	Urządzenie podłączone do zasilania
ETHERNET	Wyłączona	Brak połączenia z siecią Ethernet
	Świeci	Port podłączony do sieci Ethernet
	Miga	Wysyłanie / otrzymywanie danych
WIRELESS	Wyłączona	Punkt dostępowy (AP) jest wyłączony
	Świeci	Punkt dostępowy (AP) jest włączony
	Miga	Wysyłanie / otrzymywanie danych
ADSL	Wyłączona	Brak sygnału ADSL
	Świeci	Sygnał ADSL ustanowiony
	Miga	Ustanawianie sygnału ADSL
INTERNET	Wyłączona	Brak połączenia internetowego
	Świeci	Podłączono do Internetu
	Miga	Wysyłanie / otrzymywanie danych

Tylni Panel



Oznaczenie	Używane do...
ADSL (RJ-11)	podłączenia kabla telefonicznego.
ETHERNET 1-4 (RJ-45)	podłączenia urządzeń sieciowych kablem Ethernet.
RESET	resetowania urządzenia (należy przytrzymać przez 10 sek.).
9V DC	podłączenia dołączonego zasilacza sieciowego (9V 1A).
ON/OFF	włączania / wyłączania urządzenia.

Ustawienia fabryczne

Przed zmianą konfiguracji urządzenia zapoznaj się ustawieniami fabrycznymi.

Adres IP	192.168.1.1
Maska podsieci	255. 255. 255.0
SSID	yournetworkname
Serwer DHCP	Włączony
Pula adresowa serwera DHCP	253 adresów IP od 192.168.1.2
Czas dzierżawy adresu	3600 sekund (1 godzina)
Nazwa użytkownika	admin
Hasło	admin

Zalecane jest jak najszybsze ustawienie nazwy użytkownika i hasła.

W przypadku zgubienia hasła będzie konieczne przywrócenie ustawień fabrycznych urządzenia. Procedura ta została opisana na następnej stronie.

Resetowanie urządzenia

- Włącz urządzenie i poczekaj ok. 2 minut na jego inicjalizację.
- Naciśnij i przytrzymaj przez 10 sekund przycisk **RESET** znajdujący się na tylnym panelu urządzenia.

Podłączenie Cerberusa 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 autodiagnostyki 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 podsięci.

Konfiguracja właściwości sieci

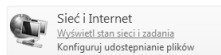
Ten rozdział wyjaśnia jak skonfigurować komputer, aby mógł poprawnie komunikować się z routerem Cerberus ADSL2+ Wi-Fi za pośrednictwem sieci LAN bądź WLAN. Komputer musi być wyposażony w kartę sieciową podłączoną bezpośrednio do routera Cerberus ADSL2+ Wi-Fi lub za pośrednictwem koncentratora (HUB). Jeśli jest to karta Wi-Fi, musi mieć ona ten sam identyfikator sesji ESSID oraz połączyć się z siecią utworzoną przez router. Komputer musi mieć zainstalowany i skonfigurowany protokół TCP/IP w celu uzyskania adresu IP z serwera DHCP lub skorzystać ze stałego adresu IP spójnego z podsiecią, w której pracuje router. Domyślny adres routera to 192.168.1.1, a maska podsięci 255.255.255.0. Najlepszym i najprostszym sposobem konfiguracji komputera jest ustawienie automatycznego pobierania adresu IP z serwera DHCP routera Cerberus ADSL2+ Wi-Fi.

Postępuj wg poniższych wskazówek, aby skonfigurować środowisko sieciowe w komputerze. Przed rozpoczęciem konfiguracji sprawdź komponenty sieciowe w komputerze. Jeśli Router ADSL będzie podłączony do komputera przez port LAN lub WLAN, musi być zainstalowany protokół TCP/IP oraz karta sieciowa.

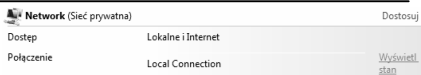
Windows Vista

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).

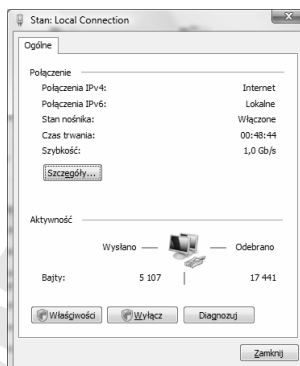
1. Kliknij **Start** → **Panel sterowania**.
2. Kliknij **Wyświetl stan sieci i zadania**.



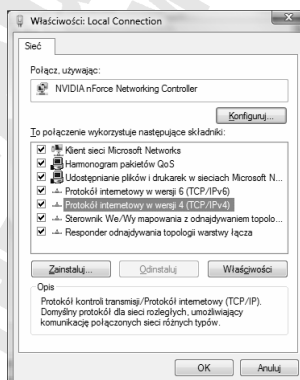
3. Kliknij **Wyświetl stan** dla właściwego połączenia.



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

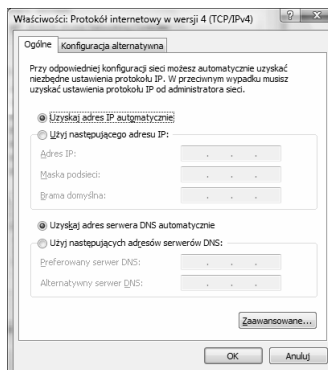


5. Na zakładce **Ogólne** zaznacz **Protokół internetowy w wersji 4 (TCP/IPv4)** i kliknij **Właściwości**.



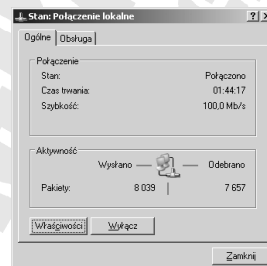
6. Na zakładce **Ogólne** zaznacz **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**.

7. Kliknij **OK**, aby zapisać ustawienia i zamknąć okno **Właściwości: Protokół internetowy w wersji 4 (TCP/IPv4)**.

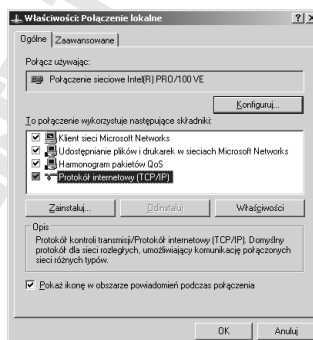


Windows 2000/XP

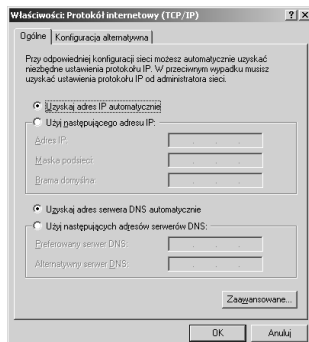
1. Kliknij **Start** → **Ustawienia** → **Panel sterowania**.
2. Dwukrotnie kliknij na ikonie **Połączenia sieciowe** (2000/XP widoku klasycznym) lub **Połączenia sieciowe i internetowe** a następnie **Połączenia sieciowe** (XP w widoku domyślnym).
3. Dwukrotnie kliknij na **Połączenie lokalne**.
4. Na zakładce **Ogólne** kliknij **Właściwości**.



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

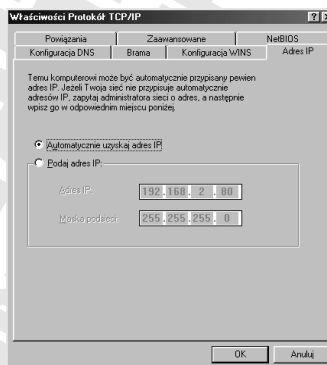
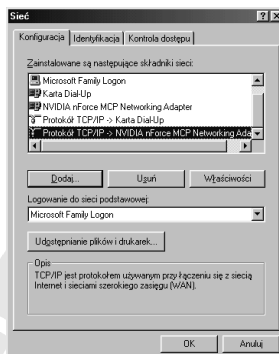


6. Na zakładce **Ogólne** zaznacz **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**.
7. Kliknij **OK**, aby zapisać ustawienia i zamknąć okno **Właściwości: Protokół internetowy (TCP/IP)**.

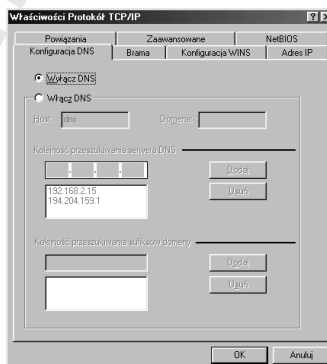


Windows 95/98/Me

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**.



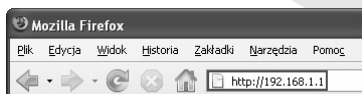
Aby sprawdzić czy karta posiada właściwy adres IP, kliknij **Start** > **Uruchom** i wpisz **cmd** (Win 2000/XP) lub **command** (Win 98/ME) wpisz w linię poleceń **ipconfig /all**, a następnie sprawdź czy wpis **IP Address** dla odpowiedniej karty sieciowej ma wartość **192.168.1.x**

Konfiguracja routera przez WWW

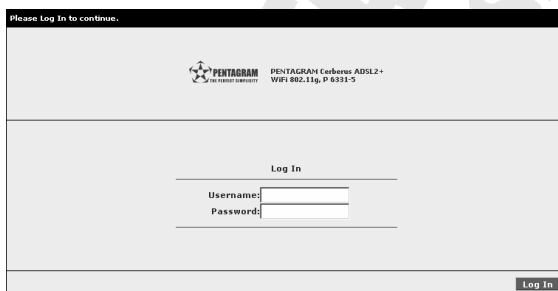
Router Cerberus ADSL2+ Wi-Fi może być konfigurowany przez przeglądarkę internetową, która jest standardową aplikacją zintegrowaną z większością systemów operacyjnych. Router oferuje bardzo prosty i przejrzysty interfejs graficzny służący do konfiguracji nawet zaawansowanych opcji sieciowych.

Logowanie

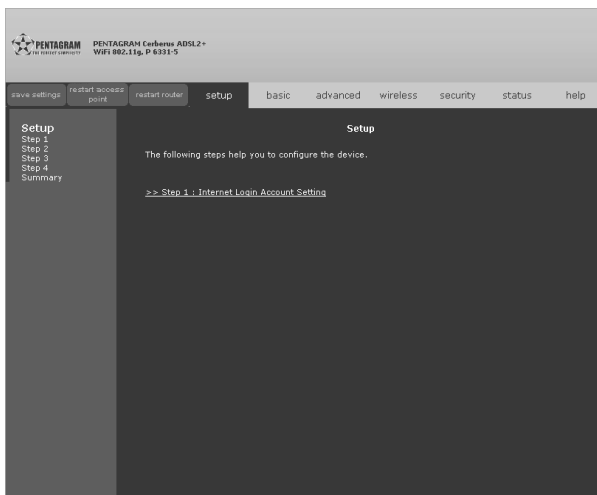
1. Uruchom przeglądarkę internetową
2. W pasku adresu wpisz domyślny adres IP:: <http://192.168.1.1>



3. Wpisz nazwę użytkownika (**username**) i hasło (**password**) – domyślnie **admin / admin**

A screenshot of the router's web-based login interface. At the top, it says "Please Log In to continue." Below this is the Pentagram logo and the text "PENTAGRAM Cerberus ADSL2+ WiFi 802.11g, P 6331-5". In the center, there is a "Log In" section with two input fields: "Username:" and "Password:". A "Log In" button is located at the bottom right of the form area.

Nawigacja



Przyciski

- **Apply** – Kliknij, aby zastosować zmiany w konfiguracji. Przycisk Apply nie zapisuje ustawień i są one przywracane do ostatnich zapisanych wartości przy restarcie routera.
- **Cancel** – Kliknij, aby anulować zmiany i powrócić do ostatniej zapisanej konfiguracji.

Polecenia

- **Save Settings** – Kliknij, aby zapisać zmiany w konfiguracji.
- **Restart Access Point** – Kliknij, aby zrestartować punkt dostępowy (Access Point) i połączenie bezprzewodowe.
- **Restart Router** – Kliknij, aby zrestartować router.

Zakładki

Na stronie konfiguracyjnej znajdują się poniższe zakładki:

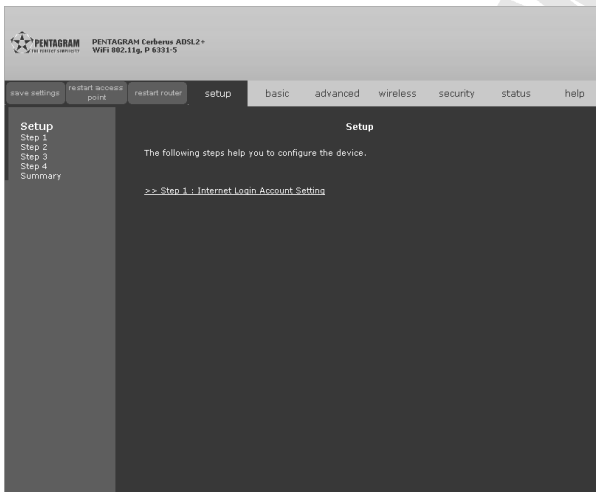
- **Setup**
- **Basic**
- **Advanced**
- **Wireless**
- **Security**
- **Status**
- **Help**

Trudniejsze pojęcia:

- **Multipleksing** - protokoły mogą być przenoszone wirtualnymi kanałami (VC) na dwa sposoby. Upewnij się, że wybrałeś metodę multipleksowania używaną przez swojego usługodawcę:
 - Multipleksing oparty na VC** – w tej metodzie każdy protokół jest przydzielony do specyficznego wirtualnego kanału, np.: kanałem VC1 jest przenoszony IP, itd. Ta metoda przeważa w środowiskach, w których dynamiczne tworzenie dużej liczby kanałów wirtualnych ATM jest szybkie i ekonomiczne.
 - Multipleksing oparty na LLC** – w tej metodzie jeden wirtualny kanał przenosi wiele protokołów a informacje identyfikujące protokoły znajdują się w nagłówku każdego pakietu. Metoda ta wymaga szerszego pasma i dodatkowego przetwarzania, ale może mieć przewagę w środowiskach, w których używanie oddzielnych kanałów dla każdego protokołu nie jest praktyczne, np. jeśli koszty są silnie uzależnione od ilości jednoczesnych kanałów wirtualnych.
- **VPI i VCI** - upewnij się, że używasz wartości dla **VPI** (Virtual Path Identifier - identyfikator ścieżki wirtualnej) i **VCI** (Virtual Channel Identifier - identyfikator kanału wirtualnego) podanych przez usługodawcę. Poprawny zakres dla VPI to 0 do 255, a zakres dla VCI to 32 do 65535 (wartości 0-31 są zarezerwowane na potrzeby lokalnego zarządzania ruchem ATM).
- **PPPoA** – Point-to-Point Protocol over ATM Adaptation Layer 5 (AAL5) (PPPoA) pozwala na kontrolę dostępu i naliczanie opłat w sposób podobny do połączeń dodzwanianych (dial-up) używających PPP. Router używa enkapsulacji sesji PPP bazując na RFC1483 i wysyła wirtualnym połączeniem ATM PVC do urządzenia DSLAM usługodawcy.
- **PPPoE** – Point-to-Point Protocol over Ethernet pozwala na kontrolę dostępu i naliczanie opłat w sposób podobny do połączeń dodzwanianych (dial-up) używających PPP. Router mostkuje sesję PPP przez Ethernet (PPP over Ethernet, RFC 2516) z twojego komputera do wirtualnego połączenia ATM PVC połączonego do koncentratora dostępowego ADSL (ADSL Access Concentrator), gdzie sesja PPP jest kończona. Pojedyncze połączenie PVC może obsłużyć dowolną ilość sesji PPP z twojej sieci LAN.

Zakładka Setup

Zakładka Setup pomoże ci skonfigurować najważniejsze ustawienia routera i połączenia internetowego. Kreator ten poprowadzi cię krok po kroku przez wszystkie niezbędne do działania routera opcje i jego użycie do konfiguracji ADSL jest bardzo zalecane.



Kliknij **Step 1: Internet Login Account Setting**, aby kontynuować.

Internet Login Account Setting (Ustawienia konta internetowego)

Wprowadź **User ID** (nazwa użytkownika), **Password** (hasło), **VPI** (Virtual Path Identifier), **VCI** (Virtual Channel Identifier) i wybierz protokół z rozwijanej listy **Protocol**. Nazwa użytkownika musi być wpisana tak samo jak podał ją usługodawca (zazwyczaj użytkownik@domena, gdzie domena określa nazwę usługi i należy ją wpisać dokładnie tak, jak to podał usługodawca).

Kliknij **Previous**, aby powrócić do poprzedniego ekranu lub **Next**, aby kontynuować.

Wireless LAN Configuration (Konfiguracja sieci bezprzewodowej)

Wireless LAN Configuration

This is to specify the network name of your wireless local area network.

Wireless Network Name / SSID
Enter a name (SSID) for your wireless network.

OR

Request Setup Wizard to generate a unique SSID for you.

Country Standard

Wireless Channel

Hide your Wireless Network Name / SSID

Note:

1. Your system's wireless network adapter must have the same SSID as the wireless router to access the network wirelessly.
2. You can also make your Wireless Network Name/ SSID invisible to other wireless users by hiding your SSID.
3. Specify the wireless channel for your network. All wireless clients must use the same channel to access to the router.

<< Previous To Continue, Click Next..... Next >>

W polu **Wireless Network Name / SSID** wpisz nazwę sieci bezprzewodowej/identyfikator sesji (SSID) albo kliknij **Generate SSID**, aby automatycznie wygenerować unikalny SSID dla swojej sieci WLAN. Z listy **Country Standard** wybierz swój kraj/region, wybierz kanał, na którym będzie działać twoja sieć (**Wireless Channel**) i wybierz z listy **Hide your Wireless Network Name / SSID** czy SSID ma być ukryty (**Yes**) czy propagowany (**No**).

Kliknij **Previous**, aby powrócić do poprzedniego ekranu lub **Next**, aby kontynuować.

Wireless LAN Security (Zabezpieczenie sieci bezprzewodowej)

Wireless LAN Security

This is to ensure privacy by preventing unauthorized users from accessing your wireless network.

Enable Wireless Security

Click for the wizard to create a unique 64 bit/128 bit Encryption Key. Alternatively, you can manually enter a 10 or 26 digits Hexadecimal keys.

Cipher **Encryption Key**

For a 64 bit Network Key, (10 digits among (0-9) or (a-f)/(A-F), e.g. 52ab4d92ba

For a 128 bit Network Key, (26 digits among (0-9) or (a-f)/(A-F), e.g. 85cd8fc2a070e663cc9896d2b

<< Previous To Continue, Click Next..... Next >>

Zaznacz **Enable Wireless Security**, aby włączyć szyfrowanie WEP sieci bezprzewodowej, z listy **Cipher** wybierz długość klucza (64 bits lub 128 bits) i kliknij **Generate**, aby wygenerować klucz lub wpisz swój własny w pole **Encryption Key**. W każdej chwili możesz zmienić klucz szyfrujący WEP lub wybrać inną metodę szyfrowania w menu **Security** zakładki **Wireless**.

Kliknij **Previous**, aby powrócić do poprzedniego ekranu lub **Next**, aby kontynuować.

System Password (Hasło systemowe)

Zaznacz **Enable Authentication**, aby włączyć ochronę hasłem, wpisz nazwę użytkownika (**User Name**) i hasło w pola **Password** i **Confirmed Password** oraz wprowadź czas bezczynności na stronie konfiguracyjnej, po którym będzie trzeba ponownie wprowadzić hasło (**Idle Timeout**). Podana nazwa użytkownika i hasło będą wymagane, aby zalogować się do strony konfiguracyjnej routera.

Kliknij **Previous**, aby powrócić do poprzedniego ekranu lub **Next**, aby kontynuować.

Summary (Podsumowanie)

Jeśli informacje na tej stronie są prawidłowe, możesz je zapisać do pliku (**save**) lub wydrukować (**print**).

Kliknij **Previous**, aby powrócić do poprzedniego ekranu lub **Finish**, aby zapisać ustawienia i zrestartować router.

Zakładka Basic

Ta zakładka udostępnia podstawowe informacje i możliwości konfiguracji routera.

PENTAGRAM CERBERUS ADSL2+ WI-FI (P.6331-5)

save settings restart access point restart router **setup** basic advanced wireless security status help

Basic Home

Connection Information		Router Information	
DSL	Down	System Uptime	0 hours 37 minutes
Downstream / Upstream (Kbps)	0/0	Model	ADSL2+ Wireless G Router
Internet	Not Connected	Firmware Version	120.110.1
Connected Time	0	Ethernet MAC address	00:30:0A:6B:C6:4C
Connection Type	PPPoA	DSL MAC address	00:30:0A:6B:C6:4D
Username	username	AP MAC	00:00:00:00:00:00
IP Address	N/A	NAT	Enabled
Default Gateway	N/A	Firewall	Enabled
Primary DNS	N/A		
Secondary DNS	N/A		
<input type="button" value="Connect"/>			
Local Network		Wireless Network	
LAN IP Address	192.168.1.1	Network Name / SSID	younetworkname
DHCP	Enabled	Security Type	None
DHCP Range	192.168.1.2 - 192.168.1.254	WEP Encryption Key	Disabled
Ethernet	Connected		

Home (Domowa)

Basic Home

Connection Information		Router Information	
DSL	Down	System Uptime	0 hours 37 minutes
Downstream / Upstream (Kbps)	0/0	Model	ADSL2+ Wireless G Router
Internet	Not Connected	Firmware Version	120.110.1
Connected Time	0	Ethernet MAC address	00:30:0A:6B:C6:4C
Connection Type	PPPoA	DSL MAC address	00:30:0A:6B:C6:4D
Username	username	AP MAC	00:00:00:00:00:00
IP Address	N/A	NAT	Enabled
Default Gateway	N/A	Firewall	Enabled
Primary DNS	N/A		
Secondary DNS	N/A		
<input type="button" value="Connect"/>			
Local Network		Wireless Network	
LAN IP Address	192.168.1.1	Network Name / SSID	younetworkname
DHCP	Enabled	Security Type	None
DHCP Range	192.168.1.2 - 192.168.1.254	WEP Encryption Key	Disabled
Ethernet	Connected		

Na tej stronie znajdują się wszystkie wymagane informacje dotyczące połączenia z Internetem (**Connection Information**), siecią lokalną (**Local Network**), siecią bezprzewodową (**Wireless Network**) oraz informacje o routerze (**Router Information**). Z poziomu tej strony możesz także spróbować nawiązać połączenie internetowe (**Connect**) lub je rozłączyć (**Disconnect**).

Quick Start (Szybki start)

The screenshot shows a 'Quick Start' configuration window. It contains the following fields and options:

- User ID:** A text input field containing 'username'. Below it is an example: 'Example: user@ispname'.
- Password:** A text input field with masked characters '*****'. Below it is the text 'Provided by your ISP'.
- Protocol:** A dropdown menu currently set to 'PPPoA_VC-Mux'.
- VPI:** A text input field containing '0'.
- VCI:** A text input field containing '35'.
- Connect:** A button located at the bottom left of the form.

User ID – Wpisz nazwę użytkownika dla swojego połączenia PPPoE/PPPoA.

Password – Wpisz hasło dla swojego połączenia PPPoE/PPPoA.

Protocol – Wybierz z listy enkapsulację i typ multipleksingu.

VPI – Wpisz wartość **VPI** (Virtual Path Identifier - identyfikator ścieżki wirtualnej). Poprawny zakres dla VPI to 0 do 255.

VCI – Wpisz wartość **VCI** (Virtual Channel Identifier - identyfikator kanału wirtualnego). Poprawny zakres dla VCI to 32 do 65535 (wartości 0-31 są zarezerwowane na potrzeby lokalnego zarządzania ruchem ATM).

Connect – Ustanów połączenie używając powyższych ustawień.

LAN configuration (Konfiguracja sieci LAN)

The screenshot shows a 'LAN Group 1 Configuration' window. It contains the following fields and options:

- IP Address:** 192.168.1.1
- Netmask:** 255.255.255.0
- Default Gateway:** (empty field)
- Host Name:** login
- Domain:** router
- Enable DHCP Server:** (checked)
- Assign ISP DNS, SNTP:** (unchecked)
- Start IP:** 192.168.1.2
- End IP:** 192.168.1.254
- Lease Time:** 3600 Seconds
- Enable DHCP Relay:** (checked)
- Relay IP:** 0.0.0.3
- Server and Relay Off:** (checked)
- Buttons:** Apply and Cancel at the bottom right.

IP Address – Domyślny adres IP routera (jak pokazano) to 192.168.1.1.

Netmask – Domyślna maska podsieci routera to 255.255.255.0. Ta maska umożliwia routerowi obsłużenie 254 użytkowników. Jeśli chcesz zwiększyć ilość obsługiwanych użytkowników musisz zmienić maskę podsieci.

Default Gateway – Brama domyślna jest urządzeniem routującym używanym do przekazywania ruchu nie adresowanego do żadnej stacji w lokalnej podsieci. Adres IP bramy domyślnej powinieneś otrzymać od swojego usługodawcy internetowego.

Host Name – Nazwa hosta wraz z domeną (**Domain**) tworzą unikalny identyfikator routera. Może to być dowolny ciąg alfanumeryczny niezawierający spacji.

Domain – Nazwa domeny wraz z nazwą hosta (**Host Name**) tworzą unikalny identyfikator routera. Aby uzyskać dostęp do strony konfiguracyjnej routera w pasku adresu przeglądarki możesz wpisać **192.168.1.1** (adres IP) lub **login.router** (nazwa_hosta.domena).

Enable DHCP Server – Włączenie lub wyłączenie serwera DHCP. Domyślnie serwer DHCP jest włączony (dla sieci LAN). Jeśli w twojej sieci już istnieje serwer DHCP musisz wyłączyć albo jego albo serwer DHCP routera.

Assign ISP DNS, SNTP – Jeśli ta opcja jest włączona, router będzie rozgłaszał swój adres IP jako serwer DNS, jeśli jest wyłączona router będzie przekazywał adresy DNS uzyskane z sieci WAN.

Start IP / End IP – Wpisz początkowy/końcowy puli adresów IP, które będą przydzielane urządzeniom przez serwer DHCP

Lease Time – Czas dzierżawy to czas, na który klient otrzymuje od serwera DHCP dynamiczny adres IP. Po zakończeniu tego czasu serwer DHCP albo odświeża dzierżawę albo przydziela klientowi nowy adres IP. Domyślna wartość to 3600 sekund (1 godzina). Maksymalna wartość to 999999 sekund (około 278 godzin).

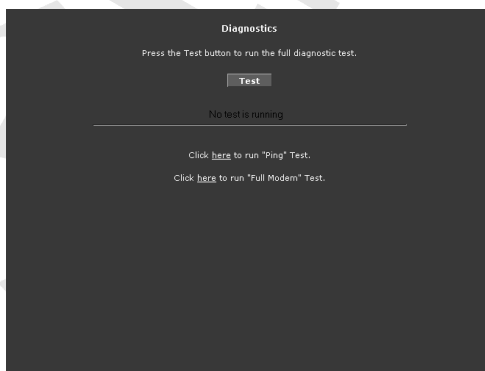
Enable DHCP Relay – Oprócz możliwości działania jako serwer DHCP, router wspiera także przekazywanie DHCP (DHCP Relay). Gdy router działa jako serwer DHCP, sam przydziela adresy IP klientom sieci LAN. Kiedy brama sieciowa jest skonfigurowana jako przekazywacz DHCP, router przekazuje żądania i odpowiedzi DHCP między klientami i zewnętrznym serwerem DHCP.

Relay IP – Adres IP serwera DHCP, do którego będą przekazywane żądania DHCP.

Server and Relay Off – Wyłączenie serwera i przekazywania DHCP. Po wyłączeniu obu tych opcji administrator sieci musi ręcznie skonfigurować parametry sieciowe każdego hosta w sieci. Jeden adres IP może być przypisany tylko do jednego hosta. Router musi się znajdować w tej samej podsieci co pozostałe hosty.

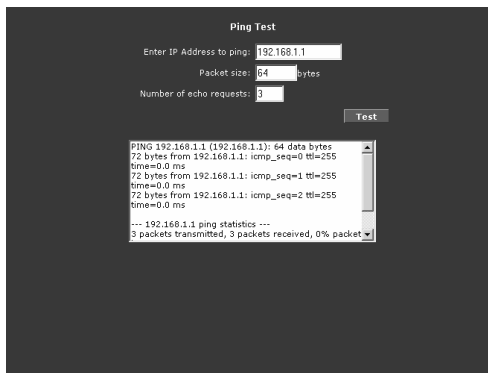
Diagnostics (Diagnostyka)

Testy diagnostyczne są przeprowadzane w celu sprawdzenia czy router jest prawidłowo podłączony do sieci WAN. Przeprowadzenie testu może zająć kilka sekund. Przed uruchomieniem testu upewnij się, że linia DSL została podłączona.



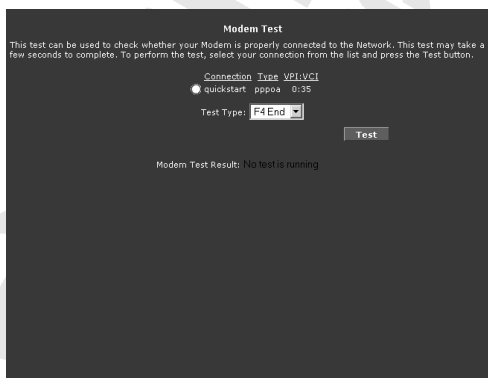
Aby wykonać test należy wybrać połączenie z listy i kliknąć **Test**. Możesz także wykonać **“Ping” Test** lub **“Full Modem” Test**:

- **Ping Test (Test ping)**



Zmień lub pozostaw domyślne wartości następujących pól: **Enter the IP address to ping** (adres IP, do którego będą wysłane pakiety ping), **Packet size** (rozmiar pakietu) i **Number of echo request** (ilość żądań echo) i kliknij **Test**. Rezultaty testu zostaną wyświetlone na stronie. Jeśli test został zakończony pomyślnie, oznacza to, że protokół TCP/IP działa poprawnie. Jeśli test zakończył się niepowodzeniem, spróbuj zrestartować router.

- **Full Modem Test (Pełny test modemu)**



Wybierz połączenie z listy **Connection** i rodzaj testu z listy **Test Type** i kliknij **Test**.

Zakładka Advanced

Zakładka Advanced udostępnia zaawansowane ustawienia konfiguracji dla istniejących połączeń a także umożliwi tworzenie nowych. Przynajmniej jedno połączenie WAN musi zostać skonfigurowane przed rozpoczęciem dostosowywania zaawansowanych opcji konfiguracyjnych WAN. Przynajmniej jedna grupa LAN (LAN group) musi być zdefiniowana przed rozpoczęciem dostosowywania zaawansowanych opcji konfiguracyjnych LAN.

PENTAGRAM Cerberus ADSL2+
Wi-Fi 982.1ip, P.6331-5

save settings | restart access point | restart router | setup | basic | **advanced** | wireless | security | status | help

Advanced

WAN
LAN
Application
QoS
Routing
System Password
Firmware Upgrade
Restore To Default

Advanced

The Advanced section lets you configure advanced features like LAN Configuration, SNTP, IGMP, Bridge(MAC) Filters, LAN clients, etc.

Lan Configuration	Allows changes to be made to IP addresses and option to enable DHCP server.
LAN Clients	Allows user to join specified LAN groups.
UPnP	Enables computer to auto-detect and adapt to hardware changes.
SNTP	Short for Simple Network Time Protocol, a simplified version of NTP. Allows the user to synchronize with a specified time server.
SNMP	Allows user to manage "SNMP" Agents and "Traps".
Port Forwarding	Configure Firewall and NAT pass-through to your hosted applications.
Bridge Filter	Allows user to enable / disable bridge filters to destination ports.
LAN Clients	Configure LAN Clients.
Easy Connect Configuration	Allow user to access Internet without changes to PC Network Settings.
IGMP Proxy	Configure Multicast pass-through for different connections.
Web Access Control	Configure access control list for remote Web access.
SSH Access Control	Configure access control list for remote SSH access.
Policy Routing	Configure Policy Routing information.
Ingress	Configure Ingress information.
Egress	Configure Egress information.
Shaper	Configure Shaper information.
Routing	Consists of static and dynamic routing.

WAN / New Connection (Nowe połączenie)

Wygląd tej strony zależy od wybranego z listy **Type** rodzaju połączenia. Zapisane połączenia są dostępne na końcu menu WAN.

PPPoE Connection Setup

Name: Type: **PPPoE** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

PPP Settings **PVC Settings**

Encapsulation: LLC VC

Username: PVC: **New**

Password: VPI: VCI:

Idle Timeout: secs QoS: **UBR**

Keep Alive: min PCR: cps

Authentication: Auto CHAP PAP SCR: cps

MTU: bytes On Demand: Default Gateway: MBS: cells

Enforce MTU: Debug: Valid Rx: CDVT: usecs

PPP Unnumbered: Host Trigger: **Configure**

Auto PVC:

Apply **Delete** **Cancel**

PPPoA Connection Setup

Name: Type: **PPPoA** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

PPP Settings **PVC Settings**

Encapsulation: LLC VC

Username: VPI: VCI:

Password: QoS: **UBR**

Idle Timeout: secs

Keep Alive: min

Authentication: Auto CHAP PAP PCR: cps

MTU: bytes On Demand: Default Gateway: SCR: cps

Enforce MTU: Debug: Valid Rx: MBS: cells

PPP Unnumbered: Host Trigger: **Configure**

Auto PVC:

Apply **Delete** **Cancel**

Static Connection Setup

Name: Type: **Static** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

Static Settings **PVC Settings**

Encapsulation: LLC VC PVC: **New**

IP Address: VPI: VCI:

Mask: QoS: **UBR**

Default Gateway: PCR: cps

DNS 1: SCR: cps

DNS 2: MBS: cells

DNS 3: CDVT: usecs

Mode: Bridged Routed Auto PVC:

Apply **Delete** **Cancel**

DHCP Connection Setup

Name: Type: **DHCP** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

DHCP Settings **PVC Settings**

Encapsulation: LLC VC PVC: **New**

IP Address: VPI: VCI:

Mask: QoS: **UBR**

Gateway: PCR: cps

Default Gateway: SCR: cps

Renew **Release** MBS: cells

Auto PVC:

Apply **Delete** **Cancel**

Bridged Connection Setup

Name: Type: **Bridge** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

Bridge Settings **PVC Settings**

Encapsulation: LLC VC PVC: **New**

Select LAN: **LAN group 1** VPI: VCI:

QoS: **UBR**

PCR: cps

SCR: cps

MBS: cells

CDVT: usecs

Auto PVC:

Apply **Delete** **Cancel**

CLIP Connection Setup

Name: Type: **CLIP** Sharing: **Disable**

Options: NAT Firewall VLAN ID: Priority Bits:

CLIP Settings **PVC Settings**

IP Address: PVC: **New**

Mask: VPI: VCI:

ARP Servers: QoS: **UBR**

Default Gateway: PCR: cps

SCR: cps

MBS: cells

CDVT: usecs

Auto PVC:

Apply **Delete** **Cancel**

Name – Wpisz nazwę tego połączenia.

Type – Protokół używany do nawiązania tego połączenia.

Sharing – Wybierz sposób współdzielenia tego połączenia: **Disabled** (wyłączone), **Enabled** (włączone) lub **VLAN** (Virtual LAN – wirtualna sieć lokalna).

Options – Włączenie lub wyłączenie usług NAT/Firewall dla tego połączenia.

VLAN ID – Wpisz identyfikator sieci VLAN.

Priority Bits – Zdefiniuj priorytet użytkownika (User Priority) dla sieci VLAN.

PVC Settings (Ustawienia PVC)

PVC – Wybierz wcześniej zdefiniowany kanał wirtualny (PVC – Predefined Virtual Channel) który chcesz użyć (tylko przy wybranej opcji **Enabled** lub **VLAN** na liście **Sharing**).

VPI – identyfikator ścieżki wirtualnej. Poprawny zakres to 0 do 255

VCI – identyfikator kanału wirtualnego. Poprawny zakres to 32 do 65535 (wartości 0-31 są zarezerwowane na potrzeby lokalnego zarządzania ruchem ATM).

QoS – wybierz klasę ruchu dla wybranego połączenia. Dostępne są **CBR** (Constant Bit Rate – stała przepływność), **VBR** (Variable Bit Rate – zmienna przepływność) i **UBR** (Unspecified Bit Rate – nieustalona przepływność). Ustawienia tych klas są kontrolowane przez poniższe parametry (PCR, SCR, MBS).

CBR (Constant Bit Rate) – połączenie o stałej i niezmiennej przepustowości. Jedyny parametr jaki należy skonfigurować to PCR.

UBR (Unspecified Data Rate) – połączenia o niezdefiniowanej przepustowości. Jedyny parametr jaki należy skonfigurować to PCR.

rtVBR (real time Variable Bit Rate) – połączenia, które mimo zmiennej przepustowości wymagają dokładnego zgrania czasowego między źródłem a celem sygnału. Parametry jaki należy skonfigurować to PCR, SCR i MBS.

nrtVBR (non real time Variable Bit Rate) – połączenia o zmiennej przepustowości, niewymagające zgrania czasowego, ale nadal wymagające ustawienia dostępności pasma. Parametry jaki należy skonfigurować to PCR, SCR i MBS.

PCR (Peak Cell Rate) – maksymalna możliwa szybkość wysyłania komórek. Parametr ten może być niższy (ale nie wyższy) od maksymalnej szybkości linii. Jedna komórka ATM to 54 bajtów (424 bitów), więc przy maksymalnej szybkości 832 Kbps maksymalna wartość PCR to 1962 komórek na sekundę. Ta wartość nie jest gwarantowana ze względu na zależność od szybkości linii.

SCR (Sustained Cell Rate) – przeciętna szybkość wysyłania komórek w pakietach a także parametr dla ruchu pakietowego. SCR nie może być większy od PCR. Domyślna wartość parametru to 0 komórek na sekundę.

MBS (Maximum Burst Size) – maksymalna ilość komórek, która może być wysłana z prędkością PCR. Po osiągnięciu wartości MBS prędkość spada poniżej SCR póki średnia prędkość nie wyrówna się do wartości SCR. Po wyrównaniu więcej komórek (aż do wartości MBS) może być przesłanych z prędkością PCR.

CDVT (Cell Delay Variation Tolerance) – Tolerancja sieci ATM na odstępny między komórkami.

Auto PVC – Router spróbuje automatycznie wykryć parametry PVC.

Ustawienia zależne od wybranego typu połączenia

• PPP Settings (PPPoA/PPPoE)

Encapsulation – Wybierz metodę enkapsulacji pakietów.

Username – Wpisz nazwę użytkownika dla swojego połączenia PPPoE/PPPoA.

Password – Wpisz hasło dla swojego połączenia PPPoE/PPPoA.

Idle Timeout – Gdy opcja **On Demand** jest zaznaczona, wpisz czas nieaktywności połączenia (w minutach), po którym zostanie ono rozłączone.

Keep Alive – Wpisz czas pomiędzy wysyłanymi pakietami Keep Alive.

Authentication – Wybierz metodę uwierzytelnienia połączenia: **Auto** (zalecane), **CHAP** (Challenge Handshake Authentication Protocol) lub **PAP** (Password Authentication Protocol).

MTU – Określa rozmiar MTU (Maximum Transmission Unit - największa jednostka transmisji) dla protokołu TCP.

On Demand – Łączenie “na żądanie”. Zalecane dla połączeń rozliczanych za czas połączenia.

Default Gateway – Wybierz czy to połączenie będzie korzystać z domyślnej bramy.

Enforce MTU (PPPoE only) – Zaznacz tą opcję by wymusić rozmiar MTU.

PPP Unnumbered – Połączenie PPP nie będzie miało przydzielonego adresu IP (niezalecane).

Host Trigger – Gdy opcja **On Demand** jest zaznaczona, zaznacz tą opcję i kliknij **Configure** aby skonfigurować warunki inicjalizacji połączenia.

- **Static Settings**

Encapsulation – Wybierz metodę enkapsulacji pakietów.

IP Address – Wpisz statyczny adres IP.

Mask – Wpisz maskę podsieci.

Default Gateway – Wpisz adres IP bramy.

DNS 1-3 – Wpisz adresy IP serwerów DNS (w kolejności w jakiej mają być odpytywane).

Mode – Wybierz czy połączenie będzie mostkowane (**Bridged**) czy routowane (**Routed**).

- **DHCP Settings**

Encapsulation, IP Address, Mask, Gateway – Parametry uzyskane z serwera DHCP.

Default Gateway – Wybierz czy to połączenie będzie korzystać z domyślnej bramy.

Użyj przycisków by odnowić (**Renew**) lub zwolnić (**Release**) dzierżawę parametrów uzyskanych z serwera DHCP.

- **Bridge Settings**

Encapsulation – Wybierz metodę enkapsulacji pakietów.

Select LAN – Wybierz grupę LAN (LAN Group) z której pakiety będą mostkowane do portu WAN.

- **CLIP**

IP Address – Wpisz adres IP.

Mask – Wpisz maskę podsieci.

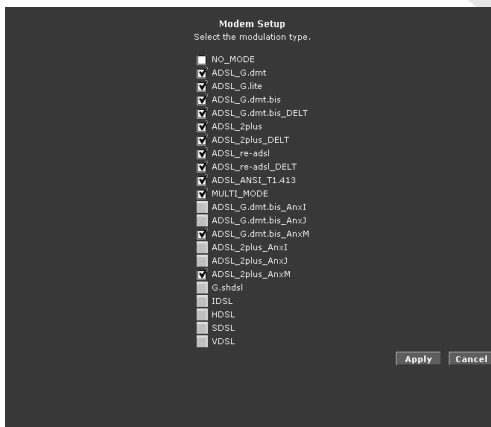
ARP Server – Wpisz adres IP serwera ARP.

Default Gateway – Wpisz adres IP bramy.



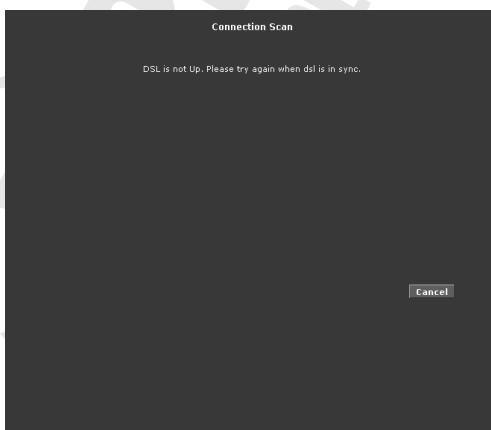
WAN / ADSL Modulation (Modulacja ADSL)

Strona ADSL Modulation pozwala na wybranie dowolnej kombinacji trybów pracy DSL. Pozostaw domyślne wartości jeśli nie jesteś pewien lub usługodawca nie dostarczył informacji na ten temat.. W większości przypadków zmiany na tej stronie nie są konieczne.



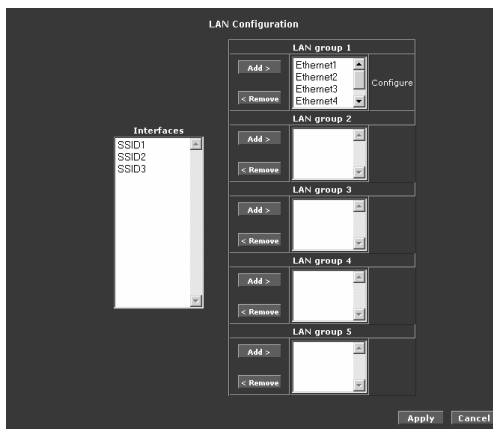
WAN / Connection Scan (Skanowanie połączenia)

Ta opcja pomaga użytkownikowi na wykrycie ustawień PVC używanych przez usługodawcę. Przed rozpoczęciem procesu skanowania upewnij się, że linia telefoniczna jest podłączona do routera.



Kliknij **Scan** aby rozpocząć skanowanie połączenia.

LAN / LAN Configuration (Konfiguracja sieci LAN)

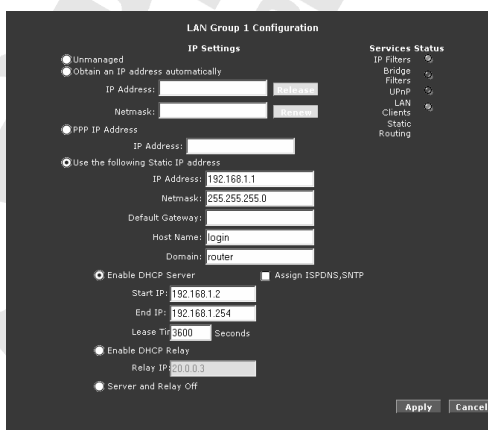


Interfaces – Lista dostępnych i nieprzydzielonych interfejsów sieciowych routera.

LAN Group 1-5 – Każda grupa LAN (LAN Group) może zostać skonfigurowana jako oddzielna podsieć i każdy interfejs sieciowy routera można przydzielić do dowolnej grupy. Aby dodać interfejs do grupy LAN, wybierz go z listy nieprzydzielonych i kliknij **Add** w żądanej grupie. Jeśli chcesz usunąć interfejs z grupy, zaznacz go i kliknij **Remove**. Jeśli w grupie znajduje się przynajmniej jeden interfejs, możesz kliknąć na **Configure** aby otworzyć stronę **LAN Group x Configuration**.

- **LAN Group x configuration (Konfiguracja grupy LAN x)**

Ta strona pozwala na konfigurację ustawień każdej grupy LAN. Możesz także podejrzeć jakie usługi są włączone dla danej grupy – zielony kolor oznacza, że usługa jest włączona; czerwony kolor oznacza, że usługa jest wyłączona.



Unmanaged (nie zarządzane)

Unmanaged to stan, w którym grupa LAN nie jest skonfigurowana i nie został przydzielony adres IP dla mostka.

Obtain IP address automatically (Uzyskaj automatycznie adres IP)

Gdy ta opcja jest zaznaczona, router zachowuje się jak klient DHCP i wysyła żądanie do serwera DHCP o przydzielenie adresu IP po stronie sieci lokalnej. Użyj przycisków by odnowić (**Renew**) lub zwolnić (**Release**) parametry uzyskanych z serwera DHCP. Przydzielony adres IP i maska podsieci pojawiają się w polach **IP Address** i **Netmask**.

PPP IP Address (Adres IP połączenia PPP)

Włącza/wyłącza opcję PPP unnumbered (nienumerowane PPP). Wpisany w pole **IP Address** adres IP powinien być inny niż adres portu WAN, ale powinien znajdować się w tej samej podsieci.

Use the following Static IP address (Statyczny adres IP)

Ta opcja umożliwi na skonfigurowanie statycznego adresu IP routera.

IP Address – Domyślny adres IP routera (jak pokazano) to 192.168.1.1.

Netmask – Domyślna maska podsieci routera to 255.255.255.0. Ta maska umożliwi routerowi obsługę 254 użytkowników. Jeśli chcesz zwiększyć ilość obsługiwanych użytkowników musisz zmienić maskę podsieci.

Default Gateway – Brama domyślna jest urządzeniem routującym używanym do przekazywania ruchu nie adresowanego do żadnej stacji w lokalnej podsieci. Adres IP bramy domyślnej powinien być inny niż adres routera.

Host Name – Nazwa hosta wraz z domeną (**Domain**) tworzą unikalny identyfikator routera. Może to być dowolny ciąg alfanumeryczny niezawierający spacji.

Domain – Nazwa domeny wraz z nazwą hosta (**Host Name**) tworzą unikalny identyfikator routera. Aby uzyskać dostęp do strony konfiguracyjnej routera w pasku adresu przeglądarki możesz wpisać **192.168.1.1** (adres IP) lub **login.router** (nazwa_hosta.domena).

Enable DHCP Server – Włączenie lub wyłączenie serwera DHCP. Domyślnie serwer DHCP jest włączony (dla sieci LAN). Jeśli w twojej sieci już istnieje serwer DHCP musisz wyłączyć albo jego albo serwer DHCP routera.

Assign ISP DNS, SNTP – Jeśli ta opcja jest włączona router będzie rozgłaszał swój adres IP jako serwer DNS, jeśli jest wyłączona router będzie przekazywał adresy DNS uzyskane z sieci WAN.

Start IP / End IP – Wpisz początkowy/końcowy puli adresów IP, które będą przydzielane urządzeniom przez serwer DHCP

Lease Time – Czas dzierżawy to czas, na który klient otrzymuje od serwera DHCP dynamiczny adres IP. Po zakończeniu tego czasu serwer DHCP albo odświeża dzierżawę albo przydziela klientowi nowy adres IP. Domyślna wartość to 3600 sekund (1 godzina). Maksymalna wartość to 999999 sekund (około 278 godzin).

Enable DHCP Relay – Oprócz możliwości działania jako serwer DHCP, router wspiera także przekazywanie DHCP (DHCP Relay). Gdy router działa jako serwer DHCP, sam przydziela adresy IP klientom sieci LAN. Kiedy brama sieciowa jest skonfigurowana jako przełącznik DHCP, router przekazuje żądania i odpowiedzi DHCP między klientami i zewnętrznym serwerem DHCP.

Relay IP – Adres IP serwera DHCP, do którego będą przekazywane żądania DHCP.

Server and Relay Off – Wyłączenie serwera i przekazywania DHCP. Po wyłączeniu obu tych opcji administrator sieci musi ręcznie skonfigurować parametry sieciowe każdego hosta w sieci. Jeden adres IP może być przypisany tylko do jednego hosta. Router musi się znajdować w tej samej podsieci co pozostałe hosty.

LAN / LAN Clients (Klienci LAN)

Strona LAN Clients pozwala na przeglądanie i dodawanie komputerów do grupy LAN. Każdy komputer ma przydzielony dynamiczny lub statyczny (ręcznie ustawiony) adres IP. Możesz dodawać statyczne adresy IP (należące do podsieci LAN routera) używając strony LAN Clients. Każdy istniejący statyczny adres IP znajdujący się w puli adresowej serwera DHCP może zostać usunięty.

LAN Clients

To add a LAN Client, Enter IP Address and Hostname, then click Apply.

Select LAN Connection: LAN group 1

Enter IP Address:

Hostname:

MAC Address:

Dynamic Addresses

Reserve	IP Address	Hostname	MAC	Type
<input checked="" type="checkbox"/>	192.168.1.2	samothnia	00:50:8d:f3:72:87	Dynamic

Apply Cancel

Select LAN Connection – Wybierz grupę LAN, którą chcesz edytować.

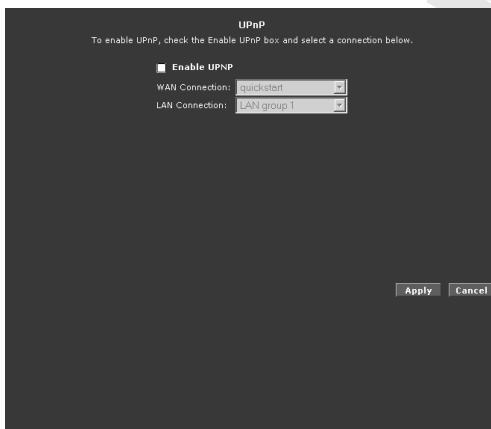
Enter IP Address (adres IP) / **Hostname** (nazwa hosta) / **MAC Address** (adres MAC) – Wypełnij te pola i kliknij **Apply**, aby dodać określonego hosta do listy statycznych adresów.

Static Addresses – Lista wszystkich hostów, którzy otrzymają zawsze ten sam adres IP z serwera DHCP – adresy te nie będą przydzielane do innych hostów. Zaznacz pole **Delete** i kliknij **Apply**, aby usunąć wybranego użytkownika z listy statycznych adresów. Podczas następnego połączenia użytkownik ten otrzyma nowy dynamiczny adres IP.

Dynamic Addresses – Lista wszystkich hostów, którzy otrzymali adres IP z serwera DHCP routera. Kliknij **Reserve** a następnie **Apply** aby przenieść zaznaczone hosty na listę Static Addresses.

Application / UPnP

Universal plug and play (UPnP), NAT oraz firewall traversal umożliwiają przepuszczenie ruchu sieciowego dla aplikacji korzystających z protokołu UPnP. Ta funkcja wymaga aktywnego połączenia WAN. W dodatku komputer powinien również obsługiwać tą funkcję. W przypadku istnienia wielu połączeń WAN należy wybrać to, na którym obecny jest ruch przychodzący, np. domyślne połączenie WAN.



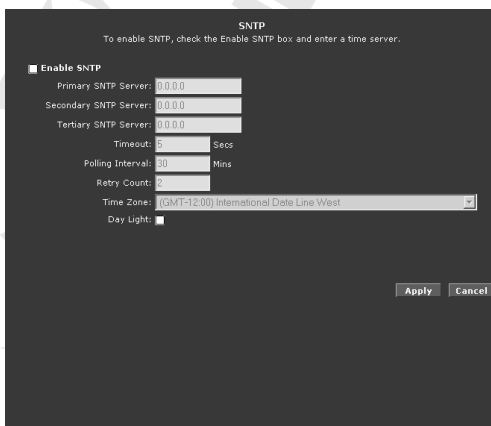
Enable UPnP – Włącz obsługę UPnP.

WAN Connection – Wybierz połączenie WAN, które będzie wykorzystywał UPnP.

LAN Connection – Wybierz połączenie LAN, które będzie wykorzystywał UPnP.

Application / SNTP

Simple network timing protocol (SNTP) jest protokołem używanym do synchronizowania czasu systemowego z publicznymi serwerami czasu SNTP. Do komunikacji między klientami i serwerami jest używany protokół UDP na porcie 123.



Enable SNTP – Włącz synchronizację czasu przez SNTP.

Primary SNTP Server – Adres IP lub nazwa hosta pierwszorzędного serwera SNTP. Informacja ta może być dostarczone przez usługodawcę lub zdefiniowana przez użytkownika.

Secondary SNTP Server – Adres IP lub nazwa hosta drugorzędного serwera SNTP. Informacja ta może być dostarczone przez usługodawcę lub zdefiniowana przez użytkownika.

Tertiary SNTP Server – Adres IP lub nazwa hosta trzeciorzędного serwera SNTP. Informacja ta może być dostarczone przez usługodawcę lub zdefiniowana przez użytkownika.

Timeout – Jeśli routerowi nie udało się zsynchronizować czasu w podanym w tym polu czasie następuje ponownie próby połączenia.

Polling Interval – Czas między udaną synchronizacją czasu a następną próbą połączenia z serwerem SNTP.

Retry Count – Ilość prób nawiązania połączenia z serwerem, po której router przechodzi do kolejnego serwera.

Time Zone – Strefa czasowa, w której znajduje się router.

Day Light – Zaznacz tą opcję aby włączyć czas letni. Router nie zmienia automatycznie czasu z letniego na zimowy i przy każdej zmianie należy ręcznie przestawić tą opcję.

Application / SNMP

SNMP (Simple Network Management Protocol) jest protokołem wspomagającym rozwiązywanie problemów i zarządzanie i używa protokołu UDP na porcie 161 do komunikacji między klientami a serwerami. SNMP używa agentów i baz informacji zarządzania MIB (management information base) do spełnienia wymagań zarządzania. Agent to oddzielna stacja, która może zażądać danych od agentów SNMP znajdujących się w sieci. Agenci używają baz MIB jako słowników zarządzalnych obiektów. Każde urządzenie zarządzalne przez SNMP ma przynajmniej jednego agenta mogącego odpowiadać na żądania NMS (Network Management Station – sieciowa stacja zarządzająca). Agent SNMP wspiera komunikaty GETS, SETS i TRAPS dla 4 grup w MIB-II: System, Interface, IP i ICMP. Agent SNMP obsługuje trzy nazwy uwierzytelniające Community.

The screenshot shows the 'SNMP Management' configuration page. It includes sections for enabling the agent and traps, and defining community names and access rights. The 'Community' section is a table with two columns: 'Name' and 'Access Right'. The 'Traps' section is a table with three columns: 'Destination IP', 'Trap Community', and 'Trap Version'.

Enable SNMP Agent – Zaznacz aby włączyć agenta SNMP na routerze.

Enable SNMP Traps – Zaznacz aby włączyć komunikaty SNMP Traps na routerze..

Name / Location / Contact – Informacje o urządzeniu ułatwiające identyfikację i kontakt.

Vendor OID – Object ID – Unikalny identyfikator tego urządzenia.

Community – Wpisz nazwę Community (**Name**) i wybierz prawa dostępu (**Access Right**).

Traps – Wpisz adres IP (**Destination IP**) menedżera SNMP (**Trap Community**), do którego będą wysyłane komunikaty Trap. Należy także z listy **Trap Version** wybrać wersję komunikatów Trap.

Application / IGMP Proxy

Hosty IP używają IGMP (Internet Group Management Protocol – protokół zarządzania grupami internetowymi) do raportowania sąsiednim routerom o członkostwie w grupach multikastingowych. W podobny sposób routery multikastingowe używają IGMP do wykrywania do jakich grup multikastingowych należą hosty, komunikujące się z nimi. Twój router obsługuje IGMP Proxy, który służy do obsługi komunikatów IGMP. Po włączeniu tej opcji router pełni rolę Proxy (serwera pośredniczącego) dla hostów z sieci LAN wysyłających żądania dołączenia/opuszczenia grupy multikastingowej lub dla routera multikastingowego wysyłającego pakiety do grup multikastingowych do sieci WAN.

Multikasting jest formą ograniczonej transmisji. UDP jest wykorzystywany do wysyłania datagramów do wszystkich hostów znajdujących się w tak zwanej grupie hostów (multikastingowej). Grupa hostów jest zestawem jednego lub więcej hostów identyfikowanych przez jeden docelowy adres IP. Poniższe reguły dotyczą grup hostów:

- Każdy może dowolnie dołączyć do grupy lub ją opuścić.
- Nie ma ograniczeń dotyczących położenia hosta.
- Nie ma ograniczeń dotyczących ilości członków należących do grupy.
- Host może należeć do więcej niż jednej grupy hostów.
- Hosty niebędące członkami grupy mogą wysłać do niej datagramy UDP.

Multikasting jest przydatny kiedy trzeba przesłać te same informacje do więcej niż jednego urządzenia. Na przykład: jeśli jedno urządzenie jest odpowiedzialne za zbieranie danych potrzebnych przez wiele innych urządzeń, multikasting jest idealnym rozwiązaniem. Główną przewagą używania multikastingu zamiast wysyłania tej samej informacji do wielu urządzeń jest obniżenie obciążenia sieci. Multikasting umożliwia także otrzymywanie strumieni wideo z serwerów multikastingowych. Strona IGMP Proxy umożliwia na włączenie multikastingu na dostępnych połączeniach WAN i LAN.

Możesz skonfigurować każdy interfejs WAN lub LAN jako:

Upstream – Interfejs przesyłający żądania od hostów do routera multikastingowego.

Downstream – Interfejs przesyłający dane od routera multikastingowego do hostów znajdujących się w bazie grup multikastingowych.

Ignore – Żadne żądania IGMP ani dane multikastingowe nie są przekazywane.

Application / TR-068 WAN Access (Zdalny dostęp)

Strona TR-068 WAN Access umożliwia na danie komuś (np.: wsparcie techniczne) tymczasowego zezwolenia na dostęp do routera z sieci WAN. Od momentu utworzenia konta, użytkownik ma 20 minut na zalogowanie się, w przeciwnym wypadku konto wygasa. Jeśli użytkownik się zalogował a czas jego bezczynności będzie wynosić 20 minut zostanie on wylogowany a konto wygaśnie.



Enable WAN Access Update
To Enable Webpage Update from WAN side

WAN Update:

WAN Access:

User Name: tech

Password:

Port: 51003

Apply Cancel

WAN Update – Pozwala temu użytkownikowi na zmianę ustawień WAN.

WAN Access – Pozwala temu użytkownikowi na dostęp do WAN.

User Name / Password – Nazwa użytkownika i hasło potrzebne do uwierzytelnienia.

Port – Numer portu zdalnego dostępu.

Aby uzyskać zdalny dostęp do routera należy wpisać w przeglądarkę następujący adres:

http(s)://WAN IP routera:numer portu (np. ***http://10.10.10.5:51003***)

Application / TR-069

Strona TR-069 pozwala na ustawienie parametrów łącza, które nie będzie widoczne dla użytkowników końcowych. TR-069 to protokół zarządzający CPE ze strony sieci WAN, przeznaczony do komunikacji między CPE (Customer Premise Equipment – urządzenie w lokalu klienta) i serwerami automatycznej konfiguracji (Auto-Configuration Server – ACS). Protokół CWMP (CPE WAN Management Protocol) definiuje mechanizm sterujący bezpieczną automatyczną konfiguracją CPE, a także zawiera inne funkcje zarządzania.

Protokół CWMP wspiera wiele funkcji do zarządzania zbiorem urządzeń CPE, włączając w to najważniejsze:

- Automatyczna konfiguracja i dynamiczne przydzielanie usług
- Zarządzanie obrazami oprogramowania i firmware
- Monitorowanie stanu i wydajności
- Diagnostyka

TR-069

TR-069 is enabled by default. Set the ACS URL below.

ACS URL:

Periodic Inform Enabled:

Periodic Inform Interval:

ACS Connection Request

Username:

Password:

ACS URL – Adres serwera ACS.

Periodic Inform Enabled – Zaznacz tą opcję jeśli chcesz włączyć okresowe powiadamianie.

Periodic Inform Interval – Odstęp między dwoma połączeniami okresowego powiadamiania.

ACS Connect – Kliknij, aby połączyć z ACS. Po ustanowieniu połączenia serwer ACS zaktualizuje wartości ACS URL, Periodic Inform Enabled i Periodic Inform Interval.

ACS Connection Request – Nazwa użytkownika (**Username**) i hasło (**Password**) wymagane do podłączenia do serwera ACS.

Application / NAT Services (Usługi NAT)

Jeśli dostępny jest więcej niż jeden publiczny adres IP przydzielany przez usługodawcę dodatkowe adresy mogą zostać użyte do mapowania serwerów w sieci LAN. Jeden publiczny adres IP zostanie wykorzystany do zapewnienia użytkownikom dostępu do Internetu przez NAT i będzie podstawowym adresem IP routera. Pozostałe adresy mogą zostać przypisane do serwerów znajdujących się w sieci LAN.

The screenshot shows a configuration window titled "NAT Services". It contains several input fields: "Name" (text), "Type" (dropdown menu showing "N/A"), "LAN IP" (text), "Subnet LAN IP" (text), "Start Public IP" (text), "End Public IP" (text), and "Connection" (dropdown menu showing "N/A"). Below these fields is a table with the following columns: "Name", "Type", "LAN IP", "Subnet LAN IP", "Start Public IP", "End Public IP", "Connection", "Edit", and "Delete". The table is currently empty. At the bottom right of the window are "Apply" and "Cancel" buttons.

Name – Nazwa wyświetlana na liście.

Type – Router wspiera trzy rodzaje mapowań NAT:

- **One to One** – jeden do jednego – router tłumaczy jeden prywatny adres IP na jeden publiczny adres IP.
- **Many to Many** – wielu do wielu – router tłumaczy wiele prywatnych adresów IP na współdzielone publiczne adresy IP.
- **Server** – – serwer – ten typ pozwala na określenie wewnętrznych serwerów za NATem, które mają być widoczne z sieci zewnętrznych.

LAN IP – Adres IP hosta w sieci lokalnej.

Subnet LAN IP – Dostępny tylko dla mapowania **Many to Many**. Wpisz maskę podsieci adresów IP w sieci LAN.

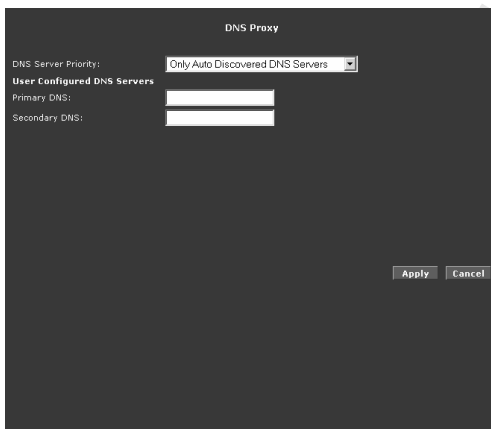
Start Public IP – Publiczny adres IP dla mapowania **One to One** lub **Server**. Początkowy publiczny adres IP dla mapowania **Many to Many**.

End Public IP – Końcowy publiczny adres IP dla mapowania **Many to Many**.

Connection – Połączenie WAN, które będzie używane przez mapowania NAT.

Application / DNS Proxy

DNS Proxy określa podstawowy i drugorzędny serwer DNS.



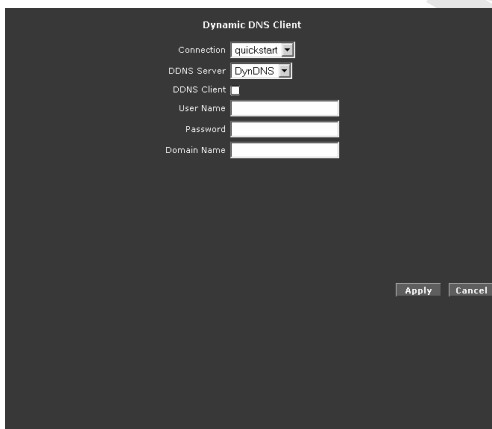
DNS Server Priority – Wybierz, które serwery DNS mają zostać użyte: Auto Discovered (automatycznie wykryte podczas nawiązywania połączenia) czy User Configured (wpisane w pola poniżej):

- **Only Auto Discovered DNS Servers** – Tylko automatycznie wykryte.
- **Only User Configured DNS Servers** – Tylko zdefiniowane przez użytkownika.
- **Auto Discovered then User Configured** – Automatycznie wykryte a następnie zdefiniowane przez użytkownika.
- **User Configured then Auto Discovered** – Zdefiniowane przez użytkownika a następnie automatycznie wykryte.

Primary / Secondary DNS – Wpisz adresy IP podstawowego i drugorzędного serwera DNS.

Application / Dynamic DNS Client (Klient DDNS)

Dynamic DNS (dynamiczny DNS) pozwala na wykorzystanie usług dostawcy DDNS. Usługa Dynamic DNS będzie powiązana z adresem IP WAN routera, nawet po zmianie przez usługodawcę adresu IP routera. Usługa ta jest przydatna gdy przy serwerach www i ftp. Musisz mieć zarejestrowane konto u jednego z dostawców DDNS, np. DynDNS (bez opłat) – <http://www.dyndns.org> lub TZO – <http://www.tzo.com> .



Connection – Połączenie WAN, do którego przypisana będzie usługa DDNS.

DDNS Server – Dostawca usługi DDNS.

DDNS Client – Zaznacz tą opcję by uruchomić usługę DDNS.

User Name – Nazwa użytkownika w systemie dostawcy usługi DDNS – wpisz nazwę dokładnie w takiej postaci w jakiej otrzymałeś ją od dostawcy usługi DDNS.

Password – Hasło w systemie dostawcy usługi DDNS.

Domain Name – Nazwa domenowa przydzielana przez dostawcę usługi DDNS do adresu IP.

Application / Easy Connect Configuration (Łatwe połączenie)

Funkcja Easy Connect umożliwia wykorzystanie zasobów sieciowych bez konieczności zmiany domyślnej konfiguracji ustawień sieciowych komputera, np. TCP/IP, Proxy, DNS.



Enable Easy Connect – Zaznacz, aby włączyć opcję Easy Connect.

Auto IP – Wszystkie poprawne ustawienia TCP/IP komputera użytkownika pozwolą na przeglądanie sieci bez konieczności zmiany adresu IP.

Auto DNS – Adres IP serwera w konfiguracji komputera nie ma znaczenia, funkcja Auto DNS pozwala na przeglądanie sieci mimo niepoprawnie wpisanego adresu serwera DNS.

Auto NetBIOS – Pozwala serwerowi proxy na użycie dowolnej nazwy. Jedynym warunkiem jest to, że brama routera MUSI znajdować się w prywatnym zakresie adresów IP.

Prywatne zakresy IP:

Klasa A: 10.0.0.0 ~ 10.255.255.255

Klasa B: 172.16.0.0 ~ 172.31.255.255

Klasa C: 192.168.0.0 ~ 192.168.255.255

Auto Proxy – Odnosi się do dowolnego poprawnego prywatnego adresu IP z dowolnym numerem portu. Na przykład, po wpisaniu w przeglądarce 1234 funkcja Auto Proxy nadal pozwoli na przeglądanie sieci. Ustawienie dowolnego publicznego adresu IP jako proxy spowoduje, że funkcja Auto Proxy nie zostanie użyta. **Uwaga:** Numer portu, który ma być użyty musi być ustawiony zarówno w przeglądarce jak i w Auto Proxy Ports.

Application / Port Triggering

Port triggering jest wyspecjalizowaną formą przekazywania portów (port forwarding), która umożliwia na uzyskanie dostępu do komputerów znajdujących się za NATem. W momencie gdy klient w sieci LAN wykonuje wychodzące połączenie na określony port na serwerze zostaje otwarty określony port przychodzący dla tego klienta.

Name – Wpisz nazwę reguły.

Start / End Trigger Port – Wpisz zakres portów na serwerze, z którymi połączenie spowoduje otwarcie portów przychodzących.

Start / End Open Port – Wpisz zakres portów, które mają zostać otwarte.

Protocol Type – Wybierz protokół, którego użycie może spowodować otwarcie portu lub który będzie umożliwiał dostęp do otwartego portu.

Connection – Połączenie WAN, które będzie używało funkcji Port Triggering.

Application / Port Forwarding (Przekazywanie portów)

Przekazywanie portów (Port forwarding lub virtual server) pozwala na przekierowanie przychodzącego ruchu do konkretnego hosta w sieci LAN na podstawie protokołu i numeru portu. Przekazywanie portów umożliwia dostarczanie lokalnych usług (na przykład serwer www) dla klientów internetowych lub granie w gry internetowe. Przekazywanie portów jest konfigurowane osobno dla każdej grupy LAN.



WAN Connection – Wybierz połączenie WAN używane do przekazywania portów.

Allow Incoming Ping – Zaznacz aby zezwolić na przychodzące pakiety Ping.

Select LAN Group / LAN IP – Wybierz grupę LAN i adres IP w sieci LAN, dla którego chcesz skonfigurować reguły.

New IP – Otwiera stronę **LAN Clients**, na której możesz dodać nowy statyczny adres IP (więcej szczegółów znajdziesz w części **LAN / LAN Clients**).

DMZ – Otwiera stronę **DMZ Settings**, na której możesz włączyć i skonfigurować DMZ.

Custom Port Forwarding – Otwiera stronę **Custom Port Forwarding**, która umożliwia tworzenie bardziej zaawansowanych reguł.

Category – Reguły są pogrupowane w zależności od ich zastosowania. Można tworzyć własne reguły w kategorii **User**.

Available Rules – Lista wszystkich dostępnych reguł w wybranej kategorii. Wybierz regułę i kliknij **Add**, aby dodać ją do listy zastosowanych reguł (**Applied Rules**).

Applied Rules – Lista wszystkich reguł zastosowanych dla wybranego hosta. Wybierz regułę i kliknij **Remove**, aby usunąć ją z listy zastosowanych reguł (**Applied Rules**).

New – Aktywne tylko w kategorii **User**. Otwiera stronę **Rule Management**.

View – Otwiera stronę **Rule Management** ze szczegółowymi danymi o wybranej regule.

Delete – Aktywne tylko w kategorii **User**. Użyj tego przycisku, aby usunąć wybraną regułę.

Poniższe strony mogą być otwarte ze strony Port Forwarding:

- **Rule Management (New Rule)**

Strona Rule Management pozwala na tworzenie nowych reguł. Aby stworzyć nową regułę wypełnij pola **Rule Name** (nazwa reguły), **Protocol** (protokół), **Port Start** (port początkowy), **Port End** (port końcowy) i **Port Map** (mapowany port) a następnie kliknij **Apply**. Stworzone reguły mogą być także wykorzystane do konfiguracji filtrów IP (IP Filters), które znajdują się w zakładce Security.

- **DMZ**

Skonfigurowanie hosta w sieci lokalnej jako strefy zdemilitaryzowanej (demilitarized zone – DMZ) przekazuje cały ruch, który nie został przekierowany do innego hosta przez przekazywanie portów, na adres IP tego hosta. Umożliwia to dostęp do tego hosta z sieci Internet. Funkcja ta jest domyślnie wyłączona. Włączenie DMZ powoduje zwiększenie bezpieczeństwa sieci dla hostów znajdujących się za zaporą firewall.

Aby włączyć DMZ zaznacz **Enable DMZ**, a następnie wybierz parametry hosta DMZ list **Select your WAN Connection** (wybierz połączenie WAN), **Select LAN Group** (wybierz grupę LAN) i **Select LAN IP Address** (wybierz adres IP sieci LAN) i kliknij **Apply**.

- **Custom Port Forwarding**

Strona Custom Port Forwarding umożliwia utworzenie 15 spersonalizowanych reguł przekazywania portów, aby umożliwić działanie określonych usług lub aplikacji, na przykład równoległego działania NAT/NAPT.

Application / Bridge Filters (Filtry mostów)

Strona Bridge Filters umożliwia włączenie, dodanie, edycję i kasowanie reguł filtrujących. Po włączeniu filtrowania mostów każda ramka jest porównywana w kolejności z każdą zdefiniowaną regułą. Kiedy reguła jest spełniona podejmowana jest zdefiniowana akcja (zezwoleń – allow lub zabronienie – deny). Można skonfigurować do 20 reguł filtrów.

Bridge Filters

Enable Bridge Filters

Enable Bridge Filter Management Interface

Select LAN: LAN group 1

Bridge Filter Management Interface: Ethernet 1

Src MAC	Src Port	Dest MAC	Dest Port	Protocol	Mode
00-00-00-00-00-00	ANY	00-00-00-00-00-00	ANY	PPPoE Session	Deny

Buttons: Add, Edit, Apply, Cancel

Enable Bridge Filters – Zaznacz, aby włączyć opcję filtrowania mostów.

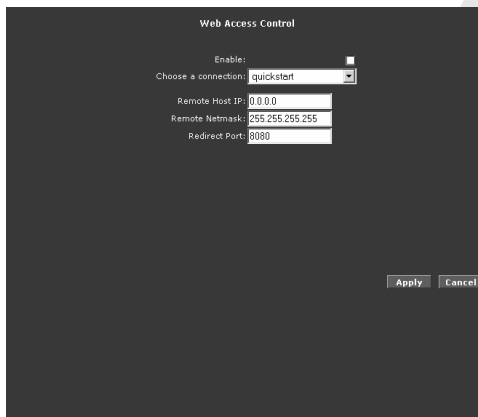
Enable Bridge Filters Management interface – Zaznacz, aby włączyć wybrany z listy **Bridge Filters Management interface** jako interfejs zarządzający filtrowaniem mostów.

Select LAN – Wybierz grupę LAN, dla której reguły chcesz skonfigurować.

Aby dodać regułę, wpisz **Src MAC** (źródłowy adres MAC), **Dest MAC** (docelowy adres MAC) i wybierz z list **Src Port** (port źródłowy), **Dest Port** (port docelowy), **Protocol** (protokół) i typ filtrowania (**Mode**) a następnie kliknij **Add**. Możesz także edytować lub usunąć regułę klikając odpowiednio w polu **Edit** lub **Delete** dla danej reguły.

Application / Web Access Control (Kontrola dostępu zdalnego)

Strona Web Access Control umożliwia skonfigurowanie zdalnego dostępu do routera (z sieci WAN), np z domu lub biura.



Enable – Zaznacz aby włączyć dostęp zdalny do routera.

Choose a connection – Wybierz połączenie WAN, które będzie użyte do dostępu zdalnego.

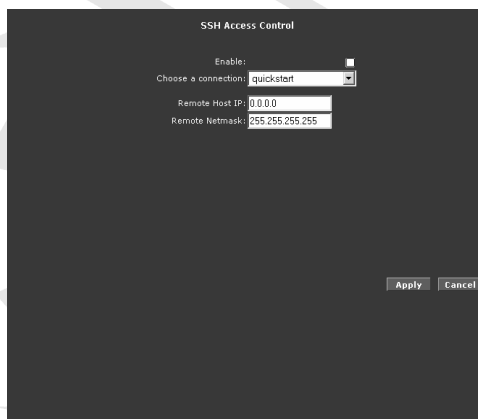
Remote Host IP – Adres IP hosta, posiadającego uprawnienia do dostępu zdalnego.

Remote Netmask – Zmiana podsieci umożliwia większej ilości hostów na dostęp zdalny.

Redirect Port – Port, na którym router będzie nasłuchiwać na żądanie dostępu zdalnego.

Application / SSH Access Control (Kontrola dostępu SSH)

Strona SSH Access Control umożliwia skonfigurowanie dostępu do routera z sieci WAN za pośrednictwem SSH.



Enable – Zaznacz aby włączyć dostęp przez SSH do routera.

Choose a connection – Wybierz połączenie WAN, które będzie użyte do dostępu przez SSH.

Remote Host IP – Adres IP hosta, posiadającego uprawnienia do dostępu przez SSH.

Remote Netmask – Zmiana podsieci umożliwia większej ilości hostów na dostęp przez SSH.

QoS

Quality of service pozwala administratorom sieci na skonfigurowanie routerów w sposób, pozwalający na spełnienie żądań dla przesyłu głosu i wideo.

Różne sieci używają innych oznaczeń QoS, np.:

- sieć ToS: bity ToS w nagłówku IP
- sieć VLAN: bity priorytetu (priority bits) w nagłówku VLAN
- sieć DSCP: używa tylko 5 bitów z CoS
- WLAN: nagłówek WLAN QoS.

Struktura QoS jest wspierana przez wszystkie wymienione powyżej sieci. Jak się porozumiewają? Jak można się upewnić, że priorytet z jednej sieci zostanie przeniesiony do drugiej? Dlatego jako wspólny język dla mapowań QoS zostały wprowadzone klasy (CoS – Class of Service). Po włączeniu QoS, router ma pełną kontrolę nad pakietami w czasie między ich przybyciem do routera a ich wyjściem z routera. Sposób działania jest następujący: Mapowanie domenowe (bity ToS, bity priorytetu, etc.) pakietu musi zostać przetłumaczone na CoS po wejściu do routera, i vice versa, CoS pakietu musi zostać przetłumaczone z powrotem na mapowanie domenowe przy opuszczaniu routera.

Istnieje 6 typów CoS (wg priorytetu):

- CoS1
- CoS2
- CoS3
- CoS4
- CoS5
- CoS6

Reguły są następujące:

1. CoS1 ma najwyższy priorytet i jest używany do ruchu wymagającego natychmiastowego przekazania (expedited forwarding – EF). CoS1 jest zawsze obsługiwany do zakończenia.
2. CoS2-CoS5 są używane dla klas zapewnionego przekazania (assured forwarding – AF). Te klasy są obsługiwane wg ścisłej zasady, na podstawie następującego schematu: CoS2 > CoS3 > CoS4 > CoS5
3. CoS6 jest dla ruchu typu najlepszy wysiłek (best effort – BE). CoS6 jest obsługiwany tylko wtedy kiedy nie ma potrzeby obsłużenia innej klasy. Jeśli QoS nie jest włączony, cały ruch jest traktowany jak CoS6.

Powinieneś zapoznać się dodatkowo z poniższymi pojęciami:

- Ingress: Pakiety przychodzące do routera z interfejsu WAN/LAN.
- Egress: Pakiety wychodzące z routera do interfejsu WAN/LAN.
- Trusted mode (tryb ufny): Router uznaje mapowanie domenowe (bit ToS, WME, priorytet użytkownika VLAN).
- Untrusted mode (tryb nieufny): Router nie uznaje mapowania domenowego. Jest to domyślne ustawienie QoS.
- Traffic Conditioning Agreement (TCA): TCA musi zostać zdefiniowane dla każdego interfejsu:
 - Mapowania Ingress (Domena =>CoS)
 - Mapowania Egress (CoS => Domena)
 - Untrusted mode (domyślny tryb nieufny)
- Shaper

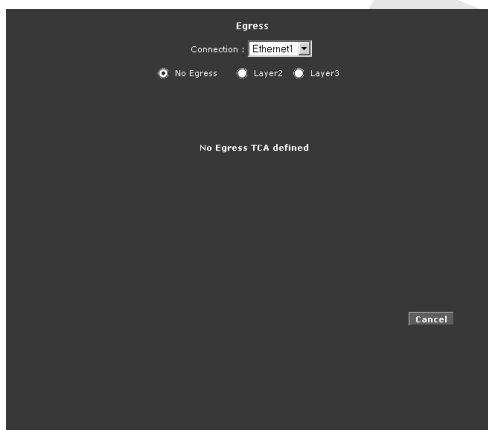
QoS / Egress

Dla pakietów wychodzących z routera, oznaczenia CoS muszą zostać przetłumaczone na mapowania zrozumiałe dla domen sieciowych. Odwrócenie CoS i mapowanie domenowe jest konfigurowane przy użyciu Egress.

Są trzy typy ustawienia Egress:

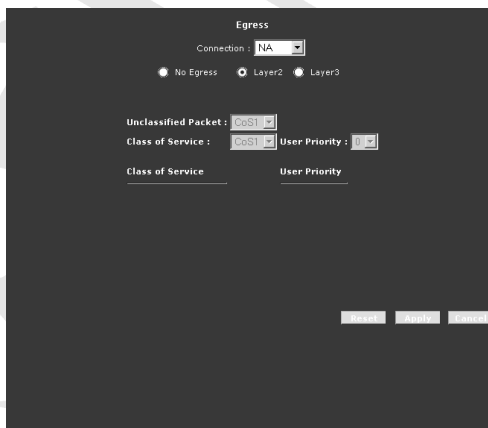
- **No Egress Mode (Bez Egress)**

Domyślne ustawienie dla wszystkich interfejsów to No Egress. W tym trybie mapowania domenowe pakietów nie są zmieniane.



- **Layer 2 (Warstwa 2)**

Strona Layer 2 umożliwia mapowanie CoS wychodzących pakietów na bity priorytetu (priority bits), które są używane w sieciach VLAN. Ta opcja jest obsługiwana tylko dla połączeń interfejsu WAN.



Interface – Wybierz interfejs WAN, dla którego ma zostać skonfigurowany QoS wychodzących pakietów; interfejsy LAN nie mogą być wybrane, ze względu na obsługę VLAN tylko po stronie WAN.

Unclassified Packet – Niektóre lokalnie wygenerowane pakiety mogą nie być sklasyfikowane i dlatego nie posiadają wartości CoS, np. pakiet kontrolny PPP lub pakiet ARP. Możesz zdefiniować w tym polu CoS dla wszystkich niesklasyfikowanych pakietów wychodzących w warstwie 2, które uzyskają priorytet na podstawie reguł, które stworzysz. Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6. Domyślną wartością jest CoS1 (zalecane).

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

User Priority – Wartość User Priority (priorytet użytkownika – bit priorytetu) w sieci VLAN. Do wyboru są wartości: 0, 1, 2, 3, 4, 5, 6, 7.

- **Layer 3 (Warstwa 3)**

Strona Layer 3 umożliwia mapowanie CoS wychodzących pakietów na bity ToS, aby oznaczenie priorytetu mogło zostać przeniesione do sieci IP.



Egress

Connection: Ethernet

No Egress Layer2 Layer3

Default Non-IP: CoS1

Class of Service: CoS1 Translated TOS:

Class of Service Translated TOS

Reset Apply Cancel

Interface – Wybierz interfejs, dla którego ma zostać skonfigurowany QoS wychodzących pakietów.

Default Non-IP – Niektóre lokalnie wygenerowane pakiety mogą nie posiadać wartości CoS (np. pakiety ARP). Możesz zdefiniować w tym polu CoS dla wszystkich pakietów bez nagłówka IP wychodzących w warstwie 3. Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6. Domyślną wartością jest CoS1 (zalecane).

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

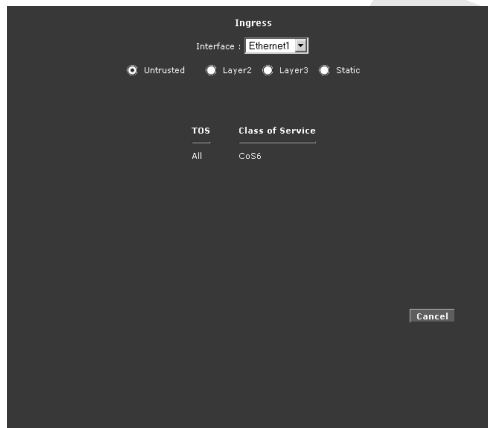
Translated TOS – Wartość tego pola powinna wynosić od 1 do 255.

QoS / Ingress

Ingress umożliwia skonfigurowanie QoS dla pakietów przychodzących do routera. Mapowania domenowe są zamieniane na CoS, aby oznaczenia priorytetu zostały zachowane. Są trzy typy ustawienia Ingress:

- **Untrusted Mode (Tryb nieufny)**

Tryb nieufny jest domyślnym trybem dla wszystkich interfejsów. W tym trybie router nie uznaje mapowań domenowych i wszystkie pakiety są traktowane jako CoS6.



- **Layer 2 (Warstwa 2)**

Strona Layer 2 umożliwia mapowanie przychodzących pakietów z priorytetem VLAN na CoS. Interfejsy LAN nie mogą być wybrane, ze względu na obsługę VLAN tylko po stronie WAN..



Interface – Wybierz interfejs WAN, dla którego ma zostać skonfigurowany QoS przychodzących pakietów; interfejsy LAN nie mogą być wybrane, ze względu na obsługę VLAN tylko po stronie WAN.

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

User Priority – Wartość User Priority (priorytet użytkownika – bit priorytetu) w sieci VLAN. Do wyboru są wartości: 0, 1, 2, 3, 4, 5, 6, 7.

Uwagi:

- Każdy bit priorytetu bez przypisanego CoS będzie traktowany jako CoS6.
 - Każdy nieskonfigurowany interfejs WAN korzysta z domyślnego trybu Untrusted.
- **Layer 3 (Warstwa 3)**
Strona Layer 3 umożliwia mapowanie bitów ToS przychodzących pakietów na CoS, dla każdego interfejsu WAN/LAN.



Interface – Możesz skonfigurować QoS dla ruchu warstwy 3 (IP) dla każdego interfejsu WAN i LAN..

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

TOS – Wartość tego pola powinna wynosić od 1 do 255.

Default Non-IP – Możesz zdefiniować w tym polu CoS dla wszystkich pakietów bez nagłówka IP przychodzących warstwy 3 (np. pakiety ARP). Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6. Domyślną wartością jest CoS1 (zalecane).

Uwagi:

- Każdy bit priorytetu bez przypisanego CoS będzie traktowany jako CoS6.
- Każdy nieskonfigurowany interfejs WAN korzysta z domyślnego trybu Untrusted.

- **Static (Statyczne)**

Strona Static pozwala na ustawienie stałego CoS dla wszystkich pakietów odebranych przez interfejs WAN lub LAN.

Interface – Wybierz połączenie, aby skonfigurować dla niego CoS.

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

QoS / QoS Shaper Configuration

Strona Shaper Configuration umożliwia ukształtowanie priorytetów ruchu na podstawie jednego z trzech algorytmów:

- HTB
- Low Latency Queue Discipline
- PRIOWRR

Uwaga: Wymagane jest skonfigurowanie Egress jeśli funkcja Shaper jest skonfigurowana dla tego połączenia.

Interface – Do wyboru są wszystkie interfejsy WAN i LAN oprócz WLAN, który nie obsługuje funkcji Shaper. Interfejs należy wybrać przed konfiguracją funkcji Shaper.

Max Rate – To pole jest dostępne dla ustawień HTB Queue Discipline oraz Low Latency Queue Discipline, które kształtują ruch bazując na ilości przesyłanych danych.

HTB Queue Discipline – HTB (Hierarchical Token Bucket) jest algorytmem sterującym ruchem w sieci na podstawie limitów prędkości przesyłu ustalonych dla każdej klasy CoSx, na podstawie których będzie kształtowany ruch. Na przykład: Jeśli limit CoS1 jest ustawiony na 100Kbps to nawet jeśli dane CoS1 są wysyłane do interfejsu z prędkością 300Kbps, zostaną one wysłane tylko z prędkością 100Kbps.

Low Latency Queue Discipline – Algorytm ten jest bardzo podobny do HTB – jedyną różnicą jest brat limitu prędkości przesyłu dla klasy CoS1. Korzystając z przykładu z poprzedniego algorytmu dane CoS1 nie są limitowane do prędkości 100Kbps i zostaną wysłane z prędkością 300Kbps. Efektem ubocznym może być „zapchanie” łącza poprzez złe skonfigurowanie strumienia.

PRIOWRR – Ten algorytm bazuje na wyważeniu priorytetów klas CoS2-CoS6. Kolejki CoS1 mają najwyższy priorytet i nie są kontrolowane przez algorytm WRR. Algorytm ten jest podobny do Low Latency Queue discipline – różnicą jest to, że PRIOWRR bazuje na ilości pakietów a nie ilości przesyłanych danych.

QoS / Policy Routing Configuration (Konfiguracja zasad routowania)

Strona Policy Routing Configuration umożliwia konfigurację zasad routowania i QoS.

Ingress Interface	DSCP	Source IP	Destination IP	Source Port Start	Destination Port Start	Protocol	Local Mark	Delete
Dest Interface	CoS	Mask	Mask	Source Port End	Destination Port End	Source MAC		

Ingress Interface – Interfejs ruchu przychodzącego dla reguły Policy Routing. Do wyboru są interfejsy LAN, WAN, Locally generated (ruch generowany lokalnie) i N/A (not applicable – nie dotyczy). Przykładami ruchu generowanego lokalnie są: pakiety głosowe, pakiety wygenerowane przez aplikacje takie jak DNS, DHCP, etc.

Destination Interface – Interfejs ruchu przychodzącego dla reguły Policy Routing. Lista zawiera wszystkie interfejsy LAN i WAN.

DiffServ Code Point – Wartość pola DiffServ code point (DSCP) powinna mieścić się między 1 a 255. Nie można skonfigurować tylko tego pola – wymagane jest także skonfigurowanie także innych pól, takich jak adresy IP, Source MAC (źródłowy adres MAC) i/lub interfejs Ingress.

Class of Service – Do wyboru są wartości (wg priorytetu – malejąco): CoS1, CoS2, CoS3, CoS4, CoS5 i CoS6.

Source IP – Adres IP źródła ruchu.

Mask – Maska podsieci źródłowego adresu IP. To pole jest wymagane, gdy wpisany został źródłowy adres IP.

Destination IP – Docelowy adres IP ruchu.

Mask – Maska podsieci docelowego adresu IP. To pole jest wymagane, gdy wpisany został docelowy adres IP.

Protocol – Wybór używanego protokołu: TCP, UDP, ICMP, Specify (określ), and none (żaden). Po wybraniu Specify, w polu obok należy wpisać numer protokołu. Nie można skonfigurować tylko tego pola – wymagane jest także skonfigurowanie także innych pól, takich jak adresy IP, Source MAC (źródłowy adres MAC) i/lub interfejs Ingress. To pole jest także wymagane po wpisaniu portów źródłowych lub docelowych.

Source Port – Port źródłowy (lub zakres) protokołu. Należy najpierw wybrać protokół.

Destination Port – Port docelowy (lub zakres) protokołu. Należy najpierw wybrać protokół.

Source MAC – Adres MAC źródła ruchu.

Local Routing Mark – To pole jest dostępne tylko po wybraniu Locally Generated w polu Ingress Interface. Znaczniki (mark) dla ruchu DNS generowanego przez różne aplikacje są wymienione poniżej:

- Dynamic DNS: 0xE1
- Dynamic Proxy: 0xE2
- Web Server: 0xE3
- MSNTP: 0xE4
- DHCP Server: 0xE5
- IP tables Utility: 0xE6
- PPP Deamon: 0xE7
- IP Route: 0xE8
- ATM Library: 0xE9
- NET Tools: 0xEA
- RIP: 0xEB
- RIP v2: 0xEC
- UPNP: 0xEE
- Busybox Utility: 0xEF
- Configuration Manager: 0xF0
- DropBear Utility: 0xF1
- Voice: 0

Aktualnie algorytmy routowania podejmują działania na zasadzie adresu docelowego, np. tylko docelowy adres IP i maska podsieci są obsługiwane. Strona Policy Routing umożliwia routowanie pakietów na podstawie różnych pól w pakiecie.

Poniższe pola mogą zostać skonfigurowane dla funkcji Policy Routing:

- Docelowy adres IP/maska podsieci
- Źródłowy adres IP/maska podsieci
- Źródłowy adres MAC
- Protokół (TCP, UDP, ICMP, etc)
- Port źródłowy
- Port docelowy
- Interfejs przychodzący
- DSCP

Routing / Static Routing (Routing statyczny)

Jeśli router jest podłączony do więcej niż jednej sieci, może być potrzebna konfiguracja routingu statycznego pomiędzy nimi. Routing statyczny to predefiniowana droga jaką informacja sieciowa musi przebyć, aby dotrzeć do określonego hosta czy sieci. Routing statyczny może być także użyty do umożliwienia dostępu do Internetu użytkownikom różnych sieci.



Static Routing

Choose a connection: quickstart

New Destination IP: Mask: 255.255.255.0

Gateway: Metric: 0

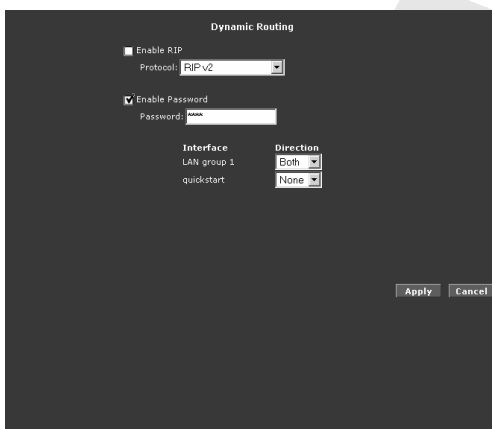
The Routing Table is empty.

Apply Cancel

Pole **New Destination IP** (nowe docelowe IP) jest adresem zdalnego hosta lub sieci, do którego ma zostać przypisana stała trasa. Dla standardowej domeny IP klasy C, adres sieciowy to pierwsze trzy oktety pola **New Destination IP**, ostatni oktet powinien wynosić zero. Maska podsieci wpisana w polu **Mask** identyfikuje, która część adresu IP określa sieć a która hosta. Dla całej podsieci klasy C maska podsieci wynosi 255.255.255.0. Adres IP bramy (**Gateway**) umożliwi ustawienie adresu IP bramy, z której będzie korzystał zdalna sieć/host.

Routing / Dynamic Routing (Routing dynamiczny)

Routing dynamiczny pozwala routerowi na automatyczne dostosowanie do fizycznych zmian sieci. Przy użyciu protokołu RIP router określa trasę pakietów sieciowych opierając się na jak najmniejszej ilości skoków między źródłem a celem. Protokół RIP regularnie rozgłasza informacje o routingu do innych routerów w sieci. **Direction** określa kierunek, w którym trasy RIP będą aktualizowane. Wybranie **In** oznacza, że router będzie tylko przyjmował informacje RIP. Wybranie **Both** oznacza, że router będzie przyjmował informacje RIP i wysyłał dalej zaktualizowane informacje RIP.



The screenshot shows the 'Dynamic Routing' configuration window. It has a dark background with white text. At the top, it says 'Dynamic Routing'. Below that, there are several settings:

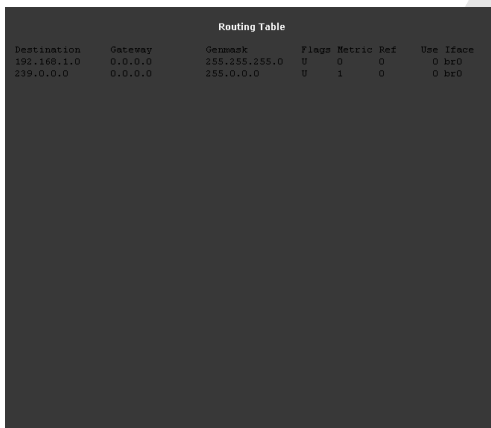
- Enable RIP
- Protocol: RIP v2 (dropdown menu)
- Enable Password
- Password: none (text field)
- Interface: LAN group 1 (dropdown menu)
- quickstart (checkbox, checked)
- Direction: Both (dropdown menu)
- None (dropdown menu)

At the bottom right, there are two buttons: 'Apply' and 'Cancel'.

Wykorzystany protokół jest zależny od całej sieci. Większość sieci wspiera RIP v1. Jeśli **RIP v1** jest wybrany, dane routingu będą wysyłane w formacie RIP v1. Jeśli **RIP v2** jest wybrany, dane routingu będą wysyłane w formacie RIP v2 używając transmisji w podsieci (subnet broadcasting). Jeśli **RIP v1 Compatible** jest wybrany, dane routingu będą wysyłane w formacie RIP v2 przy użyciu multikastingu.

Routing Table (Tablica routingu)

Tablica routingu wyświetla informacje używane przez routery podczas przekazywania pakietów. Pakiety są routowane zgodnie z docelowymi adresami IP pakietów.



Destination	Gateway	Genmask	Flags	Metric	Ref	Use	iface
192.168.1.0	0.0.0.0	255.255.255.0	0	0	0	0	br0
219.0.0.0	0.0.0.0	255.0.0.0	0	1	0	0	br0

System Password (Hasło systemowe)



System Password
System Password is used to change your User Name or Password.

Enable Authentication:

User Name:

Password:

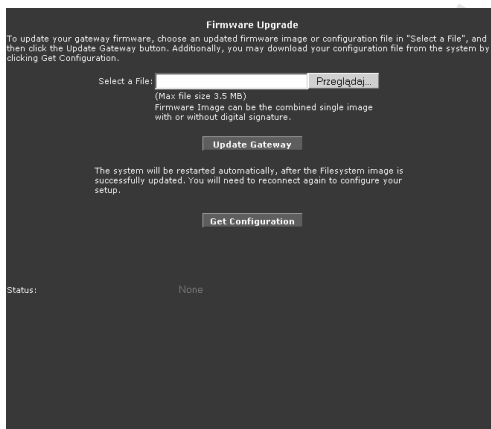
Confirmed Password:

Idle Timeout: minutes

Zaznacz pole **Enable Authentication** (bardzo zalecane), wpisz nazwę użytkownika (**User Name**) i hasło w pola **Password** oraz **Confirmed Password** i wpisz czas wygaśnięcia sesji (**Idle Timeout**). Podczas logowania do strony konfiguracyjnej użyj podanych na tej stronie nazwy użytkownika i hasła.

Firmware Upgrade (Aktualizacja firmware)

Uwaga: Upewnij się, że używasz prawidłowego pliku do aktualizacji firmware!



The screenshot shows a web interface for firmware upgrade. At the top, it says "Firmware Upgrade". Below that, there is a paragraph of instructions: "To update your gateway firmware, choose an updated firmware image or configuration file in 'Select a File', and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration." There is a "Select a File:" label followed by a file input field and a "Przejrzyj..." button. Below the input field, it says "(Max file size 3.5 MB)" and "Firmware Images can be the combined single image with or without digital signature." There is an "Update Gateway" button. Below that, there is a paragraph: "The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup." There is a "Get Configuration" button. At the bottom left, it says "Status:" and in the center, it says "None".

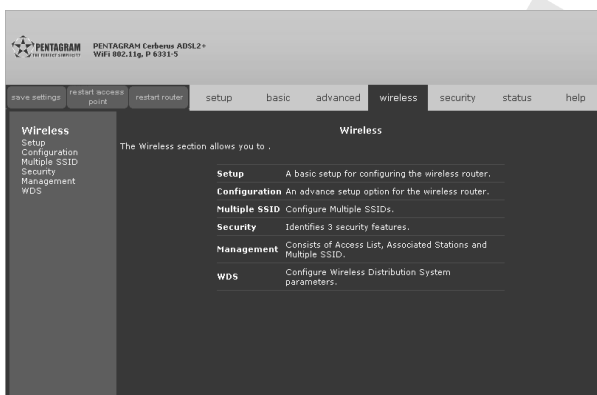
Kliknij **Browse** i zlokalizuj plik z firmware. Następnie kliknij **Update Gateway**. Proces aktualizacji może potrwać kilka minut. Upewnij się, że źródło zasilania nie zostanie odłączone od routera w tym czasie. Po zakończeniu aktualizacji router zostanie zrestartowany. Po ponownym uruchomieniu należy ponownie się zalogować do strony konfiguracyjnej.

Restore to Default (Przywrócenie ustawień domyślnych)

Kliknij **OK** jeśli chcesz przywrócić wszystkie ustawienia do wartości domyślnych.

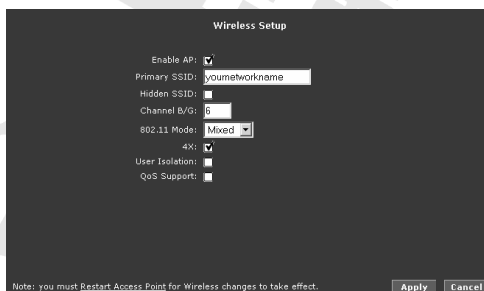
Zakładka Wireless

Zakładka Wireless pozwala na zmianę wszystkich ustawień sieci bezprzewodowej.



Setup

Domyślny identyfikator sesji sieci bezprzewodowej (SSID) to *yournetworkname*. SSID stanowi nazwę sieci bezprzewodowej utworzonej przez router. Klient sieci bezprzewodowej musi mieć skonfigurowany ten sam SSID. Na tej stronie można włączyć lub wyłączyć bezprzewodowy punkt dostępowy (Access Point – AP). Wyłączenie punktu dostępowego wyłączy emisję sygnału sieci bezprzewodowej przez router.



Enable AP – Po zaznaczeniu router będzie pełnił funkcję punktu dostępowego.

Primary SSID – Podstawowy identyfikator SSID jest unikalną nazwą identyfikującą sieć WLAN utworzoną przez router. Klienci sieci WLAN podłączający się do routera muszą posiadać ten sam SSID.

Hidden SSID – Zaznacz tę opcję jeśli nie chcesz by SSID nie był rozgłaszany – klient nie pozna SSID tej sieci przez zwykłe skanowanie połączeń. Po odznaczeniu SSID będzie normalnie rozgłaszany i klient będzie mógł poznać SSID przez skanowanie połączeń.

Channel B/G – Wybierz kanał używany przez router przy tworzeniu sieci bezprzewodowej.

802.11 Mode – Wybierz standard, który będzie obsługiwany przez to połączenie: **Mixed** (B i G), **B only** (tylko B), **B+** lub **G only** (tylko G).

User Isolation – Zaznacz tę opcję, jeśli chcesz zablokować ruch pomiędzy klientami sieci bezprzewodowej.

QoS Support – Zaznacz tą opcję, jeśli chcesz aby reguły QoS były zastosowane dla połączenia sieci bezprzewodowej.

Configuration (Konfiguracja)

Dla zaawansowanych użytkowników istnieje możliwość zmiany bardziej zaawansowanych ustawień sieci bezprzewodowej.

Beacon Interval – Częstotliwość transmitowania przez router pakietu Beacon. Wpisz wartość między 20 a 1000. Beacon jest pakietem synchronizującym sieć bezprzewodową transmitowanym przez router.

DTIM Period – Wpisz wartość pomiędzy 1 a 255, częstotliwość wysyłania przez router pakietu DTIM (Delivery Traffic Indication Message).

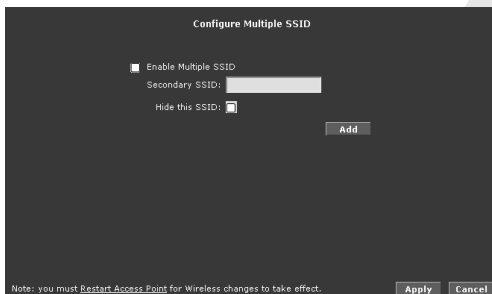
RTS Threshold – Próg wielkości ramki RTS (Request To Send – żądanie wysłania) do wywołania handshake RTS/CTS (wymiana ramek RTS i CTS; Clear To Send – gotowe do wysłania). Dane z wielkością ramki przekraczającą tą wartość wywoła handshake RTS/CTS. Ustawienie wartości przekraczającej maksymalną MSDU (MAC Service Data Unit) wyłączy tą opcję. Ustawienie wartości 0 włącza handshake RTS/CTS.

Frag Threshold – Próg (liczba bajtów) granicy fragmentacji przekazywanych wiadomości. Jest to największy rozmiar fragmentu danych, który może być przesłany.

Multi Domain Capability – Multi Domain Capability dodaje do każdej ramki Beacon Country Information Element. Country Information Element umożliwia zidentyfikowanie obszaru regulacyjnego (Regulatory Domain), na którym znajduje się router. Dostępne kanały (Channels) i poziomy siły sygnału (Power Levels) są zawarte w Country Information Element.

Multiple SSID (Dodatkowe SSID)

Strona Multiple SSID umożliwia dodanie pomocniczych SSID. Pole SSID może zawierać do 32 znaków alfanumerycznych. Zmień VLAN ID na wartość różną od zera (pomiędzy 1 a 4095).



Enable Multiple SSID – Zaznacz, aby włączyć funkcję dodatkowych SSID.

Aby dodać dodatkowy SSID, wpisz jego nazwę w polu **Secondary SSID**, zaznacz **Hide SSID** jeśli ten SSID ma nie być rozgłaszany i kliknij **Add**. Wszystkie pomocnicze SSID zostaną wyświetlone na liście poniżej. Aby usunąć SSID zaznacz pole w kolumnie **Delete** dla odpowiedniego SSID. Można dodać do trzech SSID. Po utworzeniu dodatkowych SSID zaleca się ich zabezpieczenie na stronie **Wireless Security**.

Wireless Security (Zabezpieczenie sieci bezprzewodowej)

Bardzo ważną sprawą jest zabezpieczenie dostępu do sieci bezprzewodowej. Umożliwia to zablokowanie dostępu do sieci i routera osobom nieupoważnionym. Domyślnie połączenie nie jest zabezpieczone (None).



• WEP

Protokół WEP zabezpiecza sieć poprzez szyfrowanie danych wysyłanych siecią WLAN. Można ustawić do 4 zestawów kluczy dla klientów bezprzewodowych. Router obsługuje trzy poziomy szyfrowania WEP: 64-bit, 128-bit i 256-bit. Przy użyciu WEP, każda stacja musi mieć ustawiony ten sam klucz używany do odszyfrowywania. Każda sieciowa karta bezprzewodowa i router muszą mieć ręcznie ustawiony ten sam klucz.

Aby włączyć szyfrowanie WEP zaznacz opcję **Enable WEP Wireless Security**, wybierz sposób uwierzytelniania z listy **Authentication Type**, Wybierz, który klucz szyfrujący będzie użyty, wybierz jego siłę (**Cipher**) i wpisz klucz w pole **Encryption Key**: dowolne 10 (Cipher: 64 bits), 26 (Cipher: 128: bits) lub 58 (Cipher: 256 bits) cyfr heksadecymalnych ("0-9", "A-F").

• 802.1x

Protokół 802.1x stanowi opartą na porcie kontrolę dostępu do sieci i utrzymuje port sieciowy zamknięty aż do zakończenia procesu uwierzytelnienia. 802.1x jest oparty na protokole EAP (Extensible Authentication Protocol). Wiadomości EAP od klienta wymagającego uwierzytelnienia do serwera uwierzytelniającego zwykle korzystają z protokołu RADIUS (Remote Authentication Dial-In User Service).

Server IP Address – Wpisz adres IP serwera uwierzytelniającego RADIUS.

Port – Wpisz port uwierzytelnienia na serwerze RADIUS.

Secret – Wpisz Shared Secret używany przez serwer RADIUS.

Group Key Interval – Wpisz czas, co który będzie zmieniany w całej sieci klucz grupy. changed across the whole network.

- **WPA**

WPA (W-Fi Protected Access) do szyfrowania danych wykorzystuje protokół TKIP (Temporal Key Integrity Protocol) i rozwiązuje wiele problemów, które istnieją w WEP, np. używa dynamicznych kluczy. WPA generuje nowy klucz szyfrujący za każdym razem gdy urządzenie bezprzewodowe usiłuje nawiązać połączenie z punktem dostępowym routera. Protokoły 802.1x, EAP i RADIUS są wykorzystywane w celu polepszenia uwierzytelnienia. Tak jak w przypadku WEP, klucze mogą być wpisane ręcznie (pre-shared keys – PSK); jednakże serwer uwierzytelniający RADIUS umożliwia automatyczne generowanie klucza uwierzytelniającego i uwierzytelnienie wielu stacji firmowych. WPA2, znany także jako 802.11i, używa do szyfrowania protokołu AES-CCMP (Advanced Encryption Standard Counter Code CBC-MAC Protocol).

WPA / WPA2 / AnyWPA – Wybierz wersję protokołu WPA, który będzie użyty do uwierzytelnienia tego połączenia.

Enable WPA2 Pre-authentication – Tylko dla WPA2/AnyWPA. Pre-authentication utrzymuje port sieciowy zamknięty aż do zakończenia procesu uwierzytelnienia.

Group Key Interval – Wpisz czas, co który będzie zmieniany w całej sieci klucz grupy.

Radius Server – Zaznacz tą opcję, aby użyć serwera RADIUS do uwierzytelniania WPA. Podaj Adres IP (**IP Address**), **Port** uwierzytelnienia i Shared **Secret** używane przez serwer RADIUS.

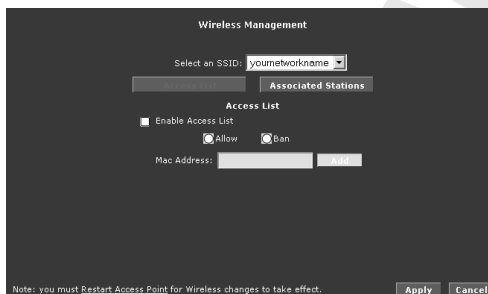
Pre-Shared Key – Zaznacz tą opcję, aby użyć ustalonego klucza (Pre-Shared Key – PSK) do uwierzytelniania WPA. Zarówno router jak i stacje klienckie muszą mieć ustawiony ten sam klucz PSK do przesyłu danych (podobnie do kluczy WEP).

Wireless Management (Zarządzanie siecią bezprzewodową)

Strona Wireless management umożliwia dodanie dodatkowego poziomu zabezpieczenia sieci bezprzewodowej routera.

- **Access List (Lista dostępowa)**

Lista dostępu umożliwia nadanie lub odebranie praw dostępu do sieci bezprzewodowej na podstawie adresu MAC.



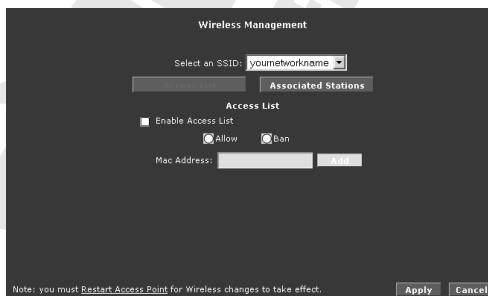
Enable Access List – Zaznacz to pole, aby włączyć listę dostępową (Access List).

Allow – Tylko klienci dodani do listy będą mogli podłączyć się do sieci bezprzewodowej routera. Klienci spoza listy nie będą mogli podłączyć się do tej sieci.

Ban – Tylko klienci dodani do listy nie będą mogli podłączyć się do sieci bezprzewodowej routera. Klienci spoza listy będą mogli podłączyć się do tej sieci.

- **Associated Stations (Powiązane stacje)**

Klienci połączeni do punktu dostępowego routera są wyświetleni na poniższej liście.



Aby zabrać klientowi prawa dostępu do sieci bezprzewodowej, zaznacz pole w kolumnie **Ban Station** dla tego klienta.

Wireless Distribution System

Wireless distribution system (WDS) jest systemem umożliwiającym łączenie bezprzewodowych sieci kilku punktów dostępowych w jedną dużą sieć bezprzewodową. WDS umożliwia klientom z urządzeniami przenośnymi na pozostanie w zasięgu jednej sieci i korzystaniu z jej zasobów nawet po przejściu na np. drugi koniec budynku.

WDS Mode – Dostępne są poniższe tryby WDS:

- Bridge – W trybie Bridge, BSS punktu dostępowego routera (Basic Service Set – blok sieci bezprzewodowej utworzony przez punkt dostępowy) jest włączony.
- Repeater – W trybie Repeater, BSS punktu dostępowego routera jest wyłączony podczas połączenia z punktem dostępowym wyższej warstwy.
- Crude – W trybie Crude, BSS punktu dostępowego routera jest zawsze włączony; ale połączenia między punktami dostępowymi są statyczne i nie są utrzymywane.
- Disabled (Domyślne) – WDS jest wyłączone.

W przypadku trybów Bridge i Repeater, WDS używa protokołu zarządzającego do ustanowienia i utrzymania połączeń między punktami dostępowymi.

WDS Name – Nazwa identyfikująca sieć WDS. Maksymalna długość nazwy to 8 znaków. Dwie lub więcej sieci WDS może działać na tym samym obszarze.

Activate as Root – To pole musi być zaznaczone, gdy router jest głównym punktem dostępowym (WDS root) w hierarchii WDS. Tylko jeden punkt dostępowy może pełnić funkcję WDS root. To pole jest niedostępne w trybie Crude.

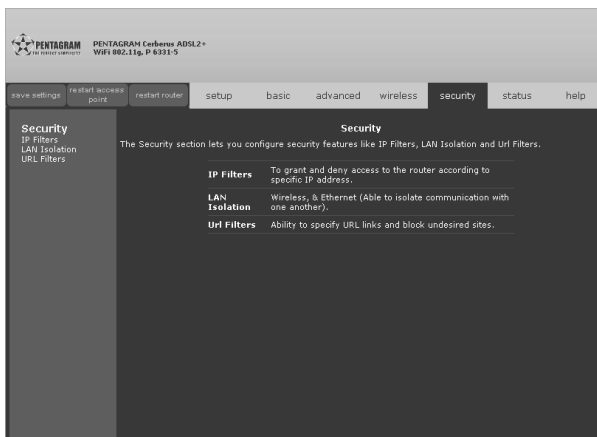
WDS Privacy – Zaznaczenie tej opcji nakazuje menedżerowi WDS używać zabezpieczonego połączenia między punktami dostępowymi w sieci WDS. Ustawienia zabezpieczeń wszystkich punktów dostępowych sieci WDS muszą być jednakowe. To pole jest niedostępne w trybie Crude.

Secret – Klucz prywatny składający się z 32 znaków alfanumerycznych.

Uplink Connection – Identyfikator BSS urządzenia umieszczonego wyżej w hierarchii WDS. Uplink nie może być ustawiony gdy opcja **Activate as Root** jest aktywna.

Downlink Connection – Identyfikator BSS urządzenia umieszczonego niżej w hierarchii WDS podłączonego do tego punktu dostępowego. Można skonfigurować do czterech urządzeń Downlink.

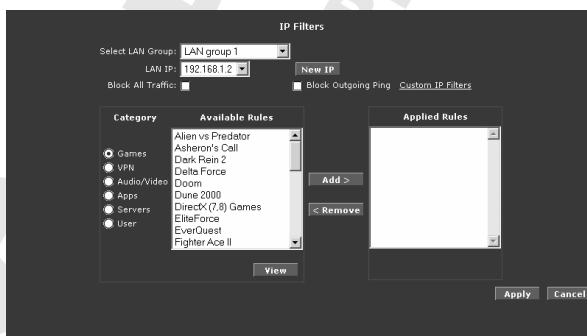
Zakładka Security



IP Filters (Filtrowanie IP)

Filtrowanie IP umożliwia blokowanie określonych aplikacji i usług bazując na adresie IP urządzenia w sieci LAN. Na tej stronie można zablokować określony ruch (np: dostęp do www) lub cały ruch danego hosta w sieci lokalnej.

Baza zdefiniowanych reguł filtrowania IP umożliwia dodanie jednej lub więcej reguł dla jednego lub więcej członka wybranej grupy LAN. Można wyświetlić szczegóły każdej reguły, które pogrupowane są w kategorie.. Można także stworzyć, edytować i usuwać własne reguły filtrowania IP.



Select LAN Group / LAN IP – Wybierz grupę LAN a następnie adres IP hosta, dla którego chcesz skonfigurować reguły. Wybranie **Any** na liście **LAN IP** spowoduje ustawienie reguł dla wszystkich członków wybranej grupy.

New IP – Otwiera stronę **LAN Clients**, na której możesz dodać nowy statyczny adres IP (więcej szczegółów znajdziesz w części **LAN / LAN Clients**).

Block All Traffic – Zaznacz to pole, aby zablokować cały ruch sieciowy dla wybranego hosta.

Block Outgoing Ping – Zaznacz, aby blokować pakiety Ping wysyłane przez tego hosta.

Custom IP Filters – Otwiera stronę **Custom IP Filters**, która umożliwi tworzenie bardziej zaawansowanych reguł.

Category – Reguły są pogrupowane w zależności od ich zastosowania. Można tworzyć własne reguły w kategorii **User**.

Available Rules – Lista wszystkich dostępnych reguł w wybranej kategorii. Wybierz regułę i kliknij **Add**, aby dodać ją do listy zastosowanych reguł (**Applied Rules**).

Applied Rules – Lista wszystkich reguł zastosowanych dla wybranego hosta. Wybierz regułę i kliknij **Remove**, aby usunąć ją z listy zastosowanych reguł (**Applied Rules**).

New – Aktywne tylko w kategorii **User**. Otwiera stronę **Rule Management**.

View – Otwiera stronę **Rule Management** ze szczegółowymi danymi o wybranej regule.

Delete – Aktywne tylko w kategorii **User**. Użyj tego przycisku, aby usunąć wybraną regułę.

Poniższe strony mogą być otwarte ze strony IP Filters:

- **Rule Management (New Rule)**

Strona Rule Management pozwala na tworzenie nowych reguł. Aby stworzyć nową regułę wypełnij pola **Rule Name** (nazwa reguły), **Protocol** (protokół), **Port Start** (port początkowy), **Port End** (port końcowy) i **Port Map** (mapowany port) a następnie kliknij **Apply**. Stworzone reguły mogą być także wykorzystane do konfiguracji filtrów IP (IP Filters), które znajdują się w zakładce Security.

- **Custom IP Filters**

Strona Custom IP Filters umożliwia utworzenie 15 spersonalizowanych reguł filtrowania IP, aby zablokować działanie określonych usług lub aplikacji,

LAN Isolation (Odosobnienie sieci LAN)

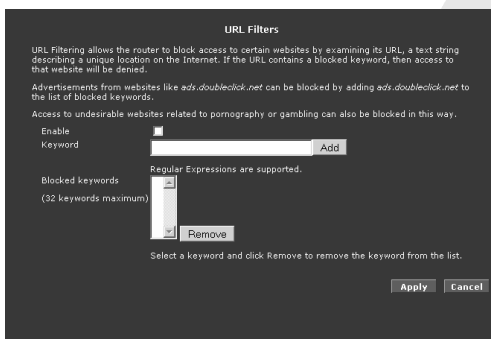
Odosobnienie sieci LAN umożliwia wyłączenie możliwości komunikacji pomiędzy dwoma grupami LAN. Umożliwia to na zabezpieczenie informacji w wydzielonej części sieci LAN od jej segmentów dostępnych publicznie.



Zaznacz odpowiednie pole, aby zablokować ruch między dwoma grupami LAN.

URL Filters (Filtrowanie URL)

Filtrowanie URL pozwala na blokowanie dostępu do stron na podstawie ich adresu URL. Jeśli URL zawiera zablokowane słowo kluczowe, dostęp do tej strony zostaje zablokowany.



URL Filters

URL Filtering allows the router to block access to certain websites by examining its URL, a text string describing a unique location on the Internet. If the URL contains a blocked keyword, then access to that website will be denied.

Advertisements from websites like *ads.doubleclick.net* can be blocked by adding *ads.doubleclick.net* to the list of blocked keywords.

Access to undesirable websites related to pornography or gambling can also be blocked in this way.

Enable

Keyword

Blocked keywords
(32 keywords maximum)

Regular Expressions are supported.

Select a keyword and click Remove to remove the keyword from the list.

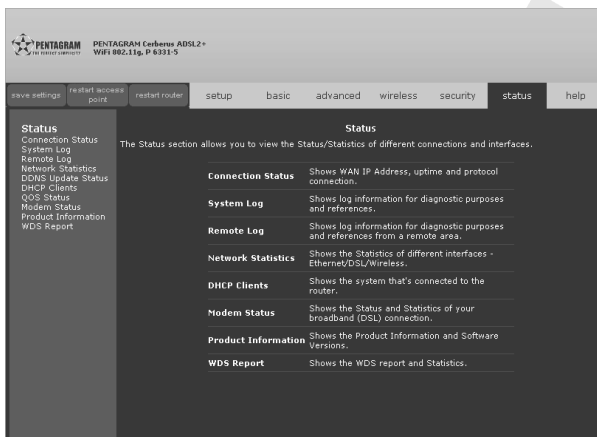
Enable – Zaznacz to pole, aby włączyć filtrowanie URL.

Keyword – Wpisz w to pole słowo kluczowe i kliknij **Add**, aby dodać je do listy.

Blocked keywords – Lista zablokowanych słów kluczowych. Zaznacz słowo kluczowe i kliknij **Remove**, aby usunąć je z listy.

Zakładka Status

Zakładka Status udostępnia informacje o stanie różnych połączeń i interfejsów.



Connection Status (Stan połączenia)

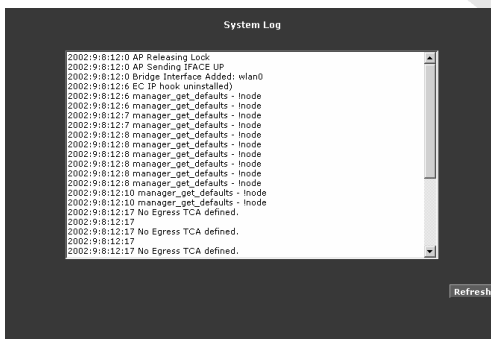
Na stronie Connection Status wyświetlany jest typ protokołu, adres IP po stronie WAN, stan połączenia i długość jego trwania.

Connection Status (1)						
Resolution	Tune	IP	State	Online	Disconnect Reason	
quickstart	pppoe	N/A	Not Connected	0	DSL line is Disconnected	

[Refresh](#)

System Log (Dziennik systemowy)

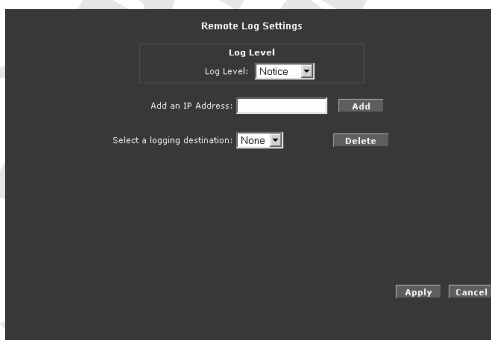
Strona System Log pokazuje dziennik systemowy routera. W zależności od poziomu ważności, dziennik może tworzyć raporty, które będą wysyłane do zdalnego hosta (jeśli włączona jest funkcja Remote Logging).



Remote Log (Dziennik zdalny)

Dziennik zdalny umożliwia przekazywanie wszystkich logowanych informacji do jednego (lub więcej) zdalnego komputera. Typ informacji przekazywanych do zdalnego komputera zależy od poziomu ważności informacji. Każda wiadomość dziennika ma przypisany poziom ważności, który określa drastyczność wydarzenia.

Podczas konfigurowania zdalnego dziennika należy określić poziom ważności. Wiadomości dziennika na poziomie równym lub wyższym wybranemu zostaną wysłane do serwera logowania i mogą zostać podejrzane za pomocą odpowiedniej aplikacji, którą można ściągnąć z sieci.



Aby włączyć zdalny dziennik:

- Wybierz poziom ważności z listy **Log Level**. Poniżej opisane jest wszystkie 8 poziomów ważności (w kolejności od najwyższego).
 - Panic** – Błąd systemowy lub inne warunki powodujące, że router przestaje działać.
 - Alert** – Sytuacja alarmowa wymagająca natychmiastowej interwencji, np. zepsuta systemowa baza danych.
 - Critical** – Sytuacja krytyczna, np. błąd pamięci wewnętrznej.
 - Error** – Błędy mniej poważne niż w poziomach Panic, Alert i Critical.

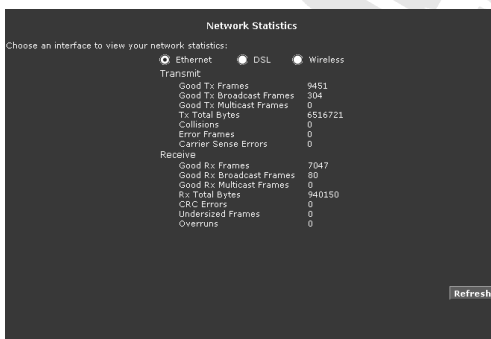
- **Warning** – Sytuacje wymagające obserwacji.
 - **Notice** (Domyślny) – Sytuacje nie będące błędami ale mogące wymagać dodatkowej uwagi.
 - **Info** – Wydarzenia nie będące błędami.
 - **Debug** – Informacje debugowania. Wybierz ten poziom tylko na polecenie przedstawiciela pomocy technicznej.
2. W pole **Add an IP Address field** wpisz adres IP, na który będą wysyłane raporty i kliknij **Add**.
 3. Kliknij **Apply**. Adres IP pojawi się na liście **Select a logging destination**.

Aby wyłączyć dziennik zdalny wybierz z listy **Select a logging destination** adres IP, który ma zostać usunięty i kliknij **Delete**.

Network Statistics (Statystyki sieci)

Statystyki poszczególnych sieci znajdują się w poszczególnych kategoriach tej strony.

• Network Statistics – Ethernet



Network Statistics

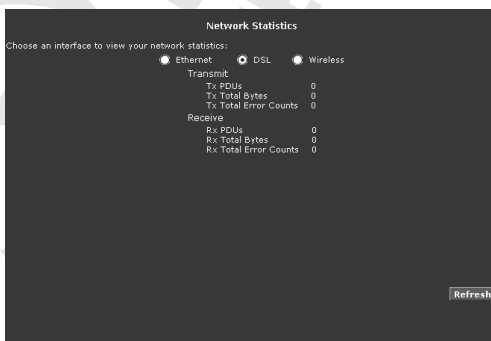
Choose an interface to view your network statistics:

Ethernet DSL Wireless

Transmit	
Good Tx Frames	9451
Good Tx Broadcast Frames	304
Good Tx Multicast Frames	0
Tx Total Bytes	6516721
Collisions	0
Error Frames	0
Carrier Sense Errors	0
Receive	
Good Rx Frames	7047
Good Rx Broadcast Frames	80
Good Rx Multicast Frames	0
Rx Total Bytes	940150
CRC Errors	0
Undersized Frames	0
Overruns	0

Refresh

• Network Statistics – DSL



Network Statistics

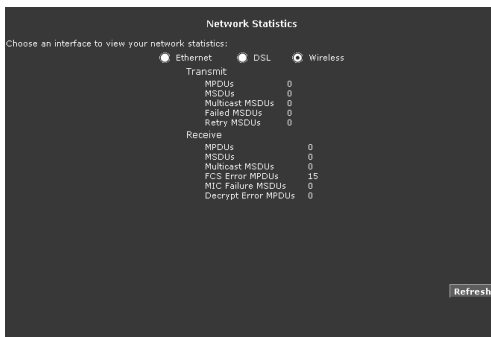
Choose an interface to view your network statistics:

Ethernet DSL Wireless

Transmit	
Tx PDUs	0
Tx Total Bytes	0
Tx Total Error Counts	0
Receive	
Rx PDUs	0
Rx Total Bytes	0
Rx Total Error Counts	0

Refresh

- **Network Statistics – Wireless**



DDNS Update Status (Aktualizacja stanu DDNS)

Strona DDNS Update Status wyświetla stan usługi DDNS dla połączenia WAN. Domyślnie funkcja DDNS jest wyłączona. Po włączeniu usługi DDNS klient aktualizuje się za każdym razem gdy router otrzymuje od usługodawcy nowy adres IP.



DHCP Clients (Klienci DHCP)

Strona DHCP Clients wyświetla adresy MAC, adresy IP, nazwy hosta i czas dzierżawy.

MAC Address	IP Address	Host Name	Lease Time
00:80:8d:f3:72:87	192.168.1.2	samothnia	0 days 0:33:47

QoS Status (Stan QoS)

Ta strona wyświetla statystyki QoS i pakietów.

```

QoS STATUS

QoS Framework : Enabled
Scheduling Algorithm : Strict Round-Robin

NQM Received Statistics      NQM Dropped Statistics
Cos1 Pkts received : 0      Cos1 Pkts received : 0
Cos2 Pkts received : 0      Cos2 Pkts received : 0
Cos3 Pkts received : 0      Cos3 Pkts received : 0
Cos4 Pkts received : 0      Cos4 Pkts received : 0
Cos5 Pkts received : 0      Cos5 Pkts received : 0
Cos6 Pkts received : 15031  Cos6 Pkts received : 0

NQM Congestion Control      Translation Statistics
Cos1 Queue : Empty          Pkts Remarkd : 93
Cos2 Queue : Empty          Pkts Unchanged : 0
Cos3 Queue : Empty          Non-Ip Pkts Marked : 5
Cos4 Queue : Empty          Unclassified Ip Pkts Marked : 13
Cos5 Queue : Empty          Unclassified Non-Ip Pkts Marked : 3
Cos6 Queue : Empty          Unclassified Layer2 Pkts : 0
Congestion State : Not Congested

Classification Statistics
Classification Errors : 0
Unclassified Packets : 0 Fragmented Packets = 0

```

Modem Status (Stan modemu)

Na tej stronie wyświetlone są statystyki dotyczące wbudowanego modemu ADSL.

Modem Status	
Modem Status	
Connection Status	Disconnected
Us Rate (kbits)	0
Ds Rate (kbits)	0
US Margin	0
DS Margin	0
Trained Modulation	NO_MODE
LOS Errors	0
DS Line Attenuation	0
US Line Attenuation	0
Peak Cell Rate	0 calls per sec
CRC Rx Fast	0
CRC Tx Fast	0
CRC Rx Interleaved	0
CRC Tx Interleaved	0
Path Mode	Fast Path
DSL Statistics	
Near End F4 Loop Back Count	0
Near End F5 Loop Back Count	0

[Refresh](#)

Product Information (Informacje o produkcie)

Na tej stronie znaleźć można wszystkie informacje dotyczące routera i jego oprogramowania.

Product Information	
Product Information	
Model Number	ADSL2+ Wireless G Router
Ethernet MAC	00:30:0A:68:C6:4D
DSL MAC	00:30:0A:68:C6:4D
AP MAC	00:12:06:53:48:a6
Software Versions	
Gateway	3.7.0
Firmware	120.110.1
ATM Driver	7.01.00.10
DSL HAL	7.01.00.08
DSL Softapump	7.01.00.00 Annex A
SAR HAL	01.07.20
PDSP Firmware	0.54
Wireless Firmware	3.4.0.41
Wireless APDK	6.4.4.27
Boot Loader	1.4.0.4

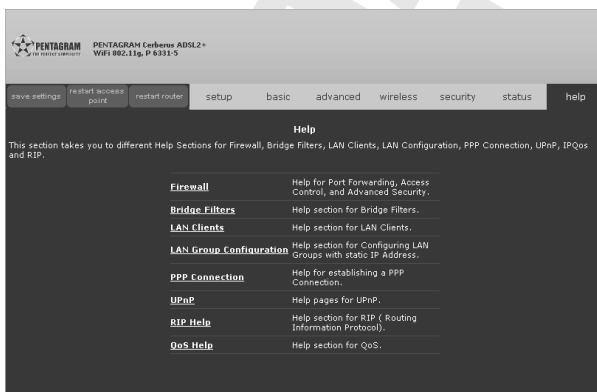
WDS Report (Raport WDS)

Ta strona wyświetla informacje dotyczące WDS w sieci bezprzewodowej: konfiguracja WDS, stan WDS, statystyki zarządzania WDS, baza danych WDS.



Zakładka Help

Zakładka Help umożliwi wyświetlenie pomocy dotyczącej poszczególnych funkcji routera.



Rozwiązywanie problemów

Jeśli router nie pracuje poprawnie, przed skontaktowaniem się z pomocą techniczną serwisu lub usługodawcy zapoznaj się z informacjami zawartymi w tym rozdziale.

Użycie diod LED do zdiagnozowania problemu

Diody LED mogą być pomocne przy odnalezieniu prawdopodobnej przyczyny problemu.

Dioda zasilania POWER

Jeśli dioda POWER na przednim panelu nie świeci się:

1. upewnij się, że zasilacz jest podłączony do routera i odpowiedniego źródła zasilania. Używaj tylko dołączonego zasilacza;
2. upewnij się, że zarówno router jak i źródło zasilania są włączone i router jest odpowiednio zasilany;
3. wyłącz i włącz router;
4. jeśli powyższe kroki nie rozwiązały problemu skontaktuj się z dostawcą sprzętu.

Dioda połączenia ETHERNETx

Jeśli dioda ETHERNETx na przednim panelu nie świeci się:

1. sprawdź połączenie kabla łączącego router z komputerem lub koncentratorem;
2. sprawdź czy użyty kabel nie jest uszkodzony;
3. upewnij się, że karta sieciowa zainstalowana w komputerze działa poprawnie;
4. jeśli powyższe kroki nie rozwiązały problemu skontaktuj się z dostawcą sprzętu.

Dioda połączenia ADSL

Jeśli dioda ADSL na przednim panelu nie świeci się:

1. sprawdź kabel telefoniczny i jego podłączenie do portu routera i gniazdka telefonicznego;
2. upewnij się, że usługodawca uruchomił usługę ADSL dla twojej linii telefonicznej;
3. zresetuj swoją linię ADSL aby ponownie ustanowić połączenie z DSLAM;
4. jeśli powyższe kroki nie rozwiązały problemu skontaktuj się z dostawcą sprzętu.

Problem z konfiguracją przez przeglądarkę

Jeśli nie można uzyskać dostępu do strony konfiguracyjnej:

1. upewnij się, że używasz poprawnego adresu IP routera i sprawdź ten adres;
2. upewnij się, że nie jest uruchomiona żadna sesja konsoli;
3. sprawdź czy włączony jest dostęp do routera przez przeglądarkę. Jeśli dostęp do strony konfiguracyjnej routera jest ograniczony do ustalonych adresów IP upewnij się, że twój komputer jest na liście adresów IP posiadających uprawnienia dostępowe;
4. przy dostępie ze strony WAN zdalny dostęp do routera musi być skonfigurowany w sposób umożliwiający dostęp do strony konfiguracyjnej od strony WAN;
5. przy dostępie z sieci LAN zarówno komputer jak i router muszą się znajdować w tej samej podsieci;

6. jeśli adres IP routera został zmieniony należy w pasku adresowym przeglądarki wpisać nowy adres;
7. usuń wszystkie filtry blokujące dostęp do usług www dla sieci LAN i WAN.

Jeśli strona konfiguracyjna nie jest wyświetlana poprawnie:

1. upewnij się, że używasz przeglądarki Internet Explorer 5.0 lub nowszej / kompatybilnej;
2. usuń wszystkie tymczasowe pliki internetowe w swojej przeglądarce.

Problemy z logowaniem

Jeśli zapomniałeś nazwy użytkownika i/lub hasła:

1. domyślna nazwa użytkownika i hasło to **admin** – wielkość liter ma znaczenie;
2. naciśnij i przytrzymaj przez ok. 10 sekund przycisk **RESET** znajdujący się w tylnej części obudowy routera – WSZYSTKIE ustawienia routera zostaną przywrócone do wartości fabrycznych;

Problemy z komunikacją z siecią LAN

Jeśli nie możesz połączyć się z routerem z sieci LAN ani nie widzisz komputerów w tej sieci:

1. sprawdź diody ETHERNETx na przednim panelu routera. Każde połączenie do portu LAN routera powinno spowodować zaświecenie się odpowiadającej portowi diody na przednim panelu. Jeśli po podłączeniu komputera dioda nie zaświeciła się sprawdź kabel, jego podłączenie do routera i komputera i wyłącz na czas sprawdzania połączenia oprogramowanie firewall;
2. upewnij się, że router i komputer(y) znajdują się w tej samej podsieci.

Problemy z komunikacją z siecią WAN

Jeśli nawiązanie połączenia ADSL się nie powiodło:

1. sprawdź połączenie kabla telefonicznego do routera i gniazdka telefonicznego. Dioda ADSL na przednim panelu powinna być zapalona;
2. upewnij się, że wartości VPI, VCI, enkapsulacji i multipleksingu są takie same jak otrzymane od twojego usługodawcy;
3. zrestartuj router i w razie dalszych problemów z nawiązaniem połączenia skontaktuj się z usługodawcą w celu weryfikacji otrzymanych od niego wartości VPI, VCI, enkapsulacji i multipleksingu (nazewnictwo może się różnić w zależności od usługodawcy).

Jeśli router nie otrzymuje od usługodawcy adresu IP:

1. upewnij się, że wszystkie urządzenia podłączone do tej samej linii telefonicznej co router są połączone do gniazdka przez filtr (chyba, że posiadasz ogólny rozdzielacz lub filtr zainstalowany przez wykwalifikowanego elektryka) i upewnij się, że wszystkie filtry są prawidłowo zainstalowane;
2. brak lub niepoprawna instalacja filtrów na linii może powodować problemy z połączeniem ADSL lub częste zrywanie tego połączenia.

Jeśli połączenie ADSL często traci synchronizację (rozłączenia):

1. adres IP jest przydzielony po dokonaniu autoryzacji użytkownika. Autoryzacja może być dokonana na podstawie nazwy użytkownika i hasła, adresu MAC lub nazwy hosta. Wszystkie potrzebne do autoryzacji informacje powinieneś otrzymać od usługodawcy;
2. nazwa użytkownika i hasło są wymagane tylko dla połączeń PPPoE i PPPoA. Upewnij się, że wpisałeś poprawną nazwę użytkownika i hasło (wielkość liter ma znaczenie).

Problemy z połączeniem do sieci Internet

Jeśli nie możesz się połączyć z Internetem:

1. upewnij się, że router jest włączony i połączony z siecią;
2. jeśli dioda ADSL się nie świeci przejdź do części **Dioda połączenia ADSL** w tym rozdziale;
3. sprawdź ustawienia WAN;
4. upewnij się, że wpisane nazwa użytkownika i hasło są prawidłowe;
5. w przypadku korzystania z sieci bezprzewodowej upewnij się, że router i komputer korzystają z tej samej sieci – identyczny identyfikator ESSID, kanał i klucze WEP (przy włączonym szyfrowaniu WEP).

Jeśli połączenie jest zrywane:

1. dla połączeń PPPoA lub PPPoE sprawdź czas bezczynności, po którym router będzie się rozłączał (opcja **Idle Timeout** w oknie konfiguracji połączenia);
2. skontaktuj się ze swoim usługodawcą.

W przypadku wystąpienia problemów nie wymienionych w tym rozdziale sprawdź porady znajdujące się na stronie www.pentagram.pl a następnie skontaktuj się z autoryzowanym serwisem firmy PENTAGRAM.

