

Dynamode

MODEM ADSL

**Instrukcja obsługi
dla użytkowników zaawansowanych**

R-ADSL-C4-2

SPIS TREŚCI

1.	Konfiguracja WAN	3
	PPP przez sieć ATM (PPPoA)	3
	PPP przez sieć Ethernet (PPPoE)	5
	Routing z tunelowaniem MAC (MER)	8
	IP przez sieć ATM (IPoA)	10
	Bridging (mostkowanie).....	12
2.	Serwer DHCP	14
	Pula adresów serwera DHCP	14
	Uruchamianie trybu Serwera DHCP	14
	Uruchamianie trybu przekaźnika DHCP	15
3.	Przekaźnik DNS	15
4.	Dynamiczny DNS.....	16
5.	NAT.....	17
	Wirtualne serwery.....	18
	Wyzwalanie portów.....	19
	DMZ Host.....	20
6.	Zabezpieczenia	
	Filtrowanie adresów IP.....	21
	Konfiguracja Filtrowania wychodzących IP	21
	Konfiguracja Filtrowania przychodzących IP	22
	Filtrowanie adresów MAC	23
	Kontrola rodzicielska.....	24
7.	Routing	
	Bramka domyślna.....	25
	Trasowanie statyczne.....	26
	Protokół RIP.....	27
8.	Diagnostyka.....	29
9.	Kopia zapasowa i odzyskiwanie ustawień.....	29
	Kopia zapasowa	30
	Uaktualnianie.....	30
	Odzyskiwanie ustawień domyślnych.....	30
10.	Agent SNMP	31
11.	Kontrola dostępu.....	32
	Usługi.....	32
	Adresy IP	32
	Hasła.....	32
12.	Czas internetowy.....	33
13.	Uaktualnianie oprogramowania.....	34
	Tryb HTTP.....	34
	Tryb TFTP	34
14.	Mapowanie portów	35

Konfiguracja WAN

Interfejsy urządzenia po stronie portu WAN wykorzystywane są do komunikacji przez port DSL. Interfejs WAN składa się z dwóch warstw: interfejs niższego poziomu ATM VC i interfejs protokolarny wyższego poziomu:

- Interfejs ATM VC umożliwia komunikację przy użyciu protokołu Asynchronous Transfer Mode (Tryb Transferu Asynchronicznego). Protokół ATM dostarcza format transmisji danych powszechny wśród różnych systemów sprzętowych, stanowiących podstawę Internetu. Właściwości obwodu wirtualnego (VC) interfejsu ATM VC identyfikują unikalną ścieżkę, której twój router ADSL używa do komunikacji w sieci opartej na ATM i urządzeniach centrali firmy telefonicznej.
- Interfejs (y) protokolarny(e) wyższego poziomu pracuje „ponad” interfejsem ATM VC. Interfejs wyższego poziomu obsługuje protokoły wymagane do zalogowania i wymiany danych z serwerami dostępu Usługodawcy Internetowego (ISP). ISP może używać kilku różnych protokołów, włączając protokół Point-to-Point Protocol (PPPoE lub PPPoA), Routing z tunelowaniem MAC (MER), lub IP przez sieć ATM (IPoA). Upewnij się, aby stworzyć odpowiedni typ interfejsu WAN, którego wymaga twój Usługodawca.

Po przypisaniu odpowiedniej wartości ATM VC, wymaganej dla modemu przez twojego ISP, możesz skonfigurować jeden z interfejsów WAN wyższego poziomu, aby umożliwić komunikację z Usługodawcą Internetowym.


Poniżej przedstawiono sposoby konfiguracji modemu, jeden po drugim, umożliwiające pracę z różnego typu połączeniami:

- **PPP przez sieć ATM (PPPoA)**

Skrót PPPoA oznacza Point to Point Protocol over ATM Adaptation Layer 5 (AAL5). Połączenie to zapewnia kontrolę dostępu i funkcję billingowania podobną do stosowanej w usługach dial-up opartych na protokole PPP. Modem enkapsuluje sesję PPP bazującą na RFC1483 i przesyła ją przez ATM PVC (Stały Obwód Wirtualny) do koncentratora cyfrowych linii abonenckich DSLAM (digital subscriber line access multiplexer) Usługodawcy Internetowego. Więcej informacji na temat PPPoA można uzyskać w RFC 2364, na tomista na temat samego protokołu PPP w RFC 1661.

W tym trybie funkcja NAT jest domyślnie włączona i nie może zostać wyłączona.

Aby dodać PVC w PPPoA należy postępować wg poniższych instrukcji:

1. Jeśli strona konfiguracji sieci WAN nie jest aktualnie wyświetlana kliknij Advanced Setup (Konfiguracja zaawansowana), a następnie kliknij przycisk **WAN** w menu.
2. Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona konfiguracji ATM PVC.
3. W polach VPI i VCI wstaw wartości VPI/VCI

Upewnij się, że używasz prawidłowych wartości Identyfikatora Ścieżki Wirtualnej (VPI) i Identyfikatora Kanału Wirtualnego (VCI), które zostały tobie przypisane. Zakres dozwolony dla VPI to 0 do 255, a dla VCI to 0 do 65535.


Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona Typu Połączenia.

4. Wybierz opcję PPP over ATM (PPPoA) aby wybrać połączenie typu PPPoA.

Z listy wyboru Trybów Enkapsulacji wybierz tryb jakiego wymaga twój ISP. Poniżej opisano cechy charakterystyczne każdego z nich:

LLC/SNAP-BRIDGING: W tym przypadku VC przenosi wiele protokołów z protokołem identyfikującym informacje zawarte w nagłówku każdego pakietu. Pomimo poszerzonego pasma i dodatkowego czasu potrzebnego na przygotowanie do wykonania operacji, metoda ta może być korzystna, jeśli nie jest stosowana praktyka posiadania osobnego VC dla każdego przenoszonych protokołu, np. w przypadku dużego zapotrzebowania na równoczesne VC.

VC/MUX: W tym przypadku, na podstawie wcześniejszego wzajemnego porozumienia, każdy protokół zostaje przypisany do określonego Obwodu Wirtualnego; np. VC1 przenosi adres IP, itd. Multipleksowanie oparte na Obwodach Wirtualnych może stać się dominujące w środowisku, w którym dynamiczne tworzenie dużej liczby Wirtualnych Obwodów ATM jest szybkie i ekonomiczne.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona z Nazwą Użytkownika i Hasłem PPP.

5. Wstaw Nazwę Użytkownika/Hasło otrzymane od ISP.

Z listy wyboru Metod Uwierzytelniania, wybierz typ zabezpieczenia PPP jakie ma być użyte w tym połączeniu. Domyślnie Metoda Uwierzytelniania ustawiona jest na AUTO. Zaleca się pozostawienie opcji AUTO dla Metody Uwierzytelniania, jednak w razie konieczności możesz wybrać PAP, CHAP lub MSCHAP.


Modem można skonfigurować w ten sposób, aby w przypadku braku aktywności przez określony czas zakończył połączenie, poprzez zaznaczenie opcji Dial on Demand (Połącz na żądanie) i wpisanie odpowiedniej wartości w oknie czas bezczynności. Wartość ta powinna zawierać się w zakresie 1 do 4320 minut. Opcja ta oznacza, iż połączenie zostaje nawiązane jedynie w przypadku otrzymania danych, a następnie, po określonym czasie, zostaje zakończone.

Rozszerzenie IP protokołu PPP jest specjalną funkcją, używaną przez niektórych Usługodawców. Funkcję tą należy aktywować jedynie w przypadku, gdy Usługodawca tego wymaga. Rozszerzenie IP protokołu PPP wspiera następujące warunki:

- Zezwala na to, aby w sieci LAN znajdował się tylko jeden komputer PC.

- Publiczny adres IP, przypisany zdalnie przy użyciu protokołu PPP/IPCP nie jest używany w interfejsie WAN protokołu PPP. Zamiast tego jest przesyłany do interfejsu LAN komputera PC za pośrednictwem DHCP. Tylko jeden PC w sieci LAN może zostać podłączony zdalnie, ponieważ serwer DHCP w ramach bramki ADSL może przypisać tylko jeden adres IP urządzeniu LAN.
- NAPT i firewall są wyłączone w przypadku wyboru tej opcji.
- Bramka ADSL staje się bramką domyślną i serwerem DNS dla komputera PC poprzez serwer DHCP, używając adresu IP interfejsu LAN.
- Bramka ADSL rozszerza podsieć adresów IP zdalnego usługodawcy na komputer z sieci LAN. Oznacza to, że komputer PC staje się hostem, należącym do tej samej podsieci adresów IP.

Bramka ADSL mostkuje pakiety IP pomiędzy portami WAN i LAN, chyba że pakiet jest adresowany na LAN-owy adres IP bramki.


Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona Enable IGMP Multicast (Włącz Multicast protokołu IGMP) i WAN Service (Obsługa WAN).



6. Na stronie znaleźć można poniższe pola wyboru i pola tekstowe:

Enable IGMP Multicast (Uruchom Multicast IGMP): Funkcja ta może być używana, aby zezwolić interfejsowi WAN na przesyłanie dalej wiadomości protokołu IGMP (Internet Group Management Protocol), które otrzymuje dla komputerów PC znajdujących się w sieci LAN.

Enable WAN Service (Uruchom obsługę WAN): Funkcja ta może być używana, aby aktywować to połączenie.

Service Name (Nazwa usługi): Nazwa używana do identyfikacji tego połączenia.

Po zakończeniu konfiguracji tego pola kliknij przycisk  na wyświetlanej stronie, pojawi się strona WAN Setup – Summary (Konfiguracja sieci WAN – Podsumowanie).

7. Na wyświetlanej stronie możesz kliknąć przycisk  w celu zachowania ustawień, lub  w celu wykonania dowolnych modyfikacji.

UWAGA: Aby aktywować ten interfejs WAN i dalej konfigurować w nim usługi musisz zrestartować system.

- **PPP przez Ethernet (PPPoE)**

Modem wspiera protokół PPPoE (Point-to-Point Protocol over Ethernet). PPPoE jest projektem standardu stowarzyszenia IETF (RFC 2516), opisującym w jaki sposób komputer PC

współpracuje z połączeniem nawiązywanym za pomocą modemu szerokopasmowego (DSL, kablowy, bezprzewodowy itd.). Opcja PPPoE ma zastosowanie dla połączeń dial-up używających protokołu PPPoE.

Dla usługodawców PPPoE oferuje metodę dostępu i uwierzytelniania, które działają z istniejącymi systemami kontroli dostępu (np. Radius). PPPoE oferuje metodę logowania i uwierzytelniania, która może być aktywowana przez oprogramowanie Dial-Up Networking firmy Microsoft, dzięki czemu użytkownicy systemu Windows nie muszą uczyć się stosowania nowych procedur.


Jedną z zalet PPPoE jest funkcja znana jako dynamiczny dobór usług, czyli możliwość udzielania dostępu do wielu usług sieciowych. Daje to usługodawcy możliwość łatwego tworzenia i oferowania nowych usług IP dla odbiorców indywidualnych.

Od strony eksploatacyjnej, PPPoE oszczędza wiele wysiłku zarówno ze strony twojej jak i Usługodawcy Internetowego (ISP), ponieważ nie wymaga żadnej specyficznej konfiguracji modemu szerokopasmowego po stronie klienta.

Dzięki zaimplementowaniu PPPoE bezpośrednio w modemie (rzadziej w pojedynczych komputerach), komputery w sieci LAN nie potrzebują żadnego PPPoE, ponieważ modem przejmuje część zadań. Ponadto dzięki funkcji NAT wszystkie komputery w sieci LAN będą miały dostęp.

W tym trybie funkcja NAT jest domyślnie włączona i nie może zostać wyłączona.

Aby dodać PVC w PPPoE należy postępować wg poniższych instrukcji:

1. Jeśli strona konfiguracji sieci WAN nie jest aktualnie wyświetlana kliknij Advanced Setup (Konfiguracja zaawansowana), a następnie kliknij przycisk **WAN** w menu.
2. Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona konfiguracji ATM PVC.
3. W polach VPI i VCI wstaw wartości VPI/VCI

Upewnij się, że używasz prawidłowych wartości Identyfikatora Ścieżki Wirtualnej (VPI) i Identyfikatora Kanału Wirtualnego (VCI), które zostały tobie przypisane. Zakres dozwolony dla VPI to 0 do 255, a dla VCI to 0 do 65535.

Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona Typu Połączenia.


4. Wybierz opcję PPP over ATM (PPPoE) aby wybrać połączenie typu PPPoE.

Z listy wyboru Trybów Enkapsulacji wybierz tryb jakiego wymaga twój ISP. Poniżej opisano cechy charakterystyczne każdego z nich:

LLC/SNAP-BRIDGING: W tym przypadku VC przenosi wiele protokołów z protokołem

identyfikującym informacje zawarte w nagłówku każdego pakietu. Pomimo poszerzonego pasma i dodatkowego czasu potrzebnego na przygotowanie do wykonania operacji, metoda ta może być korzystna, jeśli nie jest stosowana praktyka posiadania osobnego VC dla każdego przenoszonego protokołu, np. w przypadku dużego zapotrzebowania na równoczesne VC.

VC/MUX: W tym przypadku, na podstawie wcześniejszego wzajemnego porozumienia, każdy protokół zostaje przypisany do określonego Obwodu Wirtualnego; np. VC1 przenosi adres IP, itd. Multipleksowanie oparte na Obwodach Wirtualnych może stać się dominujące w środowisku, w którym dynamiczne tworzenie dużej liczby Wirtualnych Obwodów ATM jest szybkie i ekonomiczne.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona z Nazwą Użytkownika i Hasłem PPP.

5. Wstaw Nazwę Użytkownika/Hasło otrzymane od ISP.


Z listy wyboru Metod Uwierzytelniania, wybierz typ zabezpieczenia PPP jakie ma być użyte w tym połączeniu. Domyślnie Metoda Uwierzytelniania ustawiona jest na AUTO. Zaleca się pozostawienie opcji AUTO dla Metody Uwierzytelniania, jednak w razie konieczności możesz wybrać PAP, CHAP lub MSCHAP.

Modem można skonfigurować w ten sposób, aby w przypadku braku aktywności przez określony czas zakończył połączenie, poprzez zaznaczenie opcji Dial on Demand (Połącz na żądanie) i wpisanie odpowiedniej wartości w oknie czas bezczynności. Wartość ta powinna zawierać się w zakresie 1 do 4320 minut. Opcja ta oznacza, iż połączenie zostaje nawiązane jedynie w przypadku otrzymania danych, a następnie, po określonym czasie, zostaje zakończone.

Rozszerzenie IP protokołu PPP IP jest specjalną funkcją, używaną przez niektórych Usługodawców. Funkcję tą należy aktywować jedynie w przypadku, gdy Usługodawca tego wymaga. Rozszerzenie IP protokołu PPP wspiera następujące warunki:

- Zezwala na to, aby w sieci LAN znajdował się tylko jeden komputer PC.
- Publiczny adres IP, przypisany zdalnie przy użyciu protokołu PPP/IPCP nie jest używany w interfejsie WAN protokołu PPP. Zamiast tego jest przesyłany do interfejsu LAN komputera PC za pośrednictwem DHCP. Tylko jeden PC w sieci LAN może zostać podłączony zdalnie, ponieważ serwer DHCP w ramach bramki ADSL może przypisać tylko jeden adres IP urządzeniu LAN.
- NAPT i firewall są wyłączone w przypadku wyboru tej opcji.
- Bramka ADSL staje się bramką domyślną i serwerem DNS dla komputera PC poprzez serwer DHCP, używając adresu IP interfejsu LAN.
- Bramka ADSL rozszerza podsieć adresów IP zdalnego usługodawcy na komputer z sieci LAN. Oznacza to, że komputer PC staje się hostem, należącym do tej samej podsieci adresów IP.

- Bramka ADSL mostkuje pakiety IP pomiędzy portami WAN i LAN, chyba że pakiet jest adresowany na LAN-owy adres IP bramki.


Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona Enable IGMP Multicast (Włącz Multicast protokołu IGMP) i WAN Service (Obsługa WAN).



6. Na stronie znaleźć można poniższe pola wyboru i pola tekstowe:

Enable IGMP Multicast (Uruchom Multicast IGMP): Funkcja ta może być używana, aby zezwolić interfejsowi WAN na przesyłanie dalej wiadomości protokołu IGMP (Internet Group Management Protocol), które otrzymuje dla komputerów PC znajdujących się w sieci LAN.

Enable WAN Service (Uruchom obsługę WAN): Funkcja ta może być używana, aby aktywować to połączenie.

Service Name (Nazwa usługi): Nazwa używana do identyfikacji tego połączenia.

Po zakończeniu konfiguracji tego pola kliknij przycisk  na wyświetlanej stronie, pojawi się strona WAN Setup – Summary (Konfiguracja sieci WAN – Podsumowanie).


7. Na wyświetlanej stronie możesz kliknąć przycisk  w celu zachowania ustawień, lub  w celu wykonania dowolnych modyfikacji.

UWAGA: Aby aktywować ten interfejs WAN i dalej konfigurować w nim usługi musisz zrestartować system.

- **Routing z tunelowaniem MAC (MER)**

Routing z tunelowaniem MAC (MER) jest implementowany tylko w sieciowym protokole IP. Pakiety IP są routowane między interfejsem Ethernet i WAN, a następnie formatowane w taki sposób, aby były zrozumiałe dla środowiska mostkowanego. Np. enkapsuluje routowane ramki Ethernet na mostkowane komórki ATM. MER wymaga określenia adresu IP bramki. Informację tą możesz uzyskać od swojego Usługodawcy Internetowego.

Aby dodać PVC w MER należy postępować wg poniższych instrukcji:

1. Jeśli strona konfiguracji sieci WAN nie jest aktualnie wyświetlana kliknij Advanced Setup (Konfiguracja zaawansowana), a następnie kliknij przycisk **WAN** w menu.
2. Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona konfiguracji ATM PVC.
3. W polach VPI i VCI wstaw wartości VPI/VCI

Upewnij się, że używasz prawidłowych wartości Identyfikatora Ścieżki Wirtualnej (VPI) i Identyfikatora Kanału Wirtualnego (VCI), które zostały tobie przypisane. Zakres dozwolony dla VPI to 0 do 255, a dla VCI to 0 do 65535.


Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona Typu Połączenia.

4. Zaznacz opcję MAC Encapsulation Routing (MER) aby wybrać typ połączenia MER

Z listy wyboru Trybów Enkapsulacji wybierz tryb jakiego wymaga twój ISP. Poniżej opisano cechy charakterystyczne każdego z nich:

LLC/SNAP-BRIDGING: W tym przypadku VC przenosi wiele protokołów z protokołem identyfikującym informacje zawarte w nagłówku każdego pakietu. Pomimo poszerzonego pasma i dodatkowego czasu potrzebnego na przygotowanie do wykonania operacji, metoda ta może być korzystna, jeśli nie jest stosowana praktyka posiadania osobnego VC dla każdego przenoszonego protokołu, np. w przypadku dużego zapotrzebowania na równoczesne VC.

VC/MUX: W tym przypadku, na podstawie wcześniejszego wzajemnego porozumienia, każdy protokół zostaje przypisany do określonego Obwodu Wirtualnego; np. VC1 przenosi adres IP, itd. Multipleksowanie oparte na Obwodach Wirtualnych może stać się dominujące w środowisku, w którym dynamiczne tworzenie dużej liczby Wirtualnych Obwodów ATM jest szybkie i ekonomiczne.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona Konfiguracji adresu IP sieci WAN.

5. Na tej stronie należy skonfigurować adres IP sieci WAN/maskę podsieci, bramkę domyślną i informacje dotyczące serwera DNS.


Możesz skonfigurować modem tak, aby pobierał adres IP/maskę podsieci automatycznie od ISP przez wybór opcji Obtain an IP address automatically (Uzyskaj adres IP automatycznie), lub wybrać opcję Use the following IP address (Użyj następującego adresu IP) i wstawić adres IP sieci WAN/maskę podsieci ręcznie.

Bramka domyślna może zostać przydzielona automatycznie przez twój ISP, skonfigurowana ręcznie przez podanie stałego adresu IP lub wybrana z listy wyboru Use WAN Interface (Użyj interfejsu WAN).

Tak jak bramka, adres serwera DNS może zostać przydzielony automatycznie przez twój ISP lub skonfigurowana ręcznie.

UWAGA: Funkcja DHCP może zostać włączona dla PVC w trybie MER jeśli zaznaczono opcję

"Obtain an IP address automatically" (Uzyskaj adres IP automatycznie). Zmiana adresu bramki domyślnej lub serwera DNS ma wpływ na cały system. Skonfigurowanie ich przez wstawienie wartości statycznych spowoduje wyłączenie opcji automatycznego przydzielania z DHCP lub innego połączenia WAN.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona konfiguracji Translacji Adresów Sieciowych NAT.

6. Na stronie znaleźć można poniższe pola wyboru i pola tekstowe:


Enable NAT (Uruchom NAT): Funkcja Translacji Adresów Sieciowych (NAT) umożliwia dzielenie jednego adresu IP sieci WAN przez wiele komputerów w twojej lokalnej sieci LAN.



Enable Firewall (Uruchom Firewall): Opcja ta umożliwia ustalenie stanu funkcji firewall w interfejsie IPoA. Zauważ, iż firewall w interfejsie PPPoE lub PPPoA jest zawsze włączony.

Enable IGMP Multicast (Uruchom Multicast IGMP): Funkcja ta może być używana, aby zezwolić interfejsowi WAN na przesyłanie dalej wiadomości protokołu IGMP (Internet Group Management Protocol), które otrzymuje dla komputerów PC znajdujących się w sieci LAN.

Enable WAN Service (Uruchom obsługę WAN): Funkcja ta może być używana, aby aktywować to połączenie.

Service Name (Nazwa usługi): Nazwa używana do identyfikacji tego połączenia.

Po zakończeniu konfiguracji tego pola kliknij przycisk  na wyświetlanej stronie, pojawi się strona WAN Setup – Summary (Konfiguracja sieci WAN – Podsumowanie).


7. Na wyświetlanej stronie możesz kliknąć przycisk  w celu zachowania ustawień, lub  w celu wykonania dowolnych modyfikacji.

UWAGA: Aby aktywować ten interfejs WAN i dalej konfigurować w nim usługi musisz zrestartować system.

- **IP przez ATM (IPoA)**

Interfejs IPoA może być używany do wymiany pakietów IP za pośrednictwem sieci ATM. Tego typu interfejs stosowany jest zazwyczaj w środowiskach rozwoju produktu, w celu wyeliminowania niepotrzebnych zmiennych podczas testowania procesów warstwy IP.

Aby dodać PVC w IPoA należy postępować wg poniższych instrukcji:

1. Jeśli strona konfiguracji sieci WAN nie jest aktualnie wyświetlana kliknij Advanced Setup (Konfiguracja zaawansowana), a następnie kliknij przycisk **WAN** w menu.
2. Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona konfiguracji ATM PVC.
3. W polach VPI i VCI wstaw wartości VPI/VCI

Upewnij się, że używasz prawidłowych wartości Identyfikatora Ścieżki Wirtualnej (VPI) i Identyfikatora Kanału Wirtualnego (VCI), które zostały tobie przypisane. Zakres dozwolony dla VPI to 0 do 255, a dla VCI to 0 do 65535.


Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona Typu Połączenia.

4. Zaznacz opcję IP over ATM (IpoA), aby wybrać typ połączenia IPoA

Z listy wyboru Trybów Enkapsulacji wybierz tryb jakiego wymaga twój ISP. Poniżej opisano cechy charakterystyczne każdego z nich:

LLC/SNAP-BRIDGING: W tym przypadku VC przenosi wiele protokołów z protokołem identyfikującym informacje zawarte w nagłówku każdego pakietu. Pomimo poszerzonego pasma i dodatkowego czasu potrzebnego na przygotowanie do wykonania operacji, metoda ta może być korzystna, jeśli nie jest stosowana praktyka posiadania osobnego VC dla każdego przenoszonego protokołu, np. w przypadku dużego zapotrzebowania na równoczesne VC.

VC/MUX: W tym przypadku, na podstawie wcześniejszego wzajemnego porozumienia, każdy protokół zostaje przypisany do określonego Obwodu Wirtualnego; np. VC1 przenosi adres IP, itd. Multipleksowanie oparte na Obwodach Wirtualnych może stać się dominujące w środowisku, w którym dynamiczne tworzenie dużej liczby Wirtualnych Obwodów ATM jest szybkie i ekonomiczne.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona Konfiguracji adresu IP sieci WAN.


5. Wstaw adres IP sieci WAN i Maskę Podsieci WAN otrzymane od ISP.

Możesz zmienić bramkę domyślną i informacje dotyczące serwera DNS w modemie.

Aby skonfigurować bramkę domyślną wybierz interfejs z listy wyboru Use WAN Interface (Użyj interfejsu sieci WAN) lub w polu Gateway IP address (Adres IP bramki), wpisz adres IP bramki, otrzymany od ISP. Następnie wstaw adresy IP podstawowego/zapasowego DNS, aby skonfigurować serwer DNS.

UWAGA: Funkcja DHCP w trybie IPoA nie jest wspierana. Zmiana adresu bramki domyślnej lub

serwera DNS ma wpływ na cały system. Skonfigurowanie ich przez wstawienie wartości statycznych spowoduje wyłączenie opcji automatycznego przydzielania z innego połączenia WAN.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie, pojawi się strona konfiguracji Translacji Adresów Sieciowych NAT.

6. Na stronie znaleźć można poniższe pola wyboru i pola tekstowe:


Enable NAT (Uruchom NAT): Funkcja Translacji Adresów Sieciowych (NAT) umożliwia dzielenie jednego adresu IP sieci WAN przez wiele komputerów w twojej lokalnej sieci LAN.

Enable Firewall (Uruchom Firewall): Opcja ta umożliwia ustalenie stanu funkcji firewall w interfejsie IPoA. Zauważ, iż firewall w interfejsie PPPoE lub PPPoA jest zawsze włączony.


Enable IGMP Multicast (Uruchom Multicast IGMP): Funkcja ta może być używana, aby zezwolić interfejsowi WAN na przesyłanie dalej wiadomości protokołu IGMP (Internet Group Management Protocol), które otrzymuje dla komputerów PC znajdujących się w sieci LAN.

Enable WAN Service (Uruchom obsługę WAN): Funkcja ta może być używana, aby aktywować to połączenie.

Service Name (Nazwa usługi): Nazwa używana do identyfikacji tego połączenia.

Po zakończeniu konfiguracji tego pola kliknij przycisk  na wyświetlanej stronie, pojawi się strona WAN Setup – Summary (Konfiguracja sieci WAN – Podsumowanie).


7. Na wyświetlanej stronie możesz kliknąć przycisk  w celu zachowania ustawień, lub

 w celu wykonania dowolnych modyfikacji.


UWAGA: Aby aktywować ten interfejs WAN i dalej konfigurować w nim usługi musisz zrestartować system.

- **Bridging (Mostkowanie)**

Aby dodać PVC w trybie Bridging należy postępować wg poniższych instrukcji:

1. Jeśli strona konfiguracji sieci WAN nie jest aktualnie wyświetlana kliknij Advanced Setup (Konfiguracja zaawansowana), a następnie kliknij przycisk **WAN** w menu.
2. Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona konfiguracji ATM PVC.
3. W polach VPI i VCI wstaw wartości VPI/VCI

Upewnij się, że używasz prawidłowych wartości Identyfikatora Ścieżki Wirtualnej (VPI) i Identyfikatora Kanału Wirtualnego (VCI), które zostały tobie przypisane. Zakres dozwolony dla VPI to 0 do 255, a dla VCI to 0 do 65535.

Po kliknięciu przycisku  na wyświetlanej stronie, pojawi się strona Typu Połączenia.


4. Zaznacz opcję Bridging, aby wybrać typ połączenia Bridging

Z listy wyboru Trybów Enkapsulacji wybierz tryb jakiego wymaga twój ISP. Poniżej opisano cechy charakterystyczne każdego z nich:


LLC/SNAP-BRIDGING: W tym przypadku VC przenosi wiele protokołów z protokołem identyfikującym informacje zawarte w nagłówku każdego pakietu. Pomimo poszerzonego pasma i dodatkowego czasu potrzebnego na przygotowanie do wykonania operacji, metoda ta może być korzystna, jeśli nie jest stosowana praktyka posiadania osobnego VC dla każdego przenoszonych protokołu, np. w przypadku dużego zapotrzebowania na równoczesne VC.

VC/MUX: W tym przypadku, na podstawie wcześniejszego wzajemnego porozumienia, każdy protokół zostaje przypisany do określonego Obwodu Wirtualnego; np. VC1 przenosi adres IP, itd. Multipleksowanie oparte na Obwodach Wirtualnych może stać się dominujące w środowisku, w którym dynamiczne tworzenie dużej liczby Wirtualnych Obwodów ATM jest szybkie i ekonomiczne.

Po zakończeniu kliknij przycisk  na wyświetlanej stronie.

Wybierz opcję Enable Bridge Service (Uruchom usługę mostka) na wyświetlanej stronie i wstaw nazwę połączenia, aby aktywować połączenie. Kliknij przycisk  na wyświetlanej stronie, pojawi się strona WAN Setup – Summary (Konfiguracja sieci WAN – Podsumowanie).

5. Na wyświetlanej stronie możesz kliknąć przycisk  w celu zachowania ustawień, lub

 w celu wykonania dowolnych modyfikacji.

UWAGA: Aby aktywować ten interfejs WAN i dalej konfigurować w nim usługi musisz zrestartować system.

Serwer DHCP

DHCP jest protokołem umożliwiającym administratorowi sieci centralne zarządzanie przypisywaniem i dystrybucją informacji IP wśród komputerów w sieci.

Uruchamiając opcję DHCP w sieci zezwalasz urządzeniu – takiemu jak router ADSL – na przypisywanie tymczasowych adresów IP komputerom, kiedy podłączone są do sieci. Urządzenie przypisujące adres nazywane jest *serwerem DHCP*, natomiast urządzenie otrzymujące adres to *klient DHCP*.

Urządzenie może być skonfigurowane jako serwer DHCP, lub agent przekazujący.

- Jeśli skonfigurujesz urządzenie jako *serwer DHCP*, będzie ono utrzymywać pulę adresów i rozdzielać je wśród komputerów w sieci LAN. Jeśli pula adresów zawierać będzie prywatne adresy IP, musisz także skonfigurować usługę NAT, tak aby adresy prywatne mogły być przetłumaczone na twój publiczny adres IP w Internecie.
- Jeśli twój Usługodawca Internetowy udostępnia funkcję serwera DHCP dla twojej sieci, to możesz skonfigurować swoje urządzenie jako *agent przekazujący DHCP*. W momencie, gdy komputer loguje się w sieci, router ADSL kontaktuje się z twoim ISP w celu uzyskania koniecznych informacji IP, a następnie przekazuje je do tego komputera.

UWAGA: Serwer DHCP może pracować tylko w trybie routingu z wyłączoną opcją PPP IP extension (rozszerzenie IP protokołu PPP). Przekaznik serwera DHCP może pracować tylko w trybie MER z wyłączoną funkcją NAT.

Pula adresów serwera DHCP



Pula adresów IP zawiera zazwyczaj prywatne adresy, których zakres możesz zdefiniować. Administratorzy sieci LAN stosują prywatne adresy IP najczęściej tylko wewnątrz swoich sieci.

Pula adresów DHCP może być użyta także do dystrybucji większej liczby publicznych adresów IP, w przypadku gdy np. trzeba je rozdzielić wśród większej liczby komputerów w sieci LAN.

Uruchamianie trybu serwera DHCP

1. W oknie "Local Area Network (LAN) Setup" (Konfiguracja sieci lokalnej LAN), wybierz "Enable DHCP Server" (Uruchom serwer DHCP).
2. Wstaw odpowiednie wartości w oknach Start IP Address (początkowy adres IP), End IP Address (końcowy adres IP), oraz Leased Time (okres ważności dzierżawy adresu IP, w godzinach):
 - **Start IP Address:** Jest to adres IP pierwszego adresu w zakresie. Wartość musi być niższa lub równa wartości końcowej zakresu. Wartość domyślna to 192.168.1.2.
 - **End IP Address:** Jest to adres IP ostatniego adresu w zakresie. Wartość musi być większa lub równa wartości początkowej zakresu. Wartość domyślna to 192.168.1.254.
 - **Leased Time (w godzinach):** Jest to okres, przez jaki serwer przypisuje adres IP do klienta, w przypadku gdy on sam nie wymaga jakiegoś określonego czasu dzierżawy. Wartość domyślna



to 24 godziny (jeden dzień).

3. Po zakończeniu definiowania zakresu adresów kliknij przycisk  aby zachować zmiany lub kliknij  aby zapisać zmiany i zrestartować urządzenie.

UWAGA: Zmiany wchodzi w życie dopiero po przeładowaniu systemu.

Uruchamianie trybu przełącznika DHCP

Niektórzy Usługodawcy Internetowi udostępniają swoim klientom, pracującym w sieciach domowych/małych biurach funkcję serwera. W takim przypadku możesz skonfigurować urządzenie jako agent przekazujący DHCP. W momencie, gdy komputer chce połączyć się z siecią Internet, router ADSL kontaktuje się z twoim ISP w celu uzyskania adresu IP i innych koniecznych informacji, a następnie przekazuje je do tego komputera.

1. W oknie "Local Area Network (LAN) Setup" (Konfiguracja sieci lokalnej LAN), wybierz "Enable DHCP Server" (Uruchom serwer DHCP).
2. W polu **DHCP Server Address (Adres serwera DHCP)**, wpisz adres IP serwera DHCP twojego Usługodawcy Internetowego.
3. Po zakończeniu definiowania zakresu adresów kliknij przycisk  aby zachować zmiany lub kliknij  aby zapisać zmiany i zrestartować urządzenie.

UWAGA: Zmiany wchodzi w życie dopiero po przeładowaniu systemu.

Przełącznik DNS

Jeśli jako adres DNS podasz adres IP interfejsu LAN urządzenia, ADSL automatycznie tworzy **przełącznik DNS**; tj. ponieważ urządzenie samo nie jest serwerem DNS, dlatego przesyła żądania odnalezienia nazwy domeny, które otrzymuje od komputerów w sieci LAN, do serwera DNS Usługodawcy Internetowego. Następnie odpowiedź otrzymaną od serwera DNS przekazuje do komputera PC.

Urządzenie tworząc przełącznik DNS musi przechowywać dane dotyczące adresów IP serwerów DNS. Może nauczyć się tych adresów w jeden z poniższych sposobów:


- **Automatic Assigned DNS (Automatyczne przypisywanie DNS):** Router zaakceptuje pierwsze przyporządkowanie DNS, otrzymane z jednego ze Stałych Obwodów Wirtualnych (PVC), uruchamianych podczas nawiązywania połączenia PPPoA, PPPoE lub MER/DHCP.
- **Configured on the ADSL router (Skonfigurowany w routerze ADSL):** Możesz użyć funkcji DNS urządzenia w celu określenia adresów DNS Usługodawcy Internetowego. Te skonfigurowane adresy będą używane jako podstawowy i zapasowy adres serwera DNS.

W celu skonfigurowania przełącznika DNS należy wykonać poniższe operacje:

1. Skonfiguruj komputery sieci LAN tak, aby używały adresu IP routera ADSL jako adresu serwera DNS.
2. Jeśli strona DNS Server Configuration (Konfiguracji serwera DNS) nie jest aktualnie wyświetlana, kliknij Advanced Setup\DNS (Konfiguracja zaawansowana/DNS), a następnie wybierz opcję **DNS Server** w menu wyboru.
3. Jeśli chcesz automatycznie skonfigurować **przełącznik DNS**, zaznacz opcję "Enable Automatic Assigned DNS" (Uruchom automatyczne przypisywanie DNS), a adresy DNS zapamiętane przez router będą używane przez przełącznik DNS.

--LUB--

Jeśli chcesz skonfigurować **przełącznik DNS** ręcznie, musisz skonfigurować adresy DNS w routerze ADSL wg poniższej instrukcji:

- a. Odznacz opcję "Enable Automatic Assigned DNS".
- b. Wpisz adresy IP serwerów DNS w polach Primary DNS Server (Podstawowy serwer DNS) i Secondary DNS server (Zapasowy serwer DNS).
- c. Kliknij przycisk  aby zapamiętać konfigurację w pamięci flash.

UWAGA: Zmiany wchodzi w życie dopiero po przeładowaniu systemu.

Dynamiczny DNS

Dynamiczny DNS (DDNS) jest usługą, która ułatwia dostęp do Internetu hostom w sieci LAN, nawet jeśli ich dynamicznie przypisywane adresy IP ulegają częstym zmianom.

DDNS jest usługą przydatną, kiedy masz w sieci hosta (na którym uruchomiony jest np. serwer sieci Web), który otrzymuje z serwera DHCP dynamicznie przypisywany adres IP. Użytkownik w sieci Internet uzyskuje zazwyczaj dostęp do hosta wpisując jego nazwę w przeglądarce internetowej. Internetowy serwer DNS rozwiązuje następnie tą nazwę na adres IP, zgodnie z wymaganiami dotyczącymi procesu przetwarzania protokołów w sieci Internet. Jednak w przypadku, gdy adres IP hosta jest przypisywany dynamicznie (np. przez serwer DHCP) to może ulegać częstym zmianom. W takim przypadku serwer DNS może posiadać nieaktualne dane i może nie być zdolny do rozwiązania nazwy hosta na aktualny adres IP.



Jeśli host jest zarejestrowany u usługodawcy DDNS, usługodawca ten jest automatycznie informowany przez hosta o każdej zmianie adresu IP, po czym rozsyła tą informację do systemu serwerów DNS.

Przed skonfigurowaniem usługi DDNS w modemie, musisz najpierw zarejestrować nazwę swojego hosta(-ów) u wspieranego usługodawcy DDNS. Aktualnie modem wspiera następujących usługodawców:

- Tzolkin Corporation: www.tzo.com
- Dynamic Network Services, Inc.: www.dyndns.org

Aby modem korzystał z tej usługi należy, po zarejestrowaniu nazwy hosta, skonfigurować go w następujący sposób: Najpierw przypisujesz te nazwy hostów do publicznego interfejsu modemu. Następnie wprowadzasz informacje dotyczące usługodawcy DDNS, u którego host został zarejestrowany.

Aby skonfigurować funkcję Dynamic DNS należy postępować wg poniższych instrukcji:

1. Jeśli strona Dynamic DNS (Dynamiczny DNS) nie jest aktualnie wyświetlana, kliknij Advanced Setup\DNS (Konfiguracja zaawansowana/DNS), a następnie wybierz opcję **Dynamic DNS** w menu wyboru
2. Kliknij .
3. Na stronie Add Dynamic DDNS (dodaj Dynamiczny DNS), wybierz lub wpisz w odpowiednich polach wymagane informacje:
 - **D-DNS provider (Usługodawca D-DNS)**: Określ usługodawcę DDNS, u którego zarejestrowałeś nazwy hostów.
 - DynDNS.org = Dynamic Network Services, Inc.
 - TZO = Tzolkin Corporation
 - **Host name (Nazwa hosta)**: Wpisz kompletną nazwę DNS hosta, podaną wcześniej u operatora usług DDNS.
 - **Interface (Interfejs)**: Określ interfejs publiczny urządzenia. Dla każdego interfejsu możesz określić tylko jedną usługę DDNS.
 - **Username & Password (Nazwa użytkownika i Hasło)**: Wstaw informacje dotyczące logowania w serwisie DynDNS.org.
 - **Email & Key (Adres email i Klucz)**: Wstaw informacje dotyczące logowania w serwisie TZO.
4. Po zakończeniu kliknij przycisk .

NAT

Translacja Adresów Sieciowych jest metodą ukrywania prywatnych adresów IP, których używasz w swojej sieci LAN i ich translacji na publiczny adres IP, używany przez ciebie w sieci Internet. Możesz definiować zasady NAT, aby dokładnie określić jak i kiedy dokonywać translacji pomiędzy adresem publicznym IP i adresami prywatnymi.

W typowej konfiguracji NAT, Usługodawca ISP udostępnia ci tylko jeden adres IP, do użytku w całej twojej sieci. Następnie każdemu komputerowi w swojej sieci LAN ty przypisujesz unikalny, prywatny adres IP. W routerze ADSL konfigurujesz zasadę NAT, która określa, iż jeśli któryś z twoich komputerów zechce w dowolnym momencie skomunikować się z siecią Internet, (tj. wysłać i odbierać pakiety IP) to jego prywatny adres IP - do którego odniesienie znajduje się w każdym pakiecie - zostanie zastąpiony publicznym adresem IP routera.

Ponieważ, po stworzeniu i zastosowaniu tej zasady NAT, źródłowy adres IP w pakiecie danych zostaje zamieniony, dlatego dla innych komputerów w sieci Internet wygląda to tak, że pakiety danych pochodzą z komputera, któremu przypisano twój publiczny adres IP (w tym przypadku z routera ADSL).

Zasadę NAT można definiować dalej, tak aby ukryć port źródłowy w pakiecie danych (np. zmienić go na inny), dzięki czemu komputery w sieci zewnętrznej nie będą w stanie stwierdzić z jakiego portu pochodzą dane. Pakiety danych, które pojawiają się jako odpowiedź zawierają publiczny adres IP w miejscu adresu



Importer i dystrybutor: Konsorcjum FEN Sp z o.o. ul. Dąbrowskiego 273A, 60-406 Poznań, sales@fen.pl
docelowego i zamaskowany (zmieniony) port źródłowy. Router ADSL zamienia adres IP i port źródłowy z powrotem na wartości oryginalne (dzięki śledzeniu zmian dokonanych wcześniej), a następnie przekierowuje pakiety do odpowiedniego komputera.


Powyższe zasady NAT dostarczają następujących korzyści:

- Eliminują potrzebę zakupu kilku publicznych adresów IP dla komputerów w sieci LAN. Możesz stworzyć swoje własne, prywatne adresy IP, bez ponoszenia jakichkolwiek kosztów, a następnie przetłumaczyć je na publiczny adres IP, w momencie gdy twoje komputery będą korzystały z dostępu do sieci Internet.
- Zapewniają bezpieczeństwo twojej sieci LAN, umożliwiając przypisywanie prywatnych adresów IP, a następnie zamianę tych adresów wraz z portami źródłowymi, zanim twój komputer połączy się z siecią Internet.

Funkcja NAT tego typu nazywana jest *network address port translation* (NAPT, Translacja Portów Adresów Sieciowych). Usługi **Virtual Server (Wirtualne Serwery)** i **Port Triggering (Przekazywanie Portów)** bazują na funkcji NAPT. Poniżej przedstawiono instrukcję konfiguracji Wirtualnych Serwerów i Przekazywania Portów.

UWAGA: Funkcja NAT będzie wyświetlana w menu wyboru jedynie wtedy, gdy zostanie ona włączona w konfiguracji PVC.

Wirtualne Serwery

1. Jeśli strona NAT -- Virtual Server Setup (Konfiguracja Wirtualnego Serwera) nie jest aktualnie wyświetlana, kliknij Advanced Setup\DNS (Konfiguracja zaawansowana/DNS), a następnie wybierz opcję **Virtual Servers** w menu wyboru
2. Kliknij przycisk  aby wyświetlić stronę NAT -- Virtual Servers.
3. Możesz skonfigurować Wirtualne Serwery korzystając ze wstępnie skonfigurowanych ustawień:
 - a. Wybierz opcję "Select a Service" (Wybierz usługę).
 - b. Z listy wyboru Select a Service wybierz żadaną, wstępnie zdefiniowaną usługę.

--LUB--

Jeśli na liście nie ma odpowiedniej usługi, której chcesz użyć, możesz skonfigurować ją samemu:

- a. Wybierz opcję "Custom Server" (Własny serwer).
 - b. Wpisz nazwę usługi w polu Custom Server.
4. W tabeli uzupełnij poniższe informacje:
 - **External Port Start (Początkowy port zewnętrzny):** Najniższy numer portu zakresu portów zewnętrznych.


- **External Port Stop (Końcowy port zewnętrzny):** Najwyższy numer portu zakresu portów zewnętrznych.
 - **Protocol (Protokół):** Protokół, dla którego ta zasada ma zastosowanie.
 - **Internal Port Start (Początkowy port wewnętrzny):** Najniższy numer portu zakresu portów wewnętrznych.
 - **Internal Port Stop (Końcowy port wewnętrzny):** Najwyższy numer portu zakresu portów wewnętrznych.
5. Kliknij przycisk  aby zachować i zastosować skonfigurowane zasady. Zwróć uwagę, iż skonfigurować można maksymalnie 32 wpisy.

Virtual Servers Table (Tabela wirtualnych serwerów) zawiera listę zasad, w kolejności w jakiej zostały wpisane (od góry do dołu, jedna po drugiej). W momencie, gdy pakiet danych pasuje do zasady, postępuje się z nim zgodnie z tą zasadą i nie jest on już poddawany działaniu innych zasad.

UWAGA: Jeśli skonfigurujesz opcję [DMZ host](#), wszystkie pakiety dla adresów innych niż sprecyzowany na tej stronie przesyłane są do określonego urządzenia DMZ.

Wyzwalanie portów


Port triggering jest opcją podobną do [wirtualnego serwera](#), oprócz tego, że tworzy dynamiczny lub tymczasową dziurę w firewallu. Wyzwalanie portów jest bardziej bezpieczne niż wirtualny serwer, ale nie wspiera ono jednoczesnego użycia tych samych portów przez kilka systemów. Umożliwia systemom zdalnym uzyskanie dostępu przez firewall bramki.

1. Jeśli strona NAT – Port Triggering Setup (Konfiguracja wyzwalania portów) nie jest aktualnie wyświetlana, kliknij Advanced Setup\DNS (Konfiguracja zaawansowana/DNS), a następnie wybierz opcję **Port Triggering** w menu wyboru
2. Kliknij przycisk  aby wyświetlić stronę NAT – Port Triggering page.
3. Możesz skonfigurować Wyzwalanie Portów korzystając ze wstępnie skonfigurowanych ustawień:
 - a. Wybierz opcję "Select an application" (Wybierz aplikację).
 - b. Z listy wyboru Select an application wybierz żadaną, wstępnie zdefiniowaną aplikację.

--LUB--

Jeśli na liście nie ma odpowiedniej aplikacji, której chcesz użyć, możesz skonfigurować ją samemu:

- c. Wybierz opcję "Custom application" (Własna aplikacja).
 - d. Wpisz nazwę usługi w polu Custom application.
4. W tabeli uzupełnij poniższe informacje:

- **Trigger Port Start (Początkowy port wyzwalania):** Najniższy numer portu zakresu portów wyzwalanych.
 - **Trigger Port End (Końcowy port przekazywania):** Najwyższy numer portu zakresu portów wyzwalanych.
 - **Trigger Protocol (Protokół wyzwalania):** Wybierz TCP, UDP lub kombinację TCP & UDP.
 - **Open Port Start (Początkowy port otwarty):** Najniższy numer portu zakresu portów otwartych.
 - **Open Port End (Końcowy port otwarty):** Najwyższy numer portu zakresu portów otwartych.
 - **Open Protocol (Protokół otwarty):** Wybierz TCP, UDP lub kombinację TCP & UDP.
5. Kliknij przycisk  aby zachować i zastosować skonfigurowane zasady. Zwróć uwagę, iż skonfigurować można maksymalnie 32 wpisy.

Port Triggering Table (Tabela portów wyzwalanych) zawiera listę zasad, w kolejności w jakiej zostały wpisane (od góry do dołu, jedna po drugiej). W momencie, gdy pakiet danych pasuje do zasady, postępuje się z nim zgodnie z tą zasadą i nie jest on już poddawany działaniu innych zasad.

UWAGA: Jeśli skonfigurujesz opcję [DMZ host](#), wszystkie pakiety dla adresów innych niż sprecyzowany na tej stronie przesyłane są do określonego urządzenia DMZ.


UWAGA: Wyzwalanie portów jest dostępne dla jednej, aktywnej sesji. Funkcja ta nie wspiera jednoczesnego wyzwalania portów dla kilku klientów.

DMZ Host

Wśród terminów internetowych DMZ odnosi się do komputerów dostępnych zarówno w sieci publicznej jak i prywatnej (np. publiczny serwer Web firmy). Pakiety wchodząca na interfejs – zarówno z sieci LAN jak i ze źródła zewnętrznego – poddawane są działaniu zespołu zabezpieczeń ograniczających, istniejących pomiędzy interfejsami publicznymi i prywatnymi.

Jeśli w twojej sieci znajduje się komputer PC, który nie potrafi prawidłowo korzystać z aplikacji Internetowych znajdując się za routerem ADSL, to możesz skonfigurować dla tego klienta nieograniczone połączenie z siecią Internet. Dodanie klienta do DMZ (Strefy Zdemilitaryzowanej) może wystawić twoją sieć lokalną na wiele potencjalnych niebezpieczeństw, dlatego używaj tej opcji jedynie w ostateczności.

Aby skonfigurować funkcję DMZ Host należy postępować wg poniższych instrukcji:

1. Jeśli strona NAT -- DMZ Host nie jest aktualnie wyświetlana, kliknij Advanced Setup\DNS (Konfiguracja zaawansowana/DNS), a następnie wybierz opcję **DMZ Host** w menu wyboru
2. W polu DMZ Host IP Address wstaw adres IP komputera, który będzie zachowywał się jak Host DMZ.
3. Kliknij przycisk  aby zachować i zastosować nowe ustawienia.

Filtrowanie adresów IP

Opcja filtrowania adresów IP umożliwia tworzenie zasad kontroli danych przychodzących i wychodzących, przekazywanych między siecią LAN i Internetem, a także wewnątrz LAN. Funkcja ta jest aktywna jedynie w trybie routingu.

Możesz tworzyć zasady filtrowania adresów IP, aby blokować próby uzyskania dostępu do określonego typu danych lub lokalizacji w sieci Internet, przez komputery w twojej sieci LAN. Możesz także przekazywać dane przychodzące do komputerów w sieci LAN.


Definiując zasadę filtracji adresów IP i uruchamiając ją instruujesz router ADSL, że ma badać pakiety danych, czy spełnia kryteria określone w zasadzie. Kryteria mogą dotyczyć protokołów sieciowych lub internetowych niesionych przez pakiet, kierunku, w którym jest przesyłany (np. z sieci LAN do Internetu i vice versa), adresu IP komputera wysyłającego dane, docelowego adresu IP i innych cech charakterystycznych pakietu danych.

Jeśli pakiet spełni ustalone w zasadzie kryteria, może być zarówno zaakceptowany (przekazany w kierunku swojego celu) lub odrzucony, w zależności od typu filtra.

Poniższy temat opisuje sposób konfiguracji filtra IP dla wychodzącego i przychodzącego ruchu IP:

Konfiguracja Filtrowania wychodzących IP

Domyślnie, cały wychodzący z sieci LAN ruch IP jest akceptowany, ale część ruchu IP może być ZABLOKOWANA przez skonfigurowanie filtrów:

1. Jeśli strona Outgoing IP Filtering Setup (Konfiguracja Filtrowania wychodzących IP) nie jest aktualnie wyświetlana, kliknij Advanced Setup\ Security\IP Filtering , a następnie wybierz opcję **Outgoing** w menu wyboru
2. Kliknij przycisk .
3. W oknie Add IP Filter -- Outgoing, wstaw lub wybierz odpowiednie dane w każdym polu, dotyczącym twojej zasady. Poniżej opisano znaczenie poszczególnych pól:
 - **Filter Name (Nazwa filtru):** Nazwa identyfikująca zasadę, to pole jest konieczne dla konfiguracji zasady filtrowania IP.
 - **Protocol (Protokół):** Kryteria protokołu IP, które muszą zostać spełnione, aby zasada została przywołana. Pozostawienie tego pola pustego będzie oznaczało, że dowolny protokół będzie spełniał tą zasadę.
 - **Source IP Address (Adres IP źródła):** Kryteria adresu IP dla komputera źródłowego, z którego pochodzi pakiet. Pozostawienie tego pola pustego będzie oznaczało, że każdy IP będzie spełniał tą zasadę.
 - **Source Subnet Mask (Maska podsieci źródła):** Maska podsieci dla źródłowego adresu IP. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.
 - **Source Port (port lub port:port, Port źródła) :** Kryteria numeru portu dla komputera źródłowego (z którego pochodzi pakiet). W tym polu możesz wstawić pojedynczy port, lub

zakres portów w formacie port:port. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.


- **Destination IP Address (Adres IP miejsca docelowego):** Kryteria adresu IP dla komputera docelowego (np. adres IP komputera, do którego pakiet jest wysyłany). Pozostawienie tego pola pustego będzie oznaczało, że każdy IP będzie spełniał tą zasadę.
- **Destination Subnet Mask (Maska podsieci miejsca docelowego):** Maska podsieci dla docelowego adresu IP. Jeśli pole Destination IP Address pozostawiono puste, to pole też powinno być puste.
- **Destination Port (port lub port:port, Port miejsca docelowego):** Kryteria numeru portu dla komputera źródłowego (z którego pochodzi pakiet). W tym polu możesz wstawić pojedynczy port, lub zakres portów w formacie port:port. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.

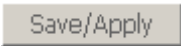
4. Po zakończeniu, kliknij przycisk  aby zachować i zastosować zasadę.

Konfiguracja Filtrowania przychodzących IP

Domyślnie, cały przychodzący z sieci WAN ruch IP jest blokowany, gdy firewall jest uruchomiony.

Jednakże, część ruchu IP może być AKCEPTOWANA przez skonfigurowanie filtrów:

1. Jeśli strona Incoming IP Filtering Setup (Konfiguracja Filtrowania przychodzących IP) nie jest aktualnie wyświetlana, kliknij Advanced Setup \ Security \ IP Filtering, a następnie wybierz opcję **Incoming** w menu wyboru
2. Kliknij przycisk .
3. W oknie Add IP Filter -- Incoming, wstaw lub wybierz odpowiednie dane w każdym polu, dotyczącym twojej zasady. Poniżej opisano znaczenie poszczególnych pól:
 - **Filter Name (Nazwa filtru):** Nazwa identyfikująca zasadę, to pole jest konieczne dla konfiguracji zasady filtrowania IP.
 - **Protocol (Protokół):** Kryteria protokołu IP, które muszą zostać spełnione, aby zasada została przywołana. Pozostawienie tego pola pustego będzie oznaczało, że dowolny protokół będzie spełniał tą zasadę.
 - **Source IP Address (Adres IP źródła):** Kryteria adresu IP dla komputera źródłowego, z którego pochodzi pakiet. Pozostawienie tego pola pustego będzie oznaczało, że każdy IP będzie spełniał tą zasadę.
 - **Source Subnet Mask (Maska podsieci źródła):** Maska podsieci dla źródłowego adresu IP. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.
 - **Source Port (port lub port:port, Port źródła):** Kryteria numeru portu dla komputera źródłowego (z którego pochodzi pakiet). W tym polu możesz wstawić pojedynczy port, lub zakres portów w formacie port:port. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.

- **Destination IP Address (Adres IP miejsca docelowego):** Kryteria adresu IP dla komputera docelowego (np. adres IP komputera, do którego pakiet jest wysyłany). Pozostawienie tego pola pustego będzie oznaczało, że każdy IP będzie spełniał tą zasadę.
 - **Destination Subnet Mask (Maska podsieci miejsca docelowego):** Maska podsieci dla docelowego adresu IP. Jeśli pole Destination IP Address pozostawiono puste, to pole też powinno być puste.
 - **Destination Port (port lub port:port, Port miejsca docelowego):** Kryteria numeru portu dla komputera źródłowego (z którego pochodzi pakiet). W tym polu możesz wstawić pojedynczy port, lub zakres portów w formacie port:port. Jeśli pole Source IP Address pozostawiono puste, to pole też powinno być puste.
5. Wybierz interfejs(-y) WAN, dla którego zasada ma zastosowanie.
6. Po zakończeniu, kliknij przycisk  aby zachować i zastosować zasadę.

Filtrowanie adresów MAC

Podwarstwa MAC (Media Access Control) jest Niższą z dwóch podwarstw warstwy łącza danych (warstwa 2), zdefiniowanej przez IEEE. Podwarstwa MAC obsługuje dostęp do mediów dzielonych, np. krążących tokenów lub kontencji (natężenie ruchu w sieci).




Adres MAC standaryzuje adres warstwy łącza danych, wymagany dla każdego portu i urządzenia podłączonego do sieci LAN. Inne urządzenia w sieci używają tych adresów do lokalizacji określonych portów w sieci i tworzenia oraz aktualizowania tablic routingu i struktury danych. Adresy MAC mają długość 6 bajtów i są kontrolowane przez IEEE, tzn. każde urządzenie w sieci ma unikalny, niepowtarzalny adres. Adres warstwy MAC znany jest także pod nazwą adresu sprzętowego lub adresu fizycznego.

Zasady filtrowania MAC mogą być tworzone w celu kontroli danych przychodzących i wychodzących, przekazywanych między siecią LAN i Internetem, a także wewnątrz LAN. Zasady filtrowania MAC podejmują decyzje, bazując na strukturze pakietów danych „warstwy 2” (np. pakiety Ethernet) wchodzących na interfejs urządzenia, w odróżnieniu od zasad filtrowania IP, które bazują na strukturze pakietów „warstwy 3” (np. IP)



Modem bada każdy przychodzący pakiet warstwy 2 i porównuje go z zasadami filtrowania MAC. Zasady filtrowania MAC określają jakie kryteria te adresy MAC muszą spełnić, aby zostały zakwalifikowane jako zgodne z zasadą.

Przed skonfigurowaniem zasad filtrowania MAC, powinieneś zdecydować, która z zasad globalnych filtrowania MAC powinna być stosowana: FORWARDED (przekazywane) lub BLOCKED (blokowane). „FORWARDED” oznacza, że wszystkie ramki warstwy MAC, oprócz tych, które pasują do którejkolwiek ze sprecyzowanych zasad, będą PRZEKAZYWANE. „BLOCKED” oznacza, że wszystkie ramki warstwy MAC, oprócz tych, które pasują do którejkolwiek ze sprecyzowanych zasad, będą BLOKOWANE. Ta opcja może działać tylko w trybie mostka.

Aby skonfigurować Zasady Globalne Filtrowania MAC należy postępować wg poniższych instrukcji :

1. Jeśli strona MAC Filtering Setup (Konfiguracja Filtrowania MAC) nie jest aktualnie wyświetlana, kliknij Advanced Setup\ Security, a następnie wybierz opcję **MAC Filtering** w menu wyboru
2. Kliknij przycisk .
3. Kliknij przycisk  na wyświetlanej stronie, aby przełączyć się pomiędzy zasadami globalnymi typu FORWARDED i BLOCKED, lub kliknij  aby powrócić do strony Konfiguracji Filtrowania MAC. Uwaga: Przejście z jednego typu zasad globalnych na drugi spowoduje, że wszystkie zdefiniowane zasady zostaną automatycznie usunięte! W takim przypadku będziesz musiał stworzyć zasady od nowa.

Aby skonfigurować zasady filtrowania MAC należy postępować wg poniższych instrukcji:

1. Kliknij przycisk  na stronie MAC Filtering Setup.
2. Na stronie Add MAC Filter (Dodaj filtr MAC), wstaw lub wybierz odpowiednie dane w każdym polu, dotyczącym twojej zasady. Poniżej opisano znaczenie poszczególnych pól:
 - **Protocol Type (Typ protokołu)**: Protokół, dla którego zasada ma zastosowanie.
 - **Destination MAC Address (Adres MAC miejsca docelowego)**: Adres MAC urządzenia docelowego.
 - **Source MAC Address (Adres MAC źródła)**: Adres MAC urządzenia źródłowego.
 - **Frame Direction (Kierunek ramki)**: Określ kierunek strumienia danych, dla którego zasada ma zastosowanie.
3. Wybierz interfejs (-y) WAN, dla którego zasada ma zastosowanie.
4. Po zakończeniu, kliknij przycisk  aby zachować i zastosować zasadę.



Kontrola Rodzicielska

Opcja Parental Control umożliwia użytkownikom zarządzającym siecią blokowanie dostępu do Internetu określonym hostom w sieci LAN na pewien okres. Przed rozpoczęciem konfiguracji funkcji Kontroli Rodzicielskiej upewnij się, że czas w modemie jest poprawnie ustawiony. W dziale [Czas internetowy](#) znajdziesz instrukcje na ten temat.

UWAGA: Funkcja ta jest aktywna jedynie w trybie routingu.

Aby zablokować hostowi dostęp do Internetu należy postępować wg poniższych instrukcji:

1. Jeśli strona Time of Day Restrictions (Czas restrykcji) nie jest aktualnie wyświetlana, kliknij Advanced Setup\ Security, a następnie wybierz opcję **Parental Control** w menu wyboru

2. Kliknij przycisk .
3. Na wyświetlanej stronie, wstaw lub wybierz odpowiednie dane w każdym polu, dotyczącym twojej zasady. Poniżej opisano znaczenie poszczególnych pól:
 - **User Name (Nazwa użytkownika):** Nazwa identyfikująca tą zasadę.
 - **Browser's MAC Address (Adres MAC przeglądarki):** Adres MAC komputera, w którym wyświetlana jest strona konfiguracji, jest on uzupełniany automatycznie. Jeśli chcesz zablokować komputer, z którego aktualnie korzystasz, możesz kliknąć ten przycisk.
 - **Other MAC Address (Inny adres MAC):** Wstaw adres MAC hosta, którego chcesz zablokować.
 - **Days of the week (Dni tygodnia):** Wybierz dzień (dni), kiedy chcesz uruchomić blokadę dostępu do Internetu dla komputera.
 - **Start Blocking Time (hh:mm, Czas rozpoczęcia blokowania):** Czas rozpoczęcia działania blokady dla hosta.
 - **End Blocking Time (hh:mm, Czas zakończenia blokowania):** Czas zakończenia działania blokady dla hosta.
4. Po zakończeniu, kliknij przycisk  aby zachować i zastosować zasadę.

Bramka Domyślna

Bramka domyślna jest powszechnie stosowanym typem trasowania. Definiuje ona adres IP, na który przekazywane są wszelkie dane, oprócz tych, dla których została zdefiniowana statyczna trasa IP. Za każdym razem dane przekazywane są w kierunku swojego miejsca docelowego z jednego adresu internetowego na drugi, co określa się mianem zakończenia jednego *etapu (skoku)*.

W routerze ADSL bramka domyślna kieruje cały wychodzący ruch internetowy do routera twojego Usługodawcy Internetowego. Bramka domyślna może być przypisywana automatycznie przez twojego ISP za każdym razem, gdy urządzenie negocjuje połączenie z Internetem, lub skonfigurowana ręcznie.

Aby przypisać bramkę domyślną dla routera ADSL należy postępować wg poniższych instrukcji:

1. Jeśli strona Routing – Default Gateway (Trasowanie – Bramka domyślna) nie jest aktualnie wyświetlana, kliknij Advanced Setup \ Routing, a następnie wybierz opcję **Default Gateway** w menu wyboru
2. Bramkę domyślną możesz przypisać na jeden z trzech sposobów poprzez wybór odpowiednich opcji na stronie
 - **Enable Automatic Assigned Default Gateway (Uruchom opcję automatycznego przypisywania bramki domyślnej)**

Router ADSL zaakceptuje pierwsze przyporządkowanie bramki domyślnej, otrzymane z jednego ze Stałych Obwodów Wirtualnych (PVC), uruchamianych podczas nawiązywania połączenia PPPoA, PPPoE lub MER.


UWAGA: Zmieniając opcję *Automatic Assigned Default Gateway* z niezaznaczonej na zaznaczoną musisz zrestartować router, aby adres bramki domyślnej został automatycznie przypisany.

- **Use Default Gateway IP Address (Używaj adresu IP bramki domyślnej)**

Możesz przypisać bramkę domyślną wpisując jej adres IP w polu Use Default Gateway IP Address (Użyj następującego adresu IP bramki domyślnej).

- **Use Interface (Użyj interfejsu)**

Router ADSL zaakceptuje przypisanie bramki domyślnej z wybranego przez siebie interfejsu.

3. Po zakończeniu, kliknij przycisk  aby zachować i zastosować konfigurację.

Trasowanie statyczne

W celu określenia, dokąd router ADSL powinien wysyłać dane otrzymane za pośrednictwem określonego interfejsu, można stworzyć statyczną trasę IP. Trasy określają adres IP interfejsu następnego urządzenia lub miejsca docelowego w Internecie, dokąd dane mają być przekazane, aby dotarły do ostatecznego punktu docelowo.


Każdy komputer z adresem IP i router posiada tablicę adresów IP najczęściej odwiedzanych przez jego użytkowników. Dla każdego z tych docelowych adresów IP tablica tworzy listę adresów IP węzłów, gdzie dane powinny wykonać pierwszy skok. Tablica ta znana jest pod nazwą *tablicy routingu (trasowania)* urządzenia.

Większość użytkowników nie musi definiować statycznych tras IP. W typowych, małych domowych lub biurowych sieciach LAN istniejące trasy, ustalone przez bramki domyślne dla komputerów w twojej sieci LAN oraz dla routera ADSL, stanowią najbardziej odpowiednie marszruty dla całego twojego ruchu internetowego.

- W komputerach w twojej sieci LAN bramka domyślna kieruje cały ruch internetowy do interfejsu LAN twojego routera ADSL (zakładając, że urządzenie pracuje w trybie Routingu). Komputery w sieci LAN znają adres bramki Internetowej, ponieważ albo przypisałeś im ten adres ręcznie, modyfikując ustawienia TCP/IP, albo skonfigurowałeś je tak, aby otrzymywały wymagane informacje dynamicznie z serwera DHCP w momencie łączenia z Internetem.
- W routerze ADSL bramka domyślna kieruje cały wychodzący ruch internetowy do routera twojego Usługodawcy Internetowego. Dodatkowe informacje dotyczące bramki domyślnej znajdziesz w dziale [Bramka Domyślna](#).

Jeśli twoja sieć posiada dwie lub więcej podsieci, jeśli łączysz się z dwiema lub więcej usługami ISP, lub jeśli łączysz się ze zdalną firmową siecią LAN koniecznym może okazać się zdefiniowanie określonych tras.

Aby dodać trasę IP do tablicy routingu modemu należy postępować wg poniższych instrukcji:

1. Jeśli strona Routing – Static Route (Trasowanie – Trasa statyczna) nie jest aktualnie wyświetlana, kliknij Advanced Setup\ Routing, a następnie wybierz opcję **Static Route** w menu wyboru
2. Kliknij przycisk  na wyświetlanej stronie.
3. Określ miejsce docelowe, maskę sieci i bramkę lub następny węzeł (hop) dla tej trasy.

- **Destination Network Address (Adres sieciowy miejsca docelowego):** Określa adres IP komputera docelowego w formie liczby dziesiętnej z kropkami. Miejscem docelowym może być adres IP określonego komputera lub całej sieci.
- **Subnet Mask (Maska podsieci):** Wskazuje, które części adresu docelowego odnoszą się do sieci, a które do komputera w sieci.

Zero w adresie docelowym musi pasować do zerowej części Maski Podsieci. W przeciwnym przypadku wystąpi błąd i wyświetlona zostanie wiadomość "Configure gateway for routing failed. Route: netmask and route address conflict" (Konfiguracja routingu bramki zakończona niepowodzeniem. Trasa: konflikt pomiędzy maską sieci a adresem trasy).

- **Use Gateway IP Address (Użyj adresu IP Bramki):** Określa *następny* adres IP, dokąd dane mają zostać przesłane, kiedy ich miejscem docelowym jest to, które określono w kolumnie docelowej.

Określona bramka musi być wcześniej osiągalna. To zazwyczaj oznacza, że najpierw musisz skonfigurować trasę statyczną do tej bramki. Jeśli zdefiniujesz adres jednego ze swoich lokalnych interfejsów to będzie on używany do podejmowania decyzji o interfejsie, do którego pakiety powinny być trasowane.

- **Use Interface (Użyj interfejsu):** Wymusza skojarzenie trasy z określonym urządzeniem, w przeciwnym przypadku kernel będzie starał się określić urządzenie na własny rachunek sprawdzając już istniejące trasy i urządzenia.

4. Po zakończeniu, kliknij przycisk  aby zachować i zastosować trasę.

Protokół RIP

Twój router ADSL można skonfigurować w taki sposób, aby komunikował się z innymi urządzeniami routującymi, w celu wyznaczenia najlepszej trasy przesyłania danych do ich zamierzonego celu. Urządzenie routujące przesyłają te informacje przy użyciu różnego typu protokołów IP. Poniższy rozdział opisuje sposób, w jaki skonfigurować modem, aby korzystał z jednego z nich, nazywanego Protokołem Informowania o Trasach (RIP).

RIP jest protokołem internetowym, który można skonfigurować tak, aby dzielił informacje zawarte w tablicy routingu (trasowania) z innymi urządzeniami routującymi w twojej sieci LAN, w lokalizacji twojego



ISP, lub znajdującymi się w sieciach zdalnych, połączonych z twoją siecią za pośrednictwem linii ADSL. Ogólnie protokół RIP jest używany do komunikacji z sieciami anonimowymi. Sieć anonimowa to taka, w której wszystkie komputery administrowane są przez tą samą jednostkę. Siecią anonimową może być pojedyncza sieć lub grupa kilku sieci, będących pod jedną administracją. Przykładem sieci anonimowej jest korporacyjna sieć LAN, włączając urządzenia, które mogą łączyć się z nią ze zdalnych lokalizacji, takie jak np. komputery stosowane przez telepracowników.

Każde urządzenie sieciowe, używające protokołu RIP, wysyła swoją tablicę routowania do najbliższego sąsiada co 30 sekund. Urządzenie sąsiadujące następnie przesyła te informacje do swojego kolejnego sąsiada. Procedura ta trwa do momentu, aż wszystkie urządzenia w sieci anonimowej będą posiadać ten sam zestaw tras.

Konfiguracja RIP może okazać się konieczna w przypadku zaistnienia w twojej sieci jednej z poniższych sytuacji:

- W twojej sieci znajduje się dodatkowy router lub komputer PC z uruchomioną opcją RIP (inne niż router ADSL). Aby router ADSL i twój drugi router mogły dzielić się swoimi tablicami routowania, będą musiały komunikować się ze sobą za pośrednictwem protokołu RIP.
- Twoja sieć łączy się za pośrednictwem linii ADSL z siecią zdalną, taką jak sieć korporacyjna. Aby sieci usytuowane w dwóch różnych miejscach mogły dzielić się tablicami trasowania, używanymi wewnątrz w sieci LAN, *obydwie* muszą być skonfigurowane do współpracy z protokołem RIP.
- Twój ISP wymaga, abyś uruchomił funkcję RIP w celu umożliwienia komunikacji z urządzeniami pracującymi w jego sieci.

Aby uruchomić funkcję RIP w routerze ADSL, należy postępować wg poniższych instrukcji:

1. Jeśli strona Routing -- RIP Configuration (Trasowanie – Konfiguracja RIP) nie jest aktualnie wyświetlana, kliknij Advanced Setup \ Routing, a następnie wybierz opcję **RIP** w menu wyboru.

Na stronie znajdują się przyciski wyboru, umożliwiające włączenie lub wyłączenie funkcji RIP, a także tabela z listą interfejsów, na których protokół aktualnie jest uruchomiony.

2. Na wyświetlanej stronie należy wybrać dane w kolumnach, dotyczących twojej zasady w tabeli. Poniżej znajduje się opis poszczególnych kolumn:

- **Interface (Interfejs):** Nazwa interfejsu, na którym chcesz uruchomić funkcję RIP. Interfejs LAN (zazwyczaj br0) stosowany jest do komunikacji z urządzeniami w twojej sieci LAN, które mają uruchomioną funkcję RIP. Interfejs WAN (np. PPP, MER, lub inny) stosowany jest do komunikacji z Usługodawcą Internetowym lub zdalną siecią LAN.
- **VPI/VCI:** PVC (Stały Obwód Wirtualny), którego używał ten interfejs.
- **Version (Wersja):** Wersja RIP. Wersja 1 RIP to oryginalny protokół RIP. Wybierz opcję RIP1, jeśli posiadasz urządzenia komunikujące się z tym interfejsem, które rozumieją jedynie wersję 1 RIP. Zaleca się stosowanie wersji 2 RIP, ponieważ wspiera „klasy” adresów IP (używane do





tworzenia podsieci) i inne funkcje. Wybierz opcję RIP2, jeśli wszystkie pozostałe urządzenia routujące w twojej sieci LAN wspierają tę wersję protokołu.

- **Operation (Rodzaj pracy):** Określ, w jaki sposób RIP ma funkcjonować. W Trybie Aktywnym (Active Mode) ustala się wersję(-e) RIP, jakiej interfejs będzie używał w momencie wysyłania do innych urządzeń informacji dotyczących trasowania. W Trybie Pasywnym (Passive Mode) ustala się wersję(-e) RIP, w jakiej informacje muszą być przekazywane do routera ADSL/Ethernet, aby zostały zaakceptowane przez jego tablicę routingu.
- **Enabled (Włączony):** Zaznacz tę opcję, aby uruchomić funkcję RIP na tym interfejsie.

3. Po zakończeniu, kliknij przycisk  aby zachować i zastosować konfigurację.

Diagnostyka

Na stronie diagnostyki możesz przeprowadzić serię testów diagnostycznych oprogramowania systemu i połączeń sprzętowych.

1. Kliknij opcję **Diagnostics(diagnostyka)** w menu wyboru, po prawej stronie wyświetli się strona **Diagnostics**.
2. Kliknij przycisk , oprogramowanie diagnostyczne uruchomi serię testów w celu sprawdzenia poprawności działania połączeń urządzenia. Zajmie to tylko kilka sekund. Po zakończeniu wyświetli się raport programu, informujący czy test został zakończony pomyślnie czy wystąpiły błędy.
3. Klikając przycisk  znajdujący się na stronie możesz przetestować linię DSL za pomocą żądania segmentów pętli zwrotnej OAM F4.
4. Aby zbadać pozostałe PVC kliknij  lub .

UWAGA: Aby uzyskać pomoc, dotyczącą każdego testu, kliknij przycisk *Help*, znajdujący się w prawej kolumnie tabeli wyjściowej. Skontaktuj się ze swoim Usługodawcą Internetowym w celu interpretacji rezultatów przeprowadzonych badań diagnostycznych.


Kopia zapasowa i odzyskiwanie ustawień

Wiele opcji software'owych może zostać skonfigurowane tak, aby sprostać twoim potrzebom lub wymaganiom ISP. Te dane konfiguracyjne stają się częścią obrazu oprogramowania routera. Istnieje możliwość wydobycia danych konfiguracyjnych z tego obrazu i zapisania ich w komputerze PC w postaci pliku tekstowego. Jeśli zmienisz konfigurację systemu i będziesz chciał wrócić do poprzednich ustawień, możesz zrobić to wgrywając plik konfiguracyjny z powrotem do systemu.



Opcja ta może okazać się szczególnie przydatna w przypadku, gdy otrzymasz od ISP uaktualniający plik obrazu, zawierający uaktualnienie oprogramowania. Wgranie nowego obrazu może spowodować, że twoje spersonalizowane ustawienia zostaną skasowane i zastąpione wartościami domyślnymi. Przed wgraniem nowego obrazu powinieneś zapisać ustawienia konfiguracyjne. Następnie, po wgraniu obrazu, możesz przywrócić wcześniejszą konfigurację.

Aby zapisać i przywrócić plik konfiguracyjny należy postępować wg poniższych instrukcji:




- **Kopia zapasowa**

1. Jeśli strona Settings - Backup (Konfiguracja – Kopia zapasowa) nie jest aktualnie wyświetlana, kliknij Management\settings, a następnie wybierz opcję **Backup** w menu wyboru.
2. Kliknij przycisk , pojawi się okno dialogowe systemu Windows, umożliwiające dokonanie wyboru miejsca, w którym ma zostać zapisany plik kopii. Plik o nazwie backupsettings.conf może być otwarty za pomocą dowolnego edytora tekstu. Możesz zmienić nazwę pliku, aby później móc zidentyfikować datę wykonania kopii lub inne cechy charakterystyczne konfiguracji.

- **Uaktualnianie**

1. Jeśli strona Tools -- Update Settings (Narzędzia – Uaktualnianie) nie jest aktualnie wyświetlana, kliknij Management\settings, a następnie wybierz opcję **Update** w menu wyboru.
2. Kliknij przycisk  na wyświetlanej stronie, pojawi się okno dialogowe systemu Windows, umożliwiające wybór pliku z twojego komputera PC lub z sieci. Dwukrotnie kliknij nazwę pliku, a następnie naciśnij przycisk . W czasie uaktualniania na ekranie będzie wyświetlany następujący komunikat: *Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.(Trwa uaktualnianie. Po zakończeniu router DSL zostanie zrestartowany. Ta operacja potrwa około 2 minuty.)*

- **Odzyskiwanie ustawień domyślnych**

1. Jeśli strona Tools -- Restore Default Settings (Narzędzia – odzyskiwanie ustawień domyślnych) nie jest aktualnie wyświetlana, kliknij Management\settings, a następnie wybierz opcję **Restore Default** w menu wyboru.
2. Kliknij przycisk  na wyświetlanej stronie, pojawi się okno dialogowe systemu Windows, umożliwiające potwierdzenie operacji. Kliknij  aby przywrócić ustawienia fabryczne modemu; lub kliknij , aby przerwać operację.

Agent SNMP

Protokół SNMP (Simple Network Management Protocol) (SNMP) umożliwia komputerowi hosta uzyskanie dostępu do parametrów konfiguracyjnych, wydajnościowych i innych systemów danych, znajdujących się w bazie danych modemu. Komputer hosta nazywany jest stacją zarządzającą, natomiast modem nazywany jest agentem SNMP. Dane, do których można uzyskać dostęp za pośrednictwem protokołu SNMP zapisywane są w modemie, w bazie danych o nazwie Management Information Database (MIB).

Kiedy opcja SNMP jest włączona, modem odpowiada na żądania SNMP hosta. Host może odczytywać dane z bazy MIB lub, jeśli pozwalają na to jego uprawnienia, także zapisywać w niej dane.

Poziomy uprawnień definiowane są przez społeczności SNMP (SNMP community), konfigurowane w modemie. Społeczność jest to ściśle określona grupa adresów IP. Te adresy identyfikują hosty, które mogą funkcjonować jako stacje zarządzające SNMP, mające dostęp do MIB. Każda społeczność ma zdefiniowane uprawnienia read-only (tylko odczyt) lub read/write (odczyt/zapis) .

Na dane zapisywane w MIB składają się standardowe elementy, zdefiniowane w protokole SNMP, jak i elementy specjalne, zdefiniowane przez Usługodawcę. Zawartość bazy MIB jest wstępnie skonfigurowana przez ISP i nie może być zarządzana z poziomu przeglądarki WWW..

Aby skonfigurować funkcję agenta SNMP należy postępować wg poniższych:

1. Jeśli strona SNMP - Configuration (SNMP - konfiguracja) nie jest aktualnie wyświetlana, kliknij Management, a następnie wybierz opcję **SNMP Agent** w menu wyboru.

Na stronie znajdują się przyciski wyboru, umożliwiające włączenie lub wyłączenie funkcji SNMP.

2. Na wyświetlanej stronie wpisz dane w każdym polu, dotyczącym twojej zasady. Poniżej znajduje się opis poszczególnych pól:

- **Read Community (Społeczność z uprawnieniami odczytu)**: Jest to nazwa/hasło dla społeczności SNMP, uprawnionej do odczytu wartości SNMP.
- **Set Community (Społeczność z uprawnieniami konfigurowania)**: Jest to nazwa/hasło dla społeczności SNMP, uprawnionej do ustalania wartości SNMP.
- **System Name (Nazwa systemu)**: Opcjonalna nazwa systemu SNMP.
- **System Location (Lokalizacja systemu)**: Opcjonalna lokalizacja SNMP.
- **System Contact (Kontakt systemu)**: Opcjonalny kontakt systemu SNMP.
- **Trap Manager IP (Adres IP Trap Manager)**: Adres IP trap managera SNMP, gdzie wysyłane będą komunikaty.


3. Po zakończeniu, kliknij przycisk  aby zachować i zastosować konfigurację.

Kontrola dostępu

Kontrola dostępu do modemu jest możliwa na trzy sposoby: poprzez Usługi, Adresy IP oraz Hasła. Poniżej przedstawiono sposoby ich konfiguracji.

Usługi

Możesz włączyć opcję dostępu do Managera Konfiguracji z portu WAN, dzięki czemu twój ISP może przeprowadzić konfigurację.

1. Jeśli strona Access Control -- Services (Kontrola dostępu -- Usługi) nie jest aktualnie wyświetlana, kliknij Management\Access Control, a następnie wybierz opcję **Services** w menu wyboru.
2. Tabela na tej stronie zawiera serię pól wyboru, umożliwiających włączenie lub wyłączenie dostępu do programu konfiguracyjnego przez port LAN lub WAN, za pośrednictwem protokołu FTP, HTTP, ICMP, SNMP, TELNET i TFTP.
3. Po zakończeniu, kliknij przycisk  aby zachować i zastosować konfigurację.



UWAGA: Usługi przez port WAN są nieaktywne w trybie mostka (bridge).

Adresy IP

Tryb Kontroli Dostępu Adresów IP, jeśli jest uruchomiony, umożliwia przydzielanie dostępu do lokalnych usług zarządzania adresom IP, znajdującym się na Liście Kontroli Dostępu. Jeśli tryb Kontroli Dostępu jest wyłączony system nie będzie stwierdzał zgodności adresów IP dla przychodzących pakietów. Usługami są aplikacje systemowe, znajdujące się na Liście Kontrolnej Usług, patrz rozdział [Usługi](#).

1. Jeśli strona Access Control -- IP Address (Kontrola dostępu – Adresy IP) nie jest aktualnie wyświetlana, kliknij Management\Access Control, a następnie wybierz opcję **IP Addresses** w menu wyboru.

Na stronie znajdują się opcje, umożliwiające włączenie i wyłączenie funkcji Kontroli Dostępu Adresów IP.


2. Kliknij przycisk  na wyświetlanej stronie.
3. Wstaw adres IP stacji zarządzającej, która ma uzyskać pozwolenie na dostęp do lokalnych usług zarządzania.
4. Kliknij przycisk  aby zachować i zastosować zasadę.

Hasła

W routerze ADSL skonfigurowano trzy pary nazw użytkownika i haseł, umożliwiających uzyskanie dostępu do Managera Konfiguracji. Te loginy posiadają trzy różne poziomy uprawnień:

- **admin (administrator):** Ten użytkownik posiada nieograniczony dostęp routera DSL, może zmieniać i przeglądać konfigurację modemu. Domyślne hasło dla tego użytkownika to: *password*.
- **suport (wsparcie):** To konto umożliwia technikowi ISP uzyskanie dostępu do twojego routera DSL w celach konserwacyjnych i diagnostycznych. Tego logina należy używać do zarządzania modemem z sieci WAN. Domyślne hasło dla tego użytkownika to: *supportuser*.
- **user (użytkownik):** Ten użytkownik może uzyskać dostęp do routera DSL, przeglądać ustawienia konfiguracyjne i statystyki, a także aktualizować oprogramowanie routera. Domyślne hasło dla tego użytkownika to: *normaluser*.

Istnieje możliwość zmiany haseł dla powyższych użytkowników. Poniżej opisano sposób, w jaki można to zrobić.

1. Jeśli strona Access Control -- Passwords (Kontrola dostępu – Hasła) nie jest aktualnie wyświetlana, kliknij Management\Access Control, a następnie wybierz opcję **Passwords** w menu wyboru.
2. Wybierz użytkownika z rozwijalnej listy i wpisz stare hasło w polu Old Password. Następnie w oknach New Password (Nowe hasło) i Confirm Password (Potwierdź hasło) wpisz nowe hasło.
3. Kliknij przycisk  aby zachować i zastosować zasadę.

Czas internetowy

Protokół SNTP jest uproszczoną, kliencką wersją NTP. SNTP może jedynie otrzymywać informacje dotyczące czasu z serwerów NTP i nie może pracować jako źródło informacji dotyczących czasu dla innych systemów. SNTP dostarcza informacji dotyczących czasu z dokładnością 100 milisekund względem czasu rzeczywistego. Dodatkowo, SNTP nie weryfikuje ruchu, lecz mimo to możesz skonfigurować listę dostępową, aby zapewnić pewny poziom zabezpieczeń. Klient SNTP jest bardziej podatny na nieodpowiednio zachowujące się serwery niż klient NTP, dlatego powinien być używany jedynie w przypadku, kiedy nie jest wymagany wysoki poziom weryfikacji.

Możesz skonfigurować urządzenie tak, aby pobierało dane i informacje dotyczące czasu z określonego serwera czasu NTP. Po uruchomieniu funkcji SNTP (Simple Network Time Protocol), urządzenie łączy się z serwerem czasu NTP, który przekazuje mu informacje dotyczące daty i czasu.

Aby uruchomić funkcję SNTP w modemie, należy postępować wg poniższych instrukcji:



1. Jeśli strona Time settings (Konfiguracja czasu) nie jest aktualnie wyświetlana, kliknij Management, a następnie wybierz opcję **Internet Time** w menu wyboru.
2. Zaznacz pole wyboru na wyświetlanej stronie.
3. W polach First NTP time server (Pierwszy serwer czasu NTP) i Second NTP time server (Drugi serwer czasu NTP) z rozwijalnej listy wybierz serwer czasu NTP. Jeśli chcesz użyć innego serwera czasu NTP, który nie znajduje się na liście, możesz w polu "Other" (Inny) podać adres własnego serwera czasu NTP.
4. Wybierz swoją strefę czasową z rozwijalnej listy.

5. Po zakończeniu, kliknij przycisk  aby zachować i zastosować zasadę.

Uaktualnianie oprogramowania

Jeśli dostępna jest nowa wersja oprogramowania dla twojego modemu, możesz uaktualnić urządzenie wgrываяc to oprogramowanie. Istnieją dwa tryby umożliwiające aktualizację oprogramowania modemu: tryb HTTP oraz tryb TFTP. Poniżej opisano każdy z nich.

- **Tryb HTTP**

1. Jeśli strona Tools -- Update Software (Narzędzia -- aktualizacja oprogramowania) nie jest aktualnie wyświetlana, kliknij Management, a następnie wybierz opcję **Update Software** w menu wyboru.
2. Kliknij przycisk  na wyświetlanej stronie, pojawi się okno dialogowe systemu Windows, umożliwiające wybór pliku z twojego komputera PC lub z sieci. Dwukrotnie kliknij nazwę pliku, a następnie naciśnij przycisk . W czasie uaktualniania na ekranie będzie wyświetlany następujący komunikat: *Uploading is in progress. The DSL Router will reboot upon completion. This process will take about 2 minutes.(Trwa uaktualnianie. Po zakończeniu router DSL zostanie zrestartowany. Ta operacja potrwa około 2 minuty.)*

- **Tryb TFTP**

W modemie wbudowano serwer TFTP, dzięki czemu plik aktualizujący firmware można przesłać do urządzenia za pośrednictwem klienta TFTP. Poniżej opisano sposób aktualizacji systemu w modemie za pośrednictwem klienta tftp (tftp.exe), udostępnianego wraz z systemem Windows 2000/XP.

1. Uruchom *wiersz polecenia* w systemie Windows 2000 lub Windows XP. Powinieneś zobaczyć okno ze ścieżką dostępu i znakiem zachęty w postaci aktualny_katalog\>, gdzie aktualny_katalog oznacza katalog, w którym aktualnie się znajdujesz.
2. Skopiuj obraz do katalogu aktualny_katalog.
3. Wpisz polecenie tftp w następujący sposób: aktualny_katalog\>tftp -i ip_modemu_LAN PUT nazwa_obrazu.

ip_modemu_LAN oznacza adres IP modemu na porcie LAN.

PUT przesyła plik źródłowy znajdujący się na dysku hosta lokalnego do miejsca docelowego w systemie plików hosta zdalnego (modem).




nazwa_obrazu jest nazwą pliku obrazu, skopiowanego do katalogu aktualny_katalog.

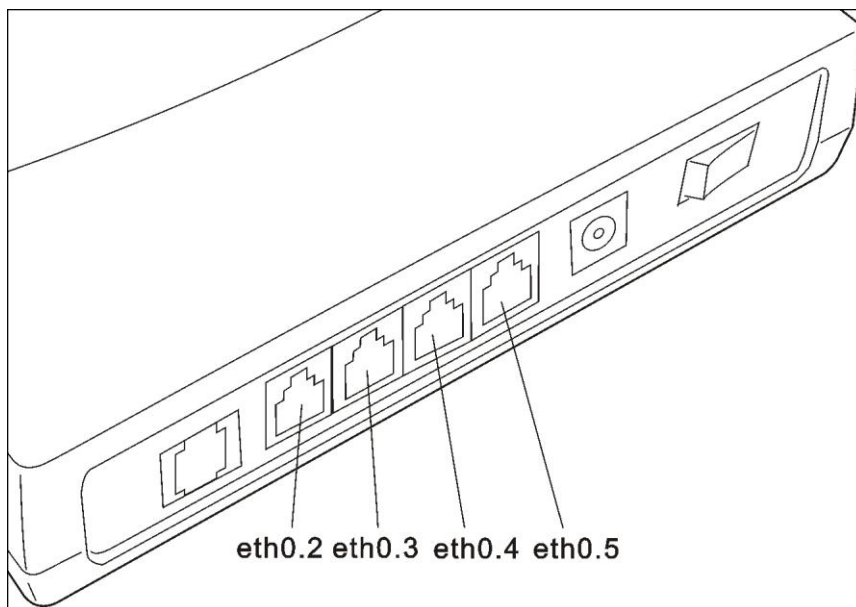
4. Po zakończeniu transferu modem zostanie automatycznie zrestartowany, a nowe oprogramowanie zostanie uruchomione.

Mapowanie portów

Mapowanie portów wspiera użycie kilku portów w PVC i grupy mostkowania. Każda grupa będzie pracować jak niezależna sieć. Aby opcja ta mogła być uruchomiona, musisz najpierw, używając przycisku Add, stworzyć grupy mapowania z odpowiednimi interfejsami LAN i WAN. Przycisk Remove umożliwia usunięcie grupy i dodanie niezgrupowanych interfejsów do Grupy domyślnej. Można skonfigurować maksymalnie 16 wpisów.

W celu skonfigurowania opcji Port Mapping (Mapowanie portów), należy postępować wg poniższych instrukcji :

1. Jeśli strona Port Mapping (Mapowanie portów) nie jest aktualnie wyświetlana, kliknij Advanced Setup, a następnie wybierz opcję Port Mapping w menu wyboru.
2. Zaznacz pole wyboru Enable virtual ports (Włącz porty wirtualne) na wyświetlanej stronie.
3. Kliknij  na wyświetlanej stronie, otworzy się strona Port Mapping Configuration (Konfiguracja Mapowania Portów).
4. W polu Group Name (Nazwa grupy) wstaw nazwę grupy.
5. Możesz użyć przycisku  aby dodać interfejs z listy Available Interfaces (Istniejących Interfejsów) do listy Grouped Interfaces (Interfejsów zgrupowanych); lub możesz użyć przycisku  aby przesunąć interfejs z listy Grouped interfaces do listy Available Interfaces. Poniższy rysunek przedstawia położenie portów sieci Ethernet.



6. Po zakończeniu, kliknij przycisk  aby zachować i zastosować konfigurację.

UWAGA: Interfejs eth0 może zostać dodany jedynie do Grupy domyślnej.



Importer i dystrybutor: Konsorcjum FEN Sp z o.o. ul. Dąbrowskiego 273A, 60-406 Poznań, sales@fen.pl

Konsorcjum FEN Sp. z o.o. prowadzi serwis gwarancyjny produktów Dynamode oferowanych w serwisie dealerskim www.fen.pl. Procedury dotyczące przyjmowania urządzeń do serwisu są odwrotne do kanału sprzedaży tzn.: w przypadku uszkodzenia urządzenia przez klienta końcowego, musi on dostarczyć produkt do miejsca jego zakupu.

Skrócone zasady reklamacji sprzętu:

Reklamowany sprzęt powinien być dostarczony w stanie kompletnym, w oryginalnym opakowaniu zabezpieczającym lub w opakowaniu zastępczym zapewniającym bezpieczne warunki transportu i przechowywania analogicznie do warunków zapewnianych przez opakowanie fabryczne.

Szczegółowe informacje dotyczące serwisu można znaleźć pod adresem www.fen.pl/serwis Konsorcjum FEN współpracuje z Europejską Platformą Recyklingu ERP w sprawie zbiórki zużytego sprzętu elektrycznego i elektronicznego. Lista punktów, w których można zostawiać niepotrzebne produkty znajduje się pod adresem www.fen.pl/download/ListazSEIE.pdf

Informacja o przepisach dotyczących ochrony środowiska Dyrektywa Europejska 2002/96/EC wymaga, aby sprzęt oznaczony symbolem znajdującym się na produkcie i/lub jego opakowaniu ("przekreślony śmietnik") nie był wyrzucany razem z innymi niesortowanymi odpadami komunalnymi. Symbol ten wskazuje, że produkt nie powinien być usuwany razem ze zwykłymi odpadami z gospodarstw domowych. Na Państwu spoczywa obowiązek wyrzucania tego i innych urządzeń elektrycznych oraz elektronicznych w wyznaczonych punktach odbioru. Pozbywanie się sprzętu we właściwy sposób i jego recykling pomogą zapobiec potencjalnie negatywnym konsekwencjom dla środowiska i zdrowia ludzkiego. W celu uzyskania szczegółowych informacji o usuwaniu starego sprzętu prosimy się zwrócić do lokalnych władz, służb oczyszczania miasta lub sklepu, w którym produkt został nabyty.

